

U.S. COUNTERTERRORISM REIMAGINED

Tracking the Biden Administration's
Effort to Reform How America
Addresses Violent Extremism

Matthew Levitt, Editor



U.S. Counterterrorism Reimagined

Tracking the Biden Administration's Effort
to Reform How America Addresses
Violent Extremism

COUNTERTERRORISM LECTURES 2021-22

Matthew Levitt
Editor



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 177

First publication: September 2022

All rights reserved. Printed in the United States of America. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without permission in writing from the publisher.

© 2022 by The Washington Institute for Near East Policy

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

Cover images (top left to bottom right): Demonstrators converge at the U.S. Capitol during the January 6 insurrection; Taliban forces patrol the Kabul airport following the U.S. troop withdrawal; Maj. Gen. Chris Donahue becomes the last U.S. service member to depart Afghanistan. Reuters/Shutterstock

Contents

- **Acknowledgments** / v
- **Abbreviations** / vi
- **Speakers** / viii
- **Introduction: Reassessing How America Counters Terrorism**
Matthew Levitt / 1
- **Countering and Exposing Terrorist Propaganda and Disinformation**
Daniel Kimmage / 9
- **Rethinking U.S. Counterterrorism Two Decades After 9/11**
Matthew Levitt, Katrina Mulligan, and Christopher Costa / 15
- **Foreign Fighters and U.S. Policy: Tracking Mobilization Hubs to Stem the Flow**
Nate Rosenblatt and Naureen Chowdhury Fink / 20
- **Preventing Domestic Terrorism: The DHS Approach and the New U.S. Strategy**
John D. Cohen / 24
- **U.S.-E.U. Counterterrorism Cooperation Twenty Years After 9/11**
Gilles de Kerchove and Oliver Onidi / 33
- **Contending with New and Old Threats: A French Perspective on Counterterrorism**
Laurent Nuñez / 37

(continued)

- **A European Perspective on Counterterrorism**
Ilkka Salmi / 49

- **Evolving Counterterrorism Priorities and Policies**
Christopher Landberg / 54

- **Building Civilian Counterterrorism Capacity: OPDAT's Role**
Jill Rose / 58

- **Addressing the Threat from Homegrown and Foreign Terrorist Organizations**
Patrick E. Reddan Jr. / 62

- **Thinking Through Non-Kinetic Counterterrorism Tools**
Robert Jenkins / 66

- **A Comprehensive Framework to Address Domestic Violent Extremism**
John D. Cohen / 69

- **Disrupting Terrorist Financing Networks**
Paul Ahern / 76

- **Non-Kinetic Tools in a Time of Competing Priorities**
Damon Stevens / 80

- **The War on Jihadism: Lessons from Twenty Years of Counterterrorism**
Marc Hecker, Elie Tenenbaum, and Louis Dugit-Gros / 86

- **NATO Counterterrorism Trends: Current and Future Threats**
Gabriele Cascone / 90

Acknowledgments

Now in its fifteenth year, The Washington Institute's Counterterrorism Lecture Series has steadily drawn senior-level counterterrorism officials, academics, and practitioners to assess the terrorist threats facing the United States and its allies, and how best to counter them. This amazing run has been possible thanks only to the hard work of dedicated Washington Institute staff.

This monograph, and the lecture series on which it is based, has been facilitated entirely by the Institute's administrative, communications, publications, and research staff. Special thanks go to publications director Maria Radacsi; senior editor George Lopez; and managing editor Jason Warshof.

No less indispensable is generous support from Jeanette and Eli Reinhard, who sponsor the Institute's Program and Counterterrorism and Intelligence, and the Fromer and Wexler families, who support my fellowship at the Institute. I offer them my heartfelt thanks.

I am grateful to be a part of the intellectual community that is the Washington Institute for Near East Policy, and thank the Institute's fellows, research assistants, and interns for their many contributions to this iteration of the lecture series. Here, I must single out for praise my partners in crime over the course of the series, Katherine Bauer and Aaron Zelin, senior fellows in the Institute's Reinhard Program who helped make these lectures possible. Finally, tremendous thanks to the program's research assistants, who did all the heavy lifting to facilitate the lectures and resulting volume: Lauren Fredericks, Hannah Labow, and Lauren von Thaden.

What follows is a snapshot of the counterterrorism issues and themes that dominated the first fifteen months of the Biden administration, from roughly late January 2021 through March 2022.

Dr. Matthew Levitt
Washington DC, September 2022

Abbreviations

AUKUS	Australia, United Kingdom, United States (military alliance)
C-UAS	counter–unmanned aircraft system
CFT	countering the financing of terrorism
CP3	Center for Prevention Programs and Partnerships
CPS	Bureau for Conflict Prevention and Stabilization (USAID)
CRCL	Office for Civil Rights and Civil Liberties (Department of Homeland Security)
CVE	countering violent extremism
DGSE	Directorate-General for External Security (France)
DVE	domestic violent extremism
FATF	Financial Action Task Force
FTO	foreign terrorist organization
GEC	Global Engagement Center (State Department)
HVE	homegrown violent extremism
I&A	Office of Intelligence and Analysis (Department of Homeland Security)
I&W	indications and warning
I2C2	interagency and international coordination cell
IS	Islamic State
MDM	mis-, dis-, and mal-information
MVE	militia violent extremism

NCTC	National Counterterrorism Center
OPDAT	Office of Overseas Prosecutorial Development, Assistance, and Training (Justice Department)
REMVE	racially and ethnically motivated violent extremism
RLA	resident legal advisor
SLTT	state, local, tribal, and territorial
TFI	Office of Terrorism and Financial Intelligence (Treasury Department)
UAS	unmanned aircraft system
VEO	violent extremist organization

Speakers

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

■ PAUL AHERN

Paul Ahern is principal deputy assistant secretary in the Office of Terrorist Financing and Financial Crimes at the U.S. Department of the Treasury. Previously, he served as assistant general counsel for enforcement and intelligence, where he oversaw the provision of legal advice concerning the full range of activities involving the Treasury Department's national security, foreign policy, law enforcement support, and customs revenue functions.

■ GABRIELE CASCONI

Gabriele Cascone spent the first part of his career as an officer in Italy's Carabinieri Corps and then joined the NATO International Staff, where he heads the Counterterrorism Section in the Emerging Security Challenges Division. His NATO career has been focused mainly on the Middle East, North Africa, and the Western Balkans.

■ JOHN D. COHEN

John D. Cohen is the U.S. Department of Homeland Security's coordinator for counterterrorism and assistant secretary for counterterrorism and threat prevention. During the Obama administration, he was acting undersecretary for intelligence and analysis and counterterrorism coordinator in the department. In addition, he has served as a direct advisor to the secretary and led the development and implementation of several high-visibility, department-wide crime prevention, counterterrorism, counterintelligence, and border/transportation security initiatives.

■ CHRISTOPHER COSTA

Christopher Costa served as special assistant to the president and National Security Council senior director for counterterrorism during the Trump administration. Currently director of the International Spy Museum, he is a thirty-four-year veteran of the Defense Department, including twenty-five years with the Army working on counterintelligence, human intelligence, and special operations.

■ LOUIS DUGIT-GROS

Louis Dugit-Gros, a 2021–22 visiting fellow at The Washington Institute, is a French diplomat and member of the Ministry for Europe and Foreign Affairs (Ministère de l'Europe et des Affaires Étrangères). The third active-duty French diplomat to be an Institute visiting fellow, Dugit-Gros previously served as the press officer for the French embassy in Morocco, a political advisor for Libya, and a desk officer for Qatar and Oman at ministry headquarters in Paris. He also worked as a research analyst for the French Ministry of Defense.

■ NAUREEN CHOWDHURY FINK

Naureen Chowdhury Fink is executive director of the Soufan Center and a former senior policy advisor on counterterrorism and sanctions at the United Kingdom Mission to the United Nations. She has also worked with the UN Counter-Terrorism Committee Executive Directorate, UN Women, and various think tanks.

■ MARC HECKER

Marc Hecker is director of research and communications at the French Institute of International Relations and editor-in-chief of *Politique Étrangère*.

■ ROBERT JENKINS

Robert Jenkins is assistant to the administrator in the Bureau for Conflict Prevention and Stabilization at the U.S. Agency for International Development. Previously, he served as deputy assistant administrator for the Bureau for Democracy, Conflict, and Humanitarian Assistance and director of USAID's Office of Transition Initiatives.

■ GILLES DE KERCHOVE

Gilles de Kerchove, a Belgian official, is the European Union counterterrorism coordinator. He served from 1995 to 2007 as director of justice and home affairs in the Council Secretariat of the European Union, and has held various other positions.

■ DANIEL KIMMAGE

Daniel Kimmage is principal deputy coordinator of the State Department's Global Engagement Center and was the GEC's acting special envoy and coordinator from January 2017 to January 2019. In these roles, he has led efforts to synchronize U.S. communications programs designed to counter terrorist recruitment and state-sponsored propaganda and disinformation. Previously, he covered CT issues for the Office of Policy Planning and as principal deputy coordinator of the Center for Strategic Counterterrorism Communications.

■ CHRISTOPHER LANDBERG

Christopher Landberg is acting principal deputy coordinator in the Bureau of Counterterrorism at the U.S. Department of State. Since September 2019, he has served as deputy coordinator for crisis response and technical policy, responsible for oversight of the Counterterrorism Bureau's Office of Technical Programs and Operations Policy and its Office of Crisis Response, Preparedness, and Special Coordination.

■ MATTHEW LEVITT

Matthew Levitt is the Fromer-Wexler Fellow at The Washington Institute and director of its Reinhard Program on Counterterrorism and Intelligence. He is a former deputy assistant secretary for intelligence and analysis at the U.S. Department of the Treasury and counterterrorism intelligence analyst at the Federal Bureau of Investigation. Levitt teaches at Georgetown University's School of Foreign Service and is the author of *Hezbollah: The Global Footprint of Lebanon's Party of God* (2013).

■ KATRINA MULLIGAN

Katrina Mulligan is acting vice president for national security and international policy at the Center for American Progress. Previously, she served in the Justice Department's National Security Division as well as in the National Security Council, Office of the Director of National Intelligence, and National Counterterrorism Center.

■ LAURENT NUÑEZ

Laurent Nuñez has served as France's national coordinator for intelligence and counterterrorism since 2020. His office is part of the French Presidential Administration and coordinates counterterrorism efforts by the French intelligence community, police, and judicial services. Previously, he served in a wide array of government positions, including junior minister and head

of the General Directorate for Interior Security (DGSI), the agency in charge of domestic security and intelligence issues.

■ OLIVIER ONIDI

Olivier Onidi is deputy director-general for migration and home affairs at the European Commission, where he has overseen the directorate's work on security issues since December 2016. His previous assignments include coordinating commission-wide efforts related to the Central Mediterranean route and the refugee crisis.

■ PATRICK E. REDDAN JR.

Patrick E. Reddan is deputy assistant director at the Federal Bureau of Investigation's Counterterrorism Division.

■ JILL ROSE

Jill Rose is deputy director in the Office of Overseas Prosecutorial Development, Assistance, and Training at the U.S. Department of Justice.

■ NATE ROSENBLATT

Nate Rosenblatt is a doctoral candidate in sociology at Nuffield College, University of Oxford, and an International Security Program fellow at New America. He has lived, worked, and conducted field research in Turkey, Syria, Iraq, Lebanon, Morocco, Kuwait, and the United Arab Emirates.

■ ILKKA SALMI

Ilkka Salmi is counterterrorism coordinator at the European Union. Previously, he was director of the Disaster Preparedness and Prevention Directorate at the European Commission and permanent secretary of Finland's Ministry of the Interior.

■ DAMON STEVENS

Damon Stevens is assistant director for strategic operational planning and national intelligence manager at the National Counterterrorism Center.

■ ELIE TENENBAUM

Elie Tenenbaum is a research fellow at the French Institute of International Relations and director of its Security Studies Center. He was a visiting fellow at Columbia University and has taught international security at Science Po and international relations history at the University of Lorraine.

Introduction: Reassessing How America Counters Terrorism

■ Matthew Levitt

The first year of the Biden administration saw a top-to-bottom reassessment of how the United States fights terrorism and violent extremism both at home and abroad. Not since the September 11 attacks has the nation undergone such a massive transformation of its counterterrorism posture.

To be sure, all U.S. administrations navigate periods of policy review and then transition from implementing the previous administration's policies to instituting their own. When it comes to counterterrorism, however, the transition under Biden has been more dramatic than under any other president in the past twenty years. Even the tremendous emphasis on counterterrorism under the George W. Bush administration resulted from the 9/11 attacks, not a process of policy review. Indeed, in the early days of his administration, President Bush had planned a pivot to Asia until al-Qaeda upturned those plans by attacking the United States.

In contrast, the Biden administration came to office with the explicit goal of reimagining what it looks like to act against terrorism and violent extremism. At home, this meant addressing the sharp rise in violent extremism from white supremacist, anti-government, and other racially and ethnically motivated violent extremist (REMVE) actors, while maintaining vigilance against the persistent threats from international terrorist groups like the Islamic State, al-Qaeda, and those inspired by them.

Even more significant by bureaucratic and budgetary standards is the long-overdue reassessment of U.S. counterterrorism operations around the world. This reflects a shift toward great power competition that predates the current administration conceptually but has only been truly implemented under Biden. It also emerged from the realization that rationalizing the U.S. counterterrorism enterprise was necessary to free up funds to address a wide range of equally important national security issues, from the rise of China and Russia (well before the Ukraine invasion) to climate change, domestic infrastructure needs, public health issues, and more.

These challenges dominated the first year of the Biden administration's national security team—punctuated by events like the messy withdrawal from Afghanistan, a steady stream of arrests and trials related to the January 6 insurrection, and plots stemming from both domestic and international extremists—and encapsulate the main themes of this Counterterrorism Lecture Series. As the Biden administration set about making these structural changes to its counterterrorism posture, it reached out to U.S. allies in Europe and international organizations such as NATO both to reassert America's commitment to multilateralism and to plan for how to jointly contend with the implications of America's reduced international counterterrorism presence.

ADDRESSING DOMESTIC AND HOMEGROWN EXTREMISM

By its very nature, the January 6 insurrection forced the Biden administration to prioritize countering disinformation and domestic violent extremism from day one. Indeed, on January 20, the president's very first full day in office, Biden called for a hundred-day comprehensive review of U.S. efforts to address domestic terrorism, a problem—a White House fact sheet later noted—“[that] has evolved into the most urgent terrorism threat the United States faces today.”¹ This led three months later to the publication of an intelligence community assessment on domestic violent extremism, with the Office of the Director of National Intelligence publishing a capsule of its findings, “Unclassified Summary of Assessment on Domestic Violent Extremism.” This summary warned that domestic violent extremists (DVEs) motivated by a range of ideologies and stirred to action by various U.S. political and societal events “pose an elevated threat to the Homeland in

2021.”² The greatest threats, the report concluded, came from lone offenders or small cells of DVEs. Among these threats, the most lethal came from REMVEs or militia violent extremists, with REMVEs most likely to carry out mass-casualty attacks targeting civilians and militias most likely to target government personnel and law enforcement officials.³

Three months later—warp speed by bureaucratic government standards—the White House issued the first ever “National Strategy for Countering Domestic Terrorism.”⁴ The strategy underscored civil rights and civil liberties protections as a national security imperative and emphasized the need for community-led programs in seeking to prevent individuals from reaching the point of committing terrorist violence.⁵ Among the underlying sources of concern for U.S. officials were societal rifts over Covid-19 public health restrictions, white supremacist efforts to foment a race war, and efforts to sow civil disorder and open space for violence in the interest of hastening societal breakdown, otherwise known as accelerationism.⁶ Particularly troubling, the FBI warned, are DVEs’ proclivity to target soft, civilian targets, including houses of worship, retail stores, and public gatherings.⁷

Meanwhile, the FBI and its sister law enforcement agencies contended with homegrown violent extremists (HVEs), which the bureau assessed as the most significant international terrorist threat facing the United States. HVEs draw inspiration from foreign terrorist organizations (FTOs) like the Islamic State (IS) and al-Qaeda but without individualized direction from these groups. HVEs nourish their grievances by consuming still-readily available propaganda, which encourages terrorist entrepreneurship, while their lack of tangible ties to an FTO and ability to radicalize and mobilize quickly and without detection pose significant challenges for counterterrorism authorities. Both IS and al-Qaeda seek to inspire HVEs to carry out attacks in their home countries, including the United States.⁸ In November 2021, a DHS National Terrorism Advisory System bulletin warned of a heightened threat environment across the United States as the holiday season approached, including by lone offenders and small groups inspired by domestic and foreign forms of violent extremism.⁹ The August 2021 U.S. withdrawal from Afghanistan, which reached a low point when IS attacked the Kabul airport, only revealed a more troubling threat environment. IS, al-Qaeda, and right-wing extremist groups alike celebrated the U.S. withdrawal, portraying it as an American defeat at the hands of the Taliban.

RECALIBRATING AMERICA'S GLOBAL COUNTERTERRORISM POSTURE

During his tenure, President Obama sought to elevate various foreign and national security policy issues as important in their own right, not only as corollaries to counterterrorism policy. But events at home and abroad, from the Boston Marathon bombing to the Syrian civil war and the rise of the Islamic State, frustrated his efforts. Under the Trump administration, dealing with the challenges posed by great power competitors China and Russia, as well as regional threats from states like North Korea and Iran, began to take precedence for the Defense Department in particular. In February 2017, chairman of the Joint Chiefs of Staff Gen. Joseph Dunford articulated a “4+1” framework for prioritizing international threats and the military capabilities required to address them, in which counterterrorism represented the “plus one” after strategic interstate competition.¹⁰ As the 2018 National Defense Strategy made clear, “inter-state strategic competition, not terrorism, is now the primary concern in U.S. national security.”¹¹ But only under the Biden administration was the idea of actually recalibrating America’s twenty-year-long international counterterrorism deployments put into effect.

Officials have struggled with the challenge of harmonizing counterterrorism and great power competition. In the years that followed the Defense Department’s declared shift in focus, confusion swirled over how to operationalize the move in terms of resource allocation or mission prioritization. Clearly, even while re-directing resources toward competing with China and Russia, the U.S. national security bureaucracy had to remain prepared for an array of terrorism threats. The production of three largely unaligned national security strategies under the Trump administration only exacerbated the problem.¹² Within weeks after taking office, the Biden administration released an interim national security strategy guidance paper noting the need to “meet the challenges not only from great powers and regional adversaries, but also violent and criminal non-state actors and extremists,” alongside threats from climate change to infectious disease and more.¹³ But like his predecessor’s strategies, Biden’s interim guidance lacked direction on how to budget limited resources across these threats.

In the view of some, the United States faces a choice between engaging in great power competition and fighting “peripheral wars” in places like Syria or Yemen—supposed remnants of an outdated war on terrorism—but cannot do both. The reality, however, is that with a modicum of strategic planning, the two efforts are mutually reinforcing, not mutually exclusive. Biden administration officials realized very

quickly that on both fronts, whether engaging in power competition or countering terrorism, Washington would have to revitalize its international alliances and multilateral engagement. U.S. officials would have to get over their traditional reluctance to share decisionmaking with key foreign partners, while those partners would have to overcome their traditional discomfort with burden sharing.¹⁴

This necessity was driven home by the very nature of America's new counterterrorism posture, which turned on its head the two-decade-long premise of U.S.-led, partner-enabled CT efforts. Now, wherever possible, operations were to be partner led and U.S. enabled. Where unique American capabilities could help allies counter threats closer to their own backyards, the United States would be willing to help with intelligence, logistics, air supply, mid-air refueling, and more. But only in those circumstances where terrorist groups threatened the U.S. homeland or American interests abroad would the United States take the lead on counterterrorism missions around the world. By definition, this involved a greater reliance on engaging foreign partners than before.

DEVELOPING NON-KINETIC COUNTERTERRORISM TOOLS

The new counterterrorism posture implicitly acknowledges that, for all its tactical success thwarting attacks and capturing or killing terrorist operatives, the past two decades of U.S. efforts—from a strategic perspective—have left much to be desired. By 2020, far more people were radicalized to violent extremism than in 2001, representing a more diversified and globally dispersed terrorist threat.

The years of devoting heavy resources to tactical counterterrorism have carried an inherent tradeoff: an emphasis on supporting kinetic missions rather than efforts to prevent violent extremism from taking root in the first place. Under the new counterterrorism posture, investments will continue to fund tactical efforts as necessary, but they will prioritize soft power programs, including intelligence forecasting, multilateral diplomacy, civilian capacity building, conflict prevention and stabilization, and anti-corruption.

Much of the current planning will be forward-looking, aimed at preventing people from becoming violent extremists or at proactively addressing issues to hinder the next round of foreign fighter mobilization. But some effort will need to be deployed immediately, to address threats such as the squalid conditions at detention camps in Syria like al-Hawl, which absent intervention could well serve as the breeding ground for the next generation of Islamist terrorists.

CT LECTURE SERIES, VOLUME 10

These pressing challenges and shifts in U.S. posture formed the backdrop of this latest lecture series, which features twenty-one speakers on a wide range of CT topics that predominated during the first fifteen months of the Biden administration. Themes include U.S. efforts to counter and expose terrorist propaganda and disinformation; implementation of the first ever U.S. strategy to counter domestic terrorism; and the efforts of departments and agencies across government to develop a robust, non-kinetic counterterrorism toolkit. Given how important re-investing in transatlantic counterterrorism cooperation is to enacting the Biden administration's reframed counterterrorism posture, the lectures also featured contributions from French, EU, and NATO counterterrorism officials. Rounding out the series, American and foreign academics pushed boundaries by offering sober critiques of the past twenty years of counterterrorism, cutting-edge ideas for dealing with tomorrow's foreign fighter mobilization, and policy recommendations for maximizing the return on the past two decades of CT investment and preserving hard-earned gains, while reshaping America's posture to make it more sustainable over the long haul.

As has been the case throughout the fifteen years of this lecture series, the following pages are intended to spark conversation and debate, not be the final word. Let the conversation begin.

NOTES

- 1 White House, “National Strategy for Countering Domestic Terrorism,” June 2021, <https://www.whitehouse.gov/wp-content/uploads/2021/06/National-Strategy-for-Countering-Domestic-Terrorism.pdf>.
- 2 Office of the Director of National Intelligence, “Unclassified Summary of Assessment on Domestic Violent Extremism,” March 17, 2021, <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2194-unclassified-summary-of-assessment-on-domestic-violent-extremism>.
- 3 Ibid.
- 4 White House, “National Strategy for Countering Domestic Terrorism,” June 2021, <https://www.whitehouse.gov/wp-content/uploads/2021/06/National-Strategy-for-Countering-Domestic-Terrorism.pdf>.
- 5 White House, “Countering Domestic Terrorism,” fact sheet, <https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/15/fact-sheet-national-strategy-for-countering-domestic-terrorism/>.
- 6 John D. Cohen, “Statement for the Record: Strategy Session on Non-Kinetic Counterterrorism Tools,” Washington Institute for Near East Policy, November 8, 2021, <https://www.washingtoninstitute.org/policy-analysis/strategy-session-non-kinetic-counterterrorism-tools>.
- 7 Patrick E. Reddan Jr., “Statement for the Record: Strategy Session on Non-Kinetic Counterterrorism Tools,” Washington Institute for Near East Policy, November 8, 2021, <https://www.washingtoninstitute.org/policy-analysis/strategy-session-non-kinetic-counterterrorism-tools>.
- 8 Ibid.
- 9 “Summary of the Terrorism Threat to the U.S. Homeland,” November 10, 2021, https://www.dhs.gov/sites/default/files/ntas/alerts/21_1110_ntas-bulletin.pdf.
- 10 Fred Dews, “Joint Chiefs Chairman Dunford on the ‘4+1 Framework’ and Meeting Transnational Threats,” *Brookings Now*, February 24, 2017, <https://www.brookings.edu/blog/brookings-now/2017/02/24/joint-chiefs-chairman-dunford-transnational-threats/>.
- 11 U.S. Department of Defense, “Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military’s Competitive Edge,” <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.
- 12 Ibid.; White House, “National Strategy for Counterterrorism,” December 2018, https://www.dni.gov/files/NCTC/documents/news_documents/NSCT.pdf; White House, *National Security Strategy of the United States of America*, December 2017, <https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.

- 13 White House, “Interim National Security Strategic Guidance,” March 2021, <https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf>.
- 14 For the European angle, see Charles Thépaut, *A Vanishing West in the Middle East: The Recent History of U.S.-Europe Cooperation in the Region*, Policy Focus 169 (Washington DC: Washington Institute, 2021), <https://www.washingtoninstitute.org/policy-analysis/vanishing-west-middle-east-recent-history-us-europe-cooperation-region>.

Countering and Exposing Terrorist Propaganda and Disinformation

Daniel Kimmage

Principal Deputy Coordinator, Global Engagement Center, U.S. Department of State

Thank you, Matt, and thank you to all of the viewers and listeners out there in the virtual world. So the Global Engagement Center (GEC), in its current form, was created by the 2017 National Defense Authorization Act. It was created to coordinate the efforts of the U.S. government to counter foreign state and nonstate propaganda and disinformation that aims to undermine the interests of the United States, our allies, and partners. This builds on two earlier efforts, both of which focused on counterterrorism, and both of which were created by executive orders. Matt mentioned one when he went through my bio: the Center for Strategic Counterterrorism Communications. The second was an earlier version of the GEC, created by a 2016 executive order and focused on countering ISIS.¹

But in 2017, Congress recognized an urgent national security imperative and expanded the Global Engagement Center's mission. Today, the GEC, at the State Department, not only focuses on terrorist propaganda but also on disinformation and propaganda spread by adversarial state actors to undermine U.S. security, policy, and those of our partners and allies. So let me talk broadly at the outset about four major GEC milestones in the recent past.

The first is our analytic work. As we have built up the GEC, one of our key goals has been to make sure that it is driven by data and analysis. To do that, we have created a team of more than thirty data scientists who analyze open-source

1. Islamic State of Iraq and al-Sham; for purposes of simplicity, used interchangeably with Islamic State (IS) over the course of these entries. Daesh, an Arabic acronym for the group, also appears.

developments in the information space. That team is producing analysis that informs actions by our State Department colleagues and our interagency partners. Also, they lead collaboration with a range of other U.S. government and international partners.

Second, we know that we cannot do this alone. However much the GEC expands, it needs to be at the hub of a much larger effort. As we have built up our own capabilities, we have also established and strengthened government-to-government partnerships that enable us to coordinate our analysis and, more importantly, our actions over the long term.

Third, we are taking proactive action globally. We are executing campaigns, programs, and initiatives to reduce the space available to bad actors for nefarious influence activities.

Finally, because we understand that technology is woven into virtually every aspect of this problem, we are trying to stay ahead of that curve as well. We have launched a comprehensive framework to drive U.S. and international coordination on technology and, specifically, on counter-disinformation technologies and their implementation. This framework was recently highlighted favorably by the National Security Commission on Artificial Intelligence, and I will talk about its components a little bit later. So the bottom line is that we have established a level of coordination that did not previously exist in the U.S. government.

Let me talk now about some of our organizational components. First among those are our threat teams. We have teams focused on Russia, China, Iran, and counterterrorism. They conduct specific operations and they also carry out interagency coordination to counter propaganda and disinformation from those threat actors.

Second are our functional teams. These include our analytics and research team, which I spoke about above in the context of its analysis, and our technology and engagement team, which I will [detail] a bit more later on.

Third, we have an interagency and international coordination cell, which—because government loves acronyms—we call the I2C2. It is comprised of liaison officers from departments and agencies, and in the case of the Department of Defense from combatant commands, so that we are connected, as we need to be, with those partners to coordinate.

Now, let me talk a bit more about our analytic support. To counter adversarial propaganda and disinformation, we really need the best possible understanding of the information environment, and we need to share that understanding with our partners both within the U.S. government and internationally. Over the past year, we have conducted analysis touching on at least seventy-seven countries.

We tailor our analytic products to the needs of our consumers, who are typically an embassy, a State Department bureau, or one of our international partners.

These reports are designed to be actionable and unclassified. There is a growing demand for open-source data and research. We do this so that when we put this in the hands of, for example, an embassy on a Tuesday morning, they can go and do something with it almost as quickly as possible, whether that is writing talking points or reallocating resources to a program that they are supporting. What we want to do is tell the embassy what is happening in a quantifiable and data-driven matter, whether or not some propaganda or disinformation event is prevalent in the information space, whether or not it is coordinated by a threat actor, whether it dovetails with prevailing sentiment among a target audience, and what can be done. We also benefit, of course, from feedback from our colleagues in the field, who have a fantastic grasp of local dynamics, politics, culture, and history. That is an iterative cycle.

Let me talk about our work in the context of the Covid-19 crisis. In January 2020, we already began to look at propaganda and disinformation in this context. It rapidly became clear that this would be an issue of global consequence, not simply in the scope of the crisis but also in our area of propaganda and disinformation. We saw Russia pushing conspiracy theories. We saw the People's Republic of China suggesting various false and nefarious narratives about the origin of the virus. So we began to see a certain narrative convergence between the Chinese and Russian efforts. These were not the only countries to push these false narratives, but they have very well-developed mechanisms and ecosystems to spread their messages to audiences around the world on a variety of platforms. We took a multifaceted approach in our efforts to counter this wave of Covid-related disinformation and propaganda.

First, we tracked all of it, beginning in January 2020. We released reports. One of our first reports looked at Russia's disinformation campaign on the virus, and how it spread through their ecosystem. Second, building on this analysis, we worked to expose these disinformation efforts. Here, I would flag for everyone: while most of our reports are for internal use, we do public products as well. Last year, we released a major report on the pillars of the Russian disinformation ecosystem, which highlights the proxy news outlets and websites that they use, but

“We saw the People’s Republic of China suggesting various false and nefarious narratives about the origin of the virus. We began to see a certain narrative convergence between the Chinese and Russian efforts. These were not the only countries to push these false narratives, but they have very well-developed mechanisms and ecosystems to spread their messages to audiences around the world on a variety of platforms.”

also focuses on the role of that ecosystem in spreading Covid-related propaganda and disinformation. Third, we worked with the media to inform the public, for example, about Beijing’s propaganda and disinformation campaigns on the [pandemic]. Finally, we provided rapid-response grants to local organizations on the frontlines fighting the adversarial narratives of the Covid “info-demic,” as some have called it.

Now, let me talk a little bit more about our threat teams. Our Russia team—it leads and coordinates U.S. interagency and global partner efforts to understand, expose, counter, and build resiliency to Russian malign influence that aims to undermine democratic systems.

Our China team focuses on three priority lines of effort. The first is to puncture People’s Republic propaganda narratives through high-quality open-source research. The second is to build resilience among civil society and the media. The third is to carry out strategic communications campaigns in reducing space for Beijing’s whole-of-government influence campaigns, propaganda, and disinformation to thrive.

Our Iran team works to deny Iran use of disinformation that undermines U.S. policy. To this end, the GEC educates and informs global partners on the threat of Iranian disinformation, including its manipulation of outcomes around elections and other international events.

“In the counterterrorism realm, our team understands that it is dealing with a fluid information environment and seeks to be agile, analytic, and proactive in countering the threats that face our homeland.”

In the counterterrorism realm, our team understands that it is dealing with a fluid information environment and seeks to be agile, analytic, and proactive in countering the threats that face our homeland. Terrorist organizations seek to leverage the online space, combining their online and offline propaganda activities to multiply the impact of their operations and build a perception that they are growing and successful movements, because those

are the movements that can pull in funding and draw recruits. Our job, of course, is to prevent this at every stage in the area of propaganda and disinformation, so that they cannot do this. I would note in the counterterrorism context an increasing focus on racially and ethnically motivated violent extremism (REMVE). That comes in addition to our existing experience countering propaganda and disinformation by groups like ISIS and al-Qaeda.

Specifically, the Global Engagement Center is a co-chair of the Communications Working Group within the Global Coalition Against Daesh/IS. The GEC [was a leader] in supporting the implementation of the de-ISIS resiliency

counter-propaganda and disinformation campaign framework. This campaign takes a population-centric approach, building resiliency among audiences in Iraq and Syria that are most vulnerable to ISIS ideology and coercion. The GEC's coordinator and special envoy serves as one of the three co-leads along with the United Kingdom and United Arab Emirates in the [coalition's] Communications Working Group, which today brings together more than fifty organizations and nations. In this role, the GEC has led discussions with Communications Working Group partners on how ISIS is exploiting the Covid-19 crisis and its propaganda, and we have explored new ways to counter the group's narratives. Our UK co-leads on the Communications Working Group are amplifying and providing analysis of the coalition's communications activities through the counter-Daesh communications cell in London, and challenging and degrading the legitimacy of ISIS globally. Through this overarching framework, members of the coalition are able to conduct activities independently of each other without fear of contradicting or duplicating the efforts of other partners.

Let me talk a little bit about some of our efforts in East Africa. Globally, we focus on building resiliency to terrorist propaganda through working with local, national, and regional partners. Specifically, we are doing this in several East African countries. We are training teachers, youth, and community leaders to detect and respond to signs of radicalization in their communities.

One program we are very proud of is called "Somali Voices," where we partner with local implementers who built websites and social media platforms focused on countering messaging from extremist organizations. They have produced thirty radio programs that were broadcast nationally on a major Somali-language station. This product had very high levels of engagement on its social media platforms, with 4.8 million people reached through Facebook and a 16 percent engagement rate, and 307,000 persons on Twitter with a 36 percent engagement rate.

As I mentioned before, we are also increasingly focused on REMVE. Specifically, we are working with the U.S. Institute of Peace on a yearlong research program in partnership with the RESOLVE academic network. This focuses on foreign online REMVE communications, information ecosystems, and audiences with a particular emphasis on Europe and Australia.

Last but certainly not least, let me talk a little bit more about our technology engagement. Our incorporation [of] assessment of technologies to counter propaganda and disinformation starts by understanding the methods and capabilities that threat actors employ. This threat actor toolkit is a continually evolving set of technologies and tactics that enable the adversary to conduct propaganda and disinformation campaigns at scale. Understanding how our adversaries are seeking to promote disinformation helps us in advancing tactics and concerns, of course, to counter them. So we are looking at all the latest techniques to, for

example, uncover fake accounts and messages pushed out by bots and trolls.

As technology continues to advance, the adversarial capabilities will be augmented by technology, but we can also identify and put technology in the service of our partners. We have a number of specific programs here. Tech Demos are biweekly and are held to provide a forum for private-sector companies to demonstrate technologies applicable to the disinformation challenge. They present these to U.S. government stakeholders. We have conducted forty-nine demos of ninety-one technologies over the last two years. We also hold Tech Challenges. These are international events that provide a forum for foreign companies to demonstrate technologies that can help with the disinformation challenge in that country and can help some of our stakeholders there. We have had two of these already, one in the United Kingdom and one in Taiwan, and we have three scheduled for 2021. The GEC provides a certain amount of funding to the winner of the challenge for local implementation. Third, we maintain a Technology Testbed. This is for the use of all U.S. departments and agencies to test the operational use of promising technologies that we identify through our Tech Demos. To date, we have tested twenty-five tools, and eight of them have been integrated into U.S. government use.

To further increase connectivity among this community of interest for the U.S. government, foreign partners, industry, and academia, we maintain an online platform called Disinfo Cloud that shares findings and information on disinformation-related challenges. This platform today has almost 1,200 members and has assessed seventy tools. We work very closely with our interagency partners, such as the Department of Defense, on counter-disinformation technologies and things that can enable them. We have established a liaison in Silicon Valley with the purpose of sharing lessons learned and developing two-way communications about foreign disinformation and propaganda with our partners in the technology industry.

To summarize, the GEC today is providing significant analytic support to the interagency and to U.S. embassies globally, to inform their actions in the information space. The GEC is operating more than a hundred programs in 120 countries. It is leading U.S. and international coordination on technology implementation through our Tech Demos, our Tech Challenges, and our Technology Testbed. We are supporting multiple international coordination mechanisms to provide a framework for coordination that can be sustained over the long term. So with that, I'll pause, and I look forward to your questions.

Rethinking U.S. Counterterrorism Two Decades After 9/11

Matthew Levitt, Katrina Mulligan, and Christopher Costa

RAPPORTEUR'S SUMMARY

MATTHEW LEVITT

The U.S. counterterrorism posture of the past twenty years has been very successful in preventing attacks, but it is no longer sustainable today. Other national and international security issues demand U.S. attention and fiscal responsibility, from the Covid-19 pandemic to the economy and climate change. Accordingly, the United States must figure out how to rationalize its CT posture.

These efforts will need to be pursued at the same time that Washington grapples with great power competition. In the “4+1” framework that guides the Defense Department’s prioritization of international threats, countering terrorism remained a top priority but was placed below other goals: namely, strategic competition with China and Russia, and regional threats from Iran and North Korea. Some believe that the United States cannot engage in “peripheral” CT-rooted conflicts (e.g., Syria, Yemen) and great power competition at the same time, but such efforts should be complementary, not mutually

“Some believe that the United States cannot engage in ‘peripheral’ CT-rooted conflicts and great power competition at the same time, but such efforts should be complementary, not mutually exclusive. Small investments in bilateral counterterrorism assistance can yield important cooperation on great power issues.”

exclusive. For example, small investments in bilateral counterterrorism assistance can yield important cooperation on great power issues.

In order to move from U.S.-led, partner-enabled military CT missions to partner-led, U.S.-enabled missions, Washington will need to repair its damaged credibility abroad and demonstrate the staying power to meet its alliance commitments over the long term. There is still a need for military and other kinetic CT assistance, but the United States needs to move concertedly toward a posture that is less military-centric and more focused on civilian capacity-building. Despite successfully preventing catastrophic attacks on the homeland, the U.S. government has done poorly in getting ahead of adversaries strategically and preventing terrorists from radicalizing people. More individuals are radicalized today than on the eve of the September 11 attacks. The State Department's Counterterrorism Partnerships Fund is one good example of how officials can better provide civilian CT assistance and training.

A smaller military footprint will require greater reliance on indicators and warnings from the intelligence community. Over the past twenty years, however, the community's CT budgets have been scaffolded on top of military CT budgets, so if the armed forces shift their deployments to other regions or threats, the funding for collection platforms will follow. Policymakers therefore need to disentangle this CT funding knot to avoid losing key intelligence support in certain areas.

U.S. messaging needs a rethink as well. CT efforts should be characterized not in terms of victory or defeat, but rather as an ongoing effort in which the United States employs various tools to compete with adversaries and disrupt terrorism. By explaining that "total victory" over terrorism is neither possible nor necessary, policymakers can build public resilience for sustained CT activities.

KATRINA MULLIGAN

Conversations about refreshing the U.S. counterterrorism architecture have been going on inside government for a while, but the country as a whole has never had a conversation about what success and failure look like in the CT domain. Following 9/11, there was a national decision to prioritize the terrorism threat, and the national security apparatus and a constellation of executive branch leaders enforced that effort quite successfully. But the challenge today is that many Americans no longer have the same level of concern about the terrorism threat. So defining success and considering what resources are necessary to achieve it are crucial.

This means discussing what America is willing to accept in the CT realm, what costs it is willing to bear, and what initiatives have succeeded or failed. Not all CT investments have yielded a good return, and an honest conversation is needed on which tools are worth keeping.

As U.S. posture changes are implemented, authorities will likely see an increased desire to manage terrorism risks through intelligence indicators and warnings. Yet CT has been a disproportionate focus of the intelligence community for quite some time, so existing capacities must be increased to support any such mitigation strategy.

Policymakers do not yet know how far diplomacy development dollars could go in countering terrorism overseas, so this remains an area worth exploring and testing. Moreover, the United States now has certain tools in its kit that did not exist twenty years ago. One of them is the State Department's Global Engagement Center, which has not been used to its maximum capacity despite being stood up in the final year of the Obama administration and staffed by the Trump administration.

In the immediate aftermath of 9/11, the country spent \$260 billion on CT efforts, and it still spends around \$175 billion per year today. The government and the public need to start talking about these expenditures as part of a tradeoff conversation, because there are a lot of other things the American people want, and a lot of other priorities that affect their lives more substantially. CT funding should not be turned off, but the United States needs to think more about what it wants instead of unquestioningly and indefinitely pursuing perfect security.

“In the immediate aftermath of 9/11, the country spent \$260 billion on CT efforts, and it still spends around \$175 billion per year today. The government and the public need to start talking about these expenditures as part of a tradeoff conversation, because a lot of other priorities affect their lives more substantially.”

CHRISTOPHER COSTA

On day one of the Trump administration, four problems demanded immediate attention from incoming CT officials. In addition to a pending raid against al-Qaeda in the Arabian Peninsula, they faced a pervasive threat against commercial airliners, an ongoing campaign to defeat the Islamic State, and a pressing need to help hostages being held overseas by terrorist groups.

“The terrorism threat has indeed evolved over time, but as Washington considers how to address these changes, there is a danger of overcorrection in the CT mission.”

be used to counter malign Iranian influence. It is important to recognize that CT operations are part of a larger gray zone theater that encompasses both tactical missions and battles for influence.

This also means that the United States should not precipitously declare victories in countries like Syria, where it still has small forces on the ground collecting important intelligence and working with foreign partners. Rather, it should increase its efforts to build and cultivate different kinds of long-term partnerships with allies, especially on the issue of counter-radicalization.

“Any U.S. strategy will need to get to the heart of the grievances that fuel domestic jihadist radicalization.”

More broadly, the terrorism threat has indeed evolved over time, but as Washington considers how to address these changes, there is a danger of overcorrection in the CT mission. Pursuing great power competition does not have to be separate from smartly deploying small CT forces overseas. For example, a deployment intended for CT purposes could also

Domestic terrorism is a priority as well. The jihadist threat is still crucial because the ideology has never been satisfactorily addressed by any presidential administration. Any U.S. strategy will need to get to the heart of the grievances that fuel domestic jihadist radicalization—something America has never done very well.

As for the threat posed by white supremacists and neo-Nazis, the 2018 National Counterterrorism Strategy reinforced the importance of focusing on that issue. These dynamics are evolving, and the current administration will have to contend with domestic terrorism head-on.

Regarding reports that President Biden has ordered a review of U.S. drone strikes, every president has the right to review past policies. Under the Trump administration, the government ensured that authorities for such operations were pushed down the chain so that decisions could be made swiftly in dynamic environments, with the appropriate mechanisms in place to avoid needless casualties. The Biden administration should conduct a review, but it should not dispense with the policy, because the policy worked—it was efficient, and it was not overly bureaucratic. CT operators who work in special operations across the field were very appreciative of these policy decisions.

Finally, Washington will always face the challenge of having to work with unsavory actors that align with the United States on CT efforts. Saudi Arabia

is a tremendous partner in the CT fight, but the killing of Jamal Khashoggi is a serious concern. At the tactical level, the United States can certainly work with its foreign partners while putting appropriate safeguards in place to prevent them from stepping outside the lines.

Foreign Fighters and U.S. Policy: Tracking Mobilization Hubs to Stem the Flow

Nate Rosenblatt and Naureen Chowdhury Fink

RAPPORTEUR'S SUMMARY

NATE ROSENBLATT

Five years ago, an Islamic State (IS) fighter smuggled himself and his family out of the organization's so-called caliphate and across the border into Turkey. Before leaving his life as a member of the IS internal security division, he stole a flash drive from his superior's desk, later offering it to European authorities in exchange for immunity from prosecution. This drive contained registration forms for approximately 3,500 fighters from around the world, making it the largest cache of publicly available IS registration data.

The data is particularly valuable due to its specificity. It reveals that many foreign fighters came from localized recruitment "hubs" of varying size, ranging from individual city neighborhoods to larger regions of a country. Some of these hubs were located in major urban centers, and others were more rural, but all of them produced disproportionately high volumes of fighters. In the Middle East, hubs that comprised just 11 percent of the region's total population contributed roughly 75 percent of its foreign fighters.

The factors that drove these fighters to the jihad in Syria and Iraq varied. For many, financial incentives outweighed the risks associated with joining IS. Others believed that affiliating themselves with the organization would offer protection

from rival armed groups or local authorities. And many were likely mirroring the actions of friends and family—for example, in one hub located in the Tunis suburbs, 81 percent of documented recruits indicated that they knew at least one person who had traveled to Syria to fight. Thus, as the scope of jihadist activity expanded in both the caliphate and the hubs, the likelihood of further individuals joining IS from one of these hubs increased as well.

Similarly, the larger the hub, the more easily IS was able to recruit new members there. In many hubs, IS members or affiliated individuals dominated the local security apparatus, so residents often found that joining the organization was their safest option. This penetration also gave IS substantial insight into local personalities and grievances, enabling recruiters to compile case studies on potential fighters and select the most advantageous circumstances for making their approach.

Several notable features distinguish fighters who originated in hubs from those who did not. First, “hub fighters” were on average three years younger than other foreign fighters. Second, they were less likely to be married or have children. Third, they were half as likely to have previous experience fighting abroad.

The latter characteristic is emblematic of the serious threat posed by hubs: they are not just the main engines of recruitment during major jihadist campaigns, but also a gateway to international jihadism when such conflicts have ebbed. IS hubs pull disproportionate numbers of recruits into the ranks of foreign fighters—militants who are known to prolong and exacerbate conflicts around the world. Many of these individuals may not have a battlefield to fight on at the moment, but they still pose a threat to local populations and U.S. national security.

“Hubs are not just the main engines of recruitment during major jihadist campaigns, but also a gateway to international jihadism when such conflicts have ebbed.”

Unfortunately, current conditions in and around recruitment hubs all but ensure a future wave of foreign fighters. The deterioration of socioeconomic prospects and political freedoms in many Middle East states is worsening grievances and inhibiting citizens’ ability to speak out without fear of retaliation by the state. Additionally, the abundance of “internationalized” civil wars in the region often inspires individuals to push back against foreign invaders and view conflicts as ideological battles. Meanwhile, a widespread unwillingness to repatriate foreign fighters is creating a cadre of semiprofessional soldiers who can migrate from conflict to conflict. By abandoning their citizens who joined IS, governments are indirectly contributing to the next wave.

NAUREN CHOWDHURY FINK

Much of the international community's appetite for investing in more-effective counterterrorism strategies waned after IS lost its territorial caliphate. Yet now is the ideal time to focus attention and resources on prevention strategies instead of simply waiting for the next crisis to surface.

During peaks of terrorist violence, a great deal of attention is paid to ideology as a motivating factor, but one must also analyze the emergence of foreign fighter hubs, since they illustrate the critical role played by a fighter's community. When an individual's friends and family are involved with an extremist group, that person's access and attraction to the group are greatly affected. These affiliations and loyalties can stretch far beyond immediate, local relationships. Many fighters, particularly in the first wave following the Syrian uprising, were compelled by a sense of vicarious grievance and affinity for those in their perceived communities abroad who were coming under immense pressure. Such motivations helped draw in foreigners from countries far outside the Levant, including Western Europe and North America.

“Approximately 20 percent of foreign fighters were female. Some were indeed manipulated or forced into the journey, but others left home out of a fervent belief in the organization's cause.”

Another powerful motivator was the presence of women and children appearing to go about their daily lives in the caliphate. Such imagery helped legitimize the IS narrative that its governance was suitable not only for frontline fighters but also for their families. Approximately 20 percent of foreign fighters were female—although they are often depicted as helpless victims tricked into immigrating to the caliphate, they had just as many motivations

to join IS as their male counterparts. Some were indeed manipulated or forced into the journey, but others left home out of a fervent belief in the organization's cause. And the fact that many women have shown continued loyalty to IS even after the caliphate's collapse helps preserve the group's legitimacy.

To stem the next flood of foreign fighters, counterterrorism practitioners must first address the conditions that make recruitment hubs so conducive to extremism. Here, the United States can draw on its local and international partnerships to foster development and build resiliency. In doing so, however, officials must be careful not to further stigmatize and isolate these hubs, which often emerge due in part to past stigmatization stemming from ethnic, class, or tribal conflicts. This will require consultation with and active participation by experienced local

actors who can identify a community's grievances and earn its trust. Additionally, civil society partners can engage individuals who hold such grievances and provide them with credible pathways to action at the state or local level.

International support can complement U.S. initiatives. The United Nations and other bodies have made considerable investments in capacity building, and these efforts should be expanded to human rights and gender-sensitive security delivery. Legal cooperation is necessary as well, not only to stop the flow of fighters and bring violent actors to justice, but also to ensure that states do not abuse counterterrorism missions in order to suppress peaceful dissent.

Moreover, the same social networks that cultivate foreign fighter hubs can also be key to the solution. A tight-knit community increases the likelihood that a vulnerable individual's path to radicalization will be interrupted by a concerned friend or family member. Thus, it is essential to provide these communities with assistance when they ask for it.

Such factors also underscore the importance of repatriating foreign fighters and shifting attention to accountability and deradicalization. When states refuse to repatriate, they worsen grievances among disaffected populations and enable networks of fighters to organize in places like al-Hawl refugee camp.¹ Instead, more individuals should be permitted to return, provided they go through the appropriate risk assessment screening processes before being reintroduced to their communities. How these former IS adherents are treated by their communities and governments will not only determine their individual reintegration prospects, but also affect where and how future recruitment hubs form.

1. Ido Levy, "The Islamic State Threat in Syria Two Years After the Caliphate," PolicyWatch 3461, Washington Institute for Near East Policy, April 1, 2021, <https://www.washingtoninstitute.org/policy-analysis/islamic-state-threat-syria-two-years-after-caliphate>.

Preventing Domestic Terrorism: The DHS Approach and the New U.S. Strategy

John D. Cohen

Counterterrorism Coordinator and Senior Official Performing the Duties of the Under Secretary, Office of Intelligence and Analysis, U.S. Department of Homeland Security

In March of 2014, I sat down with The Washington Institute to conduct a Policy Forum examining the Department of Homeland Security’s countering violent extremism (CVE) programs, just one year after the horrific bombing of the Boston Marathon the previous April. Those observations I made over seven years ago serve as a helpful data point for my remarks today. After all, many of the core challenges have stayed the same, but so much more of the landscape has since changed. Now, almost six months have passed since the events of January 6 and we are just three months short of the twentieth anniversary of September 11, so this is the perfect point to take stock of what we got right, what we got wrong, and where we are heading so that we can ensure that these types of events come to an end in our country. Therefore, I welcome the opportunity to join you today to build upon those previous remarks and share with you the direction that our expanded CVE efforts are heading now and in the future.

Last week, the Biden-Harris administration released its “National Strategy for Countering Domestic Terrorism.”¹ Reflecting a detailed review of past and current aspects of the holistic response to domestic terrorism in the United States, the strategy notes that although domestic terrorism is not a new danger to citizens in the United States, it is a threat that Americans have endured far too often in recent years. This comprehensive strategy provides a nationwide framework for the U.S. government and its partners to understand and share domestic terrorism-related information; prevent domestic terrorism recruitment and mobilization to violence; disrupt and deter domestic terrorism activity; and confront long-term contributors to domestic terrorism.

The Department of Homeland Security sits at the fulcrum of the pillars of this new strategy. Rather than give you a rundown of the department's approach to implementing the strategy, I found that looking back on my remarks from 2014 offers me a way to focus a little more on what I think are the three key aspects of the strategy.

BACK TO THE FUTURE

Back in 2014, I spoke to you about the threat of terrorism. I noted that while terrorism continued to be a concern for the United States, the nature and types of terrorism were changing and, therefore, the methods and responses to terrorism also needed to adapt to the changing times and new threat landscape. At that moment, foreign threats such as al-Qaeda in Syria and other parts of North Africa continued to be major points of concern. I also noted that on top of foreign threats, the United States must deal with domestic threats. Here, much of the focus was on foreign fighters and the rising efforts of al-Qaeda to inspire attacks in the United States, much as we had just seen in the Boston Marathon attack. Through counterterrorism and information sharing efforts, we had come a long way in terms of detecting and mitigating threats abroad. However, we needed a new toolkit to do the same domestically—especially when considering the crucial importance of also upholding civil rights and civil liberties.

The solution, as I saw it then, was evident. The Department of Homeland Security and its interagency partners had crafted an approach called countering violent extremism. Focusing on communities, CVE sought to empower local efforts to prevent violent attacks using multidisciplinary approaches aligned with all stakeholders within a community, including law enforcement, religious organizations, schools, health professionals, and so forth. Much of this effort would hinge upon building stronger ties between law enforcement and the communities. I spoke about some successful examples of this approach that worked with American Muslim and Arab communities.

I also spoke about the evolving role of the internet and social media platforms and how they must be considered as an ever-increasing number of individuals were connecting to radicalization through this avenue. At that time, the online environment was largely one where we saw recruiters either inspiring attacks or encouraging travel to fight abroad. We had yet to see the rise of social media and how it would drastically change the threat of radicalization, and of course the important issue of spreading mis-, dis-, and mal-information (MDM) was still many years away.

Looking back, I would say that the themes we identified about the threat, the

“While our focus in 2014 was on foreign and predominantly Islamic violent extremist and terrorist activities, the current primary threat is an ever-evolving domestic terrorism landscape that often sees perpetrators motivated through multiple grievances.”

need for prevention, and the importance of the online space were relevant then and have remained so. Yet hindsight allows us to see that what we saw in 2014 is now far more complex and dynamic. First, while our focus in 2014 was on foreign and predominantly Islamic violent extremist and terrorist activities, the current primary threat is an ever-evolving domestic terrorism landscape that often sees perpetrators motivated through multiple grievances. Second, while in 2014 CVE efforts appeared successful, we only later learned that many stakeholders felt maligned or unfairly targeted by the CVE approach. So while prevention remains the goal, we have now shifted to a more informed public health–infused, whole-of-society approach that seeks to address concerns from all forms of targeted violence and terrorism originating from seemingly anywhere. Third, online activity has become arguably the most powerful and frequent path to radicalization to violent extremism, becoming even more so during the Covid-19 pandemic. Because of this new reality, engagements between the Homeland Security Department and tech companies have become more frequent and more varied, and social media companies are taking a more active role in addressing radicalization to violent extremism, alongside both government and civil society.

THE THREAT LANDSCAPE

While forms of violent extremism have waxed and waned over the past century and more, the recent expansion of the threat is tied to a growing list of motivations based upon a diverse set of catalysts. Today, acts of domestic terrorism pose the most lethal and persistent terrorism-related threat to the homeland. This threat encompasses a range of domestic terrorist actors, including those advancing racially and ethnically motivated extremism (REMVE) and anti-government extremists, and it is fueled by false narratives, conspiracy theories, and extremist rhetoric spread through social media and other online platforms. An array of issues motivates these individuals, including anger over Covid restrictions, the results of the 2020 presidential election, and police use of force, as well as a broad range of extreme racial, political, anti-government, anti-law enforcement, societal, and even personal ideological beliefs. The events of January 6 have only served to embolden domestic violent extremists who harbor a volatile mix

of grievances and who are continuing to seek further opportunities to incite or commit violence.

Addressing domestic violent extremism (DVE) is a top priority for the Homeland Security Department, and we are taking immediate steps to ensure all available resources are devoted to combating it. This undertaking requires nothing less than a department-wide effort, which the secretary has already initiated. Within the first thirty days of the secretary's tenure, he designated me as the senior official to organize, plan, and oversee the department's operational coordination and response to all terrorism-related threats, including those from DVEs. He also released a National Terrorism Advisory System Bulletin in late January [2021] highlighting the domestic terrorism threat. This was the first bulletin that had been issued in the past year.

In the coming months, the department intends to continue enhancing and expanding its efforts to address the DVE threat and the factors driving its growth. Together with the FBI and other members of the intelligence community, the department seeks to better understand the growing operational collaboration between domestic terrorists in the United States and those operating in Europe and other parts of the globe. Additionally, the Homeland Security Department is enhancing public awareness and resiliency to disinformation and other false narratives that are continuing to inspire domestic extremist violence. We are doing this by both updating our "If You See Something, Say Something[®]" public awareness campaign and by refreshing the Nationwide Suspicious Activity Reporting Initiative to build our partners' abilities to identify, assess, and report tips linked to potential acts of targeted violence and terrorism, regardless of ideology.

FROM CVE TO CP3

Previous countering violent extremism efforts proved ineffective and at times harmful by engendering community mistrust exacerbated by unfair targeting of Muslim, South Asian, and Arab American communities. In response to these and additional concerns from civil rights organizations and others, the Department of Homeland Security made significant changes to its approach to targeted violence and terrorism prevention.

The Homeland Security Department stands committed to enhancing our collective ability to prevent all forms of terrorism and targeted violence.² We need to make it harder to carry out an attack and reduce the potential loss of life by preventing individuals from radicalizing to violence at the earliest possible moment.³ Achieving this objective is beyond the federal government's capability and role alone. Thus, the Homeland Security Department has adopted a whole-of-society

“We need to make it harder to carry out an attack and reduce the potential loss of life by preventing individuals from radicalizing to violence at the earliest possible moment.”

approach that builds trusted partnerships across all levels of government and among a multidisciplinary set of local actors, including houses of worship, civic organizations, health practitioners, government agencies, law enforcement, and others.

The department’s prevention mission is grounded in the public health approach for violence prevention that the Centers for Disease Control and numerous aca-

ademic experts and practitioners have supported through empirical evidence and program evaluations. Recent special issues of *American Psychologist* (2017) and *Criminology and Public Policy* (2020) represent but a portion of the growing body of scholarly literature supporting the core concepts upon which targeted violence and terrorism prevention rests—specifically, the importance of locally based prevention efforts that provide help to individuals before they commit a crime or resort to violence.

Last month, the secretary created the Center for Prevention Programs and Partnerships (CP3). This development allows the Department of Homeland Security to continue to utilize and build upon the diverse set of programmatic resources establishing and expanding local prevention frameworks, while also enhancing the impact of our outreach and engagement activities with the public concerning these prevention efforts. An effective local prevention framework succeeds by connecting all segments of a community through stakeholder engagement, public awareness, threat assessment and management, and support services. Through the provision of technical assistance services, CP3 provides subject matter assistance to establish and expand local prevention frameworks. Through grants and other financial assistance, the center invests in local prevention efforts that generate promising new practices that can also serve as models or templates for replication in other localities. Finally, through education and awareness training, CP3 ensures that all stakeholders possess the knowledge needed to recognize and take steps to prevent targeted violence and terrorism.

The public health approach to the Department of Homeland Security’s targeted violence and terrorism prevention proactively places civil rights, civil liberties, and privacy concerns at the forefront of its programs. The DHS Office for Civil Rights and Civil Liberties (CRCL), Privacy Office, and Office of the General Counsel are involved in every aspect of its prevention mission. CP3 has recently enhanced its work with CRCL to increase the visibility and involvement of the department’s civil rights and civil liberties experts in all aspects of the center’s work, including by embedding CRCL experts within CP3 internal deliberations as

part of the content-creation process. To ensure this progress is made permanent, CRCL will continue to embed a senior advisor within CP3 to ensure all targeted violence and terrorism prevention programs and initiatives maintain a clear focus on the protection of civil rights and civil liberties. Additionally, CP3 has initiated a strategic engagement process focused on proactively working with civil rights and civil liberties advocacy organizations. This process will result in a multi-tiered community engagement strategy with the goal of ensuring that civil rights and civil liberties organizations are factored in as a key component in the development and implementation of local targeted violence and terrorism prevention frameworks around the country.

The other crucial element that sets CP3 apart from prior efforts is the enhancement of its programmatic activities by speaking directly to the broadest segments of the American public about prevention efforts. Through CP3, the department is seeking to ensure that all Americans know about prevention efforts addressing targeted violence and terrorism. Later this year, the Homeland Security Department will launch a national outreach and engagement campaign aimed at elevating prevention missions and addressing many of the concerns associated with previous initiatives. In addition, the department plans to launch an information clearinghouse for prevention that will allow any locality to obtain much-needed guidance about how to establish and operate local prevention frameworks. Last, CP3 continues to work alongside the Department of Justice to ensure its prevention efforts complement broader community-based violence intervention initiatives as well as the Justice Department's Diversion and Early Engagement Program.

ONLINE LANDSCAPE

While the department's focus remains on increasing local prevention capabilities nationwide, it also recognizes that a core component of this effort is empowering our partners to identify and counter the false narratives and extremist rhetoric that incite violence and are often spread through social media and other online platforms. While protecting civil rights and civil liberties, the department will continue building upon its existing efforts and collaboration with industry and non-governmental partners to identify online narratives that incite violence, and initiate efforts to prevent and impede their spread.

“While protecting civil rights and civil liberties, the department will identify online narratives that incite violence, and initiate efforts to impede their spread.”

The department works with industry partners, particularly technology companies, to develop voluntary, innovative approaches to identify and mitigate violent extremist content, as defined by their own terms of service and community standards. This includes building greater public awareness and resilience to MDM by developing and sharing digital media literacy and online critical thinking resources. All such efforts operate with appropriate oversight to ensure the protection of civil rights and civil liberties. CP3, representing the Department of Homeland Security, along with the National Security Council and other departments and agencies, engages with technology companies on counterterrorism and terrorism prevention efforts, most notably by working through the Global Internet Forum to Counter Terrorism—an NGO bringing together the technology industry, government, civil society, and academia to foster collaboration and information sharing to address online terrorist and violent extremist activity.

Another key avenue for this work can be found in our Digital Forums on Prevention. These CP3-led forums provide participants with greater awareness of online activity that radicalizes people to violence, increase digital literacy, and offer a platform for local and sector-specific leaders to engage with tech companies, practitioners, and experts to discuss innovative responses in the digital space. In March of this year, CP3 hosted a Digital Forum focused on the online gaming and e-sports industries that included nearly three hundred attendees from nongovernmental and nonprofit organizations, state and local governments, academia, and the tech sector. Participants discussed the manipulation of gaming platforms by malicious actors, and also highlighted the (positive) ways that gaming helps provide a sense of community and fosters important protective factors against radicalization to violence, particularly in times of social isolation. In June, CP3 led another Digital Forum, focused on the public health approach to prevention through the evidence-base, technology, and threat assessment and management teams. Among the more than five hundred participants were public health prevention research experts, social service providers, mental and behavioral health practitioners, nonprofits, state, local, tribal, and territorial (SLTT) agencies, and other practitioners in attendance to discuss and share knowledge on the public health approach to prevention. And in September, we anticipate hosting another Digital Forum, focused on providing resources to civil rights and civil liberties, religious, and cultural advocacy organizations to further support these essential stakeholder communities online.

Yet here again, the Department of Homeland Security needs to do more to ensure it shares information and insights about the online space with nongovernmental partners and the public. The secretary recently created an Open Source Information Working Group to facilitate operational coordination and recommend common standards and processes necessary to bridge critical gaps

in the department's ability to gather, evaluate, assess, and share relevant open source information for identifying threats and mitigating the risk of violence, consistent with legal requirements and the protection of privacy, civil rights, and civil liberties. The DHS Open Source Information Working Group will build upon lessons learned from previous efforts and will include a line of effort to advance the department's ability to identify emerging threats, including narratives introduced by foreign and domestic violent extremist actors. The working group will use open source and other publicly available information to evaluate trends and the potential for violence, and to assess the risk associated with widespread/multiplatform amplification of such narratives and other threats. The working group will likewise develop recommendations to enhance the collection, analysis, and sharing of open source threat information within the department and with external partners, and will also identify existing impediments to achieving these objectives.

CONCLUSION

One thing that has remained constant in my thinking from 2014 to today is that prevention is unequivocally a critical requirement for solving much of what I have outlined here. As the online and threat environments continue to evolve, often in a symbiotic relationship, what is clear to me is that the Department of Homeland Security and its partners need an agile, nimble, and transparent response to address the concerns of targeted violence and terrorism. The prevention programs and partnerships that CP3 are bringing to scale hold within them the promise to address these issues well before harm is inflicted upon our communities. I look forward to continuing to work with the department to ensure that this mission reaches the level of impact that our other counterterrorism missions have achieved.

“As the online and threat environments evolve, the Department of Homeland Security and its partners need an agile, nimble, and transparent response to address the concerns of targeted violence and terrorism.”

1. White House, “National Strategy for Countering Domestic Terrorism,” June 2021, <https://www.whitehouse.gov/wp-content/uploads/2021/06/National-Strategy-for-Countering-Domestic-Terrorism.pdf>.
2. In 2019, the department added “targeted violence” to its prevention mission to expand beyond terrorism. The goals of any targeted violence attack may lack a discernible political or ideological motive but inflict the same type of trauma on communities. Consequently, the Office of Targeted Violence and Terrorism Prevention works with communities to prevent these types of attacks, which include attacks on schools, workplaces, public gatherings, and other settings.
3. Radicalizing to violence can be defined as the process wherein an individual comes to believe that the threat or use of unlawful violence is necessary or justified to accomplish a goal. It is limited to the process by which individuals come to engage in terrorism or targeted violence.

U.S.-E.U. Counterterrorism Cooperation Twenty Years After 9/11

Gilles de Kerchove and Olivier Onidi

RAPPORTEUR'S SUMMARY

GILLES DE KERCHOVE

Although today's threats are often larger and more complicated than those of two decades ago, our ability to counter them has expanded exponentially. Europe and its closest partner, the United States, now have far fewer vulnerabilities due to their joint effort to share information, build state capacity, and devise creative solutions.

Their commitment to fostering an excellent information sharing environment has been particularly fruitful. For example, after the FBI gave Europol the names of over 4,500 individuals detained in northeast Syria, the list was entered into the Schengen Information System, allowing European states to identify these individuals should they attempt to cross borders. U.S. and NATO information sharing in Afghanistan has proven instrumental as well.

Still, the relationship is not without its obstacles. When addressing hate speech, differences in legislation make it difficult to reconcile freedom of expression and constitutional challenges. In particular, First Amendment protections can inhibit how the United States responds to transatlantic threats, while European states can outlaw hate speech and put substantial

“First Amendment protections can inhibit how the United States responds to transatlantic threats, while European states can outlaw hate speech and put substantial pressure on social media companies to remove such content from their platforms.”

pressure on social media companies to remove such content from their platforms. Similarly, new European legislation mandates that social media companies remove any terrorist content that has been flagged on their platforms within one hour.

Controversy also surrounds how countries have dealt with terrorism suspects, first at Guantánamo Bay and now at al-Hawl and other Syrian camps. Europe's counterterrorism leaders have long encouraged Washington to close Guantánamo and return to a normal judicial approach in the fight against terrorism. Likewise, the United States has encouraged European states to repatriate citizens who traveled to the Islamic State's so-called caliphate and are now kept in deplorable conditions in northeast Syrian camps. Given that most European Union states are unwilling to repatriate adult suspects, they have instead focused on improving camp conditions, reducing risk, and providing assistance to the Kurdish security forces that operate these camps.

Another challenge is the U.S. withdrawal from Afghanistan, which will have a major impact on the worldwide effort to stop the spread of extremism and violence in the region. The Taliban have given no sign that they will honor their pledge to halt support for al-Qaeda, leaving the door open for that terrorist organization to resurge. As the United States shifts its attention to other regions of concern, European states will be forced to adjust their burden sharing and rely more heavily on intelligence—a difficult task given that military protection on the ground is crucial for intelligence gathering.

Looking ahead to the next two decades, several priorities come into focus. First, transatlantic partners must meet the growing threat posed by right-wing violent extremism or racially and ethnically motivated violent extremism (REMVE). This includes examining the tools used to combat Islamist extremism and determining which ones can be adapted for use in fighting right-wing extremism. Partner

“The United States has fallen behind Europe in designating groups as terrorist organizations—just today, for example, the United Kingdom designated the American group ‘The Base,’ while Washington has designated just one white supremacist group, the Russian Imperial Movement.”

states also need to develop a working definition of this threat, both to establish consensus and to prevent politicization of the term. The United States has fallen behind Europe in designating such groups as terrorist organizations—just today, for example, the United Kingdom designated the American group “The Base,” while Washington has designated just one white supremacist group, the Russian Imperial Movement. Listing these groups is particularly helpful for countering extremist

financing. In Europe, far-right and neo-Nazi groups often raise funds by organizing concerts, selling apparel, and hosting martial arts events. International coordination by such actors is fairly limited, yet some states and state leaders have spread disinformation and perpetuated conspiracy theories that encourage right-wing violence across the globe.

Second, the internet clearly plays a substantial role in spreading hate speech and disinformation. European states welcomed President Biden's decision to join the Christchurch Call [to Eliminate Terrorist & Violent Extremist Content Online], and while they acknowledge that the First Amendment limits how the United States may address hate speech, they believe more needs to be done. All partners should pressure social media companies to discourage and remove hate speech and terrorist content. Such companies are hardly beacons of free speech—they rely on powerful algorithms that boost certain messages while burying others. Accordingly, they need to adjust their algorithms so that they no longer amplify illegal, extremist, and terrorist content.

Third, we must continue to combat the global spread of Islamist extremism. Since the Islamic State “caliphate” was defeated, the jihad has been “Africanized,” with IS-aligned groups and other actors wreaking havoc across multiple African states. This has forced European governments to reconsider how they invest counterterrorism funds and operate in Africa. It has also highlighted the critical importance of good governance in preventing and countering violent extremism. The significance of fighting corruption, protecting human rights, and providing basic services on the ground cannot be overstated.

Elsewhere, EU members have furthered transatlantic cooperation by cracking down on terrorist financing by Lebanese Hezbollah and designating its “military wing” as a terrorist group. In Operation Cedar, for example, French authorities took down a Hezbollah money smuggling network with support from Europol and the FBI. As the United States makes inroads in its negotiations with Iran, we hope that subsequent talks will be appropriately tough on Tehran's destabilizing activities in the region, including the use of militias.

OLIVIER ONIDI

There is no doubt that the events of September 11 have driven the transatlantic counterterrorism partnership over the past two decades. Throughout this period, it became increasingly clear that our security is collective in nature, and this intimacy of mission has reinforced our resolve in fighting

violent extremism. Common values formed the bedrock of this relationship, while differences in privacy laws, freedom of speech protections, and other legal frameworks have spurred U.S. and European officials to think critically and creatively about new ways to address problems.

This collaborative relationship has facilitated several major shared successes. The Global Coalition Against Daesh/IS oversaw the removal of Abu Bakr al-Baghdadi and the destruction of the “caliphate”; today, transatlantic partners continue to operate against emerging threats in Afghanistan and the Sahel. Crucially, such cooperation has facilitated a system of integration in which states routinely invite each other to provide insight on new counterterrorism projects, tools, and strategies.

The collection and sharing of intelligence will prove all the more critical as troops withdraw from Afghanistan and terrorist groups seek safe haven in Taliban-controlled territory. Although Western powers will no longer enjoy on-

the-ground insight there, partners can continue sharing names and aliases of identified threats. European states can then feed this information into their systems to help protect their borders.

As for white supremacism, this threat is not new, but the form it takes often is. The tools and methods developed for the fight against Islamist extremism may not

“The sharing of intelligence will prove all the more critical as troops withdraw from Afghanistan and terrorist groups seek safe haven in Taliban-controlled territory.”

always translate to this different form of extremism in which ideologies overlap, international travel is minimal, and lone-wolf actors dominate. Transatlantic partners must therefore mobilize experts to define the threat, identify groups that pose a danger, and adapt their tools accordingly. The United States and EU members each have their own violent right-wing groups to counter domestically, but the internet allows these actors to transcend borders and raise funds around the world. Many such groups continue to operate on mainstream social media platforms, where they disseminate propaganda and other galvanizing materials. In response, transatlantic partners have been proactive in sharing biometric information, deploying liaison officers, setting up joint task forces, and employing other interagency methods.

Contending with New and Old Threats: A French Perspective on Counterterrorism

Laurent Nuñez

National Coordinator for Intelligence and Counter-Terrorism, France

Thank you for welcoming me to The Washington Institute. I am very happy to be able to take advantage of my visit to the American capital to [engage in discussion] with the expert community that you represent. Washington is known for the richness of its debates, and I know our debate will be most interesting tonight.

The partnership between France and the United States in the counterterrorism fight is a historic one. We may have had varying political assessments, such as during the Iraq war in 2003, but when working for the protection of our territories and citizens, we have always stood together, as in the French reaction after 9/11 or the U.S. reaction after the 2015 attacks in France.

As you know, this is the particular context for this visit: the announcement of the AUKUS [Australia, United Kingdom, United States] military alliance on September 15 opened a very serious crisis between our two countries. Our two presidents decided that bilateral conversations should take place to resolve this crisis, and this is why I am here in Washington right now.

And so to answer your questions, I thought it was important to center my talk on four points:

1. The current terrorist threat in France, which is not particularly different from that in the rest of Europe
2. The authorities' reaction to this threat
3. The resilience of French society in the face of this threat
4. Transatlantic cooperation between France and the United States in the fight against terrorism

First, the terrorist threat in France is still very high. In 2015 in France and 2016 in Belgium, we suffered several projected attacks (i.e., foreign-directed attacks) from jihadist individuals from Syria and Iraq. Quickly, we had to prepare to stop these kinds of attacks. Today, we face a different threat—from individuals already on French soil who are isolated and act based on propaganda from the Islamic State or al-Qaeda, organizations that encourage them to act close to where they

“In 2017, we talked about ‘inspired threats,’ when people would target their national territory while ‘remotely controlled’ by IS. Today, individuals can act in a totally autonomous manner without having any contact with people from Syria or Iraq.”

live. Today, most attacks in France come from this category. In 2017, we talked about “inspired threats,” when people would target their national territory while “remotely controlled” by IS. Today, individuals can act in a totally autonomous manner without having any contact with people from Syria or Iraq. Of course, for the intelligence services, detecting these individuals is harder, because people who act close to their home, inspired by IS, radicalize themselves just before acting. They are not known to the intelligence services,

who therefore may not specifically track them. So this is the challenge that our services are facing.

This so-called endogenous threat is identical in other European countries. The projected threat is less probable, but still we must devote significant attention to it for several reasons. Information sharing between the intelligence services of these countries is so important, especially between France and the United States, because the projected threat must always be taken into account. As we know, in Syria and Iraq, the Islamic State continues to survive, although clandestinely, but it is still acting and committing attacks, likely with the intention to commit terrorist acts in Europe and elsewhere in the Western world.

Another source of concern with regard to projected threats is that certain fighters in Syria and Iraq returned to their countries of origin, where they have not necessarily been brought to justice—especially in the Balkans and the Maghreb. This has attracted much of our attention because many individuals could have returned from Syria and Iraq and stayed in these territories. We also have to be careful of potential jihadist hotbeds, such as in Syria, Iraq, or the Sahel, where al-Qaeda and IS are suffering due to French and local action but still remain, or in other hotbeds like Afghanistan and Mozambique. So we must pay attention to all these jihadist hotbeds where bases of projection can be established to direct attacks on France and Europe. This is why we must be extremely vigilant in this regard.

We talk a lot about Sunni terrorist threats and endogenous threats, but we also consider other types of terrorist threats, many of which are very well known here in the United States. We have seen terrorism coming from the ultra-right and ultra-left develop in European democracies. In the last few years, French intelligence dismantled six clandestine ultra-right cells that intended to attack democratic institutions and ultimately topple those in power. This is done for various reasons—some groups hope to replace the state, while others whose members are driven by conspiracy theories will attack a state that they believe is attacking its own population. So we see these types of groups taking a lot of power. The six dismantled ultra-right groups represent a significant number even though they concern a minority of people. The characteristics of these groups are very similar to those of groups in the United States: they start in secret with the intention to move on to more daring action, in general envisaging terrorist actions. In France, the antiterrorist prosecution office handled those cases. At the end of 2020, we dismantled an ultra-left group that intended to pursue violent terrorist action. Thus, we are paying attention to all the various terrorist threats, which is why we depend on partnerships with the intelligence services of other countries.

The second point in my talk is the system we have put in place in France to respond to the terrorist threat. This system serves to reinforce the country's intelligence services, which have seen their human, technical, and budgetary resources as well as their judiciary means increase. As for personnel, since the election of President Emmanuel Macron in 2017, the domestic services alone have recruited about two thousand people. Since 2017–18, we have increased hiring by 20 percent in the intelligence services. We have also increased our budgetary and technical resources, which expands our ability to collect information. This effort extends to all intelligence services—domestic and external, and in particular the Directorate-General for External Security (DGSE), which is under the Department of the Army.

We have also put legislative measures in place with better follow-up for people at risk of radicalizing and resorting to terrorism. We adopted a law in October 2017 that helped us end our state of emergency. This law enables us to go to people's homes when judicially authorized, in addition to taking other measures regarding individuals suspected to have violent intentions. A system of coordination between the different services was also implemented. It is my job to oversee cooperation between the services, so we asked the intelligence services to help ensure better flow of information.

In addition, since 2001 information sharing between states has increased substantially. Since 2015, this exchange has multiplied again. Today, international cooperation on counterterrorism is at a very high level, and the exchange of information is far more fluid. As far as France is concerned, we are participating in

this information exchange, and the reinforcement of counterterrorism action is also seen at the European Union level. Of course, the EU has no powers when it comes to counterterrorism, but it does have powers to furnish a number of relevant legal tools to its member states. In that framework, several regulations have been adopted that are applicable in all European countries on matters such as the carrying of weapons, the detention of explosives, and the travel of people within the Schengen Area, which enables us to track suspected and identified people.

The measures in place since 2017 have helped us prevent thirty-six Islamist terrorist attacks and, as noted, dismantle six ultra-right groups and one ultra-left group. We must stay vigilant in order to continue seeing the results I have just discussed. This increase in [authority] for intelligence services has always been proportional and has respected the [rule] of law. Thus, the intelligence services are required to undergo controls by the Senate and National Assembly. In addition, when the services establish new measures, these are overseen by an independent administration, the National Commission for the Control of Intelligence Techniques, which thoroughly reviews the measures, thus ensuring proportionality. This generally ensures that democracies do not fall into the trap set by jihadists, which could push them toward becoming totalitarian. On the contrary, all these measures are set within a legal framework, and the [oversight] of the parliamentary delegation and the National Commission have been increased.

Regarding the current terrorist threat and societal reaction to it, the challenges we face include the legal system, international cooperation, and domestic issues. We must be vigilant about projected attacks, but they are, as noted, less probable. The challenge for intelligence services today—and I believe you face a similar threat in the United States with what you call the “domestic threat” and individuals who act without having been previously identified by the intelligence services—is to be able to identify actors of whom agencies are unaware and who may act quickly and with determination. It is very important that our services jointly consider the question of how to deal with unknown individuals whose only trace is on the internet. This raises questions for us on issues such as algorithms and the contributions that platforms can have to help detect these people. For those challenges, cooperation between states is necessary. I know that several ultra-right terrorist actors in the United States were not necessarily known by intelligence services.

My third point involves the resilience of French society and Western democracies. The reality is that after every attack, we have seen the mobilization of the local population. As you know, right now, the trial of the terrorists of the November 13, 2015, attacks is underway. One of these attacks took place at the Bataclan, which is an entertainment venue. We also had attacks the same day at the Stade de France, a football stadium in Paris, and at popular eating and drinking venues.

Now, relatives of the victims are coming forward to share their [human experience], their strength, and their resilience in their testimony.

In a few days, we will commemorate the death of Samuel Paty, the history teacher who was murdered one year ago next to his high school in a terrorist attack that was very traumatic for the country. In spite of this, the French population stood together and showed its unanimous support for the education system. So I think our resilience in the face of the terrorist threat is extremely powerful. We never let it take us where it wants to take us, which is a

“I think our resilience in the face of the terrorist threat is extremely powerful. We never let it take us where it wants to take us, which is a place of hatred and division.”

place of hatred and division. Our democracies rise above these obstacles, and we owe it to the victims of terrorism to keep our determination. Right now, I want to remember all the victims of terrorism in French territory, especially with the current trial and as we prepare to commemorate the death of Samuel Paty.

Since we are discussing this attack, I would like to briefly discuss a policy we have in France that sometimes attracts confusion, especially in English-speaking as well as Muslim-majority countries. This policy aims to fight against Islamist separatism. Until 2017–18, all the measures in place targeted violent radicalization, which means trying to identify individuals who are likely to act violently and commit terrorist attacks. This measure aims to evaluate and stop these individuals. What we and the president aimed to do in 2017 was create a policy that could identify all forms of radicalization—not just those directly expressed through violence, but also those that led people to believe that religious laws supersede those of the republic. Among these views are the lack of belief in equality for women, the placement of children in schools with all-religious programs that differ from the national education program, and opposition to public services that do not comply with religious doctrine, such as those promoting different times of access to public services for men and women. Radicalization could also include infringements on the freedom of expression, which is a basic right in our democracy.

Part of the policy, which is still in place in France, aims to identify each instance of separatism—where religious law supersedes the laws of the republic and could potentially lead to reprehensible outcomes—and act upon it. We do this in part to respond to what French Muslims are asking for and in part because this form of separatism can lead to violent action. This is why I wanted to make this digression when talking about the murder of Samuel Paty. In this particular attack, he was targeted because he was at the center of a debate, raised by political Islamist movements, following a course he gave on freedom of speech, and we saw here how religious extremism can lead to the murder of an individual by

[spotlighting] the target for terrorists. The link between religious radicalization and terrorist attacks exists. And this applies to all religions, of course. Most individuals in France completely align with our republican policies that aim to guarantee freedom of expression, freedom of conscience, and individual freedom, all of which are protected by the French republic. The republic is a space for people living together, and members of a religion cannot divide it and impose their own law, and this is what we are trying to express to our population: that the principles of our republic are the strongest. Like the United States, France is a country that upholds freedom. Of course, we respect the national traditions that each country has.

To finish with my fourth point, transatlantic cooperation on counterterrorism is very [deep]. We do work together militarily with the United States. France is the second-largest contributor to the U.S.-led coalition against ISIS. This is also true in the Sahel, where France is engaged with several partners, including the United States. On top of this, we exchange a considerable amount of intelligence and cooperate at the senior level. This is true for other countries, of course, but it is particularly true between our two countries. We do not believe that this cooperation should change considerably based on the shift taking place in America. We should not devote all of our efforts to jihadists when local terrorism, like white supremacy, has also proven to be a major threat. But just because we must look inward at our own terrorism does not mean we cannot still work together internationally. These groups in North America and Europe may not work together, but they do have similar motivations, so cooperation in this fight is essential. The approach of the racist ultra-right should be explored and exploited to help our intelligence services prepare. I want to emphasize that this counterterrorism partnership must continue in order to protect our citizens, even if the acts of terrorism change.

Q&A WITH MATTHEW LEVITT

Levitt: Let's first address the elephant in the room—is U.S.-French counterterrorism security cooperation at risk of being impacted by the fallout of the AUKUS agreement and the submarine technology deal?

Nuñez: After the announcement of the AUKUS deal, there was obviously a crisis of confidence between our two countries, which France did not appreciate. It wasn't just an issue of commercial interest, but also an issue of trust and confidence in our collaborative efforts. President Biden and President Macron have

[sought] to launch bilateral discussions. We are now in this phase. We will continue to discuss in a transparent and frank fashion.

Levitt: So the United States and France see the terrorist threats facing each country slightly differently. In the United States, we're paying a lot more attention to white supremacists and other domestic violent extremist threats. And as you noted, in France the most pressing threats come from the radical jihadist milieu, even as there are also far-right and far-left threats. But I wonder, coming off the Trump administration, which wasn't so supportive of multilateral agreements, and now more recently following the Biden administration's mishandling of the Afghanistan withdrawal, if there is a bigger background and foundation for French concern about U.S. commitment to transatlantic counterterrorism cooperation, to which we've become accustomed over the years?

Nuñez: The French right-wing threat has never been neglected in France—efforts have not been aimed solely at jihadists. Jihadists have been prioritized because they pose the greatest threat to France, so it is important to stay on top of this issue. Nevertheless, right-wing groups in Europe are now getting stronger and share many of the same goals as groups in America.

They want to commit acts of violence at a massive scale. They do not appreciate institutions, they do not appreciate our government, and they do not believe that the government is there for them. As in the United States, they very quickly turn to clandestine action, which is new and did not happen in France until a couple of years ago. Of course, U.S. and French intelligence services will cooperate on this issue because it is important. We also cooperate with other states that have these issues. In France, as I mentioned in my talk, we were able to stop six ultra-right groups before they could act, but in Germany, for example, [an official] was killed, and in the United Kingdom a member of parliament was killed. We also saw what happened with the Anders Breivik tragedy in Norway.

“Right-wing groups in Europe do not appreciate institutions, they do not appreciate our government, and they do not believe that the government is there for them.”

Levitt: I'd like to follow up on your comments about what some still refer to as the “anti-separatism law.” The bill has gone through multiple name changes, of course, reflecting its sensitivity—it started off as anti-separatism and ended up as a law to reinforce republican principles. What I'd like to ask you is, what is the French government doing to make Muslim French citizens feel that this law is not targeting them, but rather reinforcing republican principles?

Nuñez: The French government works with representatives from these communities and with religious clerics. We do not want the separatism that Islamist jihadists are trying to create, and the French public, including the Muslim community, is coming to understand this goal, and they agree that they do not want to be subjected to such an extremist view. Of course, a minority feels attacked. However, our president explained in October 2020 that a segment of radicalized individuals were radicalized because the French republic was not present in areas like education, work, and the community. When this was announced, we did a lot of work with the communities, particularly in terms of urban policy, and we received a lot of support from them. Thus, we must be equal in the way we approach these communities, as we do not want to push people to become radicalized or, worse, violently radicalized. Of course, we must explain these laws, which can be complicated and difficult. But every time we have the opportunity to explain them, anywhere in the world, we take advantage of this opportunity.

Levitt: One of the most significant areas of disagreement between the United States and its European partners on counterterrorism relates to addressing extremist material on social media. It has to do with European ways of addressing privacy and America’s way of addressing First Amendment rights relating to freedom of speech. When you sit down with your American counterparts, what’s your message to them on what you would like to see America do related to the social media giants?

“We cannot be naive—part of the radicalization process, particularly for violent radicalization, happens on social media.”

Nuñez: There are multiple aspects to this question. We cannot be naive—part of the radicalization process, particularly for violent radicalization, happens on social media. Part of hate speech is also spread on social media. We have to react in a way that is clear, depending on the issue.

When it comes to counterterrorism and terrorism content, we have been working on an effort that would block content in all European countries if it is blocked in one European country. On the second issue, we must also address content that may not be considered purely terrorist material but may talk about hate, separatism, or manipulation of information. We need social media platforms to work with us in this space by self-regulating. In this way, companies can detect, moderate, and suppress messages like this. This summer, the French government adopted a law requiring social media companies to moderate certain content. Now, a similar law is being considered in the EU, the Digital Services Act. It is extremely important that social media

companies are responsible and that they remove this kind of content from their platforms. But at the same time, from an investigative point of view, we need to be able to access these platforms as quickly as possible. It is essential for the American intelligence community to help us, from a jurisdictional point of view, so that we can share information.

Levitt: Shortly before the Syrian revolution began, I was in Paris and I spoke to one of your counterparts, who told me about French Muslim teenagers who were telling their parents they were going to the South of France for spring vacation but were in fact going to Syria for a week or two. I think many people forget that there were foreign fighters flocking to Syria long before there was ISIS or Jabhat al-Nusra. Are you at all concerned about the normalization of [Syria's Bashar al-] Assad regime in terms of potential security threats to France?

Nuñez: It is true, around 2012–15 several teenagers traveled to Iraq and Syria, some supposedly for humanitarian reasons, and we realized later on that they went to fight and they became members of a terrorist organization. Right now, we do not have any additional people traveling to this area. There may be some exceptions, but most young people cannot travel to Syria and Iraq at this time. But France was very concerned about this issue—we had 1,400 young people who left France and traveled to the region, and this number was higher than that from many other European countries. But this is no longer an issue.

“It is true, around 2012–15 several teenagers traveled to Iraq and Syria, some supposedly for humanitarian reasons, and we realized later on that they went to fight and they became members of a terrorist organization.”

Levitt: One of our participants asks a bit of a historical question. At the height of ISIS in Syria, let's say 2014–16, what do you think was the relationship between ISIS and the Assad regime? Was the Assad regime in any way helping ISIS, doing business with them, releasing prisoners, et cetera?

Nuñez: I cannot answer this question, which is outside my area of expertise. What I can say is that between 2014 and 2016, all the intelligence services knew that ISIS was a terrorist group wanting to commit terrorist attacks. There was no ambiguity on what Daesh was. I will not answer on the link with the Assad regime.

Levitt: Following the withdrawal from Afghanistan, can you assess the external

terrorism threat you see emerging from there after the Taliban takeover? In your view, is it likely that we will see the reemergence of al-Qaeda in Afghanistan with the intent of carrying out attacks against the West?

Nuñez: The problem that the Taliban in Afghanistan creates for intelligence services all over the world and their fight against terrorism is related to four different problems that I believe we are all facing, and this is why we absolutely need a strong partnership with America and other Western actors. The first problem is: will the fact that the Taliban is now in charge of Afghanistan mean that it will invite people to come and train to become jihadists, like we were just discussing about Iraq and Syria between 2012, 2013, and 2014? In France, we believe this will not be a major issue for us and will not concern French citizens, as there is no longer ease of access or organized networks, but we have to remember that between 1996 and 2001, about a hundred young Frenchmen went to fight with al-Qaeda in Afghanistan. That was the first time something like this happened.

The second problem is that we must figure out if people arriving in France from Afghanistan can be properly screened and assessed.

The third problem is that parts of the Taliban will be unable to stop some members of al-Qaeda, ISIS, or Wilayat Khorasan [the name for the ISIS branch in Afghanistan] from reinstalling themselves in remote areas. Will these cells be able to prosper? We do not know if the Taliban can stop these kinds of groups from resetting in this country. As we know, Wilayat Khorasan has already conducted attacks in Afghanistan, and we don't know how the new Taliban state can address this. Thus, the risk grows larger if they cannot resolve this issue.

The fourth point, of course, is that they've finally created a state. Is it possible to inspire young people from European countries to commit attacks because they are galvanized by the fact that we left Afghanistan? This has not happened, but we are vigilant.

These are the four points that we have to deal with now that the United States and Europe have left Afghanistan. These are not minor problems, so the French intelligence services, both external and internal, are paying attention to them and are working very closely with all of their partners.

Levitt: When the Biden administration explained the decision to withdraw from Afghanistan, one point it made is that there are more pressing venues where terrorism is happening today, pointing in particular to Africa. France, of course, has been very active in counterterrorism in Africa. So I'd first like to ask you how you perceive the nature of the terrorist threats from Africa, both to French interests in Africa and to France itself back home?

Nuñez: France intervened in Mali in 2013 to prevent the state from being lost to jihadist terrorists, and we stayed in the Sahel with what we call the Barkhane group. France has remained in this area and is adapting its presence because, you are correct, al-Qaeda still exists there. There are multiple groups that feel they can gain territory and create a caliphate there, but with local and European allies, we are trying to eradicate these terrorists. This won't happen with military action alone. We work with local states to help them establish local jurisdiction, reaffirm the rule of law, and apply their sociopolitical approach to tribes and citizens in the various territories affected by the growth of al-Qaeda. It is true that we have had considerable success in this area, and we should recognize this. In particular, we neutralized the leader of the Islamic State in the Sahel [Adnan Abu Walid al-Sahrawi, killed in August 2021], and we should emphasize that we are working very hard to counter terrorist groups in these territories.

Levitt: In your remarks, you spoke about a range of terrorist threats, not just Sunni extremism but far right and far left. I'd like to ask you about Shia extremist groups as well. To start, can you speak about how you see the threat of Iranian state terrorism in Europe and France in particular, especially coming off the plot targeting the Mujahedin-e Khalq conference in Paris?

Nuñez: This is very confidential, so it is not something I can express right now. I cannot add any comments, but we are being vigilant on all forms of terrorism and paying close attention to this issue. In particular, this has been dealt with by a Belgian court. There was an attack plot in Villepinte, France, in June 2018. We were able to stop this attack, and the issue was addressed in Belgian court.

Levitt: So talking in detail about Iran is a little too sensitive. Let's talk for a second about Lebanese Hezbollah, which appears to still be active in Europe, including France. Of course, France participated in a very significant way in Operation Cedar, leading to the conviction of a Hezbollah operative in French court. In 2010, a Lebanese French professor in Lyon rented a safe house in Cyprus where Hezbollah was found to be storing ammonium nitrate. And we heard from the previous administration here that Hezbollah was moving ammonium nitrate through Europe, including through France. What is your sense of the threat from Hezbollah in France?

Nuñez: It is true that France and the United States have sometimes held different positions, especially when qualifying the different branches of Hezbollah—I know you are a specialist on the topic. I can't answer your question directly due to

confidentiality, but French services are interested in all forms of terrorism, and we take all information seriously. No information is left aside, and the French services are always motivated and focused on these questions. There are some things I cannot say or discuss, but you can be assured that we are very focused, as you can see by the June 2018 case discussed earlier.

A European Perspective on Counterterrorism

Ilkka Salmi

Counterterrorism Coordinator, European Union

It is an honor and a pleasure to speak at the start of this important conference. Many thanks to The Washington Institute for inviting me, as a European friend of the United States, to present a European perspective on counterterrorism.

The Institute has chosen this topic following the Biden administration's recalibration of America's global counterterrorism policy and a shift from military action to the use of civilian counterterrorism tools. This shift aligns the United States more closely with the European Union's approach to counterterrorism.

To be sure, the EU does recognize that military action is sometimes necessary to fight terrorist groups. Over the last twenty years, EU member states have frequently supported American use of force to fight terrorist groups worldwide, politically and militarily. France has taken the lead in a military operation to fight terrorists in the Sahel region, with strong American support. Yet the EU and its member states emphasize a preventive and law enforcement approach to counterterrorism across the globe.

I agree with President Biden that kinetic action should be an occasional last resort. Where there is no armed conflict, terrorists should be investigated and arrested by law enforcement, and then tried in a court of law, in full compliance with internationally recognized human rights standards. Violations of those standards do not just undermine our values, but they are also counterproductive from a CT perspective, as they will breed resentment against our democratic model of governance and feed terrorist propaganda.

“As the threat grows more diverse, military force may become less effective in countering terrorism.”

As the terrorist threat grows more diverse, military force may become less effective in countering terrorism. Sophisticated weaponry and high-tech detection tools are useless when we are facing lone actors who prepare their attacks without any direct assistance from terrorist organizations. In fact, in the West, none of the terrorist attacks in the last five years were perpetrated by Daesh or al-Qaeda themselves. Lone actors or small, unorganized groups, often inspired by Daesh or al-Qaeda, were responsible for each attack.

Moreover, prevention policies, law enforcement, and judicial action are the only ways to fight the growing threat of right-wing violent extremism and terrorism. Right-wing extremists and terrorists are increasingly internationally connected, aggravating the threat they pose, but there are no global right-wing terrorist organizations to fight with force of arms.

Since 9/11, we have not been winning the fight against terrorism. Islamist extremist ideology remains strong, and both the United States and European Union need to do much more to curb its spread. It transforms societies; for example, in the Sahel it has a negative impact on fundamental rights, underpins movements such as the Taliban, and contributes to radicalization.

EU ACTION

The European Union is eminently well positioned to use its financial means and

political leadership to combat terrorism with rule of law-based approaches. This is where it is able to complement and reinforce the action taken by its member states and strategic partners.

“At home, the EU is assisting its member states in a vast array of policy areas, ranging from border security to the removal of terrorist content online. Its tools to prevent terrorism include the Radicalisation Awareness Network, which pools expertise from across the EU to assist practitioners such as teachers, police officers, social workers, and prison wardens in dealing with instances of radicalization they encounter in their daily work.”

Let me highlight a number of the non-kinetic tools the EU is using to counter terrorism. At home, the EU is assisting its member states in a vast array of policy areas, ranging from border security to the removal of terrorist content online. Its tools to prevent terrorism include the Radicalisation Awareness Network, which pools expertise from across the EU to assist practitioners such as teachers, police officers, social workers, and prison wardens in dealing with instances of radicalization they encounter in their daily work.

Externally, the Union leverages its very significant development assistance to help partner countries prevent radicalization and fight terrorism more effectively. According to the Organisation for Economic Co-operation and Development, the EU institutions and member states combined account for a majority of official development assistance worldwide, surpassing the United States by a wide margin. The EU institutions have, over the last five years, vastly expanded their assistance to enhance rule of law–based counterterrorism and counter-radicalization capacities. They are now funding external projects with a total budget of about 500 million euros. This is in addition to the EU’s support to various forms of military action through the African Peace Facility, including the G5 Sahel Joint Force, the African Union mission in Somalia, and the Multinational Joint Task Force against Boko Haram.

Of the EU’s assistance to counter terrorism, prevention of radicalization accounts for about 40 percent, covering a range of issues such as extremism among youths, empowering women, promoting community dialogue, strengthening local actors, and working with media to foster resilience to radicalization. Furthermore, about 25 percent of our external CT assistance is spent to strengthen the criminal justice response to counter terrorism, 15 percent to security-sector reform, 8 percent to reinforce border security, and another 8 percent to countering the financing of terrorism.

The development of the terrorist threat in Africa is particularly worrying, with ever-larger parts of the continent being destabilized by the presence of Daesh- and al-Qaeda–affiliated terrorist groups. Experts now use the expression “Africanization of jihad.” Hence, the EU focuses its CT assistance on sub-Saharan Africa in addition to its own immediate neighborhood.

Another continuing source of concern is the situation in the camps and prisons in northeast Syria, where thousands of former Daesh fighters and their families are held. The humanitarian situation there is dire, and the control by the Kurdish militias sometimes tenuous. While there is an ongoing debate in Europe on repatriation, it should be noted that the majority in both camps and prisons are actually Syrian and Iraqi nationals. Radicalization of youth could contribute to lasting destabilization of the region and forms a ticking time bomb for our security. EU member states encourage the EU to:

- Step up its assistance to youth in rehabilitation centers and security custody
- Improve humanitarian conditions in the camps
- Increase psychosocial, educational, and other support in the camps
- Contribute to the decongestion by supporting reintegration of Syrian

nationals in communities in northeast Syria

- Buttress a possible future agreement between the Iraqi government and the United Nations on repatriation and reintegration of Iraqis in their communities

This is in support of the work and objectives of the anti-Daesh coalition.

The European Union is also a staunch supporter, politically and financially, of the UN framework for counterterrorism. The UN does indispensable work, and support to the UN is a longstanding pillar of our international engagement to counter terrorism.

LOOKING AHEAD

The EU has started to address Islamist extremist ideology with an evidence-based dialogue with partners in the Gulf who also want to turn the page and studies related to the spread of fundamentalist Islam in the Sahel, which now need to be followed up with action. As the United States is also working on these issues, it would be important to join forces. It would also be important to focus more on creating opportunities for youth. Inspired by the U.S. Stevens Initiative, the EU set up a virtual Erasmus Programme allowing students from Europe and Middle East and North Africa countries to follow classes together.

If there is one area in which urgent action is needed from the United States and the EU, it is regarding the internet. It is beyond dispute, for instance, that in parts of the developing world, such as India, Myanmar, and Ethiopia, hate speech and disinformation posted on Facebook have sparked communal violence that led to hundreds of casualties.

“Social media companies use algorithms to amplify often extreme postings at the expense of others, thus influencing the exercise of free speech. Hence, they are publishers rather than platforms.”

The EU has finally started to regulate social media, while the U.S. Congress is also debating proposals to make social media companies accountable for harmful or illegal content. One thing is clear: social media [apps] are not mere platforms on which members of the public can post content. Social media companies use algorithms to amplify often extreme postings at the expense of others, thus influencing

the exercise of free speech. Hence, they are publishers rather than platforms. This should have consequences for the way in which society holds them to account.

To wrap up: the United States is the EU's most important external partner. The United States and the EU have developed a deep and enduring cooperation on counterterrorism, including dialogue at all levels. This includes separate dialogues in the areas of homeland security (where right-wing extremism and terrorism have gained increasing prominence) and external affairs. The EU and United States also work closely together in the Global Coalition Against Daesh/IS, the Global Counterterrorism Taskforce [Counter-Terrorism Implementation Task Force], and the Global Counterterrorism Forum.

Cooperation makes the United States and the EU much stronger, not just because we exchange information and work together, but also because we inspire each other and learn from each other's successes and failures. In providing civilian assistance to partner countries across the globe, our tried-and-tested mechanisms for mutual cooperation enable us to supplement each other's activities. As the United States focuses more on civilian assistance and non-kinetic CT tools under the Biden administration, these synergies become even more important.

Evolving Counterterrorism Priorities and Policies

Christopher Landberg

*Acting Principal Deputy Coordinator, Bureau of Counterterrorism,
U.S. Department of State*

Thank you to The Washington Institute and particularly to Matt Levitt for organizing this event. Many of you have been deeply involved in counterterrorism efforts over the years, and I look forward to hearing your views about today's challenges.

After twenty years—post-9/11—of designing and implementing a national security structure focused on counterterrorism, it is a good time to assess what we have accomplished and how counterterrorism priorities and policies are evolving. This is especially true as the global terrorism landscape also continues to evolve and as we face other strategic priorities, such as countering challenges from China and Russia, and cybersecurity risks.

TERRORISM TRENDS AND THREAT PICTURE

As counterterrorism practitioners, we need to recognize this constant, fast-moving evolution, and we must adapt and calibrate our approaches to account for the much more complex operating environment. There are a few overarching themes and trends to consider when assessing today's threats:

- Our intensive national and international focus on counterterrorism since 2001 has made it much more difficult—albeit not impossible—for terrorists to pull off an attack on the U.S. homeland on the scale of 9/11.

- Terrorists are rapidly expanding to new regions plagued by lack of security and weak governance, often exploiting and leveraging local grievances and mixing with criminal elements to create a toxic mix of terrorism, organized crime, narcotics trafficking, illegal mining, and other illicit activities.
- Terrorist tools and tactics are always evolving, often in response to effective counterterrorism pressure. For example, we see terrorists shifting from large-scale, mass-casualty attacks to use of more low-tech but still lethal tools.
- Finally, terrorists of all types are effectively using the internet, especially social media platforms, to inspire and radicalize individuals to act alone in conducting attacks, which can be far more challenging to detect beforehand.

I'll make a few comments on how we see the threat environment.

ISIS's global presence has proved to be far reaching, despite the D-ISIS coalition's [Global Coalition Against Daesh/IS's] complete liberation of the physical territory ISIS once controlled in Iraq and Syria. We are deeply concerned about the thousands of foreign terrorist fighters and their associated family members who remain detained in Syria and Iraq. This is not a sustainable situation, and we continue to address it as a top priority. These individuals need to be repatriated—and, depending on their specific circumstances, either prosecuted or rehabilitated and reintegrated—otherwise, they will contribute to a new generation of terrorists.

Al-Qaeda and its affiliates also remain an enduring threat despite significant leadership losses. We are concerned about the expansion of both ISIS and al-Qaeda branches and networks in Africa and elsewhere in the past several years, as these affiliates are exploiting undergoverned spaces, conflict zones, and security gaps, adding to rising instability in many regions and raising concerns about external operations plotting.

Iran remains the major state sponsor of terrorism, providing funding and direction to a range of terrorist partners and proxies. Iran continues to engage in a wide array of destabilizing activities in the Middle East and beyond. We are also grappling with the growing transnational threat from racially and ethnically motivated violent extremist (REMVE) actors. White supremacist, anti-government, and like-minded individuals and groups are connecting across borders to target their perceived adversaries. Finally, the decision to withdraw troops from Afghanistan requires new thinking on how we will address terrorist threats that emanate from that country. This includes threats from [the Islamic

State–Khorasan] today and a potential reconstitution of al-Qaeda’s core’s operational capabilities in the future.

While this may present a daunting threat picture, we and our partners have made tremendous progress over the last twenty years. The list is extensive, but this recounting is by no means exhaustive.

- We have sharply degraded and continue to pressure ISIS and al-Qaeda leadership and affiliates and have also mobilized our allies to increase pressure on Hezbollah, al-Shabab, and other similar groups.
- We have reshaped the international counterterrorism architecture, creating overlapping layers of information sharing, watch-listing, screening, and vetting to dramatically improve aviation and border security.
- Since 2001, the United States has designated hundreds of individuals and entities as terrorists, and we have assisted partner governments to effectively implement international standards against terrorist financing.
- We are deploying foreign assistance to strengthen partnerships, increase global information sharing, and build civilian capacity in CVE, threat finance, border security, and law enforcement finishes (investigation, arrest, prosecution, and incarceration), all aimed at countering evolving terrorist threats, preventing the spread of violent extremism, and reducing the need for U.S. military boots on the ground.

COUNTERTERRORISM AT A CROSSROADS

As we look to the next twenty years, the Biden-Harris administration is strengthening the foundation of policies and principles that will guide our work moving forward. We are working to keep pace with the changing landscape by remaining clear-eyed about current and emerging threats and by integrating our global counterterrorism efforts into the broader range of national security threats and challenges. The administration has called for a greater investment in tools and capabilities to avert threats before they become imminent.

The result is we are in the middle of a major shift from a heavy reliance on a Defense Department–led counterterrorism approach, which emphasized so-called kinetic activity and the U.S. military directly removing terrorists from the battlefield, to an approach that prioritizes diplomacy, international and local partnerships, and civilian-led capacity building. This approach will put greater emphasis on law enforcement and the rule of law and is one where efforts to limit terrorist radicalization and recruitment will take on increased importance.

To respond to threats as they develop, we need a sustainable approach flexible enough to detect, identify, and respond to threats before they reach the United States or our allies and partners. We also need to keep our eyes on, and invest in, preventing the proliferation of the next generation of recruits before they start joining or supporting terrorist groups—or committing lone terrorist acts.

At the same time, we must be realistic about diminishing resources for our counterterrorism efforts, especially as more attention is devoted to other pressing national security issues, such as recovering from the Covid-19 pandemic, addressing climate change, countering cybersecurity challenges, or managing China and Russia's increasingly aggressive activities.

Burden sharing with international allies—such as we are doing with the eighty-three-member global D-ISIS coalition, probably the most successful multilateral platform ever assembled to combat terrorism—will become even more important to build the capabilities of frontline partners. Thanks again for hosting me, and I look forward to hearing the comments from [Jill Rose, deputy director of the Justice Department's Office of Overseas Prosecutorial Development, Assistance, and Training].

Building Civilian Counterterrorism Capacity: OPDAT's Role

Jill Rose

Deputy Director, Office of Overseas Prosecutorial Development, Assistance, and Training, U.S. Department of Justice

The Office of Overseas Prosecutorial Development, Assistance, and Training is the primary foreign capacity-building component of the Department of Justice. There are a total of around sixty resident and intermittent legal advisors and international cyber specialists posted at U.S. embassies around the

globe. Approximately one-third of those resident legal advisors (RLAs) are focused on counterterrorism/counterterrorism funding. The remaining two-thirds have a varied portfolio addressing corruption, [anti-money laundering], transnational criminal organizations, trafficking of humans, cyber, and intellectual property/counterfeit goods movement, among other issues.

“There are around sixty resident and intermittent legal advisors and international cyber specialists posted at U.S. embassies around the globe.”

The State Department is the primary funder for the Justice Department's legal advisor positions—we also have some Defense Department funding for DOJ legal advisors at specific commands—and it is through interagency agreements that the work plan and focus of each of these positions is determined.

In all circumstances, regardless of the funding source or the focus of the interagency agreement, we are working closely with our foreign justice-sector counterparts to build capacity and to implement change affecting national security—both that of our partners and, of course, ourselves.

How specifically does OPDAT do this? Two important ways:

Presence. As members of the interagency, we sit in the embassy and work closely with our State Department colleagues to ensure that we are focused, within our specific funding mandate, on areas of importance as set forth in the Integrated Country Strategy. Presence provides a number of benefits to our capacity-building programming:

- We are able to build meaningful, long-term relationships with our important interlocutors. The significance of relationships of trust and confidence cannot be understated—particularly as we engage with case-based mentoring with many of our prosecutive partners, whereby we offer expertise and advise on best practices to ensure successful outcomes. We also work with foreign law enforcement partners to help them understand the importance of the investigation to a successful prosecution, and with foreign judges on evidentiary and sentencing considerations in terrorism cases.
- Another benefit of presence or proximity is that most RLAs sit as members of the Embassy country team, and this offers real insight into the issues of the day or week; thus, we are able to quickly address specific and emerging concerns. This presence, or proximity, and coordination among the interagency have been emphasized in this Administration as an important approach to Counterterrorism capacity building as they recognize that those at Post have the best insight into the problem set.
- We are in situ and therefore we are nimble—we can be immediately responsive. Because of the existing relationships and because we partner with our law enforcement colleagues who are also at post, we can respond very quickly to evolving circumstances. I would like to share a recent example from Kosovo. As a result of a months-long operation—enabled by CT-funded programs implemented by the Justice Department and [the Diplomatic Security Service's Antiterrorism Assistance Program]—five arrests were made along with a massive seizure of material evidence, including automatic weapons, drones, rocket grenade launchers, tens of thousands of rounds of ammunition, explosives, and more than US\$28,000 in cash. The alleged terrorists, who were in direct communication with ISIS, were planning an imminent attack in Kosovo. The months of planning and use of covert measures and surveillance were authorized by a prosecutor who received extensive mentoring from the Justice Department RLA based in Tirana [Albania], and the law enforcement components received equipment and training from the Antiterrorism Assistance Program. This operation is a great example of how a comprehensive capacity-building program can create effective counterterrorism law enforcement teams that deliver real-world results.

Expertise. The second way we are working closely with our foreign justice-sector counterparts to build capacity and implement change affecting national security is through expertise and “reach-back.” By deploying current Justice Department lawyers—either assistant U.S. attorneys or “main justice” component attorneys—we are sending the most up-to-date legal, prosecutive expertise into the world. Our legal advisors are active prosecutors who not only are current on the legal issues, process, and procedures, they are also experienced litigators who can quickly spot evidentiary or procedural concerns whether in a common law, adversarial, or civil law system.

What is meant by reach-back? We, as current Justice Department lawyers, can access the myriad resources within the department. Our partners in the National Security Division, the Money Laundering Asset Recovery Section, Public Integrity, Computer Crimes, and the Office of International Affairs all support our capacity-building efforts and have the ability to be operational when necessary. And, of course, our law enforcement partners in the federal government also assist with capacity building.

A few notes about our broad global programs funded by [the] State [Department’s Bureau of] Counterterrorism. Our global CT programs focus on defined problem sets. Each year—Covid interruptions excepted—we along with our State and other Justice Department partners convene a Lebanese Hezbollah-focused Law Enforcement Coordination Group to discuss lessons learned from recent law enforcement actions, prosecutions, updates on sanctions, and other areas. This event usually brings together practitioners from approximately thirty countries and has resulted in new relationships that have netted positive operational results. We also have other Hezbollah-focused programs in targeted areas, where we work closely with foreign partners to build their capacity to address Hezbollah’s financing and activities.

A second global program is related to foreign terrorist fighters. OPDAT RLAs in critical locations are working with our foreign partners to build capacity on the complex legal frameworks surrounding the prosecution of returning foreign terrorist fighters and the use of collected enemy material, aka battlefield evidence, in trials of these terrorist fighters. For example, we have had tremendous success

in the Balkans, where OPDAT-mentored prosecutors have prosecuted more than 150 foreign terrorist fighter (FTF) cases. As a result of our case-based mentoring and capacity-building programs, the average sentence [length] in the Balkans has doubled. We attribute this to five factors on which we have focused with our partners:

“We have had tremendous success in the Balkans, where OPDAT-mentored prosecutors have prosecuted more than 150 foreign terrorist fighter cases.”

- Improved use of battlefield evidence in proceedings
- Improved use of evidence gathered from digital device searches
- Improved legal writing
- Improved trial advocacy to educate courts about the dangers of terrorism and foreign terrorist fighters
- Use of creative charging decisions

We also have a new project working with specific North African partners to build their capacity to use battlefield evidence as a source for investigative leads and, of course, the use of critical evidence in FTF prosecutions. Finally, we are leading a global forum to address racially and ethnically motivated violent extremism (REMVE).

I will leave it at this: Much remains to be done. We must constantly make new inroads with our foreign partners because of the diverse and diffuse nature of today's terrorists.

Addressing the Threat from Homegrown and Foreign Terrorist Organizations

Patrick Reddan Jr.

Deputy Assistant Director, FBI Counterterrorism Division

Preventing terrorist attacks, from any place, by any actor, remains the FBI's top priority. The nature of the threat posed by terrorism—both domestic and international—continues to evolve.

The greatest terrorism threat to our homeland is posed by lone actors or small cells who typically radicalize online and look to attack soft targets with easily

accessible weapons. We see these threats manifested within both domestic violent extremists (DVEs) and homegrown violent extremists (HVEs), two distinct threats, both of which are located primarily in the United States. The FBI describes individuals who commit violent criminal acts in furtherance of social or political goals stemming from domestic influences—including racial or ethnic bias, or anti-government or anti-authority sentiments—as DVEs, whereas HVEs are individuals who are inspired primarily by foreign terrorist organizations (FTOs) but are not receiving individualized direction from these organizations.

“The greatest terrorism threat to our homeland is posed by lone actors or small cells who typically radicalize online and look to attack soft targets with easily accessible weapons.”

accessible weapons. We see these threats manifested within both domestic violent extremists (DVEs) and homegrown violent extremists (HVEs), two distinct threats, both of which are located primarily in the United States. The FBI describes individuals who commit violent criminal acts in furtherance of social or political goals stemming from domestic influences—including racial or ethnic bias, or anti-government or anti-authority sentiments—as DVEs, whereas HVEs are individuals who are inspired primarily by foreign terrorist organizations (FTOs) but are not receiving individualized direction from these organizations.

Domestic and homegrown violent extremists are often motivated and inspired by a mix of sociopolitical, ideological, and personal grievances against their targets, and continue to focus on accessible targets, to include civilians, houses of worship, retail locations, and mass public gatherings. Selecting these types of

soft targets—in addition to the insular nature of their radicalization and mobilization to violence and limited discussions with others regarding their plans—increases the challenge faced by law enforcement to detect and disrupt the activities of lone actors before they occur. Some violent extremists have also continued to target law enforcement and the military as well as symbols or members of the U.S. government.

The top threats we face from DVEs are from those we categorize as racially and ethnically motivated violent extremists and anti-government or anti-authority violent extremists. While REMVEs who advocate the superiority of the white race were the primary source of lethal attacks perpetrated by DVEs in 2018 and 2019, anti-government or anti-authority violent extremists—specifically, militia violent extremists and anarchist violent extremists—were responsible for three of the four lethal DVE attacks in 2020. Notably, this included the first lethal attack committed by an anarchist violent extremist in more than twenty years.

Consistent with our mission, the FBI holds sacred the rights of individuals to peacefully exercise their First Amendment freedoms. Regardless of their specific ideology, the FBI will aggressively pursue those who seek to hijack legitimate First Amendment-protected activity by engaging in violent criminal activity such as the destruction of property and violent assaults on law enforcement officers. The FBI will actively pursue the opening of investigations when an individual uses—or threatens the use of—force, violence, or coercion in violation of federal law and in the furtherance of social or political goals.

“The FBI will aggressively pursue those who seek to hijack legitimate First Amendment-protected activity by engaging in violent criminal activity such as the destruction of property and violent assaults on law enforcement officers.”

The FBI assesses HVEs are the greatest, most immediate international terrorism threat to the homeland. As I have described, HVEs are located and radicalized primarily in the United States and are not receiving individualized direction from FTOs but are inspired largely by the Islamic State of Iraq and al-Sham (ISIS [aka Islamic State, IS]) and al-Qaeda to commit violence. An HVE’s lack of a direct connection with an FTO, ability to rapidly mobilize without detection, and frequent use of encrypted communications pose significant challenges to our ability to proactively identify and disrupt them.

The FBI remains concerned that FTOs such as ISIS and al-Qaeda intend to carry out or inspire large-scale attacks in the United States. Despite its loss of physical territory in Iraq and Syria, ISIS remains relentless in its campaign of violence against the United States and our partners—both at home and overseas. ISIS

continues to aggressively promote its hate-fueled rhetoric and attract like-minded violent extremists with a willingness to conduct attacks against the United States and our interests abroad. ISIS's successful use of social media and messaging apps to attract individuals seeking a sense of belonging is of continued concern to us. Like other foreign terrorist groups, ISIS advocates lone offender attacks in the United States and Western countries via videos and other English-language propaganda that has at times specifically advocated attacks against civilians, the military, law enforcement, and other government personnel.

Al-Qaeda maintains its desire to both conduct and inspire large-scale, spectacular attacks. Because continued pressure has degraded some of the group's senior leadership, in the near term we assess al-Qaeda is more likely to focus on cultivating its international affiliates and supporting small-scale, readily achievable attacks in regions such as East and West Africa. Over the past year, propaganda from al-Qaeda leaders continued to seek to inspire individuals to conduct attacks in the United States and other Western nations.

“Lebanese Hezbollah, Iran’s primary strategic partner, continues to conduct intelligence collection, financial activities, and procurement efforts worldwide to support its terrorist capabilities.”

Iran and its global proxies and partners, including Iraqi Shia militant groups, continue to attack and plot against the United States and our allies throughout the Middle East in response to U.S. pressure. Iran's Islamic Revolutionary Guard Corps—Qods Force continues to provide support to militant resistance groups and terrorist organizations. Lebanese Hezbollah, Iran's primary strategic partner, has sent op-

eratives to build terrorist infrastructures worldwide. Hezbollah also continues to conduct intelligence collection, financial activities, and procurement efforts worldwide to support its terrorist capabilities. FBI arrests in recent years of alleged Iranian and Hezbollah operatives in the United States suggest the government of Iran and Hezbollah each seek to establish infrastructure here, potentially for the purpose of conducting contingency planning. Qods Force commander Esmail Qaani and Hezbollah secretary-general Hassan Nasrallah have each threatened retaliation for the death of QF commander Qasem Soleimani.

As an organization, we continually adapt and rely heavily on the strength of our federal, state, local, tribal, territorial, and international partnerships to combat all terrorist threats to the United States and our interests. Our mission to mitigate terrorist attacks is further empowered by the private sector—it is essential to our understanding of the threat. Continued dialogue and working partnerships allow us to create trust, broaden the scope of the relationship, and deepen our commitment to working together. Ideally, we can create a flow of information

that runs both ways. Most importantly, it helps us develop a level of trust and confidence to communicate when or—better yet—before the threat of a terrorist attack arises. Having that relationship in place in advance of an incident is key to mitigating the threat. To that end, we use all available lawful investigative techniques and methods to combat these threats while continuing to collect, analyze, and share intelligence concerning the threats posed by violent extremists, in all their forms, who desire to harm Americans and U.S. interests. We will continue to share intelligence and encourage the sharing of information among our numerous partners via our Joint Terrorism Task Forces across the country, and our legal attaché offices around the world.

The work being done by the FBI is demanding, and we cannot afford to become complacent. We must continually seek out new technologies and solutions for the problems that exist today, as well as those on the horizon. We must build toward the future so that we are prepared to manage risk and deal with the threats we will face at home and abroad by understanding how those threats may be connected. To that end, we gather intelligence, consistent with our authorities, to help us understand and prioritize identified threats, and to determine where there are gaps. We must stay ahead of the threats we face, working with our partners to close those gaps while continuing to learn as much as we can about the threats we face today, and those we may face tomorrow.

Thinking Through Non-Kinetic Counterterrorism Tools

Robert Jenkins

*Assistant to the Administrator, Bureau for Conflict Prevention and Stabilization,
U.S. Agency for International Development*

Violent conflict can threaten stability or hinder development in countries around the globe. USAID’s mission of promoting peaceful, prosperous societies and responding to humanitarian emergencies may be jeopardized unless we elevate our role in preventing violence and resolving conflicts. We know that foreign assistance dollars alone cannot resolve the complexity of violent conflict. By providing support to locally driven solutions, USAID positions itself alongside the U.S. Department of State’s diplomatic efforts and the Department of Defense’s security-driven mission as a team to work with other countries and donors on shared objectives, while partnering with the private sector and nongovernmental groups worldwide

The USAID Bureau for Conflict Prevention and Stabilization (CPS) was created to elevate the agency’s work in countries affected by conflict and violence. Agility is at the heart of CPS. We strive to move at the *speed of relevance and offer imperfect solutions to intractable problems*. CPS does this by providing rapid, flexible

options and expertise in support of USAID objectives and U.S. national security priorities, including in fluid and dynamic environments.

Prevention is not a moment in time. It is a series of actions designed to interrupt the outbreak, escalation, or recurrence of violence and promote peace. We work

“Prevention is not a moment in time. It is a series of actions designed to interrupt the outbreak, escalation, or recurrence of violence and promote peace.”

on prevention in the middle of a conflict or an upswing in violent extremism, or before it comes to a community or region. As a senior advisor in my bureau likes to tell me, violent extremist organizations (VEOs) often feed off existing grievances already fueling conflict within a community. It is less about a religious ideology and more about governance and service delivery. USAID's preventing and countering violent extremism efforts address violence in two ways. First, we strengthen the resilience of local systems—the ways in which national and local governments, key leaders, communities, and the private sector interact—such that they themselves detect and deter violence. Second, we strive to reduce the risk of radicalization and recruitment to violence within communities.

We have learned a lot about what works—and what does not—when trying to prevent violence. For example, we found that by addressing the “push” factors alone, we improved individual and community circumstances, but did not necessarily reduce their propensity to support violence. By widening our aperture to target the dynamics through which VEOs mobilize those grievances and recruit support, we are starting to see more durable success in reducing support for violence. We have also learned how important it is to adapt quickly. We are taking advantage of changes in USAID's overall business model that allow us to pivot programming choices—even those managed through contracts—quickly. The key lesson here is that counterterrorism/countering violent extremism is not just about capacity building or training in a classic sense. It is about meeting people in terror-affected venues as they are, in their daily lives, with support that matters in the short term, *in addition* to working at institutional and transnational levels to make sure our national counterparts in government and in host security forces are not part of the problem, but contribute to a sustained solution.

How do we know we have succeeded? That is a hard question, and we are starting to better understand it and to tell the story. We measure changes in attitudes, behaviors, policies, and institutions. In development-speak, institutions are more than buildings. They are the formal and informal rules that organize social, political, and economic relationships. Changing these “rules of the game” is not a short-term effort; it takes time—and requires the U.S. government to invest in prevention in the same ways it has invested in kinetic responses over the last two decades. Thankfully, it is a lot cheaper to prevent than respond. Here are a few examples of how USAID strengthens local systems and reduces risk at the community level.

- In Indonesia, USAID partnered with local government and civil society actors to address the reintegration of former terrorists and those returning from VEOs in the Middle East.
- In Kenya, USAID helped forty-one county governments develop CVE local

action plans that align with the country’s National Action Plan and established a multi-stakeholder group called a Community Engagement Forum to oversee plan implementation.

- We have supported local radio stations and social media outlets to improve access to authentic information in ways that counter increasingly sophisticated VEO-produced content in places like Niger, Ethiopia, and Nigeria.

We are learning from what we have done right and the challenges we have faced. The U.S. Congress passed the Global Fragility Act, which, to the letter of the law, is telling us to coordinate better at preventing conflicts, curbing VEOs, and

establishing a foothold before more dollars and lives need to be sacrificed. We know we have achieved success when the country we are working in is not in the news.

“We know we have achieved success when the country we are working in is not in the news.”

The major components of USAID’s strategy, policies, and programs to address conflict and state collapse include: im-

plementing the “U.S. Strategy to Prevent Conflict and Promote Stability” mandated by the Global Fragility Act, in close concert with the Defense and State Departments;¹ implementing agency policy and programming to counter violent extremism; implementing USAID’s role in the U.S. Women, Peace, and Security strategy; leading the interagency on nonsecurity U.S. stabilization assistance; elevating USAID’s contribution to all phases of atrocity prevention; and integrating conflict-sensitive approaches into strategies to address climate change.

We have done and learned a lot, but we still have a lot of work to do to prevent conflict and counter violent extremism. We will work with our U.S. government counterparts and our partners to keep moving forward in this effort.

1. For the “U.S. Strategy to Prevent Conflict and Promote Stability,” see <https://www.state.gov/stability-strategy/>.

A Comprehensive Framework to Address Domestic Violent Extremism

John D. Cohen

Counterterrorism Coordinator and Senior Official Performing the Duties of the Under Secretary, Office of Intelligence and Analysis, U.S. Department of Homeland Security

The Department of Homeland Security confronts a wide array of threats on behalf of the American people. These threats endanger our communities and our way of life, and include terrorism perpetrated by both foreign and domestic actors. Targeted violence and terrorist threats to the United States have evolved and become more varied since the attacks on September 11, 2001. Combating these threats is and will remain a top priority for the Homeland Security Department.

In the years immediately following 9/11, we focused on foreign terrorists who sought to harm us within our borders and threaten our interests and assets abroad. In partnership with federal agencies spanning the law enforcement, counterterrorism, and intelligence communities, the Department of Homeland Security built a multilayered screening and vetting architecture to prevent certain individuals from traveling to or entering our country by air, land, or sea. We also issued a call for vigilance on the part of local communities and individuals alike.

Following 9/11, terrorism-related threats to the homeland evolved to include homegrown violent extremists—individuals inspired primarily by foreign

“In the years immediately following 9/11, the Department of Homeland Security built a multilayered screening and vetting architecture to prevent certain individuals from traveling to or entering our country by air, land, or sea.”

terrorist groups but not receiving individualized direction from those groups. According to a joint Homeland Security, FBI, and National Counterterrorism Center assessment, from 2015 to 2017 in particular, HVEs became the most prominent terrorism-related threat to the homeland. In response, we partnered with law enforcement, first responders, social workers, mental health experts, and local communities to identify possible signs of radicalization to violence and to prevent violence before it occurred. Likewise, through close collaboration with our federal, state, local, tribal, and territorial (SLTT) partners, we strengthened our capacity within the United States to identify and share threat information across all levels of government, with the private sector, and with our foreign counterparts. We are leveraging the infrastructure, processes, and partnerships that grew out of 9/11, and applying those capabilities—and the lessons learned over the past twenty years—to the diverse set of threats we face today.

Terrorism-related threats to the United States continue to evolve. U.S.-based lone actors and small groups of individuals, including both HVEs and domestic violent extremists (DVEs), represent the most significant and persistent threat to our country.

DOMESTIC VIOLENT EXTREMISM

DVE refers to individuals or movements based and operating primarily within the United States who seek to further political or social goals through unlawful acts of force or violence, without direction or inspiration from a foreign terrorist group or other foreign power. DVEs are motivated by various factors, including racial bias, perceived government overreach, conspiracy theories promoting violence, and unsubstantiated and false narratives about fraud in the 2020 presidential election, among others. The mere advocacy of political or social positions, political activism, use of strong rhetoric, or even generalized advocacy for violent tactics does not constitute violent extremism and is in general constitutionally protected speech. DVEs can fit within one or multiple categories of ideological motivation or grievances.

The intelligence community has assessed that DVEs who are motivated by a range of ideologies and galvanized by recent political and societal events in the United States pose an elevated threat to the United States. This assessment is based on a joint report in March 2021 from the Department of Homeland Security, FBI, and Office of the Director of National Intelligence, “Domestic Violent Extremism Poses Heightened Threat in 2021.”¹ The intelligence community assesses that racially and ethnically motivated violent extremists (REMVEs), including those who advocate the superiority of the white race, and militia violent

extremists (MVEs) present the most lethal DVE threats, with REMVEs most likely to conduct mass-casualty attacks against civilians and MVEs typically targeting law enforcement, elected officials, and government personnel and facilities.

The current National Terrorism Advisory System Bulletin, released August 13, 2021, further notes that through the remainder of 2021, REMVEs and anti-government or anti-authority violent extremists will remain a threat to the United States. These violent extremists may continue to seek to exploit the Covid-19 pandemic mitigation measures by viewing the potential reestablishment of public health restrictions across the United States as a rationale to conduct attacks. Additionally, some REMVEs advocate a race war and have stated that civil disorder provides opportunities to engage in violence in furtherance of agendas often derived from racial or ethnic bias—often referred to as “accelerationism.”

These DVEs are typically fueled by violent extremist rhetoric and other grievances, including false narratives and conspiracy theories, often spread through social media and other online platforms by a broad range of domestic actors, and occasionally amplified by foreign threat actors. DVEs exploit a variety of popular social media platforms, smaller websites with targeted audiences, and encrypted chat apps to recruit new adherents, plan and rally support for in-person actions, and disseminate materials that contribute to radicalization, inspiration, and mobilization to violence. DVE lone offenders and small groups will continue to pose significant detection and disruption challenges because of their ability to mobilize discreetly and independently and access weapons. The lethality of this threat is evidenced by recent attacks across the United States, including attacks against minority groups, government personnel and facilities, and critical infrastructure.

“Domestic violent extremists exploit a variety of popular social media platforms, smaller websites with targeted audiences, and encrypted chat apps.”

NATIONAL STRATEGY FOR COUNTERING DOMESTIC TERRORISM

Enhancing our collective ability to prevent all forms of terrorism and targeted violence that threaten homeland security is a top priority for the Biden-Harris administration and for the Department of Homeland Security specifically. In January of this year, President Biden directed his national security team to lead a comprehensive review of U.S. government efforts to address domestic terrorism. As a result of that review, the Biden administration released the first “National Strategy for Countering Domestic Terrorism” to address this challenge

to America's national security and improve the federal government's response.

For the first time ever, this strategy provides a nationwide framework for the U.S. government to understand and share domestic-terrorism-related information; prevent domestic terrorism recruitment and mobilization to violence; disrupt and deter domestic terrorism activity; and confront long-term contributors to domestic terrorism, while embracing the protection of privacy, civil rights, and civil liberties as a national security imperative. The Homeland Security Department worked closely with the White House and our federal interagency partners in the development of the strategy, and will continue to work closely with these partners, as well as our federal, SLTT, and nongovernmental partners as we support its implementation.

In implementing this strategy, we will remain focused on reducing the threat of violence. We must make it harder to carry out an attack and reduce the potential for loss of life by preventing radicalization and mobilization to violence. We recognize that our department cannot do this alone. Therefore, it is embracing a whole-of-society approach to combating domestic terrorism by building trust, partnerships, and collaboration across every level of government, the private sector, NGOs, and the communities we serve, while vigilantly safeguarding guaranteed First Amendment protections. We are taking a number of steps to expand our focus on this threat, while ensuring all available resources are devoted to combating domestic terrorism. These include:

- Enhancing efforts focused on the prevention of terrorism and targeted violence, including the identification and mitigation of violence through community-based prevention programs
- Expanding intelligence analysis, production, and sharing, particularly with SLTT partners
- Prioritizing partnerships with the federal interagency, as well as SLTT and nongovernmental partners—including academia, faith-based organizations, and technology and social media companies—to support our efforts to identify and combat violent extremism

THREAT PREVENTION

The Center for Prevention Programs and Partnerships (CP3) is leading our efforts to prevent domestic terrorism and targeted violence. The CP3 approach to violence prevention focuses on locally led efforts to leverage community-based partnerships that address early risk factors and ensure individuals receive help before they radicalize to violence. In support of this objective, CP3 will continue to provide financial, educational, and technical assistance, allowing our partners

to build and implement these efforts, which we call local prevention frameworks. These frameworks are tailored to each community's needs and challenges, and provide concerned community members and organizations with the tools they need to help prevent individuals from radicalizing to violence. These individuals often exhibit behaviors that are recognizable to many but best understood by those closest to them, such as classmates, friends, and family. Through local prevention frameworks, the Homeland Security Department is empowering the public to support early interventions prior to someone engaging in violence.

Our prevention efforts are closely coordinated within the department as well as with federal interagency partners. By working with the Departments of Justice, Education, Health and Human Services, and State, among others, Homeland Security is driving a whole-of-government approach to building trusted partnerships with the communities we serve. Similarly, we are leveraging these coordination efforts to identify and share best practices and lessons learned, while ensuring that past mistakes are not repeated. For example, we are establishing a CP3 detailed position within the DHS Office for Civil Rights and Civil Liberties (CRCL). This approach will ensure full coordination while avoiding any duplication of effort.

In addition to these efforts, and given the evolving threat landscape and the risks posed by DVE, including to our employees and operations, the secretary directed the department to initiate a review of how to best prevent, detect, and respond to potential domestic violent extremist threats within the department. This effort is led by our Office of the Chief Security Officer and includes a review and update of policies and procedures laying out the requirements and mechanisms for reporting insider threats and other actions associated with DVE within the department.

INTELLIGENCE ANALYSIS AND INFORMATION SHARING

The development and sharing of objective and timely intelligence are the foundation for what we do. Therefore, the Department of Homeland Security is redoubling our efforts to augment our intelligence analysis and information sharing capabilities,

“The CP3 approach to violence prevention focuses on locally led efforts to leverage community-based partnerships that address early risk factors and ensure individuals receive help before they radicalize.”

“The development and sharing of objective and timely intelligence are the foundation for what we do.”

while also reviewing how we can better access and use publicly available information to inform our analysis. The DHS Office of Intelligence and Analysis (I&A) has enhanced its ability to analyze, produce, and disseminate products that address DVE threats, including to inform our stakeholders about violent extremist narratives shared via social media and other online platforms. This includes the establishment of a dedicated domestic terrorism branch within I&A that is leading our efforts to combat this threat by using sound, timely intelligence. Concurrent with the creation of this dedicated team, I&A has continued to strengthen its partnerships across the department to ensure the proper protection of privacy, civil rights, and civil liberties, including the Office of the General Counsel, the Privacy Office, CRCL, and other Intelligence Oversight offices, through training and the regular review and oversight of departmental intelligence products.

One of the department's most important missions is to provide actionable intelligence to the broadest audience at the lowest classification level possible. As a result, the department has also refocused its efforts to augment its intelligence and information sharing capabilities in collaboration with SLTT and private-sector partners. This includes publishing and disseminating intelligence bulletins that provide our partners with greater insight into evolving threats, and situational awareness notifications that inform public safety and security planning efforts to prevent violence. I&A will also continue leveraging the National Network of Fusion Centers and our deployed intelligence professionals who collect and analyze threat information alongside SLTT partners to increase timely information sharing in accordance with applicable law and the department's privacy, civil rights, civil liberties, and intelligence oversight policies.

PARTNERSHIPS

As Secretary [of Homeland Security Alejandro] Mayorkas has noted in several instances, the department is fundamentally one of partnerships. This is at the core of what we do, and the department cannot be successful in countering terrorism threats without strong partnerships both across the federal government and with the communities we serve.

In support of this, we have increased our collaboration with the FBI, intelligence community, State Department, and other federal interagency partners to more comprehensively understand and assess the extent of operational relationships between violent extremists in the United States and those operating in other parts of the world. This increased collaboration will enhance our ability to detect those DVEs communicating with like-minded individuals overseas, especially those sharing tactics and violent materials, and communicating their intent to commit some type of violent attack. This collaboration will also improve

our watch-listing process, screening and vetting protocols, and travel pattern analyses to detect and assess travel by known or suspected terrorists.

The department is also working closely with industry partners, academia, and faith-based and nongovernmental organizations to better understand online narratives associated with domestic terrorism and targeted violence. We are working with technology companies to help inform their development of voluntary, innovative approaches to identify and mitigate violent extremist content under their terms of service and community standards, and to identify effective ways to share threat information, consistent with the law, privacy protections, and civil rights and civil liberties. We are also working to build greater public awareness and resilience to disinformation by developing, evaluating, and sharing digital media literacy tools and critical thinking resources.

No collaboration is more important than that with our SLTT partners who ensure the safety and security of our communities every day. The department is only able to execute its mission when we have strong collaboration with our law enforcement and other security partners across the country. This is especially true for I&A, which was established in part to fill a void within our nation's intelligence and information sharing architecture between federal and SLTT partners. In executing this mission, the department works closely with Homeland Security advisors in every state and territory to increase the resiliency and preparedness of our communities. Additionally, through our partnership with the National Network of Fusion Centers, the department deploys personnel to the field to share information on a broad range of threats, including terrorism. The Homeland Security Department remains committed to working closely with SLTT partners, including by sharing timely, actionable information to ensure our partners have the resources they need to keep our communities safe.

In addition to these actions, the Department of Homeland Security continues to look for opportunities to further empower our SLTT and nongovernmental partners by providing them with the resources they need to effectively address this national threat. As an example, the department designated domestic violent extremism as a national priority area within the department's Homeland Security Grant Program for the first time. We are likewise looking at opportunities to enhance how other grant programs can be more effectively leveraged to combat domestic violent extremism.

1. See https://www.dhs.gov/sites/default/files/publications/21_0301_odni_un-class-summary-of-dve-assessment-17_march-final_508.pdf.

Disrupting Terrorist Financing Networks

Paul Ahern

*Principal Deputy Secretary, Office of Terrorist Financing and Financial Crimes,
U.S. Department of the Treasury*

Thanks for the opportunity to join you all and discuss countering the financing of terrorism (CFT). Over the past two decades, Treasury and its interagency partners have recognized a simple truth—that targeting terrorist financing is key to starving terrorism—and developed deep CFT expertise, put in place a robust legal architecture, built international relationships, and drawn upon various authorities in an extensive CFT toolkit, to degrade the financial and support networks of ISIS, Al-Qaida (AQ), Hizballah, and other terrorist groups.

We have built a clear international consensus, enshrined in numerous United Nations Security Council resolutions and the Financial Action Task Force (FATF) international standards, that countries around the world cannot sit by and let violent extremists plan, finance, and train for attacks that will be carried out elsewhere, but must act as responsible global citizens to stop that threat. We have

also empowered our partners in government, the private sector, and throughout the world with the tools and information to join us in identifying and disrupting the flow of funds that help facilitate these destructive acts.

Let me give you an example of how the Treasury Department's Office of Terrorism and Financial Intelligence (TFI)

“We have built a clear international consensus that countries around the world cannot sit by and let violent extremists plan, finance, and train for attacks that will be carried out elsewhere.”

leverages policy, sanctions, enforcement, regulatory, and intelligence resources to disrupt terrorist financing networks. On September 29, the department designated two major Hezbollah financiers based in the Arabian Peninsula, along with their associates, who moved tens of millions of dollars to Hezbollah through the formal financial system and cash couriers. This action was the result of focused intelligence gathering and analysis by our Office of Intelligence and Analysis to identify accounts, assets, and transactions involved in this network, followed by the development of targeted and calibrated sanctions measures by our experts at the Office of Foreign Assets Control. This was not just a U.S. action; our Office of Terrorist Financing and Financial Crimes, in coordination with the State Department, worked closely with the government of Qatar to facilitate a coordinated designation and prosecution of these individuals that magnified the impact of our own action by further disrupting the network.

While we have had success in CFT, our work is not done. The terrorism threat continues to evolve, and so we must evolve our efforts to meet this challenge..

Domestic terrorism. While our CFT efforts have primarily been focused overseas, combating domestic terrorism is a priority for the Biden administration, as articulated in the “National Strategy for Countering Domestic Terrorism” released earlier this year. We are applying lessons learned from our experience with international terrorism to this evolving challenge, while respecting the vital constitutional protections for all Americans. Primarily led by the Financial Crimes Enforcement Network, TFI works closely with U.S. law enforcement and engages with financial institutions to help them better detect and report suspicious financial activity. We also collaborate with our State Department colleagues to assess whether foreign organizations and individuals linked to domestic terrorist activities can be designated, such as in the April 2020 designation of the Russian Imperial Movement, while engaging with foreign governments to identify and disrupt foreign individuals or entities sending money to, training, or recruiting U.S. persons. At the FATF, we co-led the first comprehensive assessment of how racially and ethnically motivated violent extremists (REMVEs) raise, move, and use funds.

Misuse of digital currency. Over the past few years, one of the priorities for the Treasury Department has been identifying and assessing the illicit finance risks associated with digital currency and taking measures to mitigate those risks. We are particularly concerned with encrypted person-to-person transfers that do not require a traditional financial institution intermediary and the money laundering and terrorist financing risk associated with these types of transactions. While most terrorist groups still primarily rely on the unregulated financial system and

“We are particularly concerned with encrypted person-to-person transfers that do not require a traditional financial institution intermediary and the money laundering and terrorist financing risk associated with these types of transactions. Within the past two years, we have identified several instances of terrorists and their supporters, raising funds in digital currency.”

cash to transfer funds, within the past two years we have identified several instances of terrorists and their supporters, including from ISIS, al-Qaeda, Hezbollah, and REMVE groups, raising funds in digital currency—an indication that these groups are growing more comfortable with using virtual assets in financing their violent purposes.

Barriers to public-sector information sharing. While public-private partnerships have grown over the last two decades, effective and timely information sharing between key government agencies involved in counterterrorism and other governments and financial institu-

tions remains a significant challenge for many jurisdictions around the world. Financial transactions such as transfers, purchases, and cash withdrawals leave a financial footprint. Sharing this valuable information aids in detecting individuals participating in or supporting terrorist acts and facilitates disruptive action, such as freezing assets and accounts or arresting and prosecuting suspects to prevent future attacks from occurring.

Lack of effective implementation. For many countries, having FATF-compliant laws is seen as sufficient to stop terrorist financing. That is not enough, and we need jurisdictions around the world to build a framework that uses these authorities and resources to actually disrupt and dismantle terrorist financial networks. This means, for example, that suspicious transaction reports related to terrorism are not simply filed with the national financial intelligence unit; this information must reach agencies that take action against terrorist financiers. When it comes to financial sanctions, jurisdictions can do much more on actually implementing these powerful tools to target terrorist financial and support networks.

I know [another presenter] is going to talk about the administration’s focus on anti-corruption, but I did want to say a few words on that. Corruption and money laundering are inextricably linked, so the response to corruption must go hand in hand with efforts to combat money laundering and terrorist finance.

At the Treasury Department, Secretary [Janet] Yellen has made implementation of anti-money laundering reforms among her highest priorities, seeking to

expeditiously advance policy and regulation that will directly and rapidly counter corruption around the world. The department is committed to advancing a number of anti-corruption priorities, namely combating kleptocracy and foreign bribery, enhancing the transparency of legal entity beneficial ownership and real estate ownership, and promoting the role of civil society in the fight against corruption.

While corruption and terrorism present distinct foreign policy and national security challenges, I did want to note an important parallel in countering financial activity associated with each. Foremost, these efforts rest on a bedrock of financial transparency through which the Treasury Department, regulators, and law enforcement can identify the ultimate owners of assets and the trail of transactions and financial networks that support an array of illicit actors. In analyzing this information, we can seize and freeze hidden assets, impose financial sanctions or pursue law enforcement responses, take regulatory action to close loopholes that are being exploited, and share targeted information with financial institutions and foreign governments so that they can act or feed back into the information cycle to better detect and report on proceeds associated with corruption, terrorist financing, and the entire scope of illicit activity.

“Corruption and money laundering are inextricably linked, so the response to corruption must go hand in hand with efforts to combat money laundering and terrorist finance.”

Non-Kinetic Tools in a Time of Competing Priorities

Damon Stevens

Assistant Director for Strategic Operational Planning and National Intelligence Manager for Counterterrorism, National Counterterrorism Center

Non-kinetic counterterrorism is a critical part of the counterterrorism toolkit that rarely gets the credit it deserves for its success over the last twenty years, and it needs to be reconsidered as the CT enterprise is in a period of transition.

The national CT effort is changing, which is a true testament to the success of the CT community and the investment by the executive branch, Congress, and the American people over the last twenty years. If the community does its job well to counter the efforts of terrorist groups, terrorism will hopefully not become the top national security priority again.

But for now, the terrorism threat has not gone away. While the threat from a strategic-level terrorist attack to the homeland is lower than it has been in the past, the United States today is facing a more geographically dispersed and ideologically diffuse threat—a threat that is enabled by a more technologically complex environment than ever before. This juxtaposition challenges the CT community to look toward the future in a time of shifting resources, creating an opportunity to ensure that the United States is focused on investing in the right capabilities and partnerships as it works to transition to a sustainable resource and capability posture.

The first natural question to ask is what combination of kinetic and non-kinetic actions is most attributable to the success of the CT community these past twenty years? If you talked to twenty practitioners and experts, you'd probably get twenty different answers. Kinetic action has undoubtedly had its intended effect—the

direct pressure placed on the leadership of al-Qaeda and ISIS has made it difficult for those groups to plan and orchestrate complex attacks on our homeland, and those tools often come [most visibly] to mind when one thinks of U.S. CT efforts. But what about other efforts?

Over the past twenty years, non-kinetic CT efforts have indisputably disrupted terrorist attacks, and have had a real impact on terrorist groups' recruitment efforts. The investments we have made over the years in working with domestic and international law enforcement, developing and imposing financial sanctions on suspected terrorists and their affiliates, and sharing intelligence within our government and with our foreign partners, especially those developing and using countering violent extremism (CVE) tools, have undoubtedly paid off.

In addition, the aggregate impact of the efforts of the worldwide CT community arguably does more day-to-day to address terrorism than anything the United States can do alone. As Luke Hartig recently highlighted in the *Atlantic*, our border-defense and our homeland security apparatus are light-years ahead of where they were twenty years ago. For terrorists hoping to enter the homeland, it is now considerably more challenging to get through the multiple layers of screening and physical security. While not always included in the category of non-kinetic CT tools, the screening and vetting tools we employ are the first, second, and third most important non-kinetic capabilities today. Furthermore, identity intelligence has become the most important discipline in the CT and transnational threats arena.

The bottom line is that there is a range of effective tools across the kinetic and non-kinetic spectrum. But there are no easy answers as to the right combination of CT tools to help determine what capabilities to protect or even invest in or, more importantly, where we can divest to ensure our country can address other pressing challenges as well.

What is clear, however, is that as we wind down military deployments overseas, non-kinetic capabilities, both traditional and nontraditional, will be more, not less, important, and by default represent a larger percentage of our national mix and therefore bear more responsibility for our continued success. So with that in

“Kinetic action has undoubtedly had its intended effect—the direct pressure placed on the leadership of al-Qaeda and ISIS has made it difficult for those groups to orchestrate complex attacks on our homeland.”

“While not always included in the category of non-kinetic CT tools, the screening and vetting we employ are the first, second, and third most important non-kinetic capabilities today.”

mind, for those of you working to maximize the impact and efficacy of the efforts highlighted today, three thoughts regarding non-kinetic tools are important if we are to succeed in this area.

1. Non-kinetic CT tools require time and space to sustain their impact, which necessitates an enduring foundation of indications and warning intelligence.
2. Non-kinetic tools supporting homeland defense and resiliency should be prioritized, and after twenty years, we have significant data on which of those have measurable impact and which do not.
3. In a time when other national security challenges may be receiving additional focus and support, CT-specific non-kinetic tools likely will benefit from clearer alignment and even potential absorption into larger substantive portfolios.

On the first point, non-kinetic tools only work when they have the time and the operational and policy space to be effective. The policy community absolutely needs the time and space to be able to employ non-kinetic tools, so accurate intelligence is vital for successful non-kinetic CT. Surprise or exigent circumstances greatly narrow our options, and if we are going to rely on a larger toolkit—and for those of you providing intellectual leadership for the development and deployment of these tools—we must focus on the necessary support and conditions to allow these tools to be utilized. Arguably, focusing on the support needed to use these tools may be more important than a given tool itself.

Twenty years ago, we made a clear strategic decision to build an intelligence and operational infrastructure to support the nation's CT efforts. Over this time, it has largely focused on putting direct pressure on terrorist leaders and organizations where they have sanctuary overseas. However, to the credit of countless professionals from across the interagency, intelligence that supports kinetic operations also supports a full range of downstream non-kinetic activities, from law enforcement actions, to diplomatic and homeland security, to messaging and CVE efforts, to treasury and diplomatic actions. The post-9/11 CT enterprise results in part from a lack of transparency and unified effort across the interagency, but over the last fifteen to twenty years, it has developed into one of the most integrated and mutually supporting communities within the national security spectrum.

This is why the maintenance of and potential investment in capabilities and partnerships to provide indications and warning (I&W) may be the most important thing we can do if we are serious about increasing the use of non-kinetics.

Only accurate intelligence, information, and insights that provide timely warning about growing threats before they mature to a point where policymakers believe their only option is direct action will give us the time and space to sustainably use non-kinetic tools.

So here is the challenge that we think about and work on every day: as we shift resources away from military deployments and the associated infrastructure that comes with them, how do we ensure we are maintaining and improving an I&W capability that allows us to focus on non-kinetic opportunities? As we transition, how do we ensure those downstream non-kinetic efforts retain the support they need to be successful?

This is crucial because non-kinetic options are most viable as proactive measures and least viable as reactive measures. Without timely intelligence and warning, all the advocacy and proper planning of non-kinetic efforts will simply be an academic exercise. So if you are interested in using non-kinetic tools, you must be sincerely interested in first ensuring there is an underlying foundation to support their use.

“Non-kinetic options are most viable as proactive measures and least viable as reactive measures.”

That brings me to my second and related point. Non-kinetic support to homeland defense and employment of tools proven effective over the last twenty years must take precedence and be ruthlessly prioritized as we stay focused on keeping the homeland safe and collectively transition our national efforts to a sustainable and enduring posture.

I mentioned at the opening that this is a time of opportunity for the CT community. We are at an inflection point. In the past, there were times when non-kinetic-focused resources, even more than kinetic actions, were arguably spread too far, wide, and thin, against many different efforts potentially limiting the enduring impact of those non-kinetic efforts.

With resource constraints come hard choices that can actually lead to more effective, efficient efforts. I mentioned the juxtaposition of lower threat to the homeland with greater dispersion of threat actors, but another important factor is that, as numerous officials have testified, the analytic community believes the most significant direct threat we face from terrorism in the United States is not an attack launched from overseas but one from lone actors and self-radicalized individuals here.

Therefore, at this point in history, we must take a hard look at that threat and resource picture and prioritize investments accordingly. This invariably means assuming some risk and possibly not being as proactive in some areas as we have in the past. In a time of declining resources, we should ensure that we use the

experience we have gained over the last twenty years to focus on what we know works, and minimize continued focus on efforts that we wish worked, or that theoretically should work but have not, to date, demonstrated measurable impact.

So, to ensure that our national efforts are ruthlessly disciplined, there are some areas where we simply must prioritize:

- **Border security and screening and vetting efforts**, which, as I mentioned at the outset, I view as arguably the most important non-kinetic CT component. This is a space that continues to have significant policy, legal, technological, and logistic opportunities that need focus, expertise, and solutions from within governments and outside intellectual leaders alike. Other efforts that focus on homeland defense and resiliency, to include diplomatic security, should also be prioritized as we do less overseas.
- **Tracking and disruption of the financial actions of terrorist groups** and their enablers. In a way, financial disruptions through sanctions or other means represent a proactive tool, like law enforcement or even traditional kinetic action, that will become more important as traditional direct action options become less available.
- The non-kinetic tools I think of most are **CVE and terrorism prevention**. We know after many years of research and real data that the radicalization process is very individual and subject to hyperlocal conditions, which makes it a true challenge for the U.S. government to programmatically have enough aggregate impact to justify the resources expended, even in resource-abundant times of investment in CT.

While some of the most exciting work in this space is now being led by the State Department and USAID, this also means that finite dollars spent domestically in the space, where we can ensure more localized impact, may come at the expense of larger overseas investments that many of us have long advocated. Similar to point one regarding indications and warning, we cannot forget that it is ultimately the protection of the homeland that, again, provides the space to eliminate the need to rely on direct action and a heavy military presence.

And this leads to my third and final point. CT-specific non-kinetic tools will likely benefit from being merged into larger substantive portfolios. This may sound out of place at a CT discussion and coming from a person from the National Counterterrorism Center, but for many non-kinetic capabilities and tools, I believe if we focus less on just the CT-specific aspects—as we like to do in the CT

community—and strive to integrate the CT aspects into broader functional or regional applications, we will be more effective in actually using those tools for CT.

There is some merit in criticism of the CT community that over the years we did not do a good job of integrating regional counterparts and their respective issues into CT discussions, decisions, or resource investments. When CT was our top priority, we had a tendency to focus just on the CT aspects of a challenge, which in many cases limited our solutions.

My point here is simple: we'll be better served if we can get broader swaths of the national security community to incorporate CT targets better than we did in years past. This will help our efforts in a world of competing priorities and limited budgets, leveraging our mission partners in the most efficient way possible.

The real world is not neatly compartmented like our bureaucratic lines, as demonstrated by the increasingly diffuse nature of the CT threat intersecting with other functional and regional security disciplines to include strategic competition, transnational crime, and humanitarian operations. Put another way, our tools to counter terrorist use of advanced and emerging technologies or the exploitation of decentralized currency mechanisms are not dissimilar to those being employed against transnational organized crime and, in some cases, even state actors.

As another example, many of the underlying causes of terrorism are also underlying causes of poor governance, poverty, political unrest, humanitarian strife, environmental catastrophe, and other challenges. This means that for those broader complex areas that have strong leadership, if we roll CT under or within them, the outcome will likely lead to greater funding and focus than when they stand alone as CT-specific niche areas. Rather than holding on to notions that these efforts are so unique and special, there is an opportunity to work closer with—and even by, with, and through—regional, political, and humanitarian efforts that can amplify results in the long run.

Conversely, the CT community has accumulated lessons learned, best practices, and scar tissue over the past twenty years in the development of these non-kinetic tools and capabilities that should serve to guide interventions against other emerging national security concerns.

So these are just a few thoughts I have as we work together to promote and improve these non-kinetic tools for our aggregated national effort. There are no magic bullets or piles of money coming, but our experience and this once-in-a-generation opportunity to reimagine how we approach these topics [could generate] an even more sustainable national effort as we all work to meet our shared goal of ensuring CT does not become number-one again.

The War on Jihadism: Lessons from Twenty Years of Counterterrorism

Marc Hecker, Elie Tenenbaum, and Louis Dugit-Gros

RAPPORTEUR'S SUMMARY

When assessing the struggle against jihadism, one can best understand the period since the 9/11 attacks as five phases of a strategic cycle, each with its own victories, losses, and guiding objectives.

1. **2001–6:** The United States is able to disrupt some jihadist cells, yet ultimately learns the limits of military intervention through failed stabilization efforts.
2. **2006–11:** Western forces adopt a counterinsurgency approach.
3. **2011–14:** The Arab Spring is followed by “jihadism’s revenge,” with the Islamic State (IS) amassing territory and power.
4. **2014–17:** The United States and its partners attempt to counter IS and other terrorist groups with a lighter military footprint.
5. **2017–21:** The current period can be thought of as a “strange victory”—a play on the title of Marc Bloch’s 1940 book, *Strange Defeat*, which concluded that the German takeover of France stemmed in part from a failure to understand that “the whole rhythm of modern warfare had changed its tempo.” Today, the West has been able to prevent the emergence of another major terrorist organization but has not adequately countered many of the forces underlying the jihadist threat.

As a potential new phase takes shape, the counterterrorism milieu is defined by a combination of tactical successes and shifting priorities. On one hand, jihadist groups such as IS and al-Qaeda central no longer pose as constant and grave a threat to Western nations as they once did. On the other hand, the challenge of measuring political gains versus costs has led to strategic frustration and war fatigue even as terrorist threats have become more geographically dispersed. Further, Washington and its partners, including France, have moved new issues to the top of their agenda—in an age of great power competition, Covid-19, and a worsening climate crisis, counterterrorism has receded to the background.

WHO WON THE WAR ON TERROR?

If assessed from a zero-sum perspective, the war on terror did not result in a clear outcome. Yet counterterrorism is best understood as an ongoing effort rather than a war—a term that suggests the possibility of final victory for one side and total defeat for the other. Jihadist groups fell short of their grander goals such as establishing a caliphate and ridding the Muslim world of Western influence, but that failure does not necessarily constitute a win for the West. Despite considerable tactical success, one could argue that the West has suffered almost as much strategic failure.

For example, even as terrorism-related deaths decreased, the number of Salafi jihadist fighters worldwide has grown significantly, while gaining ground in the battle of ideas has proven difficult for the West. It is unclear whether this represents an expansion of the jihadist movement's global footprint or an increase in the relative strength of local groups, which may be a warning sign of renewed efforts to develop global networks. In either case, the threat persists abroad and within the borders of Western nations, in the form of direct radicalization and on a continuum with rising far-right movements.

LESSONS FOR THE WEST

In the past, a tendency to underestimate and overreact often undermined the West's counterterrorism efforts. Many political leaders dismissed jihadist threats, which came at a cost—most notably before the 9/11 attacks and, later, the Islamic State's ascendance. The threat was taken more seriously at other points, but this often resulted in disproportionate responses that ultimately empowered armed groups to radicalize and recruit new adherents.

Going forward, the West must develop new mechanisms to support its counterterrorism efforts with fewer resources, emphasizing rationality and sustainability. This may include limiting the political ambitions that once drove decisionmakers toward democracy-building campaigns and liberal interventions. Instead, relying primarily on nonmilitary tools that build partner capacity may be more effective in stabilizing localities where jihadists exert considerable control.

At the same time, Western partners must remain vigilant by tracking the development of groups with local clout in

“It is possible for groups to disconnect from international terrorist networks, but proving they have done so is complicated.”

order to contain any wider aspirations they may have. It is possible for groups to disconnect from international terrorist networks, but proving they have done so is complicated; as such, the West should consider devising a vetting process to verify true independence.

In the Sahel region, France has sustained its efforts with a light military footprint of only a few thousand troops. Although fundamentally altering the dynamics of a conflict is difficult with such a limited force, the mission’s tactical successes demonstrate the advantage of a small but strategic deployment. France should follow this success by investing further in political and social measures to advance governance and development. By devoting additional resources to understanding local contexts, the West may be better equipped to offer political bargains in the service of larger goals. This approach has considerable potential if executed strategically. And it certainly does not entail negotiating with terrorists—rather, it means avoiding the impulse to systematically block internal negotiations in societies where jihadists are a fact of life.

“The French presence in the Sahel reflects the geopolitical shift away from a U.S.-led, partner-enabled approach to international security. The reliability of the United States was called into question during the Trump administration, prompting other Western powers to become more self-sufficient.”

More broadly, the French presence in the Sahel reflects the geopolitical shift away from a U.S.-led, partner-enabled approach to international security. The reliability of the United States was called into question during the Trump administration, prompting other Western powers to become more self-sufficient. Allies are now prepared to step forward and allow the United States to lead from behind—but Washington must accept that a supporting role means its agenda no longer takes precedence.

Parallel to jihadism is the threat posed by the far-right movements currently gaining traction in France and other Western nations. Jihadism is still the primary concern for many European states, but these two ideologies exist on a continuum and must be addressed as such. When thousands of Europeans (French in particular) traveled to Syria and Iraq beginning in 2013, Paris did not have an established approach to preventing violent extremism. Governments must learn from this lapse and develop robust, nonmilitary mechanisms to work against the threat. In doing so, they must be careful not to overreact or otherwise repeat past mistakes that strengthen the opposition.

OBSERVATIONS FROM LOUIS DUGIT-GROS

Western counterterrorism campaigns certainly diminished the influence of major jihadist groups, but there is no clear-cut victory given the increase in active fighters and the growing jihadist presence in alternate arenas. Perhaps this is the result of an asymmetry of will, as terrorist morale remains high while Western commitment wanes.

Whatever the case, nonmilitary tools are an important component of a successful counterterrorism strategy, as seen in the evolution of French operations in the Sahel and the emphasis on local capacity building. In the future, counterterrorism must also be considered in the context of new priorities rather than as a separate, lower priority. For example, climate change will have a serious impact on population flows, so decisionmakers need to consider how this and other unprecedented phenomena might strengthen terrorist groups in the future.

“Nonmilitary tools are an important component of a successful counterterrorism strategy, as seen in the evolution of French operations in the Sahel and the emphasis on local capacity building.”

NATO Counterterrorism Trends: Current and Future Threats

Gabriele Cascone

Head of the Counterterrorism Section, Emerging Security Challenges Division, NATO

This forum offers an opportunity to outline NATO counterterrorism trends, including what the alliance is doing on this front, how these efforts have evolved, and what factors will shape them in the future. The key date and turning point for NATO counterterrorism is 9/11. Before that event, terrorism hardly figured in NATO's work. For example, the NATO Strategic Concept approved at the 1999 summit in Washington DC only mentioned terrorism once: "Alliance security can be affected by other risks, including acts of terrorism." The 9/11 attacks changed all this, and it is important to remember that it was the only time in the alliance's seventy-three years of existence that Article 5 of the Washington Treaty—the collective defense clause—was invoked.

What happened in the past couple of decades allowed NATO to identify key tenets of its counterterrorism role. The first point is that counterterrorism is

"NATO contributes to the international community's fight against terrorism in situations where it has expertise, and where it can work in cooperation with international partners."

and remains primarily a national responsibility. The idea is that it is first up to the allies to deal with terrorist threats. The second point is that terrorism is a crosscutting issue that needs to be dealt with in the framework of all three NATO core tasks identified in the most recent Strategic Concept, from 2010: collective defense, crisis management, and

cooperative security. The third point is that NATO contributes to the international community's fight against terrorism in situations where it has expertise, and where it can work in cooperation with international partners (nations or other international organizations). The final point is that NATO's work has been based on three pillars: awareness, capabilities, and engagement. Let's consider them in some detail:

Awareness. The first area that is relevant in increasing awareness is intelligence sharing among allies. NATO has a Joint Intelligence Security Division, within which has been established a Terrorism Intelligence Cell, which periodically releases products mostly focused on strategic intelligence (trends, modus operandi, developments in geographic areas). These are the foundations that can help us better identify and determine our response to terrorism.

Another element of awareness in which we are conducting some relevant work is the role of women in terrorism and counterterrorism, including a gender perspective. It is an area that has been little understood and little considered for many years. We can do more to better understand this dimension.

The third element of the awareness work is related to human security: children in armed conflict, protection of civilians, cultural property protection, and human trafficking. These are phenomena influenced or affected by terrorism. So what role could CT play in this regard?

Capabilities. Developing capabilities is the area more closely tied with the collective defense core task. It deals with what NATO is doing among allies to support the defense of our populations and our territories from terrorist attacks. The first item worth mentioning is the Defence Against Terrorism Programme of Work created in 2004. It is focused on dealing with allied capability shortfalls and urgent requirements, conducting technological research on CT efforts, and supporting the achievement and maintenance of technological dominance and interoperability. It focuses on how technology could support our work against terrorism and deals with issues such as counter-improvised explosive device efforts, protection of harbors, and other areas.

The second element I would like to mention is the extensive work conducted on countering unmanned aircraft systems (UAS), particularly commercially modified drones. Our work is specifically related to countering low, slow, and small drones. These are becoming one of the weapons of choice for terrorist groups

“The role of women in terrorism and counterterrorism has been little understood and little considered for many years.”

“Our work is specifically related to countering low, slow, and small drones. These are becoming weapons of choice for terrorist groups around the world.”

basic issues as having a lexicon to make sure we were using the same words to speak of the same things. Today, our efforts are directed toward standardization, interoperability, and tests/exercises.

Another area to which we have devoted considerable attention is technical exploitation, aka battlefield forensics. The idea is that military forces collect a lot of information and material on the battlefield. How can we bring this into a coherent process in order to support multiple outcomes, such as intelligence, force protection, and research and development? A lot of this work has already been conducted in operations in an ad hoc manner; the challenge here is to create a coherent process.

Related to this topic is that of battlefield evidence. One possible outcome of technical exploitation is to support law enforcement and legal proceedings, particularly with respect to the prosecution of foreign terrorist fighters. In an operation, the military is the agency that gathers the information, which can then be used to help prosecute terrorists in their home countries or identify them when they try to cross borders. We have therefore developed a Battlefield Evidence Policy and program of work. Our main goal is to facilitate the sharing of information and material collected in NATO operations so that they can be used in domestic jurisdictions, whether for prosecution, investigation, or simple identification.

Engagement. The engagement pillar is about cooperation with partner countries and international organizations. Through what we call counterterrorism dialogues, we try to understand what each partner needs from NATO and in which areas NATO would be able to provide assistance. Based on this identification of their needs and our capabilities, we help each country develop a program of training, assistance, scientific projects, and so forth—all the tools that we have at our disposal in the NATO inventory to provide support. At the same time, the NATO community of partners is extensive and covers countries with various levels of expertise, so we also try to bring some of those countries into NATO’s work on capabilities where appropriate. In addition to assisting our partners, we are interested in how partners can help us do better and develop the right capabilities and measures.

around the world. To this effect, we have established a NATO Working Group on countering UAS, which operates on the basis of a work program focused on force protection, boosting security at home, and bringing coherence to NATO’s efforts. Although it may surprise some, at the beginning our work had to address such

In parallel, we keep cooperation with other international organizations high on the agenda, engaging in mutually reinforcing processes with the United Nations, Interpol, European Union, and African Union. This also allows us to support and reach out to non-NATO countries.

A final word on initial work we are conducting to identify a possible NATO role in countering terrorist financing. So far, we have identified two ideas for this strand of work. The first challenge is how to prevent terrorists from financing themselves through the looting of cultural property. We should prepare to include this in our work and in how we prepare our military forces for operational deployments. The second challenge is the exchange of financial information obtained in the course of technical exploitation/battlefield evidence activities. How could we share this information with the appropriate authorities? Preliminary contacts have been initiated with relevant international partners—Interpol, the Financial Action Task Force, the Egmont Group—to explore how to further pursue this initiative.

“We keep cooperation with other international organizations high on the agenda, engaging in mutually reinforcing processes with the United Nations, Interpol, European Union, and African Union. This also allows us to support non-NATO countries.”

SUPPLEMENTAL COMMENTS DURING Q&A

On Afghanistan, we need to remain careful in how we assess what is happening and what active players are still present there. In particular, we need to understand whether the current situation allows other terrorist groups to flourish, and to what extent these groups constitute a threat to NATO and individual allies.

In addition, our extensive operational deployment in Afghanistan helped the alliance realize that militaries can contribute a great deal more to global CT efforts in areas such as battlefield evidence, forensics, and so on. We now need to take what we learned there and from our subsequent work and integrate it into the modus operandi of our military, ensuring that this knowledge and these capabilities are maintained and developed in case future deployments require them.

Regarding NATO’s “Hub for the South,” a number of key tasks have been initiated so far, such as mapping activity in North Africa, the Middle East, the Sahel, and sub-Saharan Africa, as well as what assistance projects are being carried out in these regions. This allows us to better identify the threat and the correct trend of efforts for NATO’s work and engagement with these countries. In addition to providing products of its own, this Hub works in close cooperation with NATO headquarters in Brussels and with our military structures. Its main role is

to keep a constant eye on realities and developments south of the alliance, which is a unique asset.

Regarding the evolution of the terrorist threat in Africa, particularly in the Sahel, NATO's main area of effort at this stage is to improve the capabilities of our partners in the region. It is not so much an issue of direct involvement or deployment, but of how we can strengthen the capabilities of the countries most directly affected by terrorist groups. This includes supporting related efforts by the African Union and UN.

As for counterterrorism efforts in Syria, NATO is a member of the Global Coalition Against Daesh/IS. The main international actor in that space has been the coalition, and NATO sees its role as a contributor to the coalition's work, mostly through its NATO Mission Iraq, which focuses on training the Iraqi security forces at the tactical and institutional levels.

Regarding counter-UAS work, NATO's main U.S. interlocutor—and Washington's representative in the Working Group—is the Joint C-UAS Office in the Department of Defense. When it comes to cooperation with international organizations, much work is being done with the UN, Interpol, EU institutions, and Eurocontrol. We also reach out to industries active in the C-UAS field to learn from their research and knowledge.

As for helping partners in the Middle East and North Africa region with countering drone threats, NATO's counter-UAS work was started first and foremost to support the development of allies' capabilities. At the same time, we can obviously expect partners to knock on our door and ask for assistance. There is very interesting work that can be done, but it is important to do the right thing. We

do not procure C-UAS equipment, but we can conduct research, identify the most effective countermeasures, and so on. We are starting to conduct experiments and exercises to test different countermeasures. Also, we should not ignore that there are partners that have C-UAS capabilities comparable to those of the allies. So we are also trying to involve a number of those partners in the C-UAS Working Group.

In addition, NATO has conducted extensive CT work with many of its Middle East and North Africa partners and will continue doing so. Examples include the work with Jordan, where we conducted a mapping exercise to identify the CT

“NATO has conducted extensive CT work with many of its Middle East and North Africa partners and will continue doing so. Examples include Jordan, where we conducted a mapping exercise to identify the CT support the kingdom was already receiving from other countries and international organizations.”

support Jordan was already receiving from other countries and international organizations, thereby identifying gaps that NATO could fill. We are also putting forth significant effort in supporting Mauritania, which is not only a longstanding NATO partner but one of the G5 Sahel countries as well. (We are addressing CT and military aspects of border security.) And we have recently held discussions with Tunisia.

As for what this assistance means in practice, there is a set of different initiatives that very much depends on the demands of the partner in question. We conduct training—either in-country through mobile training teams or at specialized NATO training institutions and Centres of Excellence—we support work in integrating the defense role in national CT architectures, and we try to foster interagency work.

Regarding gender and CT, the important point is developing a more precise understanding of what role gender plays in terrorism and counterterrorism. The traditional view is that women are victims of terrorism, but women actually play all the roles, including as supporters and active members.

BOARD OF DIRECTORS

President

Jay Bernstein

Chairman

Shelly Kassen

Chairmen Emeriti

Howard P. Berkowitz

Martin J. Gross

James Schreiber

Founding President, Chairman Emerita

Barbi Weinberg

Senior Vice Presidents

Moses S. Libitzky

John Shapiro

Vice Presidents

Lynn Levy Peseckis

Lief D. Rosenblatt

Secretary

Ralph Gerson

Treasurer

Susan Wagner

Board Members

Jeffrey Abrams

Gregg Abramson

Anthony Beyer

Benjamin Breslauer, *emeritus*

Philip Friedmann

Robert Fromer

David Fuente

Michael Gelman

Roger Hertog, *emeritus*

Bruce Lane

Bud Leventhal, *emeritus*

Robin Chemers Neustein

Jeanette Garretty Reinhard

Zachary Schreiber

Mike Segal

Merryl Tisch

Diane Troderman

Gary Wexler

Richard S. Ziman

In Memoriam

Richard S. Abramson, *president*

Charles Adler, *vice president emeritus*

Fred S. Lafer, *chairman emeritus*

Michael Stein, *chairman emeritus*

Walter P. "Wally" Stern, *vice president emeritus*

BOARD OF ADVISORS

Gen. John R. Allen, USMC

Birch Evans Bayh III

Howard L. Berman

Eliot Cohen

James F. Jeffrey

Henry A. Kissinger

Joseph Lieberman

Edward Luttwak

Michael Mandelbaum

Martin Peretz

Richard Perle

Condoleezza Rice

James G. Roche

James G. Stavridis

R. James Woolsey

Mortimer Zuckerman

EXECUTIVE STAFF

Executive Director

Robert Satloff

Managing Director

Michael Singh

Counselor

Dennis Ross

Director of Research

Patrick Clawson

Director of Publications

Maria Radacsi

Director of Communications

Jeff Rubin

National Director of

Development

Dan Heckelman

Chief Financial Officer

Laura Hannah

Operations Manager

Rebecca Erdman

