NEITHER REMAINING NOR EXPANDING

THE DECLINE OF THE ISLAMIC STATE

MATTHEW LEVITT, EDITOR

COUNTERTERRORISM LECTURES 2016–17

COUNTERTERRORISM LECTURE SERIES

The entire series is available for download from the Institute's website.

Vol. 8 *Neither Remaining nor Expanding: The Decline of the Islamic State*, July 2018, PF 155, http://washin.st/pfocus155

Vol. 7 *The Rise of ISIL*, Aug. 2016, PF 148, http://washin.st/pfocus148

Vol. 6 *From the Boston Marathon to the Islamic State: Countering Violent Extremism*, April 2015, PF 139, http://washin.st/pfocus139

Vol. 5 *Finding a Balance: U.S. Security Interests and the Arab Awakening*, May 2012, PF 119, https://washin.st/pfocus119

Vol. 4 *Obama's National Security Vision: Confronting Transnational Threats with Global Cooperation*, Oct. 2010, PF 107, https://washin.st/pfocus107

Vol. 3 *Continuity and Change: Reshaping the Fight Against Terrorism*, April 2010, PF 103, https://washin.st/pfocus103

Vol. 2 *Countering Transnational Threats: Terrorism, Narco-Trafficking, and WMD Proliferation*, Feb. 2009, PF 92, https://washin.st/pfocus92

Vol. 1 *Terrorist Threat and U.S. Response: A Changing Landscape*, Sept. 2008, PF 86, https://washin.st/pfocus86

NEITHER REMAINING NOR EXPANDING

THE DECLINE OF THE ISLAMIC STATE

COUNTERTERRORISM LECTURES 2016–17

MATTHEW LEVITT
EDITOR

THE WASHINGTON INSTITUTE FOR NEAR EAST POLICY
www.washingtoninstitute.org

The opinions expressed in this Policy Focus are those of the authors and not necessarily those of The Washington Institute, its Board of Trustees, or its Board of Advisors.

Policy Focus 155

First publication: July 2018

The Washington Institute for Near East Policy
1111 19th Street NW, Suite 500
Washington, DC 20036
www.washingtoninstitute.org

Design: 1000colors

Cover photo: Screenshot from Islamic State propaganda video.

Contents

- Acknowledgments / v
- Speakers / vii
- Introduction
  Matthew Levitt / 1
- Internet Security & Privacy in the Age of the Islamic State: the view from facebook
  Monika Bickert / 15
- Terror in Europe: combating foreign fighters & homegrown networks
  Matthew Levitt, Olivier Decottignies, and Eric Rosand / 20
- Combating Genocide: reassessing the fight against the islamic state
  Matthew Levitt, Naomi Kikoler, and James F. Jeffrey / 26
- How Technology Has Transformed the Terrorist Threat Fifteen Years After 9/11
  Michael B. Steinbach / 32

(continued)

- The Evolution of Terrorism Financing: disrupting the islamic state
  Daniel L. Glaser / 43

- Stopping Extremists from Becoming Terrorists: a strategy for the trump administration
  Rand Beers, Samantha Ravich, and Matthew Levitt / 48

- Islamist Terrorism in the West
  Dick Schoof, Muhammad Fraser-Rahim, Farah Pandith, and Matthew Levitt / 53

- Preparing to Counter ISIS 2.0: european ct efforts since charlie hebdo
  Gilles de Kerchove / 63

- Lone Wolf: passing fad or terror threat of the future?
  Boaz Ganor, Bruce Hoffman, Marlene Mazel, and Matthew Levitt / 69

- Iraq's Role in Countering the Islamic State's Finances
  Ali Mohsen Al-Alaq / 74

- Hezbollah's Terror Army: how to prevent a third lebanon war
  Richard Kemp, Lord Richard Dannatt, and Klaus Naumann / 79

- From CVE to "Terrorism Prevention": assessing new u.s. policies
  William Braniff, Seamus Hughes, Shanna Batten, and Matthew Levitt / 83

Acknowledgments

THE COUNTERTERRORISM LECTURE Series has been a tremendous success over the past decade, thanks to the consummate professionalism of a great many people at The Washington Institute for Near East Policy.

This project benefits from contributions by the Institute's administrative, communications, publications, and research staff, without which neither the lecture series nor this series of monographs would be possible. Special thanks to the Institute's publications director, Mary Kalbach Horan; communications director, Jeff Rubin; online communications managing editor, R. Scott Rogers; senior editor, George Lopez; editor, Jason Warshof; associate editor, Omar al-Hashani; Arabic managing editor, Maurice Shohet; media relations associate, Ian Byrne; former communications and development associate, Alison Percich; and data services coordinator, Beverly Sprewer. The tireless efforts of operations manager Rebecca Erdman and administrative assistant Gina Vailes have allowed these events to proceed like clockwork.

My thanks extend to the Washington Institute fellows, research assistants, and interns—particularly the senior fellows of the Stein Program, Katherine Bauer and Aaron Zelin—who played a role either directly or indirectly. A number of current and former Stein Program RAs were instrumental in putting together this speaker series and volume, including A. J. Beloff, Evan Charney, Jacob Magid, Rachel Miller, Marina Poudret, Maxine Rich, Nicolette San Clemente, and Aviva Weinstein.

I am truly blessed to be a member of the intellectual community that is The Washington Institute. Although the lectures that follow, and the

insights they provide into this particularly critical turning point in the world of counterterrorism, are invaluable, this series affords merely a glimpse of the debate and discussion that take place within the Institute's walls on any given day.

Dr. Matthew Levitt
July 2017

Speakers

Note that positions listed were those held at the time of the respective lecture.

ALI MOHSEN AL-ALAQ

Ali Mohsen Al-Alaq, governor of the Central Bank of Iraq, is a policymaker and academic with three decades of experience in financial management, accounting, and analysis.

SHANNA BATTEN

Shanna Batten directs the Community Resilience Initiatives Program at the University of Maryland's Center for Health and Homeland Security. She served previously as legal advisor on the joint federal Countering Violent Extremism Task Force.

RAND BEERS

Rand Beers was the deputy assistant to the president for Homeland Security during the Obama administration. He served previously as acting secretary of Homeland Security following the resignation of Secretary Janet Napolitano in September 2013, until Jeh Johnson assumed that office the following December.

MONIKA BICKERT

Monika Bickert, who received her juris doctor from Harvard Law School, is head of global policy management at Facebook. She is a former assistant U.S. attorney in the Northern District of Illinois and was a resident legal advisor at the U.S. embassy in Bangkok.

WILLIAM BRANNIFF

William Branniff is executive director of the National Consortium for the Study of Terrorism and Responses to Terrorism (START) and a professor at the University of Maryland. He previously led the practitioner education program at West Point's Combating Terrorism Center, the nation's largest provider of CT education to government audiences.

LORD RICHARD DANNATT

Lord Richard Dannatt is a former chief of the general staff of the British Army and member of the House of Lords, where he served as a defense advisor to David Cameron. His autobiography, *Leading from the Front*, was published by Bantam Press in 2010

OLIVIER DECOTTIGNIES

Olivier Decottignies, a French career diplomat, was the 2015–16 diplomat in residence at The Washington Institute. As second counselor in the French Embassy in Iran from 2012 to 2015, he oversaw the nuclear portfolio and Iran's regional policies. Prior to this, he served in the French Ministry of Foreign Affairs in Paris, where he worked on political-military issues.

MUHAMMAD FRASER-RAHIM

Muhammad Fraser-Rahim is the executive director, North America, for the London-based counter-extremist think tank Quilliam International. His years of U.S. government service have included posts at the National Counterterrorism Center and Department of Homeland Security, where he was an expert on violent extremism.

BRUCE HOFFMAN

Bruce Hoffman is a professor at Georgetown University's Edmund A. Walsh School of Foreign Service, where he directs the Center for Security Studies and the Security Studies Program. Appointed by Congress to serve on the Independent Commission to Review the FBI's Post-9/11 Response to Terrorism and Radicalization, he was a lead author of the commission's final report.

BOAZ GANOR

Boaz Ganor is the dean and Ronald Lauder Chair for Counter-Terrorism at the Lauder School of Government, Diplomacy and Strategy, as well as founder and executive director of the International Institute for Counter-Terrorism at IDC, Herzliya, Israel.

DANIEL L. GLASER

Daniel L. Glaser serves as assistant secretary for terrorist financing in the Treasury Department's Office of Terrorism and Financial Intelligence, where he focuses on money laundering, terrorist financing, and the financing of WMD proliferation in relation to the international financial system.

SEAMUS HUGHES

Seamus Hughes is deputy director of George Washington University's Program on Extremism, a former lead staffer on CVE issues at the National Counterterrorism Center, and former senior counterterrorism advisor for the Senate Committee on Homeland Security and Governmental Affairs.

JAMES F. JEFFREY

James F. Jeffrey is the Philip Solondz Distinguished Fellow at The Washington Institute, where he focuses on U.S. diplomatic and military strategy in the Middle East, with emphasis on Turkey, Iraq, and Iran. One of the nation's most senior diplomats, Ambassador Jeffrey has held a series of highly sensitive posts in Washington D.C. and abroad.

RICHARD KEMP

Richard Kemp, a senior associate fellow of the Royal United Services Institute, was commander of British forces in Afghanistan and led the international terrorism team at Britain's Joint Intelligence Committee.

GILLES DE KERCHOVE

Gilles de Kerchove is the EU Counterterrorism Coordinator. A senior Belgian official, he served as director of justice and home affairs in the EU Council Secretariat from 1995 to 2007, among other positions.

NAOMI KIKOLER

Naomi Kikoler is the deputy director of the Simon-Skjodt Center for the Prevention of Genocide at the U.S. Holocaust Memorial Museum. She served previously as director of policy and advocacy at the Global Centre for the Responsibility to Protect and as a legal fellow with Amnesty International Canada.

MATTHEW LEVITT

Matthew Levitt is the Fromer-Wexler fellow and director of The Washington Institute's Stein Program on Counterterrorism and Intelligence (as it was then known). He is a former deputy assistant secretary for intelligence and analysis at the U.S. Department of Treasury and counterterrorism intelligence analyst at the Federal Bureau of Investigation (FBI).

MARLENE MAZEL

Marlene Mazel, an adjunct scholar at The Washington Institute, is on leave from her position as director of the Counter-Terrorism Litigation Division of the Israeli Ministry of Justice, where she directs the legal representation of Israel on litigation in foreign national courts, specifically concerning counterterrorism, national security, and international humanitarian law.

KLAUS NAUMANN

Klaus Naumann is former chief of staff of the German Bundeswehr and served as chairman of the NATO Military Committee from 1996 to 1999.

FARAH PANDITH

Farah Pandith is an adjunct senior fellow at the Council on Foreign Relations and a senior fellow at Harvard University's Belfer Center for Science and International Affairs. She also serves on the Homeland Security Advisory Council, where she cochairs the Countering Violent Extremism Subcommittee. In 2009 she was named the first-ever U.S. Special Representative to Muslim Communities.

SAMANTHA RAVICH

Samantha Ravich, an advisor to the Chertoff group, was deputy national security advisor for Vice President Cheney and served in the White House for more than five years as his representative on Asian and Middle

East affairs as well as counterterrorism and counterproliferation. Ravich served as the Republican cochair of the National Commission for Review of Research and Development Programs in the United States Intelligence Community.

ERIC ROSAND

Eric Rosand directs The Prevention Project: Organizing Against Violent Extremism, based at the Global Center on Cooperative Security. He recently left the State Department, where he served as counselor to the undersecretary for civilian security, democracy, and human rights. Previously, he was a senior official in the department's Bureau of Counterterrorism.

DICK SCHOOF

Dick Schoof has served as the national coordinator for security and counterterrorism in the Netherlands since March 2013, with responsibility for crisis management, cybersecurity, and related efforts. Previously, he served as director-general of the police force and played a leading role in creating the European Union's roadmap on information sharing.

MICHAEL STEINBACH

Michael Steinbach is executive assistant director of the FBI's National Security Branch. He has served in a variety of roles, including head of FBI operations at Guantanamo Bay, deputy on-scene commander of FBI operations in Afghanistan, legal attaché in Tel Aviv, and deputy director for law enforcement services at the CIA's Counterterrorism Center.

Introduction

■ Matthew Levitt

JUST AS this iteration of The Washington Institute's Counterterrorism Lecture Series was beginning in early 2016, a series of watershed events occurred that shaped the nature of the terrorist threat and the counterterrorism response for the duration of the Obama administration and into the new Trump administration. Islamic State attacks in the West had already become part of the CT landscape by 2016, kicked off in earnest by the Paris attacks in January 2015, continuing through the year, and culminating with the San Bernardino attack in December 2015. The new year opened with still more attacks abroad, which occurred in tandem with the group's slow but steady territorial losses on the ground in Syria and Iraq.

The Islamic State had perpetrated egregious crimes against humanity, war crimes, and ethnic cleansing from the time it stormed onto the world stage in 2014, but by 2016 the international anti-IS coalition was taking its toll on the terrorist group. As it lost territory, IS lost not only the ability to make money from natural resources but also its massive taxation (extortion) of the local population.

As IS faced battlefield defeat at the hands of coalition forces, undermining the group's self-declared territorial goal of "remaining and expanding," attacks abroad took on greater significance as a way to remain relevant and demonstrate that the group could still inflict pain on its adversaries—but now in their home countries. A review of IS-related attacks in 2016 includes multiple attacks in Turkey, the Brussels bombings, and attacks and plots in Afghanistan, Algeria, Bangladesh, Egypt, France, Germany, Indonesia, Iraq, Israel, Jordan, Kenya, Libya, Morocco, Pakistan, Philippines, Russia, Saudi Arabia, Somalia, Tunisia, United States, and Yemen.[1]

But over the course of the same year, IS forces in Iraq and Syria suffered a series of unremitting defeats. IS lost the Iraqi towns of Hit in April and Rutbah in May 2016, while offensives targeting Raqqa and Fallujah commenced in May, with the latter fully liberated in June. U.S.-backed rebels took a key IS base in Manbij, Syria, in July and took full control of the town the following month. Islamic State spokesman Abu Muhammad al-Adnani was killed during a U.S. airstrike in Syria in August, and IS lost control of its last Iraqi oil well in September. The battle to retake Mosul commenced in October, the same month IS was ousted from the symbolically significant town of Dabiq. Libyan forces formally announced the complete liberation of Sirte in December, and the year closed with U.S. officials announcing that some 50,000 ISIS fighters had been killed since Washington initiated military action against ISIS two years earlier.

These staggering losses, however, propelled Islamic State efforts to proclaim the importance of its far-flung provinces and clamor for

By 2016 the international anti-IS coalition was taking its toll on the terrorist group.

IS operatives or radicalized individuals to carry out attacks beyond Syria and Iraq. IS leader Abu Bakr al-Baghdadi released a statement in November, his first in almost a year, calling on "soldiers of the Caliphate" to "remain steadfast and do not flee when engaging the enemy," and pointing to Algeria, Tunisia, Libya, the Philippines, Yemen, and Sinai as places where IS had established functioning provinces.[2] The follow-

ing month, when IS named Abu Hassan al-Muhajir as Adnani's replacement as spokesperson, Muhajir issued an online statement urging fighters to stand their ground in Iraq and like-minded followers to execute attacks abroad. Since many foreign fighters were already making their way to other jihadi battlegrounds or back to their home countries, anxiety ran extremely high among Western security services. The 2015 Paris attacks and 2016 Brussels bombings had underscored the capabilities of such returnees, rendering as high priority the dual objectives of countering violent extremism (CVE) and contending with returning foreign fighters.

The year closed out with an Islamic State call for holiday season attacks in Europe, including attacks targeting markets and hospitals. And while such messages typically appeared on social media platforms, by December 2016 the group was instructing its members to cease using messaging applications like WhatsApp and Telegram for fear that coalition forces were leveraging data from these platforms to target Islamic State leaders. According to a February 2017 UN report, "The internal communication and recruitment methods of the group are increasingly moving towards more covert methods, such as the use of the dark web, encryption and messengers."[3] Developing policies to address terrorist abuse of social media platforms for communication, and sometimes funding as well, also garnered significant attention over the course of this lecture series.

Perhaps the most chilling pronouncement of December 2016 came from a House Homeland Security Committee report, which stated: "The United States faces its highest Islamist terror threat environment since 9/11, and much of the threat now stems from individuals who have been radicalized at home."[4]

What follows is a brief discussion of some of the key themes to emerge over the course of this iteration of the speaker series.

ISIS Attacks Abroad

The March 2016 Brussels bombings made it painfully clear that the Islamic State was determined to plan and direct attacks in the West that were far more sophisticated and lethal than so-called lone-wolf attacks. Indeed, since then, IS has carried out a number of deadly attacks abroad, including the December 2016 Berlin Christmas market attack, the 2017 New Year's Eve attack in Istanbul, and the August 2017 car ramming in Barcelona. Despite these attacks, however, IS has faced significant setbacks as it transitions into a post-caliphate era.

The Islamic State is on the verge of total battlefield defeat in both Iraq and Syria, losing more than 90 percent of its revenues since 2015.[5] The group no longer produces some of the online magazines for which it achieved worldwide notoriety, and it has even claimed responsibility for terrorist attacks it did not carry out. But despite these setbacks, the UN secretary-general concluded in his latest report on the threat posed by ISIL that "the group continues to pose a significant and evolving threat around the world."[6]

According to the report, ISIL is "now organized as a global network, with a flat hierarchy and less operational control over its affiliates."[7] In practice, this means that the Islamic State is becoming more reliant on individuals and small groups to carry out attacks, using social media, encrypted communication platforms, and the dark web to connect with its followers and regional affiliates.

Internal communication and recruitment methods of the group are increasingly more covert.

"Frustrated travelers"—those who tried unsuccessfully to travel to conflict zones and remain radicalized—as well as foreign fighter returnees and those who relocate to other battlefields will become more relevant as the IS pool of recruits dries up.[8] At the same time, members of IS and al-Qaeda have been willing to support each other's attacks, demonstrating a level of convergence between the groups that could grow over time.

Returning Foreign Terrorist Fighters

With each battlefield defeat it has faced over the past two years, the Islamic State has evolved

from a militant group governing territory to a terrorist and insurgent group operating without fixed territory. And with this progression comes an increase in the threat posed by the group in the region and beyond. Homegrown violent extremism (HVE) is one aspect of this threat; the return of battle-hardened foreign terrorist fighters yet another.

Foreign fighters trained by the Islamic State are now fleeing Iraq and Syria for their home countries. Of the approximately 30,000 fighters in Iraq, 9,000 are from East Asia, 8,000 from Europe, 6,000 from Tunisia, and 3,000 from Saudi Arabia.[9] The EU counterterrorism coordinator reported that about 1,500 Europeans, predominantly from France and Belgium, have returned home the region after training with the Islamic State.[10]

The CVE programs being developed to address these returnees are one important aspect of dealing with the threat, particularly in Europe. But these programs must be coupled with much-improved border security, if only because some of the most dangerous returning fighters are likely to use sophisticated forgeries and false documents to cross borders. Interpol has developed a number of tools that UN member states have implemented at their borders, including facial recognition software, a global foreign terrorist fighter database, and a fingerprint database.[11]

Terrorist Communications and Social Media

Social media and online communication networks have enabled groups such as IS to inspire individuals outside the territory they control to carry out attacks in the name of the Islamic

State. Additionally, the "influencers" (jihadist voices who may or may not have formal ties with major jihadist groups but who disseminate jihadist material and rhetoric) and the mirror effect of individuals "inspired" or "radicalized" by this online material, without necessarily having direct links to jihadist clerics or groups, have also taken advantage of the new media landscape.[12]

Inspire *magazine praised three prior lone-actor attacks, called for more of the same, and provided operational suggestions.*

Both al-Qaeda and IS have published online how-to guides for carrying out attacks with homemade improvised explosive devices (IEDs), vehicles, knives, arson, and more. In November 2016, for example, al-Qaeda in the Arabian Peninsula published its 16th edition of Inspire magazine, which praised three prior lone-actor attacks, called for more of the same, and provided operational suggestions for such attacks.[13] In July 2017 IS released an e-book in Turkish with instructions for conducting attacks alone.[14] Additionally, the ninth volume of the Islamic State periodical Rumiyah, published in May 2017, contained details on the ideal weapons and targets for lone-wolf attacks.[15] Indeed, the group has been pushing such attacks for years now. In a 2015 online e-book entitled How to Survive in the West: A Mujahid Guide, the group argued: "With less attacks in the West being group (networked) attacks and an increasing amount of lone-wolf attacks, it will be more difficult for intelligence agencies to stop an increasing amount of violence and chaos from spreading in the West."[16]

Social media has also helped IS affiliates to

raise funds. In one case, Ali Shukri Amin, a teenager from Virginia, used Twitter to circulate instructions on how to fund IS through Bitcoin.[17] He first began tweeting in 2014, becoming increasingly radicalized and motivated to help people join ISIS, either financially or by traveling to Syria.[18] His tweets stressed the anonymity of Bitcoin—how a donor's personal information and the amount of the contribution would remain hidden from authorities. Amin was arrested in 2015 and in June that year he pled guilty to providing material support to ISIS.[19]

Countering Violent Extremism

Over the past several years, the terrorist threat environment facing the United States and its allies has evolved into something more dangerous and complicated than ever before, with implications for both international and domestic security.

Building resilient communities capable of resisting and countering violent extremism is clearly in the national interest.

Authorities have reason to be concerned, given that the threats from homegrown violent extremists of all ideological stripes have increased significantly. In the last few years, the United States has suffered a number of HVE attacks, including the June 2016 Orlando shooting, a violent white-supremacist rally in the summer of 2017, and a November 2017 car ramming in New York City, to name just a few. As of August 2017, open investigations on approximately 1,000 potential HVEs encompassed all 50 states.[20] Border security notwithstanding, U.S. authorities are grappling with the reality that radicalization is not confined to

the Middle East; it occurs here too. Thus building resilient communities capable of resisting and countering violent extremism is clearly in the national interest.

CVE best practices are a matter of hot debate. Even the expression "countering violent extremism" has become loaded, with some associating the term with racial/religious profiling or government spying on the one hand, and some in the Trump administration preferring the more muscular term"terrorism prevention" on the other.[21] It is not clear, however, how much space this new term would allow for actual prevention efforts, what types of groups might be included in such a structure, or whether it would cover other social issues that can lead to extremism and violence.

CVE best practices are a matter of hot debate. Even the expression "countering violent extremism" has become loaded.

Preventing and countering violent extremism (P/CVE) is not a soft alternative to counterterrorism, but rather a parallel and complementary policy option for dealing with disconcerting yet lawful beliefs and activities that occur in the pre-criminal space. Although countering terrorism is a two-pronged endeavor—requiring tactical efforts to thwart attacks as well as strategic efforts to address the radicalization fueling its violence and global appeal—P/CVE is critical to *preempt* terrorist activity in the first place. By addressing the many cases of extremism that fall below the legal threshold for investigation, P/CVE efforts are attractive to law enforcement for the way they reduce the pool of potential terrorist recruits across the spectrum of violent extremist ideologies.

To be effective, it is critical to base P/CVE efforts on a public-health-style model that addresses all facets: prevention, intervention, disengagement, and rehabilitation. Since the country faces threats from across the ideological spectrum, the most effective efforts to address Islamist violent extremists will be part of a comprehensive approach that targets other types of extremists as well. The benefits of applying this model as a complement to existing violence prevention and public safety efforts are many, not least of which is that it will help build resilient communities, engender social cohesion, and represent good governance at its most fundamental level.

Preventing and countering violent extremism is not a soft alternative to counterterrorism.

Countering Terror Financing

Despite the Islamic State's territorial setbacks and loss of massive oil income, it continues to find ways to finance its insurgent and terrorist activities.

UN member states report that IS continues to move money across the Middle East by means of the hawala system and cash couriers, as it did before the fall of its caliphate.[22] Outside Syria and Iraq, such as in Libya, IS continues to raise funds through extortion and checkpoints, as well as by imposing taxes on human trafficking networks. The group also takes advantage of legitimate businesses, using them as fronts, as well as "clean" individuals able to deal with the formal financial system. As reconstruction efforts begin in territories liberated from the Islamic State,

officials fear the group may be well situated to defraud reconstruction efforts and investment in the local economy, especially through front companies in the construction and other industries.[23]

And the Islamic State still has access to sufficient funds to invest in its terrorist operations across the Middle East and beyond, far from the borders of Syria and Iraq. In Yemen, IS took advantage of the deterioration of security conditions to "plot, direct, instigate, resource, and recruit individuals for attacks against States of the region," the UN reports.[24] In Saudi Arabia, authorities disrupted a December 2017 plot to blow up Ministry of Defense headquarters buildings in Riyadh.

Farther away still, the UN reports that the Islamic State "core" provided financing for its affiliate in the Philippines during the siege of Marawi City. "Groups in the southern Philippines received hundreds of thousands of dollars from the ISIL core, through a third country, in advance of the siege," the secretary-general reported.[25]

Despite the grave picture, focused targeting of IS funds, the use of biometric data, and continued cooperation among UN member states show promise for effectively responding to IS capabilities and threats. For example, in Afghanistan, while local groups continue to receive some funding from the IS core, the local group has been encouraged to become self-sufficient, although it will struggle to survive without core support. Furthermore, support from IS in Yemen for its fellows in Somalia is considered "limited and unreliable."[26]

The Islamic State still poses serious terrorist threats, but it is slowly becoming a more limited and less reliable financial backer of its affiliates and operatives. This is a step in the right direction.

Hezbollah

Throughout this period, Hezbollah continued to present a significant threat to U.S. interests both in the Middle East and, as arrests in the United States, Europe, and South America underscore, closer to home. Iran is Hezbollah's primary benefactor, bankrolling the Lebanese political party and militant group with as much as $800 million a year in addition to weapons, training, intelligence, and logistical assistance.[27]

The war in Syria has dramatically changed Hezbollah. Once limited to jockeying for political power in Lebanon and fighting Israel, the group is now a regional player engaged in conflicts far beyond its historical area of operations (Iraq and Yemen), often in cooperation with Iran. The stron-

gest indicators of Hezbollah's transformation are structural. Since 2013, the group has added two new commands—the first on the Lebanese-Syrian border, the second within Syria itself—to its existing bases in southern and eastern Lebanon. In establishing its new presence in Syria, Hezbollah has also transferred key personnel from its traditionally paramount Southern Command along Lebanon's border with Israel.

The war in Syria has changed Hezbollah dramatically.

In March 2016, Hezbollah confirmed the death of its most prominent military figure, Mustafa Badreddine, reportedly killed in an explosion in Damascus.[28] Given Badreddine's role as head of the group's External Security Organization and its forces in Syria, his death represents Hezbollah's biggest loss since the 2008 assassination of former "chief of staff" Imad Mughniyah. Badreddine's death has Hezbollah on edge not because of the loss of the man, per se, but because the group's archenemy, Israel, was apparently not responsible. Hezbollah, it appears, now has more immediate enemies than Israel. Indeed, Hezbollah (and Iran) increasingly looked to Saudi Arabia as the cause of many of its problems, including Sunni-Shia tensions and the war in Syria.[29]

Other senior Hezbollah officers also died that year, including Ali Fayad in February and Khalil Ali Hassan in June.[30] Hezbollah has actually lost more fighters and key leaders in battles against Sunni rebels in Syria since 2012 than in all its battles and wars with Israel.[31] Although a few Hezbollah personnel were reportedly killed by Israel, including Jihad Mughniyah and Samir Kuntar, these cases are the exception.

Hezbollah's status in the wider Sunni Arab world has dropped precipitously since its height a decade ago after the 2006 Lebanon War. In the wake of that conflict, Hezbollah rode a wave of popular support across the region. A decade later, in March 2016, the Gulf Cooperation Council labeled Hezbollah a terrorist group, and the Gulf States have cracked down on Hezbollah supporters and financiers within their borders. The Arab League and the Organization of Islamic Cooperation have issued statements condemning Hezbollah as well, leading to a war of words between the group and Gulf officials.

Beyond the Middle East, Hezbollah continues to rely on a worldwide network of supporters and sympathizers to provide financial, logistical, and operational support. These aggressive efforts span the globe but have been especially pronounced in Europe and South America. The extent of Hezbollah's drug connections was underscored yet again by the Treasury narcotics kingpin designation of the Panama-based Waked Money Laundering Organization in May 2016. The press release tied to this action mentions neither Hezbollah nor Iran, but the action reportedly proved to be particularly damaging to their illicit financial conduct in the region.[32]

Investigation into Hezbollah BAC finance and facilitation networks has touched the United States as well. In October 2015, U.S. officials arrested Iman Kobeissi in Atlanta, Georgia. She was arraigned on two main charges: conspiracy to launder funds she believed to be drug money, and arranging for the sale of thousands of firearms, including military assault rifles, machine guns, and sniper rifles, to criminal groups in Iran and Lebanon, including Hezbollah. Her Hezbollah associate, Joseph Asmar, was arrested in Paris the same day and charged with money laundering conspiracy.[33]

Conclusion

As this speaker series progressed over the course of 2016, so did the coalition war against the Islamic State in Syria and Iraq. At the same time, the threat of IS-directed or -inspired attacks in the West continued to trend upward, posing significant challenges for social media companies, law enforcement and intelligence agencies, and even local communities working to build resiliency and counter the spread of violent extremism in their neighborhoods. The battle against IS still rages on, and the struggle against violent extremism will persist long after the Islamic State's demise. This volume offers a snapshot into how officials, experts, and practitioners addressed some of the

most pressing challenges of the day at the height of the battle against the Islamic State and the beginning of its decline. As authorities continue to target IS provinces worldwide and to staunch the spread of the group's violent ideology, many valuable lessons can be learned from the experience of those who took this fight to the enemy when the Islamic State was at its height.

Notes

1. See "Timeline: The Rise, Spread and Fall of the Islamic State," The Wilson Center, updated Dec. 19, 2017, http://bit.ly/2LgsYfw.
2. Abu Bakr al-Baghdadi, Nov. 2016 speech, *Rumiyah* Issue 3, http://bit.ly/2A0yqOt.
3. Fourth Report of the Secretary-General on the Threat Posed by ISIL (Da'esh) to International Peace and Security and the Range of United Nations Efforts in Support of Member States in Countering the Threat ," UN Security Council, Feb. 2, 2017, http://bit.ly/2LLLEAd.
4. "Terror Threat Snapshot," House Homeland Security Committee, Dec. 2016, http://bit.ly/2KZxLSq.
5. "Sixth Report of the Secretary-General on the Threat Posed by ISIL (Da'esh) to International Peace and Security and the Range of United Nations Efforts in Support of Member States in Countering the Threat," UN Security Council, Jan. 31, 2018, http://bit.ly/2LeySOb.
6. Ibid.
7. Ibid.
8. Ibid.
9. Matthew Levitt, "Shutting the Door to the Islamic State," *Alhurra*, Sept. 9, 2017, http://bit.ly/2LgE2t8.
10. Reuters Staff, "EU Urged to Share Data to Better Detect Militants Returning from Syria, Iraq, Dec. 7, 2016, https://reut.rs/2mkmRrw.
11. "Twentieth Report of the Analytical Support and Sanctions Monitoring Team Submitted Pursuant to Resolution 2253 (2015) Concerning ISIL (Da'esh), Al-Qaida and Associated Individuals and Entities," UN Security Council, Aug. 7, 2017, http://bit.ly/2LF1Gvv.
12. Matthew Levitt, editor, *Defeating Ideologically Inspired Violent Extremism*, Washington Institute for Near East Policy, March 2017, http://bit.ly/2mnZcqv.
13. "The 9/17 Operations," *Inspire*, Nov. 2016, http://bit.ly/2AmnA5F.
14. "Lone Wolves Handbook," June 22, 2017, http://bit.ly/2uXxW5N (original no longer available; link is to a more recent Turkish version).

15. "The Ruling on the Belligerent Christians," *Rumiyah*, May 2017, http://bit.ly/2mGjLOW.
16. "How to Survive in the West: A Mujahid Guide (2015)," http://bit.ly/2uJHSR1.
17. "A Teen's Turn to Radicalism and the U.S. Safety Net that Failed to Stop It," Yasmeen Abutaleb and Kristina Cooke, Reuters, June 6, 2016, https://reut.rs/2uMb6Pg.
18. Ibid.
19. "Virginia Teen Pleads Guilty to Providing Material Support to ISIL," DOJ, June 11, 2015, http://bit.ly/2OeYnN4.
20. "Deputy Attorney General Rosenstein Delivers Remarks at the 10th Annual Utah National Security and Antiterrorism Conference," DOJ, Aug. 30, 2017, http://bit.ly/2uLn5wD.
21. Tal Kopan, "Trump Administration Has Sought Domestic Counterterror Cuts," CNN, Nov. 1, 2017, https://cnn.it/2mCmV6n.
22. "Sixth Report of the Secretary-General on the Threat Posed by ISIL," UN Security Council, http://bit.ly/2LeySOb.
23. Ibid.
24. Ibid.
25. Ibid.
26. Ibid.
27. Anna Ahronheim, "Iran Pays $830 Million to Hezbollah," *Jerusalem Post*, Sept. 15, 2017, http://bit.ly/2utGKB5.
28. Hugh Naylor, "In Blow to Hezbollah, Senior Commander Killed in Syria," *Washington Post*, May 13, 2016, https://wapo.st/2zM8UfI.
29. Matthew Levitt, "Hezbollah's Pivot Toward the Gulf, *CTC Sentinel,* Aug. 2016, http://bit.ly/2LjXNzQ.
30. Matthew Levitt and Nadav Pollak, "Hizbullah Under Fire in Syria," Tony Blair Faith Foundation, June 9, 2016, http://bit.ly/2NkGCuA.
31. Ibid.
32. "Treasury Sanctions the Waked Money Laundering Organization," Treasury Dept, May 5, 2016, http://bit.ly/2uIwDZi.
33. "Two Hezbollah Associates Arrested on Charges of Conspiring to Launder Narcotics Proceeds and International Arms Trafficking," DOJ, Oct. 9, 2015, http://bit.ly/2NmLkIt.

FEBRUARY 26, 2016

Internet Security and Privacy in the Age of the Islamic State: The View from Facebook

■ Monika Bickert

RAPPORTEUR'S SUMMARY

FACEBOOK has long sought to ensure that its site is safe and that people are not exploiting it to promote terrorism. This is a challenge given the size of its community: currently 1.6 billion regular users, the vast majority of them outside the United States. To meet this challenge, Facebook established a set of "community standards" barring certain activities, and it enforces these standards through a content policy team based in five offices around the world. Team members have many different backgrounds (lawyers, NGO workers, etc.), but the company also realizes the necessity of consulting with outside experts. For example, it frequently reaches out to other organizations for their interpretation of terrorism-related events, including The Washington Institute.

Policy and Response

Facebook does not allow any member of a terrorist group or other violent organization to have a presence on the site. This is a broad policy, meaning that any users who are found to be members of such groups are barred from the site, regardless of what they may be talking about on their accounts. Similarly, when Facebook becomes aware that an account is supporting terrorism, it removes that user and looks at associated content and accounts. Experts have repeatedly told the company that the best way to find terrorists is to find their friends.

Another Facebook policy is to remove content supporting or promoting violent groups or their actions even if there is not sufficient cause to close that person's account. In such cases, the consequences for the user vary; first-

time violators generally get a warning, but if Facebook becomes aware of a credible threat and believes that referring information to law enforcement is necessary to prevent harm, it will do so. The company also has a robust process in place for responding to requests from law enforcement, assuming authorities can provide the appropriate court order.

Facebook receives more than a million reports of potential site violations per day, related not only to terrorism but also to bullying, harassment, child exploitation, and other prohibited behavior. These reports are assessed by real people based around the world who review content in more than forty languages and can access external translation services as needed. The trick is getting the reports to the right person for that subject matter. For example, Facebook has in-house experts who specialize in analyzing terrorism support, and they receive ongoing training from academics and researchers who come in to update the team on relevant terminology, iconography, and other information.

Of course, even when violators are shut down, they will inevitably try to come back. It is easy to create an account on Facebook, Twitter, YouTube, and other social media sites. That's by design—companies want people to use these services, and they don't want to put too many barriers in their way. As a result, these sites necessarily get the bad with the good. Facebook has measures in place to prevent the bad apples from returning, but the system is not perfect.

Promoting Counter-Speech

Facebook is mindful of the fact that removing content alone will not fix the problem—getting people to actually stand up and challenge terrorist ideology requires more. With that in mind, the company has been investing in counter-speech, which involves raising awareness, pushing back against certain kinds of speech, and encouraging people to question hateful or extremist ideology.

Users have already been creating this sort of content on the site for years. For instance, Facebook pages helped raise awareness about Boko Haram's kidnapping activities and the hashtag "#BringBackOurGirls." And in the wake of the January 2015 Charlie Hebdo attack, more than seven million people used the site to express solidarity with the victims and stand against terrorism. So Facebook knew that counter-speech was happening—what was needed was a more data-oriented approach to the issue, with the goal of empowering people to create more of this sort of speech.

Toward that end, the company began conducting research with the British think tank Demos nearly two years ago, looking at which types of Face-

book campaigns succeed against violent extremism and why. Once the factors behind that success were identified, Facebook could impart them to others who want to share the same message in other regions.

Three such factors have stood out thus far. The first is format—visual imagery is very important to a campaign's success, as is conciseness. The average viewing time that users devote to videos on social media is shockingly short, so a five-minute message is not the best way to reach an audience.

The second factor is tone. In France, for example, about a quarter of the content on pages espousing hateful ideology consists of comments standing up against that ideology.

Facebook is mindful of the fact that removing content alone will not fix the problem.

Yet much of this counter-speech is not especially constructive because it relies on an attacking approach. Through its research with Demos, Facebook has learned that positive, constructive messages are more successful in getting people to question certain ideologies. Humor and satire are particularly effective in that regard.

The third factor involves determining the most effective speaker for a given audience. For example, a government figure would probably not be very compelling to young people who are skeptical about authority—they are more likely to respond to a celebrity, a young person, or someone who has otherwise stood in their shoes. The choice of spokesperson and audience also depends on a campaign's goal, whether it be to raise awareness or actively turn people away from violent ideologies.

In addition to its work with Demos, Facebook has been supporting efforts by other groups to promote different types of counter-speech. One such group is the Institute for Strategic Dialogue, which put out research late last year about one-to-one intervention. As in other types of campaigns, tone is very important in one-to-one outreach—the institute pointed out that such conversations need to begin in a very casual, non-accusatory manner until the relationship is built up sufficiently.

Facebook is also interested in gamification, making the act of creating counterspeech fun and perhaps a bit competitive, especially for young people. The company has worked with various external groups that excel in this area, including EdVenture Partners. In collaboration with the State Department and Facebook, EdVenture has been running a program called "Peer 2 Peer," where university students from around the world compete in a semester-long course to create campaigns against violent extremism.

Over the past two years, Facebook has participated in closed-door roundtables on countering terrorism and violent extremism. Because the other companies involved in this forum remain anonymous, they can be very open with one another about what they are seeing and how they are trying to tackle these challenges, without being judged by outsiders.

Facebook also participates in working groups with Interpol and the European Union. This dialogue has been very productive—the company has learned about extremism-related trends in Europe and taken these lessons to heart when formulating its enforcement policies.

At the same time, Facebook has long been mindful of the need to protect the accounts of activists who stand against extremism and other problems. In addition to preventing hackers from compromising these accounts, the company has a very rigorous process for scrutinizing government requests for people's data, making sure they have gone through the proper channels.

Challenges Going Forward

The constantly evolving nature of social media means that new and perhaps unexpected challenges will often arise. For example, video sharing has exploded in the past few years as smartphones and networks became better equipped to handle it. But look at this development from the perspective of Facebook team members tasked with reviewing such content for violations. What do they do when the average length of posted videos doubles or triples? There are tools out there that make it easier to review

videos, separate them into more digestible segments, et cetera. But what about the audio? What if the video content is fine but the audio contains a threatening speech? At present, there is no easy answer to these questions, and Facebook will have to remain mindful of such issues as the relevant technologies evolve.

This summary was prepared by A. J. Beloff.

MARCH 25, 2015

Terror in Europe: Combating Foreign Fighters and Homegrown Networks

■ Matthew Levitt, Olivier Decottignies, and Eric Rosand

RAPPORTEUR'S SUMMARY

MATTHEW LEVITT

AFTER the tragic terrorist attacks in Brussels, Europe as a whole and Belgium in particular are facing a twofold problem. First, there is much work to be done from the counterterrorism perspective. The fact that Brussels plotter Salah Abdeslam was able to hide out in his hometown since the November attacks in Paris is a concern. Many EU member states are not yet connected to the information-sharing databases that Europol has put in place. According to Europol, around 5,000 EU citizens have traveled to warzones in Syria and Iraq, yet only 2,786 foreign terrorist fighters (FTFs) have been recorded in its database. Worse, over 90 percent of these reported fighters came from just five member states. The EU must integrate intelligence sharing more fully among all of its members.

The second problem is social integration. Many of the people who join the Islamic State (IS) feel like they have gone from "zero to hero"—for them, embracing an ideology and being a part of a group as it grows is an extremely empowering experience. The large Muslim community in the Molenbeek district of Brussels has become so isolated that their children do not attend school or speak the local language; similarly, only 8 of 114 imams in the entire capital speak any of the local languages. Molenbeek is also the second-poorest municipality in the country, with the second-youngest population, high unemployment and crime rates, and a nearly 10 percent annual population turnover.

While the Brussels attacks were a wake-up call for the rest of the world, the turning point for European counterterrorism officials was actually the thwarting of a terrorist cell in Verviers in January 2015. That raid uncovered

a plot being directed by Abdelhamid Abaaoud from Athens via cellphone; he would later play a key role in the Paris attacks as well. As a Department of Homeland Security intelligence bulletin presciently warned at the time, the multijurisdictional nature of the Verviers plot would pose a significant problem moving forward. In the United States, almost every FBI field office is working on active terrorism cases, but most are of the lone-offender variety, as seen in the San Bernardino attack last December. In Europe, however, a shift toward spectacular foreign-directed attacks has begun.

Europe lacks a robust, integrated intelligence and law enforcement system like the United States established after 9/11.

Several factors help explain this difference. First, while the United States is protected by two vast oceans, Europe is right on the doorstep of Syria and Iraq. It is easy and cheap to travel to the continent because most barriers of entry have been removed. Europe also lacks a robust, integrated intelligence and law enforcement system like the United States established after the September 11 attacks. There is no such thing as a 100 percent success rate, but America has a much better model for preventing these types of attacks—a model that Europe is just now beginning to put in place.

As a result, many local authorities in Europe lack the resources they need to cope with the current threat. For example, Molenbeek had 185 unfilled police officer positions as of last November; they have since filled 50 of them but are still 135 short. Belgium has made a lot of good

changes in the past eighteen months, including a fusion center between national and local police, but these things need time to take effect, particularly with regard to staffing.

OLIVIER DECOTTIGNIES

MATTERS of opportunity and tactical experience play a role when terrorists are choosing a city to strike: for instance, Brussels had been a staging area for the Paris operation, and Islamic State operatives were already instilled in the community. Yet the Brussels attacks also epitomize a strategic decision to extend IS operations into Europe. After carving out its self-styled caliphate in the heart of the Middle East, the group proclaimed outer "provinces" by endorsing groups in Nigeria, Libya, the Sinai, and elsewhere. With the latest attacks in Paris, Brussels, and Istanbul, it is now exporting the fight to Europe, perhaps in response to setbacks in Iraq and Syria.

Consequently, the whole of Europe is a target, with terrorist networks and procurement lines spanning the continent and plots being foiled in multiple countries. IS propagandists have issued threats against additional European cities, and the group can call on at least 5,000 FTFs

All of Europe is a target, with terrorist networks and procurement lines spanning the continent.

of European origin, not to mention homegrown radicals. IS leaders are well aware that the continent is facing multiple crises related to economics, migration, identity, and the European project itself. The recent attacks also fit within the group's notion that Western Muslims are in

a "grey zone," neither following the ways of the fantasized caliphate nor fully integrating with the Western mainstream. Through repeated terrorist attacks, IS hopes to provoke a political and security backlash against these Muslims, thus pushing them into the arms of the radicals.

Europe is not well equipped to stand up to this threat. Just as the monetary union was created without a fiscal union, free movement within Europe was established without strong security cooperation among member states or on the outer borders. The EU has conducted successful operations within the framework of its Common Security and Defense Policy, but that instrument was tailored to stabilize the EU neighborhood (e.g., in the Balkans) or resolve more distant crises (e.g., in Africa), not to defend Europe proper.

Fortunately, EU states can take several steps to improve the situation, including increased intelligence sharing, both bilaterally and in the framework of Europol; a more robust mandate for the EU's border agency, Frontex; a European Passenger Name Records system that would allow the sharing of air travel data; and improved efforts to track anonymous payments. Internal and external security cannot be separated, though. Only a handful of European countries currently meet their NATO defense spending commitments, and even fewer are actually willing to commit troops to operations. After the Paris tragedy, France invoked Article 42(7) of the Treaty on European Union, which obligates member states to extend assistance when a fellow member is attacked. In response, EU governments unanimously expressed support, with some (e.g., Germany) committing troops and capabilities to supplement or relieve French deployments in the Sahel or the Levant—deployments that benefit the whole continent.

These efforts should be deepened in the wake of Brussels, and the new security and foreign policy strategy that the EU is due to adopt this summer should reflect those priorities. The union's future depends on its ability to deliver security to citizens and assert its values with confidence, making sure that these values do not remain empty promises for those who chose to embrace the European way of life. The stakes are high, including for the United States, whose citizens can be targeted in and from the EU, and who may have to deal with a very different continent if Europeans fail in their struggle.

Europeans must also be careful not to turn the situation into "us and them." Not only does this dichotomy play right into the Islamic State's trap, it is also factually wrong. Most of the European youths who have participated in the Syrian jihad were born in France, and a third of French FTFs were not born into Muslim families—rather, they converted directly to the

IS brand of Islam. Meanwhile, European Muslims join their country's security forces in far greater number than they join IS, and they play a key role in fighting the group. The difference between Europe and the United States is that Salafist predication in EU countries puts a uniquely dangerous spin on the shared problems of poverty, unemployment, and discrimination.

Finally, it is important to note the role that ordinary crime plays in the European security equation. Many of the operatives involved in recent attacks have a history of petty or more serious crime, which is becoming an increasingly likely pathway to terrorism.

ERIC ROSAND

EUROPE'S two-pronged security problem should be framed as a near-term counterterrorism challenge and a long-term prevention challenge. In this regard, one of the biggest issues to grapple with is resources. Unfortunately, resource allocation never matches prevention rhetoric, including in the United States. The EU has the most elaborate radicalization awareness network imaginable, and it turns out great analysis and workshops. Yet this has not translated into resources being allocated at the municipal level to implement these practices.

The gaps in the EU's counterterrorism structures are not new, nor is the occurrence of large-scale terrorist attacks—European and U.S. officials have long been advocating systemic changes to address both problems. Part of the reason why the gaps persist is because the process is often driven by the lowest common denominator, with some countries simply unwilling to exert the required political will. In short, Europe is not without counterterrorism structures—they exist, they just don't work.

Another challenge lies in how European countries balance privacy and security. For too long they have emphasized privacy to a degree that interferes with security provision. The debate is so complex, and the EU system so hydra-headed, that it slows down reform efforts. This situation also complicates U.S. efforts to coordinate with the EU on counterterrorism—multiple agencies must be engaged separately, and oftentimes none of them are the actual EU Counter-Terrorism Coordinator, who in any event lacks the requisite authority because his mandate and resources are so limited.

Looking forward, a lot of the solutions to counterterrorism problems in Europe will involve empowering subnational actors such as local police forces and municipalities. Toward that end, the United States has encouraged city-to-city exchanges so that lessons learned by American authorities can be shared

and vice versa. For example, Vilvoorde, Belgium, had the highest per capita number of FTFs leaving for Iraq and Syria, so local officials traveled to Columbus, Ohio, and met with law enforcement and other authorities to discuss best practices for preventing at-risk individuals from leaving. Once they implemented these in Vilvoorde, the number of FTFs dropped dramatically.

For too long, EU countries have emphasized privacy to a degree that interferes with security.

Furthermore, several other places in Europe (e.g., Denmark and the Netherlands) have innovative community-level programs that deal with the exact same challenges Belgian authorities face in Brussels. So why aren't these programs being implemented in Molenbeek? Communications and intelligence are not the only way to track terrorist networks and catch terrorist masterminds; community members also play a role by reporting early signs of radicalization. It is no secret that Abdeslam was able to find a safe haven back home in Molenbeek; some people in that community likely could have provided notice of his presence, but Belgium's investment in that sort of intelligence gathering is not there yet.

Finally, it is worth noting that after 9/11, Europeans endlessly reminded the United States not to let its response to the attacks overreach in regard to human rights. Now that Europe is under attack, such rhetoric has decreased significantly. The risk of overreacting is real, however, so as the EU seeks a balanced approach to the latest threats, it must be sure not to create more radicalized individuals.

This summary was prepared by A. J. Beloff.

APRIL 5, 2016

Combating Genocide: Reassessing the Fight Against the Islamic State

■ Matthew Levitt, Naomi Kikoler, and James F. Jeffrey

RAPPORTEUR'S SUMMARY

MATTHEW LEVITT

THE ISLAMIC STATE adheres to a hardline Salafi jihadist ideology overlaid with an apocalyptic worldview, pitting those whom it perceives as true believers against apostates and nonbelievers. In this "us versus them" mindset, violence is a core part of the organization's DNA—it is not just permissible to kill enemies and nonbelievers, but a religious duty.

According to its English-language magazine *Dabiq*, IS denies any chance of peaceful existence with people who hold different beliefs, including Christians, Yazidis, and others. Part of the group's strategy therefore includes eliminating what it calls the "grey zone," forcing Muslims to either join the caliphate or be labeled apostates. IS aims to convince Muslims that the West will never accept them, and every violent act has this goal in mind.

The Islamic State's propensity for violence is widely known to potential recruits prior to their arrival in Syria and Iraq. According to a Dutch intelligence report, "Anyone traveling to the so-called Islamic State is knowingly opting to join a terrorist group which regards all outsiders as 'infidels' and uses excessive violence on a daily basis." While IS claims to be defending its territory, the report adds that "its idea of 'defense' includes attacking, killing, raping, or enslaving Syrians and Iraqis who do not share its beliefs, or who resist in any way."

The group employs such wanton, barbaric violence as a means of instilling fear and subjugating populations. Extreme violence also attracts attention to IS propaganda and facilitates its recruitment and fundraising efforts.

Crimes against humanity, war crimes, and genocidal actions all play into the group's overall apocalyptic vision; for example, IS celebrates slavery as "one of the signs of the Day of Judgment."

Knowing that IS purposefully uses extreme violence, and given that the international community has a responsibility to protect civilians, humanitarian considerations need to be given higher priority than they have been to date. Evidence collection teams should be immediately dispatched to liberated territory in order to document atrocities. Civilian protection teams should follow behind the military to address the needs of individuals who have suffered under the yoke of IS rule. And military planners should integrate civilian protection into their strategy for defeating the group. As the anti-IS coalition sets the stage for efforts to retake Mosul, now is the time to explore military and nonmilitary strategies that can help stabilize newly liberated areas.

NAOMI KIKOLER

INTERVIEWS conducted by the Holocaust Memorial Museum make clear that genocide and crimes against humanity have been committed against Iraq's minority populations. The Islamic State is a terrorist group that is also genocidal. It commits atrocity crimes for the strategic purpose of controlling, expelling, or exterminating populations. Any counter-IS strategy needs to address this strategic targeting of civilians.

Interviews with survivors also show that the perpetrators of crimes against humanity in Iraq are diverse, including IS personnel, local and foreign fighters, and complicit or opportunistic neighbors. Devising strategies to prevent further atrocities requires dissecting the complex and diverse dynamics that enable and motivate perpetrators. For example, one impending massacre in Mosul was delayed by a few days because of key relationships between community leaders and former Baath officials.

Accordingly, intelligence gathering and sharing is critical to combatting IS and identifying vulnerabilities in local communities. Information should be shared with different stakeholders to help map weaknesses and develop protection strategies for vulnerable populations.

Documenting atrocities is vital as well, and satellite imagery should be used to record mass graves in a timely manner. Little has been done in this regard so far, and the migration of survivors complicates investigations. International efforts to preserve and collect evidence for future prosecutions and transitional

processes would signal to minority communities that their concerns are taken seriously.

Regarding prosecution, referrals to the International Criminal Court for crimes related to various conflicts have sometimes spurred protests by China, Russia, and even the United States. Moreover, Iraq is not party to the Rome Statute, the treaty that established the court. Yet

The Islamic State commits atrocity crimes for the strategic purpose of controlling, expelling, or exterminating populations.

the Islamic State is a nonstate actor that no one wants to protect. There is also space for domestic prosecutions in Iraq and the Kurdistan Regional Government (KRG), and perhaps for genocide cases in the United States, Germany, and other countries that have generated foreign fighters.

Thus far, the government of Iraq and the international community have failed to prevent crimes perpetrated by IS. Protection of minority communities has not been prioritized despite clearly documented risks over the past ten years. In Ninawa, for example, one can find a long record of increasing attacks against minorities, growing extremism, and an expanding IS presence. Yet neither the KRG, Baghdad, nor the international community formulated a protection strategy in response to these warning signs.

Protecting minorities and civilians is therefore integral to the credibility and efficacy of any counter-IS strategy going forward. Absent this, continued atrocities will create a future Iraq without minority communities. Secretary of State John Kerry's acknowledgement of genocide is significant and necessitates action, includ-

ing preparations for stabilizing areas liberated from IS. In fact, atrocity prevention needs to be a component of any national security conversation. This requires innovation and leadership, not necessarily new resources.

Finally, liberating Mosul will probably force around 600,000 people from their homes, and they will need physical protection. Many women and children currently held by IS are likely to be used as human shields during the liberation effort. There is also significant risk of reprisal killings after operations conclude. Communities seeking to return to their homes will need protection as well, preferably from international forces, though there are ways to incorporate Baghdad and the KRG. Any local forces will require training on proper adherence to international human rights standards.

JAMES F. JEFFREY

THERE is overlap between humanitarian interventions intended to protect at-risk populations and realpolitik interventions. Even purely geopolitical interventions such as the liberation of Kuwait always involve at-risk populations, while humanitarian interventions such as the Libya operation have various geopolitical dimensions.

The West has extraordinary resources, but it frequently becomes mired in debate about interventions because many past examples have not turned out well, such as Beirut in 1983, Somalia in the early 1990s, and Afghanistan and Libya more recently. Once initial operations are over, the United States and its partners are often at risk of losing support and solidarity due to fears of quagmire, mission creep, and casualties. Yet there are examples of successful interventions. Operations in Bosnia and Kosovo met their goals. And in Iraq, a small number of troops along the Green Line prevented hostilities between Kurdish and Iraqi forces, while other positions allowed the United States to empower certain local populations to fight IS precursors.

In general, greater international support increases an intervention's legitimacy and likelihood of success. Monopoly of force is also critical, but population protection efforts have to be integrated with other efforts, and locals need to be empowered.

Having an endgame in mind is crucial, but goals need to be distinct from the effort and process. Whenever the losers in a given conflict are able and willing to respond with violence, they can restart the cycle of bloodshed that prompted the intervention in the first place. In Somalia and Beirut, the United States went in for humanitarian purposes but developed geopolitical endgames that

created new enemies. And in the midst of the 1994 NATO effort in Bosnia, Ambassador Richard Holbrooke was reluctant to prioritize war crime accountability above other considerations, believing that those marked for prosecution would see it as a political challenge and respond with open hostility. War crime accountability is necessary, but it must be separated from and subordinate to the initial establishment of monopoly of force and civilian protection.

In Iraq and Syria, there are several separate conflicts currently targeting civilians. In addition to the Islamic State's atrocities, many civilians face a larger threat from the Syrian regime and its supporters. In Iraq, the civil conflicts exacerbated by the presence of Shiite militias in Sunni areas persist in small but significant remnants, as do conflicts between Kurds and Arabs.

The West has extraordinary resources, but it frequently becomes mired in debate about interventions.

That said, civilians in IS-held territory face the worst human rights abuses and persecution. There are other reasons to target the group, but liberating the millions under its control is a worthy goal for its own sake. Once these areas are liberated, however, IS will still be able to infiltrate, attack, and retake territory, further underlining the need for a monopoly of force. And while U.S. troops are typically seen as an objective balancing force in post-crisis situations, maintaining a long-term U.S. presence absent local forces often generates geopolitical hostility.

Planning for "the day after" is always a challenge, and the White House needs to decide who has the authority and competence for these efforts. The armed forces employ stability doctrine as part of their military efforts, but they have not received clear orders for this in Iraq. Additionally, NGOs have an important role to play in relief efforts.

This summary was prepared by Patrick Schmidt.

SEPTEMBER 21, 2016

How Technology Has Transformed the Terrorist Threat Fifteen Years After 9/11

■ Michael B. Steinbach

PREPARED REMARKS

FIRST OF ALL, I would like to thank Matthew Levitt and the Washington Institute for inviting me to speak to you today. All of us have had our hands full over the last couple years as we have seen the latest wave of international terrorism emanate from Syria and Iraq with the Islamic State of Iraq and al-Sham, or ISIS. We have seen horrific examples across Europe, Africa, Southeast Asia, and here in the United States. It does not matter whether we call it directed or inspired, the cancer growing from large swaths of ungoverned space in the Middle East directly impacts the safety of our communities here at home in the United States. In fact, I cannot do my job to keep our homeland safe without looking for answers in the Middle East. This is why the Institute's focus on improving U.S. Middle East policy is so important.

That being said, today I am not going to talk about ISIS, al-Qaeda, Hezbollah, the Levant, or any other particular group or region because strategically there is another fundamental discussion that needs to take place. As a leader in the national security arena, I want to discuss adaptability. The threats we face today have evolved and continue to do so. The complex nature of the terrorism threat requires a different way of doing business than it did just a few years earlier. It requires organizations and leaders to be agile and adapt to the ever changing threat landscape. And it does not matter where the threat originates from—the Middle East, Africa, Indonesia. I was at Europol last week and leaders used the terms "complex" and "complexity" numerous times in describing the threats our nations face. Complex organisms such as ISIS require us to prioritize adaptability. So if you will, let me explain where we, as leaders, need to focus our attention in our efforts going forward.

The problem a decade ago seems so simple in today's world with today's threat. Let me flesh this statement out a bit. For simplicity, I will describe three fundamental paradigm shifts [that] security organizations like the FBI have had to deal with over the past fifteen years. The first paradigm shift is 9/11, where as an organization we were required to move from a largely reactive agency to a proactive, prevent-oriented agency. At that time, I worked on a bank robbery squad in Chicago. Success for me was to come in after a bank robbery and conduct a thorough investigation—interview witnesses, review CCTV, conduct a neighborhood canvass, etc. The goal was to identify, arrest, and prosecute the bank robber. Such a result would often be glorified in a short news story in the Chicago Tribune where our keen investigative skills were applauded. But how does this investigative model hold up against the East Africa bombings, the USS Cole attack, the 9/11 attacks? Crime committed, investigation conducted, bad guys held accountable (if still alive). To really oversimplify this example, the first paradigm shift now asked the FBI to arrest the bank robber before he robbed the bank.

Complex organisms such as ISIS require us to prioritize adaptability.

So how did we accomplish this prevent-based defense? We all know the tripwires we looked for post 9/11 were travel-based. Take for example the 2002 FBI investigation of the Lackawanna Six from New York. The group traveled overseas to an al-Qaeda camp where they trained and returned, leaving investigators a trail of records along the way. Post 9/11, this was our playbook and we were successful.

But the bad guys evolved and the second paradigm shift occurred a few years later and revolved around the anonymity of the Internet. Travel and the associated tripwires were no longer a prerequisite to conducting an attack. Now groups like al-Qaeda could inspire and radicalize remotely—Anwar al-Awlaki became the most powerful influencer in the history of terrorism, all through his online sermons. The FBI was required to adapt as well to the changing threat, and we did by focusing on forums—the watering holes—where the bad guys amassed. We developed tools to deal with this new form of threat, the inspired lone wolf.

And today—with ISIS leading the way with a dispersed and effective media apparatus—we face a third paradigm shift, which results in individuals inspired by a faceless demon, trained anonymously via a multitude of communication platforms in a dark web no agency can peer into. While the Internet facilitated terrorists' widespread reach across the globe over the last decade, the latest evolution of the threat transcends barriers like never before and again challenges us. What I am referring to is the use of social media where a message or a video can go viral and spread across the world in minutes; where any of more than 2.3 billion active social media users can push propaganda out on a public site and then continue communicating via private encrypted messages. Social media and terrorists' effective exploitation of social media concern me. 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. In other words the bad guys use the same widely available and inexpensive handheld gadget to identify both target and targeteer.

Social media is no longer just a harmless playground for our teenagers and young people; social media platforms connect many parts of our society. But by virtue of their connectivity to social media, individuals within any demographic can be a target. Groups such as ISIS have used the content from online postings to gather personal information, including photos, identities of family members, and home addresses. Today, 78 percent of Americans have at least one social media account, and more than half of the adult population accesses those platforms using a smartphone. The worldwide abundance of smartphones as social media's access point and the volume of social media use are daunting obstacles to securing the safety of our communities.

This same social media activity can also be used to identify potential recruits. Previously, even with the anonymity of the Internet, a foreign terrorist organization had to wait for an individual to come to an online forum seeking information. In today's social media age, terrorists can proactively

troll social media sites for individuals they believe may be susceptible and sympathetic to the message—think about the distinction. These potential recruits may be just looking for a place to fit in. Online recruiters feed them a steady

Partly as a result of this paradigm shift, we truly live in two distinct worlds—a physical world and a digital world.

false narrative, suggesting they join their cause and become part of something bigger; this sense of belonging appeals to individuals who seek a purpose or who crave action. And the radicalization is not just occurring when an individual accesses a site; with social media push notifications and smartphones, it's radicalization literally twenty-four hours a day, seven days a week.

More so than ever before, and partly as a result of this third paradigm shift, we truly live in two distinct worlds—a physical world and a digital world. For years, we in the law enforcement and intelligence community built out the terrorist networks through the physical world, identifying the facilitators, financiers, planners, and operators. Today we must often build out a network starting with an anonymous online moniker—with no clue as to whether the individual is male or female, young or old, in Syria or the United States. In 2015, the FBI had about seventy terrorism disruptions, with a large percentage of those investigations beginning in the digital world.

This is where the challenges of today become particularly evident with two byproducts of social media, of the digital world. Those two byproducts are volume and encryption. They are overwhelming in their span and complex-

ity. And they build an invisible barrier between us and the bad guys. Now, a bad guy has the ability to create numerous identities with a few strokes of the keyboard or swipe of the smartphone. He develops relationships and once an individual confides a willingness to act, the conversation switches to platforms with end-to-end encryption for heightened privacy. The use of encrypted communication then becomes the norm. Very few of our targets are communicating in the open today. These encrypted messages are not only hidden from the public's watchful eye but are also impenetrable by the global law enforcement community. These methods of communication among groups are becoming the norm. For example, in the spring and summer of 2015, we had about a dozen individuals in the United States planning attacks via encrypted channels with members of ISIS.

The challenge we face is to remain agile in terms of technological advances.

The challenge we face is to remain agile, specifically in terms of technological advances. As technology evolves, the bad guys adapt. We, too, need to be willing—and able—to adapt to the ever-changing threat environment. We have a tendency to fight the last war using yesterday's technology. Much of the time technology is outpacing our workforce's capabilities. So what's the answer? Let's start by digging in further on the topics of volume and encryption.

Let's start with the volume issue.

When I started as a case agent, we were taught to ask logical investigative questions—the bad guy's personal information, physical character-

istics, and associations. We'd jot the information down in our notebook and run it through the systems to see if we could glean any known connections. We've seen a scaled progression of the standard baseline collection from physical traits to phone numbers, email addresses, and now usernames, making the "standard" even more complex. To add to that, many people don't have just one phone number or one email account. I'm sure many of us in this room have a home phone number, a cell phone, an office number. We also have a personal email account, work email account. Now stop for a moment and think about the online accounts you have and all the different information you entered to create those usernames and accounts. That's a lot to keep track of personally. But now imagine those individuals who intentionally create one account after another to cover their digital bread crumbs and, ultimately, to hide from us. These digital profiles have become equally critical to our investigations.

The size and scope of these digital profiles is transforming the way we do business. Why is that? We need to track down and evaluate all of the associated digital profiles because they may be the only clues we have. To accomplish this task, we must sort through the large volume of social media connections (the noise) to find the digital profiles (the signal) that are part of our terror network. I cannot emphasize this last point too loudly—the volume of potential contacts can be in the tens of thousands. Think how that compares to the historical volume in identifying physical global networks.

For example, both the November Paris attacks and the December attack in San Bernardino contained multiple subjects with multiple online profiles. During investigations such as these, the online profiles often give insight into the subjects. Sometimes it's obvious, within the profile description or publicly shared content; most times, it's in the digital connections.

In the end, the digital investigation alone can result in an abundance of information. And that's likely an understatement. It could take us weeks to comb through the lines and lines of data and the endless connections enabled by the online world to determine what warrants our attention. This could add up to valuable time spent before we even identify the key connection. The connection, the ties to the subject—it's in the online world. It's just sitting behind a screen.

The second challenge is encryption.

Not only do we face the overwhelming volume of information we've uncovered, the second challenge is the lack of accessible information when the

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 the May 2015 shooting outside of the "Draw the Prophet" event in Garland, Texas, one of the shooters communicated with an overseas terrorist associate using an encrypted communications platform—including more than 100 times on the day of the attack. The investigation uncovered the shooter intentionally used the end-to-end encryption platform to ensure his communications would remain secure. To this day, we still do not know what the discussions were about.

Encrypted communications quickly eliminate the digital trail. These digital dead ends can be deadly for our communities.

What are we doing to set ourselves up for success in the future?

As leaders, we must look at our organizational processes and adapt to the current and emerging threat. Specifically with volume and encryption, we need to look at tools and training for the answers.

It's up to us to arm our teams with the right tools. We will always be behind if we're using yesterday's technology. Resources need to be renewed on a regular basis to ensure we are fighting the war with weapons on par with our opponents. We owe it to our people to invest in tools that will help them do their jobs better and to face the technology overload head on. When I talk about the volume of information being unmanageable at times, using technology to sort or prioritize information could save many man hours. But we need to be smart with technology—it's not just about spending money. How can we leverage technology—cloud-based solutions, cognitive computing, commercial products that can be layered on top of our classified databases? I am talking about strategic solutions. Last year we were faced with a few super users who, from safe havens in Syria, spread venomous ideology throughout the online world on behalf of ISIS. These individuals accumulated thousands of followers. For us to fully tackle not only the subjects but also to analyze their reach and identify potential additional actors, it seemed like an impossible task. At one point there were more than 30,000 associates, and the web of connections kept expanding. We learned that smart data crunching programs can help sort through the noise and allow for human analysts to focus on the true bad guys.

Importantly, we need to ensure new tools are coupled with adequate training. Tools are no good unless people know how to use them. When we

take a look at our workforce and the collective caseload and think about how it's evolved over the years, how do we adapt? How do we position our people to adapt? It's a culture shift. Throughout history it's been done time and time

Smart data-crunching programs can help sort through the noise and allow for human analysts to focus on the true bad guys.

again. The only difference this time is the speed at which we need to learn and adapt. As I said earlier, new technology comes out fast. Folks, we're not using brick phones or pagers anymore. In fact you can assume if you or I are being introduced to new technology, it's likely already been in the marketplace for some time and our kids have thoroughly mastered it.

The law enforcement and intelligence community has vast experience investigating and identifying individuals once we have resolved a biographic identity. The critical task today is to traverse the identity divide as quickly as possible, going from the anonymity of cyberspace to a live body before subjects can go—in the world of terrorism—from flash to bang.

For example, in June 2015 we became aware of an individual known only by an online moniker. This anonymous individual communicated to an overseas terrorist group that planned to conduct an attack in the United States in the coming weeks. But who was it? Male or female? Juvenile or adult? Located in the United States or overseas? Plotting to kill or ready to act? These are questions with answers hidden in an individual's digital footprint. Sometimes the answers are easy to extract, but

at other times, they are nearly impossible to find. In this case, the individual provided subtle clues that assisted us in narrowing down the geographic area. This case started like many of our cases today, beginning with an anonymous digital persona, later leading to a physical human being. There is no way to stop the growing identity divide, and technology trends indicate it will only become easier to erect identity barriers to hide a biographic identity. In this case, we resolved to the real person by utilizing a hybrid team consisting of members who had the traditional investigative skills as well as members who had the digital know-how. Without both of these components working in coordination, we would not have been as successful as we were.

It's all about being adaptive in our processes—pushing our teams to innovate and not be comfortable just because we have always done it that way. In fact, phrases like that and "why fix it if it's not broke" are poisonous declarations if our goal is truly an agile workforce. But what I am describing can be a huge shift for our workforce. Many of us grew up without cellphones and were around long before the Internet. We had to learn

Phrases like "Why fix it if it's not broke" are poisonous declarations if our goal is truly an agile workforce.

how to adjust to the connected lifestyle. We are digital immigrants. We try our best to learn the latest app but it's likely not intuitive. However, much of our younger workforce is just the opposite. We work side-by-side with individuals who have never known life without the Internet, had

a cellphone before they started high school, and navigate the online world almost as comfortably as the physical world. They are digital natives.

Digital immigrants are extremely experienced in traditional investigative practices. For digital immigrants, the street holds the answers—interviews, informants. Digital natives, on the other hand, are our colleagues with so many monitors at their desk that some are turned sideways and who are equally comfortable using Google as a noun, adjective, or verb. But we need both skill sets equally in today's fight against terrorism.

Remember, bad guys are actively looking to put as many barriers between their digital and biographic identities as possible by concealing their IP address, using end-to-end encrypted messaging apps, and registering for social media with spoofed identifiers. A workforce splintered in its approach to navigating between the digital and physical worlds is doomed to fail.

Being adaptive also means looking at how these complex organizations communicate and move. As we have seen in Europe with ISIS external operations, their ability to do both has outpaced Western governments' ability to push actionable intelligence and prevent attacks. In the digital world, it's not sufficient to say information sharing is important. It's now the speed of information sharing that is critical to success. It's the difference between sending a letter through the U.S. Postal Service for delivery a few days later versus sending a message via email for delivery in a matter of seconds. In both cases the message arrives—but days is too long a timeframe if a terrorist has struck and killed in the meantime.

We must resist the urge to accept political theater post-attack where broad general statements are made that information sharing has improved. We need to allow that information sharing in itself is complex and work with partners to develop robust systems that take into account the type of information to be shared (identifiers, biometrics, analysis) and the form of information to be shared (raw data, finished intelligence). We need to have difficult discussions with intelligence agencies, security agencies, law enforcement, and border control agencies. How is the classified information being used rapidly in a usable format at a speed that is faster than a train ride or flight? It's great that CIA is sharing with MI6, but if a terrorist travels from Heathrow to Dulles undetected who cares? These solutions also require adaptive new models that consider deconfliction, access, privacy, storage, and use.

The coming year will present continued challenges as Western allies continue to squeeze ISIS's operating space. While this is a measure of success,

it will bring with it a more dangerous world in 2017 and 2018. Yet the bar remains set very high for us in this line of work: zero terrorist attacks on the homeland. To achieve this standard we need strong leadership. Whether you're in the public sector or private sector fighting, leaders in today's hyper technology-driven world must ignore sayings such as "don't fix it if it ain't broke" and instead lean forward to accepting change as the new norm. The only certainty I can give you is that I cannot predict the global landscape sufficiently to know exactly what the threat will look like. But by instilling a culture of adaptability in our organizations we can meet head on the challenges of 2017 and beyond.

OCTOBER 13, 2016

The Evolution of Terrorism Financing: Disrupting the Islamic State

■ Daniel L. Glaser

RAPPORTEUR'S SUMMARY

THE TREASURY DEPARTMENT faces a unique challenge in countering the finances of the Islamic State of Iraq and the Levant (ISIL). While traditional counterterrorist financing focuses on cutting terrorist financiers off from access to the global financial system and isolating terrorist organizations from their major source of funding, ISIL's ability to finance itself internally presents a qualitatively different challenge that requires a qualitatively different approach.

ISIL's wealth mainly comes from three sources. The first of these is the oil and gas in its territory, the sale of which generated about $500 million in 2015, primarily through internal sales. The second is taxation and extortion. As a territory-holding entity, ISIL levies various taxes and fees on the population under its control, equaling about $360 million in 2015. Third, when ISIL captured Mosul in 2014, it was able to plunder more than $500 million in cash from bank vaults. This, however, was a nonrenewable source of financing. In all, the vast wealth that ISIL has raised from these sources far outweighs external financing and other illicit activities.

Given the significance of territory to ISIL financing, the problem lends itself to a military solution. The Global Coalition to Counter ISIL launched an air campaign in November 2015 named Tidal Wave II, which targets ISIL's ability to extract, refine, and transport oil and gas. This campaign has substantially decreased ISIL's oil profits from its territory.

As ISIL loses access to territory, and thereby oil, it is increasing taxes on the local population. Yet its ability to generate revenue through taxation

is also limited because the funds flowing into its territory are limited. For some time, the Treasury Department has been working with the Iraqi government to reduce liquidity in ISIL-held areas. About a year ago, Baghdad stopped sending government salaries into these areas, instead holding them in escrow. Previously, it had been sending about $2 billion per year into ISIL territory. Even with conservative estimates of a 10 percent tax rate, that represented significant income for ISIL. The coalition has also conducted airstrikes on ISIL bulk-cash sites, destroying untold millions of dollars.

These measures are having an impact—the group has been experiencing financial distress. In late 2015, ISIL leaders in Raqqa, Syria, reduced the monthly salaries of all fighters in the province by 50 percent, and they certainly were not the first to be affected by the group's belt-tightening efforts. Internal corruption is also on the rise, spurring leaders to launch anticorruption campaigns. Arbitrary fines have increased as well, and taxation has become heavier. All of these developments are clear signs of distress as the group scrambles to make up the money it has lost.

Nevertheless, ISIL's coffers will never be completely emptied, so Treasury is continuing its efforts to prevent the group from moving and using its money. This effort starts with the Iraqis. Treasury has been working very closely with the Iraqi government, which is taking the issue quite seriously. Approximately ninety Iraqi bank branches were operating in ISIL territory when the group first took control, but Treasury has worked with the Iraqis to cut these branches completely off from their headquarters, making it more difficult for ISIL to access the financial system.

Yet the main concern in Iraq is ISIL's exploitation of exchange houses, of which there are around 1,900—far too many to effectively regulate. In the long term, Iraq needs to shrink this sector to bring the number of exchange houses down to a level that can be reasonably overseen. The challenge in the short term is what to do about exchange houses within ISIL territory. The Central Bank of Iraq has released a public list of more than a hundred such institutions, and Treasury has established active information-sharing arrangements with Iraqi officials to alert them of any suspicious exchange houses. Entities can be added to or removed from the list as territory is liberated. Financial institutions around the world need to consult this list to avoid doing business with any of the blacklisted exchange houses. Thus far, the Central Bank has blocked such houses from accessing millions of dollars, a clear sign of Iraq's commitment to the issue.

The Central Bank has also taken steps to improve the regulation of Iraq's financial system, adopting money-laundering and counterterrorist financing laws and issuing regulations to implement them. In addition to taking extraordinary steps to ensure that banks in Baghdad are appropriately regulated, it has sent teams out to places such as Kirkuk in the Kurdish region to make sure there is a uniform anti–money laundering system in place. Going forward, the Iraqi government must make this more than just a Central Bank effort; law enforcement, the Finance Ministry, the Justice Ministry, and the security services all need to be involved. To encourage this all-of-government approach, the Treasury Department helped create the U.S.-Iraq Committee to Counter Terrorist Financing, which includes all of these stakeholders.

The main concern in Iraq is ISIL's exploitation of exchange houses, of which there are far too many to effectively regulate.

Although this work starts in Iraq, it certainly does not end there. Syria is a completely different issue set. Yet because the Syrian financial sector has been cut off from the international system for some time, it is a less attractive jurisdiction for ISIL to move funds. Informal financial networks connect Syria to its traditional regional trading partners, and Treasury engages with them about associated concerns. The Assad regime has also benefited ISIL through gas deals based on an exchange of services.

As Treasury continues to work closely with regional partners to ensure that ISIL does not

gain access to local or global financial systems, it is crucial to note that military success will only increase the relevance of this work. As ISIL becomes less statelike and more of a dispersed global organization, it may become more reliant on the international financial system to raise and move money. The question then becomes: does it turn to external financing? There is no level of external financing that can make up for the billion dollars or more that ISIL can make while controlling territory like it does in Syria in Iraq. Even so, the move to a so-called "post-Caliphate" existence obliges the coalition to make an even greater effort to ensure that ISIL cannot rely on more traditional methods of terrorist financing such as foreign donors and exploitation of charities.

Outside Syria and Iraq, ISIL's various branches do not have the ability to generate their own resources the way ISIL does in its core territory. ISIL in Libya is not making money from oil there; it is focused on destroying the country's oil infrastructure rather than financially benefiting from it. There is also less wealth within the branches themselves—for example, while Mosul's bank vaults held half a billion dollars in cash, ISIL forces in Sirte, Libya, have found only around $4 million. This is a qualitatively different problem. ISIL branches are able to self-finance to a degree through crime and extortion of the local population, and they still receive money from the ISIL core.

Other terrorist organizations operating in Iraq and Syria require close attention as well. Al-Nusra Front—essentially al-Qaeda in Syria—is a dangerous organization that poses a threat to the United States. It can extract a certain amount of wealth from the territory it controls, but not to the same extent as ISIL. This gets to Treasury's classic toolbox: working with partners to make sure terrorist organizations do not have access to the financial system. A lot of progress has been made toward this end in countries such as Qatar and Kuwait, but individual financiers continue to operate in the Gulf region, and this issue needs to be addressed urgently. Qatar's recent efforts to undertake criminal prosecutions of terrorist financiers are a real sign of political will to deal with this problem.

Other groups of concern include Hezbollah, which has Iran as its chief financier. Treasury strives to isolate Hezbollah from the global financial system, and it applauds Lebanese banks for their good work since the passage of the Hezbollah International Financing Prevention Act of 2015 (HIFPA). The group's access to the Lebanese financial system has been challenged in a way many never thought possible. On this matter, it is critical to differ-

entiate between Lebanon and Hezbollah. HIFPA and the ensuing American enforcement measures are not an attack on Lebanon, but rather a move to counter Hezbollah financing. Yet Hezbollah receives the majority of its wealth from Iran, a revenue stream that is difficult to disrupt. In its dealings with Tehran, the Financial Action Task Force will likely continue to reject exceptions to its terror-financing laws, as it has in the past.

This summary was prepared by Maxine Rich.

MARCH 31, 2017

Stopping Extremists from Becoming Terrorists: A Strategy for the Trump Administration

■ Rand Beers, Samantha Ravich, and Matthew Levitt

RAPPORTEUR'S SUMMARY

RAND BEERS

I FIRST BEGAN thinking about the basic concepts behind countering violent extremism (CVE) fifty years ago as a platoon and company commander during the Vietnam War. At the time, we realized that the goal was not just to hold territory, but also to hold the people in support of the American effort. I came away with the notion that indiscriminate violence and coercion focused on an entire class of people, rather than the enemy, only creates or confirms opposition to American aims.

When I returned to government in 2009 at the Department of Homeland Security, I discovered that the previous administration had been thinking about how best to deal with extremism domestically. As the Obama administration began to carry on the Bush administration's efforts, it drew on an FBI study published several years prior that had found patterns of behavior common to perpetrators of terrorist attacks in the United States. These precursors to violence were observable, and the FBI identified four groups most likely to notice such behavioral changes: peers, family members, institutional figures (i.e., teachers or religious leaders), and other community members.

The question then arose: if people are observing this conduct, why aren't they reporting it to authorities? There are three prevailing answers to this question: (1) they do not realize the significance of the behavior, (2) they are in denial as to what it may mean about their loved one, or (3) they are reluctant to report it because the only avenue for doing so is law enforcement.

As the United States seeks answers to homegrown violent extremism, it must consider developing or bolstering non-law enforcement options for potentially problematic individuals. Although law enforcement cannot be excluded from the solution, Americans need a way to bring troubling behavior to the attention of others who may be able to help first, such as mental health professionals and social workers. Intervention programs should be combined with public outreach to inform people about radicalization patterns and the options available for reporting them. In this whole-of-community approach, disconcerting behavior can be confronted before it progresses into criminality.

In this whole-of-community approach, disconcerting behavior can be confronted before it progresses into criminality.

The federal government has a role in this approach, as seen in the CVE Grant Program established by Congress last year and the related initiative taken by U.S. Attorneys' offices around the country. Nevertheless, even federally supported CVE efforts must be grounded locally in order to build the necessary trust for good working relationships.

SAMANTHA RAVICH

IN THE WAKE of the 9/11 attacks, the United States was guided by the fundamental belief that it was at war with "a transnational terrorist movement fueled by a radical ideology of hatred, oppression, and murder." This mindset was articulated in the 2006 National Strategy for Combating Terrorism, which notes that the "war on terror" is a different kind of war. It is

a battle of arms and a battle of ideas, requiring America to fight its terrorist enemies on the battlefield while also providing alternatives to the oppressive terrorist narrative. The paradigm for combating terrorism includes all aspects of U.S. national power and influence: military, diplomatic, financial, and so forth.

Accordingly, the Bush administration's second term was marked by an interagency push to counter the terrorist threat. These early efforts focused on what the federal government could do for the country, and not enough on what local communities could do to empower themselves. As the Washington Institute study group report points out, what is needed is a preventive CVE concept that leverages not just a whole-of-government approach, but a bottom-up, whole-of-society approach.

In this regard, it would be a mistake to ignore the transnational element of CVE. After 9/11, the United States worked with its foreign partners to counter the growth of terrorism and extremism in their countries. Ironically, however, it was lax in developing such programs at home. Today, there is much Washington can learn from the successful initiatives established by its foreign partners.

Increasingly, analysts view terrorism as a process. Once it gains a foothold, it becomes self-perpetuating...

Yet the Institute's broad recommendations are intended to augment, not supplant, law enforcement. Community programs can help law enforcement get ahead of the curve on violent extremism, forming a broad base of support for public safety. Public-health models may also be applicable as the government brings these programs to a larger swath of the population.

According to a 2007 Congressional Research Service report, "Increasingly, analysts view terrorism as a process. Once it gains a foothold, it becomes self-perpetuating...Thus a process of terrorism that could potentially have been dislodged at an earlier stage with relative ease often becomes increasingly robust if left unchecked, particularly with respect to indoctrination of the young." Preventing and countering violent extremism is a key part of that early dislodging effort.

MATTHEW LEVITT

AS U.S. LAW ENFORCEMENT attempts to disrupt extremist threats to the homeland, it faces an overwhelming number of potential terrorism cases, including more than 900 investigations related to the Islamic State alone. Unsurprisingly, then, law enforcement authorities are the leading advocates for establishing programs that move the needle earlier in the radicalization process. America needs more resources that can intervene with at-risk individuals before they cross the Rubicon into criminality.

Community members are best positioned to recognize disconcerting behaviors and refer individuals to professionals capable of intervening. Those professionals in turn have a duty to warn law enforcement if they detect an imminent threat. Indeed, law enforcement is desperate for civil society partners. There have been at least four tragic cases in which the FBI investigated suspicious individuals, found no legal basis to continue, and closed the investigation, only to have the suspects later carry out terrorist attacks: the 2013 Boston Marathon bombing, the 2015 shooting in Garland, Texas, the 2016 Orlando nightclub attack, and the bombings in New Jersey and New York that same year. In each case, the bureau's hands were tied—authorities had no partners to whom they could refer these cases, and the results were disastrous. The government needs to build connective tissue between service-oriented CVE and law enforcement in a way that is not police-driven.

The first level of the whole-of-society model recommended in the Institute's report involves building resilience over a broad area. The second level focuses on individuals, neighborhoods, schools, and ethnic communities that are at higher risk of radicalization because of their exposure to extremist ideologies, contacts with radical networks, or similar factors. The third level comprises intervention options when radicalization does occur. Preventive CVE efforts should be based on geography rather than predetermined ide-

ologies, since they will differ from one community to the next. These efforts should be applied to the full spectrum of extremist ideologies: far-right, far-left, Islamist, and so forth.

It is also critical to cover the full life cycle from radicalization to rehabilitation and reintegration—a fact that Washington's European partners are quickly realizing. While the United States does not face quite the same threat as Europe (i.e., thousands of fighters returning from the Syrian battlefield), it does not have the luxury of ignoring the problem. The first American convicted on Islamic State-related charges is set to be released within the next month, and she will be among hundreds released in the next two to ten years. There are no CVE programs in U.S. prisons, nor any post-release initiatives that focus on CVE issues. Although some deride the "back end" of CVE as soft, such efforts constitute smart policy and fall squarely within the broader effort to safeguard America's national security.

In the study group meetings that produced the Institute's bipartisan report, experts expressed legitimate criticisms of CVE as it stands today. Participants also grappled with the term CVE, an acronym so toxic that it is disregarded in most every local program across the country. The answer to such criticism is not to change terms, but rather to put systems in place that address the legitimate concerns associated with these terms—while recognizing that for some people, CVE will be untenable no matter its name.

One such concern is the securitization of CVE policy. This is not surprising, given that law enforcement led the push for CVE after the Boston Marathon bombing. While law enforcement cannot be removed from the equation, it should not be the face of local programs, and authorities should adjust their approach accordingly. Local communities, law enforcement, and the federal government must work together to make all Americans safer.

This summary was prepared by Maxine Rich.

JUNE 16, 2017

Islamist Terrorism in the West

■ Dick Schoof, Muhammad Fraser-Rahim, Farah Pandith, and Matthew Levitt

RAPPORTEUR'S SUMMARY

DICK SCHOOF*

WE HAVE seen brutal attacks in Brussels, Paris, Berlin, London, Stockholm, Manchester, and again—two weeks ago—in London. The United States has faced attacks in New York City, Boston, San Bernardino, and Florida in recent years.

What we see is that the modus operandi of the attacks differ, the number of casualties differ, the targets differ, and the terrorists differ. Some of the attacks are directed and organized from outside of our countries, others are committed by homegrown actors, youngsters from our own neighborhoods, inspired by the social media and Internet.

Yet, the attacks have one crucial factor in common: fear. The attackers want to create fear. They want to intimidate ordinary people in order to prevent people in Florida from going to a nightclub, to prevent people in Manchester from going to a concert, to prevent people in New York and Amsterdam from taking a subway or bus to work—in short, to prevent people from living their lives.

A Dutch researcher used the word "theatre" as a metaphor to describe terrorism. "A theatre of fear," she called it. Terrorists want the public's, the audience's, attention. Regardless of time and place, creating fear is the main driver of the play. And I think she is right. The plot and the drivers remain the same. But the players differ.

To effectively intervene means having to know the communities they grew up in. It means we have to know the local organizations, and it means

* Edited transcript

we have to know the websites and social media that are being used to influence youngsters. It also means understanding the underpinning ideology that is a perversion and sectarian version of Islam. In short, we have to work together; at the local level, at the national level, and of course, across the border.

NCTV

These days, a question that is often posed to me as the National Coordinator for Security and Counterterrorism is: Why has the Netherlands still not been hit by an attack? Are your intelligence and your police services so effective? Are your local community programs so successful? The answer is: the terrorist threat facing the Netherlands resembles the threat facing the rest of Western Europe. The chance of an attack in

To say we have the most effective instruments, the smartest people, or the best intelligence would be to close a pact with the devil.

the Netherlands is real, as real as in any other country in Western Europe. That is why we have set our threat level at "substantial." To say we have the most effective instruments, the smartest people, or the best intelligence would be to close a pact with the devil. I would like to emphasize, a jihadist attack in the Netherlands, such as happened in the countries that surround us, is very much conceivable.

Stopping terrorists and countering violent extremism is a key priority for the Netherlands. We take a comprehensive approach, which includes prevention as well as repression. This means reaching out to local partners and con-

necting with local communities. It also includes legal instruments, such as revoking a potential terrorist's passport or even his nationality. But before going into more detail about our approach, let me share some facts and figures about the current threat in the Netherlands and Europe.

Current Threat Level

We are faced with a complex threat picture in Europe. It is more complex and diffuse than a few years ago. More than ever before we have to deal with different kinds of terrorists using several methods of attack and communication. Some are well prepared, some use a simple modus operandi. And they are aiming at a large variety of targets.

We assess that the threat posed by ISIS is a key part of the threat to the West, be it through planned attacks or inspired violence. Also, al-Qaeda retains both capability and intent to commit terrorist attacks in the West and against Western targets abroad.

Domestically, partly in reaction to the jihadist terrorist threat, we see an increase in right-wing extremism, and partly in response to that, again, in left-wing extremism. As I mentioned before, the threat level for the Netherlands remains "substantial," meaning that we consider the chance of an attack to be real, but that there are no specific indications that an attack is being prepared.

The attacks in Brussels, Paris, Berlin, Manchester, and most recently London once again show us that the work of terrorists does not stop at national borders. Terrorists ignore borders. They travel from one country to the other, often by plane, bus or train, or by car. Or they are influenced by jihadi networks and individual fighters residing in other countries or regions.

To give you a number: in Europe we're talking about an estimate of four thousand foreign terrorist fighters in a population of 750 million people. But we also see "homegrown" terrorists, those who did not travel to ISIS territory but stayed and plan or carry out terrorist attacks. Another development is one of the biggest paradoxes facing us: while ISIS is losing territory and important leaders, this does not diminish the threat of attacks against the West, also in the longer term. Because of the setbacks on the battlefield, its level of fanaticism is increasing. Now that ISIS is losing ground, there is a significant chance that more jihadists will return home or move to other conflict areas. The numbers will differ for each member state. But for the Netherlands, a few dozen seems like a realistic scenario. They won't return all at once, but gradually over an extended period.

The threat is also constantly evolving, getting ever more complex, because ISIS is renewing itself and modernizing continuously. Its fighters are now using drones with explosives in Syria and Iraq. And we also see ISIS getting more professional online. Initially, jihadists were using social media like Facebook, YouTube, and Twitter to recruit for their jihadist goals. With the help of these same social media platforms, we are now able to greatly reduce the spread of jihadist propaganda on the Internet. In response, terrorist recruiters move to the darker spaces on the Web, for example, communicating with potential recruits—young and old—by means of encrypted Telegram and WhatsApp. This makes it harder for us to detect and easier for vulnerable adults and children to fall prey.

The Dutch Approach

In the face of such challenges, how do we, in the Netherlands, counter terrorism and extremism? Based on our experience and our threat assessments over the years, we decided on a number of strategic principles, which together form the main pillars of our National Counter Terrorism Strategy.

- Our approach is threat-based and comprehensive.
- Our approach recognizes that the international and domestic spheres are interwoven.
- And it is aimed at both networks and individuals.

Let me elaborate on the principle of comprehensiveness. By comprehensive we mean we focus on preventive and repressive measures. Let me start with prevention, or countering violent extremism. A key point of departure is that no one is born a terrorist. People, youngsters, become terrorists under the influence of others, be it through the Internet or in their own neighborhoods.

Early identification and intervention are key to preventing and combating radicalization. In order to do so, local and national authorities and all other organizations involved need to work closely together. Civil society organizations and communities are important partners. I read in a recent Policy Note by The Washington Institute that the researchers agreed with us—that in order to defeat ideologically inspired violent extremism, we must involve local communities.

In the case of the Netherlands, when one of the organizations or local youth workers picks up signs of potential radicalization, the person in question is discussed in a so-called "multidisciplinary case management team." In these teams the police, members of local government, and the Public Pros-

ecution Service (OM) share information on persons of concern, both those in the Netherlands and those who joined terrorist organizations such as ISIS abroad. Depending on the characteristics of the case, members of the Child Care

Early identification and intervention are key to preventing and combating radicalization.

and Protection Board, the Dutch Association of Mental Health, or the Rehabilitation Services may join in this case management team.

In this setting, tailor-made interventions are weighed and imposed on an individual level. They can for example decide to give the family extra support, and in the case of minors they can initiate child protection measures. Depending on the case, this can result in a minor being taken away from his/her family and placed into the care of the local authority. The team can also initiate the process of having someone's passport revoked, or of taking preventive measures such as a contact ban or an area ban.

Regarding repression, I just mentioned that no one is born as a terrorist, but when someone becomes one, we will act. Over the past few years we have successfully implemented a set of measures to effectively combat terrorism. Recently, three laws entered into force that expand the Dutch government's powers to combat terrorism.

For example, when in the interest of national security it is possible to revoke someone's Dutch citizenship in case of dual nationality. Another measure is to impose a periodic duty to report or an exclusion/restraining order for certain high-risk locations, e.g. international airports. This can be enforced by electronic monitoring (an ankle brace).

And regarding returning foreign fighters, we have a set of measures we can take. Those who return are immediately arrested on arrival. They are then questioned and, where possible, prosecuted on the basis of a criminal investigation.

At the same time, we must make an assessment of the threat that is posed by each returnee:

- What is the reason why someone returned?
- Will he or she continue fighting the West from within?
- Is he or she likely to plan an attack?

Based on these questions and others it is decided which interventions are best suited to minimize the potential threat. For example, some measures that can function as an alternative to pretrial detention or incarceration are a reporting duty, or a restraining/exclusion order. When we cannot prosecute someone but we think they could still pose a threat, the authorities will keep an eye on the person in question.

Communication

Let me make one more point: the importance of communication. We believe that open and effective communication to the public about the current threat and new developments is extremely important. We believe that by sharing our threat analysis four times a year, we make the public more aware and more able to create the right mindset about the threat. We think that they become more capable of dealing with the news and the sometimes horrifying pictures we see on the Internet.

We are aware, of course, that this open way of communication might raise some questions. I recently gave a lecture at the Free University in Amsterdam and one of the students, a twenty-year-old girl, asked me why my organization had warned about a "sign" relating to terrorism regarding a popular dance festival in Amsterdam. She told me that until she heard about this "sign," she had been relaxed and was ready to have a great day with her friends, but when she heard about our warning, she felt concerned. Would she still able to enjoy the festival or should she stay at home for security reasons?

My answer to her question about why we gave the warning was: as the National Coordinator on Security and Counterterrorism, I give an honest assessment and want to be as open as possible about this. Not to create fear, but to be realistic and create a mindset that will help people when something does happen. Our main message is as follows:

- We cannot guarantee that an attack will not happen, but we will say that we do everything we can to prevent it.
- We do not want people to be paranoid, but we do not want people to be naive either.
- We do not want to create fear, but we do want people to be alert.

Conclusion

I started by talking about the attacks both of our continents have had to endure. We share a number of the same problems. Youngsters from Washington DC and children from Dutch neighborhoods might come into contact with radical beliefs; they might be inspired or influenced by the Internet.

As the recent Washington Institute Policy Note indicates, we need to "get ahead of the curve" in countering terrorism and extremism. And let me add: let's work together, let's exchange best practices from our own experiences, and let us be alert, not alarmed.

MUHAMMAD FRASER-RAHIM

EXTREMISTS are adapting and learning more effectively than ever before. Indeed, counterterrorism analysts have noted the evolution from large-scale spectacular attacks to low-tech, high-impact strikes. Yet while countering violent extremism is a mighty challenge, officials and analysts must be very careful not to confuse such extremism with Muslim beliefs.

For definitional purposes, Islam is a worldview, a value system, and a belief system practiced by some 1.5 billion Muslims across the globe. Islamism, by comparison, is a political ideology that supports a draconian interpretation of Islam that is narrow, rigid, strict, and mostly legalistic. Islamism has modern manifestations throughout the world. Some Islamist groups serve as gateways to more violent organizations, including terrorist organizations. Such groups can—if left unchecked—lead people down the path to extremism to groups like al-Qaeda, al-Shabab, Boko Haram, and the Islamic State. Islamists envision a mythical, theocratic pan-Islamic state that, frankly, never existed and exploit that idea to mobilize people to violence. Islamist ideology, combined with Salafi theology, effectively creates the modern manifestation of Salafi-jihadism.

So what needs to be done? Violent extremist ideology must be isolated from mainstream Islam. Who can do that? In the view of many, challeng-

ing and changing the radical narrative cannot be accomplished by secular individuals alone. The most effective voices to counter Salafi extremism are those of devout, practicing Muslims who see this issue as a cancer within their faith. Here in the West, individuals and institutions must challenge those texts and ideas that foster repugnant, misogynistic, or violent ideas.

The most effective voices to counter Salafi extremism are those of devout Muslims who see this issue as a cancer within their faith.

These may be legally protected ideas within Western democracies, but people must nevertheless fight the ideology and taboos just as they would fight homophobia and racism, or other destructive "isms."

FARAH PANDITH

ONE MUST be frank in asking why, sixteen years after the 9/11 attacks, the same challenges of extremism and terrorism have recurred over and over again. Indeed, the issue is hardly limited to the Islamic State—it is far greater than that.

Further, what counterterrorism experts learned a decade ago, when they first began examining the ideology of extremist groups, still applies today. Local solutions are the answer, credible and valid influencers can make a difference to their peers, and government has a very limited role to play. Returning to these basics is necessary to achieve progress in countering extremist ideology.

In applying these basic principles, officials must cultivate networks of like-minded thinkers who

are schooled in the latest technologies and can saturate communication channels with alternative ideas to counter those peddling in extremism. Relatedly, government money was insufficient a decade ago to help grassroots NGOs on the frontlines, and it surely remains insufficient now.

Today, one billion young Muslims throughout the world are younger than thirty. (The roughly 1.6 billion Muslims worldwide constitute about one-fourth of humanity.) That is the pool from which groups like the Islamic State recruit. By 2030, the world's Muslim population will have grown to 2 billion, meaning that a failure to comprehensively address the root causes of Islamist extremism will require the same soul-searching in a decade in which society is engaged now.

Returning to the basics, and employing lessons learned over the past decade, will indeed require funding so that a plan can be executed at an appropriate scale. Small pilot programs around the world will not be enough to compete with IS and similar groups. The United States, one could persuasively argue, has not yet even tried to go "all in" with such an approach. With determination, a strategy can succeed if it is both kinetic and nonkinetic, brought to a greater scale, and fundamentally serious.

MATTHEW LEVITT

IN LOOKING ahead to the defeat of the Islamic State and the so-called caliphate in Syria and Iraq, analysts and officials must also take a step back. Even as the jihadist group loses territory and suffers battlefield defeats, the threat it poses in the region and around the world remains acute.

The first related serious problem involves returning terrorist fighters, especially in Europe, where hundreds of the several thousand foreign fighters have already come back. Even with the best intelligence, the use of very high-quality false documents to reenter Europe means that authorities will be unable to identify all returnees. Indeed, Britain has already reported people attempting to return with such sophisticated false documents.

In the United States, the returning foreign terrorist fighter threat is nowhere near the scale of that in Europe—America has only about three hundred fighters who either traveled abroad to Syria, Iraq, or Libya or attempted to do so—but over the next five to ten years, the release of hundreds of convicted terrorists from U.S. prisons will change the situation. The United States does not have countering violent extremism programs as such within its prisons, nor does it have CVE programs built into its probationary systems, aimed at helping people reintegrate into society. This is why the

United States, too, could face a threat on a scale similar to that in Europe. Notably, the first woman convicted on charges related to the Islamic State is expected to be released very soon.

Getting ahead of the radicalization curve requires localizing efforts to the greatest extent possible. Moreover, the most effective figures for countering the future lure of terrorism will not be analysts or officers; they will be clinical social workers, psychologists, and teachers. These frontline professionals, through their early involvement with at-risk individuals, can help prevent radicalization before it takes root. Such a local strategy can stop the mobilization of many other extremist ideologies as well. All in all, any approach to radicalization must have a whole-of-society orientation, while complementing existing counterterrorism efforts by government officials.

The most daunting obstacle to success is inadequate funding for local, community-led CVE initiatives. The federal government cannot and should not be the only funding source for such endeavors. Civil society and private companies must also bear some of this financial responsibility, because the threat of violent extremism affects everyone, justifying the whole-of-society—not only a whole-of-government—approach. Generally, efforts should move from the bottom up, not the top down.

Meanwhile, law enforcement and intelligence agencies are clamoring for local networks with which they can partner to address cases of radicalization that fall below the legal threshold for prosecution. Time and again, it turns out that people who end up carrying out attacks had previously crossed the radar of law enforcement. In many of these cases, the suspects were investigated, yet officers ultimately determined their behavior was disturbing but in no way illegal.

In a democratic society, radical thought should not be criminalized but related ideas must be challenged. And when law enforcement officials encounter individuals espousing such dangerous but protected ideas, they must have in place local networks of social workers, psychologists, and others as ready partners. Then, when a future Orlando shooter comes along showing disturbing but not illegal behaviors, the FBI or local law enforcement will have in mind someone or some group to which it can hand off the case.

This summary was prepared by Nicolette San Clemente.

JUNE 23, 2017

Preparing to Counter ISIS 2.0: European CT Efforts Since Charlie Hebdo

■ Gilles de Kerchove

PREPARED REMARKS

DAESH (aka the Islamic State) is being pushed out of vast swathes of the territory it once controlled and, despite propaganda proclaiming otherwise, the group's military defeat in Iraq and Syria is inevitable. But defeat in traditional military terms will not spell the end of the threat we face on both sides of the Atlantic.

Our enemies are adapting to their new reality and, as the physical caliphate collapses, the virtual caliphate is rising from the flames. ISIS 2.0 will not be beaten by military might alone. The European Union and its member states are working hard to tackle this increasingly hidden, often crude, and unpredictable threat.

In January 2015, the Charlie Hebdo attacks in Paris marked a steep change in European counterterrorism cooperation. Just one month after the attack, European heads of state and government met in Brussels and committed to an ambitious blueprint for enhanced cooperation across three broad policy areas: (1) ensuring the security of citizens; (2) preventing radicalization and safeguarding values; and (3) cooperating with our international partners. Impressive progress has been made by the EU and its member states across all three portfolios.

Further still, recognizing the political importance of the issue, the president of the European Commission has appointed a Commissioner for the Security Union, Sir Julian King, in order to bring greater political focus to the commission's efforts.

Our enemies should be under no doubt that our collective capability and our collective resolve to defeat them and their heinous ideology are infi-

nitely stronger than theirs. Last night (June 22), the heads of state and government of the EU met again in Brussels and committed to yet further cooperation and even greater ambition in this regard.

Ensuring the Security of Citizens

We have seen an unprecedented leap forward in information exchange, interoperability, and in police and intelligence cooperation and capability. This has taken place both through EU agencies such as Europol and its new European Counter Terrorism Centre (ECTC) and through structures outside of the EU such as the Counter Terrorism Group (CTG).

We have seen an unprecedented leap forward in information exchange, interoperability, and in police and intelligence cooperation and capability.

The creation of new capabilities through legislation such as the Passenger Name Record (PNR) directive is making powerful new tools available across the Union. PNR, for example, allows member states to process data provided by airlines in order to identify high-risk travelers. PNR is no silver bullet, but it can disrupt our adversaries from traveling freely across Europe by helping to identify both known and unknown terrorist fighters traveling to or returning from conflict zones.

Other tools such as the Schengen Information System II (SIS II) have been enhanced and hold the details of thousands of foreign terrorist fighters. This provides further opportunities to identify, disrupt, or monitor terrorists moving

throughout the EU. It allows for richer intelligence pictures to be generated and a framework for efficient cooperation at the border. For example, one case saw a foreign terrorist fighter trying to return to the Netherlands through Turkey and Germany. The individual was identified through SIS II, and Dutch authorities were able to stop him immediately for questioning upon arrival at Schiphol Airport.

The legislative response to the threat has been measured and effective. Laws have been tightened across the EU to criminalize travel for terrorist purposes, to tackle terrorist finance, and to make it far more difficult for terrorists to acquire firearms and explosive precursors and detonators.

Borders have been made more secure, and mandatory checks—at the external border—of all persons, including EU citizens, have been introduced, subject to closely monitored transition periods.

These collective efforts, among numerous others, have clearly had a positive effect on the security of our citizens. The trend toward cruder methods of attack remains a challenge, but it does indicate that firearms and explosives have indeed become harder to access. The change in the numbers of Europeans traveling to the conflict zone can also, in part, be attributed to the steps the EU has taken. The numbers are stark: Those Europeans traveling to join Daesh reached almost 4,800 by the end of 2015. In 2016, fewer than 100 EU residents were able to reach Syria and Iraq, and little more than a few dozen have been successful in 2017.

Preventing Radicalization and Safeguarding Values

The EU has been leading efforts in the virtual space since July 2015 through the creation of Europol's Internet Referral Unit (EU IRU). This unique multilingual capability has been working to reduce terrorist and extremist online propaganda on global platforms and to provide operational support to high-profile investigations. During its first dedicated two-day operation, the team analyzed and actioned over 1,800 pieces of Daesh- and al-Qaeda-affiliated content in nine different languages hosted by thirty-five different platforms.

The creation of the Internet Forum, which sees EU interior ministers and Internet companies working together to tackle the online threat, presents a significant opportunity to tackle ISIS 2.0. We have built strong foundations and ambition is high, but a step change is indeed necessary to meet the scale of the challenge. The Internet companies, led by Facebook, are already working

on technical innovations to achieve this, including methods of detecting terrorist content automatically. The path to achieving this will not be easy, but it must be achieved if we are to protect our citizens and, crucially, our children.

The Radicalisation Awareness Network (RAN) connects over 2,400 frontline practitioners across the EU working to counter radicalization across all sectors. These deep subject matter experts (including on the education, health, and prison sectors) bring their experience and knowledge together to learn from each other and to develop actionable recommendations for policymakers. The network has been strengthened with €25 million additional funding over four years and established as a Centre of Excellence for the EU.

Work to support member states in tackling prison radicalization is under way with funding made available for rehabilitation and deradicalization programs, risk-assessment tools, and training.

With an eye to the future, work to improve education and youth-employment prospects is also an essential pillar of our work in this area. Programs such as Erasmus+ have been strengthened to foster inclusion and promotion of fundamental values. Significant funding has been made available for new policies and projects and for grassroots initiatives.

International Cooperation

Political and security cooperation with our partners in the region is at an all-time high and is more important than ever. We have deployed counterterrorism experts to EU delegations in high-priority partner countries and are developing comprehensive CT-assistance programs with countries such as Tunisia, Lebanon, and Jordan. Our EU agencies, including Eurojust, Europol, Frontex, and the European Police College (CEPOL), have been reinforced in order to support these programs.

And of course, it goes without saying that the United States is a crucial partner in all of our activity. We have concluded a PNR agreement with the United States and maintain highly effective access to the Terrorist Finance Tracking Program (TFTP) through requests made by Europol. The TFTP has proven a very valuable tool in the investigations into the recent terrorist attacks in Europe. There has been a considerable rise in requests, which resulted in a high number of intelligence leads—more than 35,000 since the EU-U.S. TFTP Agreement in 2010 (more than 80 percent of those leads were provided in 2015 and 2016 in reaction to the terrorist attacks).

Almost half of these relate to foreign fighters. More broadly, the level of information exchange through Europol and Eurojust and, of course, bilaterally with the member states is essential to our tackling the threat both in the United States and Europe and around the world.

Conclusion

While some attacks have penetrated our collective defenses with tragic consequences, we can be certain that our collective actions have contributed to numerous plots being disrupted, and vulnerable citizens have been prevented from being radicalized or traveling for jihad in the battlefields of Syria or Iraq.

The Radicalisation Awareness Network connects over 2,400 frontline practitioners across the EU working to counter radicalization across all sectors.

Crucially, if we are to face down the threat of ISIS 2.0, we will need to scale up our efforts to tackle the virtual caliphate. The EU is well positioned, but we will need our international partners and, most important, the online industry to step up to the mark. As the British prime minister said just this month, enough is indeed enough. The Internet giants, who are such a central part of our societies, must bring their full capabilities to the table and help us safeguard our children and vulnerable citizens from false religious narratives and from violent extremism.

We have achieved a significant amount in a very short period of time, but there remains much to do. We must act strategically and we

must act together to share the burden. Our priorities for tackling ISIS 2.0 must now include defeating its agents in the virtual caliphate and ensuring the safety of our citizens in the face of the increasingly unpredictable and hidden acts of terrorism that the virtual caliphate inspires. We must also develop new methods of analyzing big data and using artificial intelligence to assist us. Finally, we would be foolish to simply focus on the short to medium term. True success against ISIS 2.0 will require the defeat of its delusional ideology and the victory of our shared values. The European Union will remain in support of our member states and our international partners for the long haul. Together, we have seen graver challenges than this before and triumphed in the face of them.

JULY 31, 2017

Lone Wolf: Passing Fad or Terror Threat of the Future?

■ Boaz Ganor, Bruce Hoffman, Marlene Mazel, and Matthew Levitt

RAPPORTEUR'S SUMMARY

BOAZ GANOR

A LONE WOLF is an individual who has become radicalized and, as a result, decides to carry out an act of terrorism. Many scholars have challenged the validity of the term, questioning whether lone wolves, or "personal initiative attackers," are indeed acting on their own. Yet while the lone wolf may be ideologically inspired by a terrorist organization, he or she receives no operational or other support from such an organization and, thus, is indeed acting alone.

Although not a threat to be taken lightly, lone wolf attacks—typically perpetrated with light weaponry such as knives, axes, or bulldozers—generally result in low casualty numbers. Given that lone wolf attacks are a growing phenomenon, however, and that terrorists are always looking for new techniques, counterterrorism professionals must not underestimate the danger they pose to the public.

To prevent lone wolf attacks, officials must understand the reasoning behind them. First and foremost, terrorists are rational actors who weigh the costs and benefits of engaging in terrorism. Indeed, determining the motives of lone wolves can be difficult, given that they differ from person to person. One universally shared "benefit," though, appears to be feelings of honor and satisfaction.

In order to accrue honor and praise for carrying out a lone wolf attack, perpetrators oftentimes post their intentions on social media before striking. Such exposure offers an opportunity for intelligence analysts to cooperate with social media outlets and collect open-source information before attacks

occur. Furthermore, experts should create mechanisms to identify radical messages online and develop big data capabilities to monitor and control the discourse. Some such efforts are no doubt already under way, but additional work must be done to learn how this data can best be utilized to stop attacks.

BRUCE HOFFMAN

THE LONE WOLF model of terrorism is not new. In 2001, the deputy leader of al-Qaeda, Ayman al-Zawahiri, called for individuals to attack Jews and Americans with knives, Molotov cocktails, or other homemade devices. But only since the rise of the Islamic State (IS) has the lone wolf phenomenon entered the mainstream as a terrorism model.

Unlike strikes by formalized groups, lone wolf attacks are much harder to predict and … leave no trails that authorities can track.

IS has used social media to reach a wide audience and encourage lone wolf attacks. Unlike the experienced terrorists who executed the September 11 attacks, the Islamic State's lone wolf model provides an opportunity for anyone to participate in terrorism. In particular, IS has made terrorism more accessible by providing guidance on how, where, and when to carry out an attack, often manipulating vulnerable individuals to act.

The lone wolf model poses a new challenge for law enforcement and counterterrorism professionals. Unlike strikes by formalized terrorist groups, lone wolf attacks are much harder to

predict and individuals typically leave no trails that authorities can track. And although lone wolf attacks are less violent than other forms of terrorism, the sheer number of lone wolf threats may overwhelm and distract intelligence and law enforcement authorities.

In 2015, French authorities were thus tracking a huge number of individuals, and they lost sight of the larger and more lethal terrorist plots that were later carried out in Paris that November. This demonstrates why it is critical that law enforcement and counterterrorism experts pay serious attention to a wide range of threats, in particular large-scale plots, and not become too consumed with tracking potential lone wolves.

MARLENE MAZEL

ISRAEL, like Europe, has experienced an increase in lone wolf attacks over the past few years. These attacks appear to be perpetrated mainly by Palestinian youth who are not affiliated with or trained by any terrorist organizations.

Questions thus arise regarding why more Palestinian youth are engaging in terrorism; what underlying conditions stir them to perpetrate such violence; whether the Palestinian leadership, including the Palestinian Authority (PA), has engaged in incitement through glorification of specific acts; what effect, if any, such potential incitement has had on future attackers; and what corresponding lessons can be drawn about radicalization and lone wolves.

In a study focused specifically on Palestinian lone wolf attacks carried out between October 2015 and September 2016, findings showed 105 attacks carried out by youth, using knives (the most common weapon), guns, or explosive devices. Approximately 60 percent of the attackers were sixteen or seventeen years old, while the remaining 40 percent were younger.

The study, which drew on the attackers' names as reported in public databases, indeed showed institutional incitement by the PA and the Palestinian leadership, including through the posting of official flyers praising the youth as martyrs, complete with the Fatah imprimatur and pictures of the late Palestinian leader Yasser Arafat; statements that implicitly endorse the terrorist acts; public visits to the families of killed terrorists, generating broad media coverage; and formal military funerals extolling the acts.

The data thus far also suggests a possible correlation between institutional incitement and the frequency of terrorist attacks. During the peak period of stabbings, October 2015 through March 2016, PA institutional glorification was at its highest level. From April 2016 through September 2016, the preliminary data suggests a decrease in such institutional glorification, paralleling a drop in stabbings. PA incitement may thus have contributed to the general inflammatory environment—but questions remain on the ways in which such incitement may shape the views, behaviors, and actions of youth. Also, these trends could well have been affected by other environmental factors, and further research is needed to understand the correlation between specific acts of terrorism and specific cases of Palestinian institutional incitement.

The data thus far also suggests a possible correlation between institutional incitement and the frequency of terrorist attacks.

Even though the results from the study discussed here are preliminary—and the study itself is still in process—one can clearly deduce the critical need to understand and eliminate all incentives for youth to commit terrorist attacks. Reducing official glorification of such acts, along with payments to attackers' families, is essential. Furthermore, if Palestinian youth can be dissuaded from engaging in terrorism, as this study suggests, the Palestinian government, educators, and media must stop all forms of institutional incitement and, rather, send unified and consistent messages unequivocally condemning all acts of terrorism.

MATTHEW LEVITT

IN THE PAST, "lone wolf" has been a misnomer. Men and women considered lone wolves were known to law enforcement, and even if they were not acting under the direction of a terrorist organization, they were nonetheless connected to a group in some capacity, if only by ideology. Now, however, the Islamic State seeks to project power and influence beyond its territorial borders and infiltrate the West even as its official "caliphate" is in decline. Many individuals in the West have been, and will continue to be, inspired to act in the name of the Islamic State. Therefore, the "lone offender" phenomenon is very real.

IS has successfully recruited lone offenders in large part owing to its strong presence on social media. This past month, the jihadist group released an e-book in Turkish with instructions for conducting attacks alone. Additionally, the ninth volume of the IS periodical Rumiyah, published in May, contained details on the ideal weapons and targets for lone wolf attacks.

Given the rising threat of individual attacks from both IS and al-Qaeda, officials must consider the most effective methods for countering IS propaganda and addressing radicalization. Google, for example, has made efforts to provide countermessaging for certain searches and continues to extensively research how to effectively subvert radical messages online. While in some instances social media can be a resource for law enforcement to predict attacks, not all lone wolves post their intentions online in advance. Additionally, in a country as large as the United States, authorities often face challenges in detecting and responding to such warnings in a timely manner.

As well as on the Internet, countering violent extremism (CVE) must take place in communities. Although every case of radicalization has its own nuances, using a public health model enables community members, such as religious leaders, to be involved in deradicalization efforts and to identify models and messages that best address the needs of their respective communities. These CVE efforts are not meant to replace law enforcement or intelligence professionals but rather to work in tandem with them.

This summary was prepared by Aviva Weinstein.

OCTOBER 16, 2017

Iraq's Role in Countering the Islamic State's Finances

■ Ali Mohsen Al-Alaq

EDITED TRANSCRIPT

GOOD MORNING. I'm very pleased to have the opportunity to meet with you today. I'd like to highlight some important issues around our country, Iraq. First of all, I'd like to say that after years of patience, determination, and costly efforts, a clear picture of Iraq is emerging. It is an image of a country with a growing capacity to manage its affairs in a very modern fashion and to make the investments needed to secure a better future. In building a state—a peaceful, new Iraq—we are making progress across many fronts, the security and economic fronts chief among them.

Despite all this progress, challenges remain. Virtually every day in news reports from Iraq, the military support the country has received from foreign partners is on display. Sixty-eight nations are members of the military coalition united in an effort to destroy ISIS [as the Islamic State is also known]. But international support for Iraq extends well beyond military support to include economic and financial cooperation as well. Reconstruction is backed by key international stakeholders, and Iraq is hopeful that the donors' conference to be held in Kuwait in the coming months will help the country. Indeed, the conflict with ISIS caused very wide disruptions, including the emergence of some three million internally displaced persons.

Now, in looking closely at the macroeconomic picture, I'd like to point out some indicators from the recent IMF report, released in September 2017. Inflation remains—according to the IMF report—very low, at less than 1 percent. Real GDP [growth] was about 11 percent in 2016. The overall balance of payments was stronger than the program during the first half of 2017. Also, the spread between the official and parallel exchange rates for U.S. dollars

decreased from 10 percent in December 2016 to 6.7 percent in September 2017. Iraq successfully issued $1 billion in euro bonds in early August 2017 and enjoyed about $6.7 billion worth of investors' demand—suggesting a very positive credit outlook for the country. The stock of gross reserves of the Central Bank of Iraq (CBI) exceeded the agreed-upon program floor by about $4 billion for 2017, as of now. The gross public debt remained below the suggested program ceiling.

International support for Iraq extends well beyond military support to include economic and financial cooperation as well.

Hit by the fall of oil prices and ISIS, the government has started to implement a program of fiscal conservation to maintain debt and external sustainability. Given the current oil price projections and the implementation of fiscal conservation and of the stand-by arrangement (SBA), the fiscal and current account deficit should be eliminated by 2022, on schedule according to the program.

The CBI is committed to maintaining the peg to the U.S. dollar; the peg provides a key nominal anchor in a highly uncertain environment wherein policy capacity is affected by the conflict with the Islamic State. The CBI has removed all exchange restrictions and multiple-currency practices. To maintain macroeconomic stability, the government is committed to pursuing its fiscal conservation efforts to bring spending in line with available resources in 2017. To minimize the impact of fiscal conservation on the population, the government will continue to protect social spending, such as for health, education, and the social safety net.

Now, I'd like to talk about the CBI during uncertain times, in uncertain environments. Maybe I was not very lucky to have moved to the Central Bank at the end of 2014, because we faced two big shocks: one was, as you know, Daesh [another name for the Islamic State], and the other was the sharp decline in oil prices. They went down during 2015 by 40 percent, and in 2016 by 70 percent. So that was really a big challenge for the CBI. We have moved, at the Central Bank, because of all those challenges, from monetary stability to financial stability and economic growth in order to deal with the challenges created by those two shocks. We have taken many corresponding measures. For example, we have worked very hard with the government to navigate the financial difficulties of the period through quantitative easing. Thus, the Central Bank has discounted treasury bills from the government by about $20 billion so far, a high amount when measured against the total national budget. Steps also included enhancing and supporting the private banking sector, safeguarding the financial sector from financial crimes and money laundering, and developing the national strategy for anti-laundering and countering the financing of terrorism. The latter entailed developing the national strategy for AML/CFT, implementing the AML/CFT bill within the Central Bank, and establishing an AML/CFT national council. In that regard, I think we have done a lot with our international partners, at a very difficult time, to face the Islamic State. So we tried our best to cut off all the [ISIS] financial networks from the system, including hundreds of [suspect] exchange shops and wire transfer companies. Also, we submitted some cases to the court, facilitating a first for our country: the hearing of such cases in front of the court... So it gives an indication that the new laws in place, the new measures and regulations, the oversight for the banking sector, have all been tightened to allow for such an outcome.

I think, with our international partners, we have done a lot. On a daily basis, we share our information with these partners, helping everyone involved reach the current levels of cooperation. The last report from the Financial Action Task Force was really very positive—reflecting that the country has taken many steps in that regard.

To enhance our economy overall, we are carrying out a major initiative aimed at financing small- and medium-size enterprises. For this, the biggest program in the country's history, we allocated about $6 billion to finance the enterprises. Also, we have taken very serious steps within the Central Bank to establish new units to deal with tasks and functions that the Central Bank has never covered in the past—such as for financial inclusion, risk manage-

ment, compliance, consumer protection, provincial regulations, and risk-based audits. I think, through these measures, the Central Bank has moved from essentially the twentieth to the twenty-first century. By adding these functions, we have made this an institution to deal with all the challenges, the new tasks, that the other central banks have historically covered.

Finally, I'd like to refer to the recent developments in Kurdistan, which we feel very sad about. We are almost done defeating Daesh; the country is working very hard to rebuild and to allow people to return to their homes. Now, unfortunately, we are facing another challenge, which we hope will be solved in a political way, instead of through conflict. The latter path would be very hard for the country, which has paid a lot over the last three decades.

After the referendum, we at the Central Bank wrote right away to the prime minister of the Kurdistan Regional Government, asking if we, as a central bank, could continue doing our work there. This is because we have worked very hard with the KRG for about a year to exercise our oversight within the Kurdistan Region of Iraq. Before that, Kurdistan was really removed from CBI oversight. So, personally, I have had many meetings with the KRG prime minister, with the goal of establishing our oversight and also our supervision for the banking sector within the region. And then we signed an agreement, just two or three months ago, to open the Central Bank branch in Erbil. We have been arranging all the logistics to start working there—and indeed we have started this work. Then, when the referendum happened, I sent a letter to the prime minister asking him, as I said, if we could continue our work. The answer was positive. Yes, you can continue doing your work. So we said, from our side, we have no problem. I spoke to the government, to the prime minister, also to the parliament, about prospects for aligning Kurdistan with our constitution, so that whenever we have a positive response, we can consider that a good sign, and we can continue doing our work there.

So, for the Central Bank, we feel that if we can still do our work, we have no problem. We don't have a negative way to deal with the situation there. But the escalation is moving very fast right now, especially in the media, so we have to see where that will end. Hopefully, as I say, it will end peacefully.

Frankly, I feel that what happened is very sad, but that it can lead to permanent solutions for our relationship between federal development and the KRG—because many things happened in past years far outside the bounds of our constitution. Most such activity happened by political arrangements, which is, in my view, a very risky path—and that's what we're seeing right

now. Personally, I have expressed this perspective on many occasions. I previously served as secretary of the cabinet for eight years, and at that time I kept saying, we have to be in line with our constitution so that we don't accumulate problems that can lead to a future crisis. And that's what we are facing right now.

So what's happening now, maybe and hopefully it will lead to permanent solutions, permanent arrangements, in line with our constitution—so that we don't face these kinds of problems every time. Thank you very much.

OCTOBER 27, 2017

Hezbollah's Terror Army: How to Prevent a Third Lebanon War

■ Richard Kemp, Lord Richard Dannatt, and Klaus Naumann

RAPPORTEUR'S SUMMARY

RICHARD KEMP

THE WEST has a unique opportunity to prevent further wars between Hezbollah and Israel. Yet doing so would require many governments to change their instinctive reaction to Israeli military operations.

Currently, the prospect of Hezbollah initiating another war seems like a high probability, especially given its status as Iran's main proxy against Israel, the United States, and their allies. The High Level Military Group has few doubts that once a war begins, Israel would feel compelled to respond with significant aggression, force, and speed. And while its operations would surely follow the laws of armed conflict, they would necessarily result in extensive civilian casualties, especially in southern Lebanon.

Hezbollah knows this and in fact hopes to provoke it—the group is counting on a high casualty count to turn the international community against Israel, recognizing that many governments automatically isolate and even vilify the country whenever it defends itself against enemy attacks. Much like Hamas and similar groups, Hezbollah aims to garner enough support to put Israel on trial for war crimes. For this very reason, Israel is unlikely to consider a major preemptive campaign in Lebanon.

To change Hezbollah's calculus and avoid playing into the group's hands, Western governments should reconsider their reactions to Israel's justifiable military and counterterrorism operations—and to the terrorist attacks that spur those operations in the first place. Unfortunately, European governments are often more concerned about appeasing Arab countries in such situations. This mindset will persist so long as officials view terrorism directed at Israel differently from terrorism directed at other countries.

RICHARD DANNATT

HEZBOLLAH has made significant developments in its strategic concepts and capabilities since the 2006 Lebanon war, and understanding the resultant dangers is vital to assessing the likelihood of attack and the nature of Israel's inevitable counteroffensive. Regarding ground combat capabilities, Hezbollah has grown well beyond the terrorist or guerrilla category—it is now closer to a standard military force, with a clear chain of command and infrastructure. Its numbers have increased immensely, up to an estimated 25,000 active fighters and 20,000 reserve personnel. Around 5,000 of the active troops have completed advanced training in Iran.

Meanwhile, its arsenal has expanded to more than 100,000 rockets and missiles, of which thousands have long-range capabilities up to 250 kilometers. Ground forces are now outfitted with AK-47s, night-vision goggles, advanced antitank weapons, and upgraded explosives skills. More recently, Hezbollah has integrated a new armor support unit complete with modern tanks. It also has hundreds of unmanned aerial vehicles, advanced air defense systems, coast-to-sea cruise missiles, and significant intelligence capabilities. Combined with the combat experience Hezbollah forces have gained in Syria, these advances will allow the group to carry out operations at the company or battalion level.

In addition, Hezbollah remains the most important piece in Iran's proxy warfare strategy. Therefore, if another conflict with Israel breaks out, Tehran would likely push its other terrorist proxies around the region to come to the group's defense.

Hezbollah's basic strategic concept consists of three related parts: terrorist activity, traditional military activity, and political activity. Among other things, this interplay means that the group conducts operations without regard to the laws of war despite resembling a conventional military. For example, it has shown no compunction about using civilians as cover for its personnel, purposefully manipulating noncombatants into becoming targets. Over time, the group has transformed most Shia villages in southern Lebanon into military assets that provide infrastructure, recruitment, storage, and access to underground tunnels designed for warfare.

The international community should therefore realize that Hezbollah has become a potent threat not just to Israel, but also to the Lebanese people. During the next war, the group will no doubt aim to weaken Israel's resolve and gain a tactical advantage by attacking civilians and critical infrastructure inside Israel, perhaps even seeking to capture and hold important territory in

an effort to prove the credibility of its "resistance" stance to the Arab world. In response, Israel would surely launch a massive counteroffensive that would put the bunkered-in civilian population of southern Lebanon in grave danger.

Hezbollah remains the most important piece in Iran's proxy warfare strategy.

Finally, while the High Level Military Group's latest report focuses on preventing a third war, one might argue that the first shots have already been fired, with both sides conducting low-profile operations of various sorts against each other. In that case, it would not take much to transition from a cool war to a hot one.

KLAUS NAUMANN

GIVEN Hezbollah's improved military capabilities, desire to target Israeli civilians, and strategy of using Lebanese civilians as human shields, the next war would be decidedly worse than the previous one. If it breaks out, it could hold serious humanitarian consequences and put Western strategic interests in danger.

The West can still defuse this looming war or ameliorate its worst effects. To do so, the United States and Europe need to reevaluate their relationships with Lebanon and update their policies accordingly. Lebanon is no longer a friendly state with a terrorist group lurking at the margins. By this point, Hezbollah has managed to establish control over most of the country, leaving the government reliant on its presence and manipulating officials to neglect the people's interests for the sake of pursuing Iran's regional agenda. If the

West fails to recognize that Lebanon is no longer distinct from Hezbollah, the danger will only grow.

Hezbollah is preparing another conflict with Israel for two main reasons. The first is nothing new: both the group and its Iranian patron oppose Israel's existence. The second reason stems from Hezbollah's recent legitimacy problem in Lebanon due to losses incurred in Syria. For now, this problem is likely restraining the group from attacking Israel, since its leaders may not want to start another costly war right away. At the same time, they would likely leap at the chance of a one-off attack if the opportunity arises to burnish their domestic credentials by doing so. Yet such a move could easily spur all-out war—for example, if a miscalculation or break in the chain of command results in an attack that produces substantial Israeli civilian casualties.

The United States has already taken positive steps to prevent a third Lebanon war, such as recognizing the Iranian roots of the long-standing conflict and enacting sanctions against Tehran and Hezbollah. More immediate and firm action is required, however. The Trump administration needs to be forward thinking in this regard, mixing political, financial, and deterrent pressures on Hezbollah, the Lebanese government, and Iran. It should also state in unambiguous terms that Israel has the right to defend itself in the wake of Hezbollah attacks.

Similarly, European governments must do more to acknowledge and react to the reality of the situation. Most important, they should unequivocally designate the entirety of Hezbollah's organization as a terrorist entity, dispensing with the false distinction between its political and military activities.

International diplomacy must recognize the serious danger Hezbollah poses as well, especially with regard to the UN Interim Force in Lebanon. Neither UNIFIL nor the resolution authorizing its operations has been successful. The UN should therefore strengthen the force or reconsider its mandate, since it is not currently robust enough to be effective. Given the potential harm another war could bring to the Lebanese people, to Israel, and to European countries already reeling from refugee issues, the time to take more robust action is now.

This summary was prepared by Rachel Miller.

NOVEMBER 14, 2017

From CVE to "Terrorism Prevention": Assessing New U.S. Policies

■ William Braniff, Seamus Hughes, Shanna Batten, and Matthew Levitt

RAPPORTEUR'S SUMMARY

WILLIAM BRANIFF

THE UNITED STATES does not have a grand strategy with respect to terrorism. In the sixteen years since the attacks of September 11, 2001, the United States has relied on its criminal justice and military communities, enabled by more and better intelligence, to disrupt terrorist adversaries and prevent another large-scale attack. Along the way, however, global terrorism has reached historically high levels, triggering reactionary violence and polarizing debates about immigration and refugees, nationalism and internationalism, security and liberty, and religion. Traditional counterterrorism tools are necessary, but they appear to be insufficient in terms of mitigating terrorist violence and its deleterious political consequences over time.

To complement military and law enforcement efforts—traditional counterterrorism—the United States and the international community entertained a different paradigm, which sought to decrease the number of individuals mobilizing to violence in the first place by addressing the individual, communal, and societal factors exploited by terrorists. This emergent paradigm—countering violent extremism (CVE)—has been poorly resourced, sparsely staffed, and employed as a distant second priority to traditional counterterrorism. Since its inception, CVE has been beset by detractors who see it either as dangerously idealistic political correctness or as a euphemism for predatory counterterrorism.

The two problems, the insufficiency of traditional counterterrorism and CVE's lack of traction, are directly related to an inadequate appreciation for the essential nature of terrorism. Terrorism is primarily a form of violent

politics. Therefore, our response to terrorism must be primarily a political one. Given CVE's focus on contextual factors that enable terrorism at individual, community, and societal levels, CVE has the potential to alter the political conditions that allow for violent mobilization. Traditional counterterrorism lacks this political dimension. The CVE paradigm, if focused by a guiding principle, could directly inform a new grand strategic response to terrorism, with traditional counterterrorism serving in a necessary but subordinate role.

The CVE paradigm, if focused by a guiding principle, could directly inform a new grand strategic response to terrorism.

The collective grand strategy, inside and outside government, must be aimed at marginalizing terrorism. A marginalization grand strategy will help "right-size" traditional counterterrorism efforts. Establishing a grand strategy does not imply that terrorism should continue to be the highest priority on homeland and national security agendas at the expense of other challenges. On the contrary, a marginalization paradigm recognizes that terrorism is not an existential threat to the United States, may be subordinated to other national security concerns in a given region, and allows for more regionally contextualized support to partners for whom terrorism may or may not be a top priority.

SEAMUS HUGHES

COUNTERING violent extremism at the federal level is dead. While the Trump administration played a role in CVE's

demise, the responsibility falls on a number of actors. In the early days of the Obama administration, for example, the president put a hold on CVE programs, and it took two years to roll out a national strategy, "Empowering Local Partners to Prevent Violent Extremism in the United States." Now, the Trump administration finds itself in a similar position, pausing CVE programs and generally lacking any sort of coordination of CVE efforts at the federal level.

Indeed, the new CVE terminology introduced under the Trump administration, "terrorism prevention," could help narrow the issue. This term makes clear that the discussion is about programs and individuals crossing a particular threshold. Nevertheless, it only addresses violence, failing to acknowledge that extremism is also a large part of the issue.

Given the absence within the federal government of inherent advocates for such programs, a way must be found to provide incentives for CVE involvement. The Obama and Trump administrations have ceded CVE responsibility to the private sector, asking technology companies to remove extremist content from their sites, for example. This, however, is low-hanging fruit. The hard work, yet to be done, is creating prevention programs to address radicalization from an early stage.

Despite these challenges, domestic CVE programs can be saved. CVE may be moving away from the model of a federally directed program with interagency cooperation, but new efforts could empower local partners to do the work, such as in existing programs in New York and Denver. However, the federal government should be involved in quality control, encourage best practices for community engagement, and support cooperation between state and local officials.

SHANNA BATTEN

THE TERMINOLOGY used to describe countering violent extremism efforts must convey the intention, focus, and strategy of any CVE approach. The newest term, "terrorism prevention," entails a certain flexible ambiguity. Particularly given the lack of substantive U.S. domestic terrorism laws and the hesitancy to identify certain acts of terrorism as such, notably in Charlottesville in August 2017, communities are uncertain of their role in so-called terrorism-prevention efforts. Their uncertainty leads to misunderstandings and, ultimately, ambivalence.

To build trust within communities, CVE messaging cannot be left up to random interpretation, which can result in the faulty impression that

efforts to counter violent extremism are attempts, whether direct or indirect, to coopt communities into engaging in investigations and surveillance efforts. To the contrary, these efforts should remain within the purview of law enforcement and intelligence agencies.

Instead, a paradigm shift must now occur, similar to that playing out in societal understandings of domestic and sexual violence. This shift must acknowledge that violence, not ideology, is at the center of prevention work. The term "ideologically influenced violence" would clearly articulate violence as the target, while demonstrating that the U.S. government recognizes a variety of ideologies and a spectrum of radicalization. Indeed, shifting the language is the first step to achieving a transparent strategy and actual improvements in this form of violence prevention. Transparency in strategy, for its part, provides communities with concrete information and helps establish the trust critical to building their resilience.

Ideologically influenced violence can be addressed in a hands-on way at both micro- and macro-community levels. The federal government, which is best positioned as a convener and supporter for such activities, must likewise invest in the needs of communities. Meanwhile, comprehensive prevention means listening to communities and meeting them where they are—taking in both their vulnerabilities and their priorities. Using an assets-based approach, actors must collaboratively determine what resources and networks can be best employed to strengthen communities. Such a strategy must be flexible enough to be adapted to different communities. It must also build awareness that radicalization to violence is a process and that prevention efforts must respect civil liberties.

MATTHEW LEVITT

ADOPTING "terrorism prevention" to describe CVE efforts may not seem a particularly consequential change in language, considering that CVE terminology has gone through many iterations in the past few years. In fact, changing the lexicon could be a positive thing, since many people outside the Beltway are uncomfortable with the term CVE. What is troubling is that the new terminology does not make clear how much room it leaves for genuine prevention efforts, or what types of terrorism will be its focus.

While the Trump administration's evaluation of CVE programs continues to develop, some change is already evident. The Department of Homeland

Security has put greater emphasis on allocating grants to law enforcement over community service organizations, and to groups addressing Islamist extremism over other far-left or far-right extremism. Indeed, many people and organizations are uncomfortable accepting these grants because of the heavy and nearly exclusive focus on law enforcement and Islamist extremism.

It is troubling that the new terminology does not make clear how much room it leaves for genuine prevention efforts.

Further, redirecting CVE terminology to focus specifically on "terrorism" may undermine efforts to convince community members that they are part of the solution to violent extremism in their communities, rather than, potentially, part of a problem. A public health model that moves beyond an exclusively law enforcement focus, and instead involves community members, would be a more worthwhile CVE approach. Indeed, law enforcement agencies themselves typically clamor for just such an approach. Additionally, it is important to consider the sources of funding for CVE programs, because these too send a message. The U.S. Departments of Health and Human Services and of Education, for example, have huge pots of money that could be dedicated to prevention efforts, but these may not be available for a program focused exclusively on terrorism prevention.

Meanwhile, focusing on border-protection solutions in the wake of terrorist attacks is easy politics but poor counterterrorism policy. Pro-

tecting our borders is important, but alone such a policy ignores the reality that radicalization happens here in the United States. Radicalization does not stop at the border, so it is critical to have programs that address violent extremist ideologies early on, and work to counter a broad spectrum of extremism, including Islamist, right-wing, and left-wing extremism, as well as other at-risk behaviors in a community. It is not clear that "terrorism prevention" will fit this bill.

This summary was prepared by Aviva Weinstein.

THE WASHINGTON INSTITUTE FOR NEAR EAST POLICY

THE WASHINGTON INSTITUTE FOR NEAR EAST POLICY
www.washingtoninstitute.org