Combating Terrorism Center
AT WEST POINT

JSOU PRESS
JOINT SPECIAL OPERATIONS UNIVERSITY

THE COMPOUND ERA OF U.S. COUNTERTERRORISM

Don Rassler | August 2023

The Compound Era of U.S. Counterterrorism

Don Rassler

Joint Special Operations University

JSOU PRESS
JOINT SPECIAL OPERATIONS UNIVERSITY

Combating Terrorism Center at West Point

United States Military Academy

www.ctc.westpoint.edu

August 2023

Cover Photo: A man walking into an uncertain future (Getty Images)

CONTACT

Combating Terrorism Center

U.S. Military Academy

752 Thayer Road, Mahan Hall

West Point, NY 10996

Phone: (845) 938-8495

Web: www.ctc.westpoint.edu

ACKNOWLEDGMENTS

The author would like to thank the researchers and practitioners who have been monitoring, and writing about, the evolution of the extremism and terrorism landscapes over the past several years. A big thank-you also goes to Joint Special Operations University (JSOU) President Dr. Ike Wilson, LTC Lukas Berg, and key members of the JSOU research and press team, including Dr. David Oakley and Cameron Cobb. We appreciate the partnership and look forward to future collaborations. This report would also not have been possible without support from my CTC teammates, especially COL Sean Morrow, Dr. Daniel Milton, and our 'get things done wizard' Kristina Hummel.

About the Author

Don Rassler is an Assistant Professor in the Department of Social Sciences and Director of Strategic Initiatives at the Combating Terrorism Center (CTC) at the U.S. Military Academy. His research interests are focused on how terrorist groups innovate and use technology; counterterrorism performance; and understanding the changing dynamics of militancy in Asia. X: @DonRassler

TABLE OF CONTENTS

Executive Summary

The past several years have been a period of transition for the U.S. counterterrorism enterprise. During this time, the United States has had to navigate, and adapt U.S. CT posture and approaches to, a shift in U.S. national security priorities; a complex, diverse, and ever-evolving threat landscape; and ongoing technological change that is transforming the worlds of extremism, terrorism, and counterterrorism.

In addition, the United States has simultaneously been working to define what the next chapter of U.S. counterterrorism should look like and how the U.S. CT community needs to evolve so it can anticipate, understand, and respond to the varied threats it will face in the years ahead.

To help drive change, the United States should frame the counterterrorism moment it finds itself as the compound era of U.S. CT. This new era is being shaped by three primary characteristics: multiple priorities; a broad range of threats, including mixed ones; and a more diverse CT landscape.

How well the United States responds to and adapts to change and challenges that are occurring across these three areas will have an important bearing on the future effectiveness of U.S. counterterrorism.

This report proceeds in three parts. It first outlines characteristics that define the compound era of U.S. CT and the utility associated with this framing. The body of the report then explores some of the key trends and factors that have been impacting and driving change across the extremism, terrorism, and CT landscapes. The report also discusses some of the implications of these trends and outlines 11 priorities that can help guide the U.S. counterterrorism community's evolution during this new era.

The trends that this report highlights will be familiar to CT practitioners and researchers; they are generally known and not 'new.' They have been substantively spotlighted and research about them has been curated in this report so practitioners, policymakers, and researchers have a resource that discusses these trends and their implications in one place—so they can be better considered.

These key trends include:

Span: A Diverse, Geographically Diffuse, and Complex Array of Threats
Today, the United States and its partners need to determine ways to proactively manage and confront the threat posed by a more diverse, geographically diffuse, and complex array of extremists.

The challenge of span cuts across international and domestic terrorism threats and requires that careful consideration be given to the threats that can and should be covered, and the associated risks and tradeoffs; indicators and warnings that help to signal when a threat deserves more attention; and how coverage of less priority, but still dangerous, terror threats can be distributed and/or developed.

Structure: A Spectrum of Organizing Forms and Modalities
Another core complicating factor is that today's extremist and terrorism threats manifest in different organizational forms and derive their support—and in some cases capabilities—by leveraging different approaches, such as attacks that are remotely encouraged, or enabled, from afar. Not only is there a good amount of variance in just how much organizational attributes matter or threat ecosystems rely on them, these preferences have also been evolving.

These dynamics create detection challenges and make it hard for CT practitioners to gain analytical or operational efficiencies across threat streams, as how a group, network, or ecosystem functions, and how an individual can interact with each form, can vary from one threat type to the next.

Movement and Style: Interactive, Intersectional, and Fluid
Important changes are also affecting the movement and style of terrorism and extremism threats.

This includes an emerged set of participatory dynamics that have made today's terror landscape more interactive and gamified, where momentum and the ability of an individual to customize—to tailor and frame their attack in their own idiosyncratic terms and link it to a broader array of incidents—is helping to drive the pace and impact of threats, and push threats in new directions.

These participatory dynamics, which have been underpinned by profound changes in how individuals communicate and receive information, have also been transforming the way individuals and networks interact with, adopt, and communicate extremist ideas, and how extremists can learn, actualize their plans, federate, and enable others.

The net effect is that extremism and terrorism is both more fluid and intersectional than it has been in the past, a trendline that has led to a rise in more blended, individually customized, and composite-based threats, and that holds the potential to lead to more change and some unique collaborations.

Speed, Views on Violence, and Potential Scale

Today's terrorism landscape is also being shaped by the accessibility of extremist content and the greater normalization or 'mainstreaming' of such content in the United States, dynamics that have led to two important and troubling effects.

First, the internet has sped up the time it takes an individual to radicalize. For practitioners, this means they have less time to identify individuals operating across a distributed array of digital platforms who have radicalized *and* less time to discern which individuals do, and do not, pose a threat.

Second, hate and 'us versus them' discussions have become a more regular feature of public discourse, and that extremist discourse has become increasingly 'mainstreamed' in the United States. Polls and academic research have highlighted American concerns about the "increased danger of politically motivated violence"[1] and how Americans' "acceptance of political violence has been rising,"[2] dynamics which suggest that the ongoing normalization of hate is likely to lead to more real-world violence.

Technology Continues to Enable and Constrain—and It Remains a Key Locus of Competition

Access to technology has the power to create new opportunities and challenges for all actors, and as a result, it remains a key area where extremists and counter-extremists compete to identify weaknesses and/or gain an advantage. The existence of this competitive 'space' is not new, but the characteristics of the space have been changing, and changing in ways that lower barriers to entry and enhance the ability of non-state actors to develop new advantages, overcome power imbalances, and innovate.

The open technological revolution has also been reshaping the words of counterterrorism and intelligence. Not only has it broadened the array of commercial technologies and capabilities to which security practitioners have access, it has also been shifting the number, type, and diversity of actors and stakeholders operating in the CT space, and the dynamics of who designs, manages, owns, and has access to, or influence over, specific platforms and approaches.

Since the pace and scale of technological change is projected to only increase over the next several decades, it is likely that these issues will only become more profound and complicated and require more collaboration and partnerships across the world of CT, not less.

Suggested Priorities to Help Guide the Future of U.S. CT

These changes present several challenges and implications for the U.S. and international CT communities. For the United States, one core challenge is how it can keep pace with changes in the environment *and* better anticipate how those changes are likely to enhance or amplify known threats—as well as lead to the creation of new ones—that have the potential to surprise. It also needs to consider how it can do so during an era of enhanced complexity dominated by less U.S. government attention and resources devoted to CT. That is going to involve some tradeoffs and consideration given to, or a reimagining of, the ways in which the United States' approach to counterterrorism should evolve.

As the U.S. government adjusts to meet the moment and build-out the next chapter of U.S. CT, it would

1 Emily Guskin, "A Wide Majority of Americans are Concerned about Politically Motivated Violence," *Washington Post*, November 4, 2022.

2 Rachel Kleinfeld, "The Rise of Political Violence in the United States and Damage to Our Democracy," Testimony to the Select Committee to Investigate the January 6th Attack on the United States Capitol, March 31, 2022.

be wise to develop approaches that mirror the intersectional and compound nature of today's terrorism and extremism threats in ways that are possible. Eleven priorities can help guide the transition.

First, the United States should strategically frame the counterterrorism moment. This report has put forward one suggestion for how it could do so.

Second, the United States should be honest and transparent about its CT track record, including the successes, failures, and limits of prior CT strategies, and the extremist and terrorism threats it faces.

Third, there is a need for the United States to evaluate whether it is appropriately postured and structured to meet today's complex terrorism threats, and that it has the authorities and tools it needs to confront a range of threats, especially those posed by domestic and homegrown extremists.

Fourth, due to the complexity of the terror landscape, the United States should take steps to preserve expertise and institutional memory on key terror movements that it has worked hard to develop.

Fifth, to do more with less and better understand change, the United States should invest more in partnerships. For the U.S. government, this is likely going to require that it identify how it can either be more inclusive or get more comfortable sharing data, knowledge, and know-how to build trust and provide reciprocal forms of value to partners whose expertise, technology, or capabilities are important to advance U.S. CT objectives.

Sixth, identifying and understanding risk is a central feature that the United States needs to get 'right' if it wants to maintain strategic focus on great power threats. It should leverage expertise that exists outside of government to either validate or update U.S. terror risk evaluation approaches.

Seventh, the future of U.S. CT will be driven by data and technology and how the country is able to leverage those two key inputs in a combined way. This is going to require, as many have noted, that the United States make smart investments in technology, artificial intelligence, and automation; that it develop new tradecraft and tools that allow analysts and operators to quickly create insights from diverse types of data; and that it provide opportunities to develop its workforce, all while building out the infrastructure, culture, and talent needed to support the data-driven CT workforce of the future.

Eighth, to meet the compound CT moment, the United States should also be more intersectional in how it studies and approaches problems, and the options it develops to respond to those challenges. For example, if not already being done, the National Counterterrorism Center should consider embedding a liaison at the Central Intelligence Agency's China Mission Center.

Ninth, CT-relevant authorities is another area where the United States should continue its efforts to be more intersectional. For example, a building partner capacity program focused on intelligence network development could help a country like the Philippines to better leverage data to counter the Islamic State in Mindanao, understand the structure and patterns of behavior of China's maritime militia, and explore networks responsible for cyber incidents.

Despite the U.S. government's best efforts, terrorism attacks will still unfortunately happen. And so, a tenth area that the United States should consider investing more in and further developing are efforts to bolster the American public's resilience to terrorism through messaging. Such initiatives would build on prior work done in this area, including approaches taken by Israel and Canada.

Finally, during this period of transition, the U.S. CT community should embrace experiments and create mechanisms to enable them. One small way this could be done is by holding an annual project concept day, a mechanism for CT community members regardless of level to pitch project ideas that are designed to solve a problem or advance a specific U.S. CT priority to senior CT leaders.

The current moment is a tough and unique time for U.S. counterterrorism, but it is also an exciting one filled with a lot of opportunities to innovate, evolve, and forge a better and more sustainable path.

Introduction

For more than 15 years after 9/11, counterterrorism served as the preeminent concern and orientation point for U.S. national security. That era is over. The United States has prioritized and shifted focus toward great power rivalry and interstate competition, with strategic emphasis placed on countering threats posed by China, Russia, and Iran. Counterterrorism, due to the persistent and ongoing threat of terrorism, remains a priority, but for the U.S. government it is now a second-tier one.

This priority shift has had and continues to have a broad and disruptive impact on the U.S. counterterrorism enterprise. It has forced the U.S. counterterrorism community to confront and spend more time examining some hard questions such as 'do we have the right priorities,' 'what level of terrorism risk is prudent to assume,' 'have we been effective and where have our efforts failed,' 'how can we improve,' and 'how can we streamline, 'right size,' or gain efficiencies across the CT mission.'[3]

Over the past several years, as part of this transition, the U.S. national security community has had to grapple with what CT looks like during this new era, and how these two key priorities—great power competition and counterterrorism—intersect or nest with one another. This is because the United States needs to figure out how it can effectively pursue and make progress toward advancing both priorities at the same time. A core part of the pathway to that goal is for the United States to not draw hard boundaries between these two problem-sets but to instead, as many have highlighted,[4] identify how America's counterterrorism capabilities and pursuits can complement efforts to bolster U.S. influence, access, and placement in key areas, or at least be leveraged to keep the terrorism threat 'in-check' enough so the United States can remain focused on more strategic threats.[5]

This is not to say that boundaries between these two national security challenges do not matter; they still matter a great deal, as there are limits to where, or just how much, CT and great power competition efforts overlap and the extent to which they can or should be nested. To avoid overlap for overlap's sake, the U.S. national security enterprise needs a clearer view of the areas where these two priorities converge, and how investments in each area can be leveraged to advance one another.

To help aid that transition, the United States should strategically frame the current CT moment as the compound era of U.S. counterterrorism. The term "compound"—"a thing that is composed of two or more separate elements; a mixture"[6]—is being used intentionally here, as during this new counterterrorism chapter, the United States and its partners are having to grapple with an evolving and more mixed environment across three key areas: priorities, terror threats, and counterterrorism.

At a strategic level, the United States is navigating a less narrow, more mixed set of priorities than it has over the past two decades—a period over which counterterrorism was the leading U.S. national security objective. The renewed emphasis on great power competition increases the likelihood of state-to-state level conflict. But it also—as other commentators have pointed out—raises the specter that future conflict between states will be more blended and that it may manifest, or at least be shaped by, irregular or asymmetric activity, including political violence by non-state actors. The proxy war fought between the United States and Soviet Union in Afghanistan, which principally shaped the evolution of al-Qa`ida and the Soviet Union's collapse, is an important case in point in this regard.

---

3 For context, see Russell E. Travers, "Counterterrorism in an Era of Competing Priorities," Washington Institute for Near East Policy, November 8, 2019.

4 For examples, see Matthew Levitt, "Rethinking U.S. Efforts on Counterterrorism: Towards a Sustainable Plan Two Decades after 9/11," Washington Institute for Near East Policy, March 8, 2021; Daniel Byman, "The Role of Terrorism in Great Power Competition," National Interest, April 23, 2022; Marcus Hicks, "Countering Terrorism While Competing with Great Power Rivals: Mutually Reinforcing, Not Mutually Exclusive," Modern War Institute, March 29, 2021.

5 For context on this point, see Nicholas Rasmussen's discussion on the need to suppress terror threats. Nicholas Rasmussen, "Navigating the Dynamic Homeland Threat Landscape," Remarks given at Washington Institute for Near East Policy, May 18, 2023.

6 Oxford language dictionary.

The nature of today's extremist and terrorism threat landscapes is the second area that defines the compound CT era. The United States has always had to deal with different types of terrorism, from the Unabomber to the Oklahoma City bombing and 9/11, but the terror threat landscape the United States confronts today is more mixed and the span of threats is broader and more diverse. The extremism landscape, which helps give rise to terrorism, is also more complex, dynamic, and broadly more interactive. Today's terror threat landscape is more compound in character.

Technology, and open access to technology, has also been shaping the counterterrorism landscape: the third principal area that defines today's CT era. Over the past two decades, there has been a rise in the number of stakeholders or 'players' who either have been meaningfully shaping, or have a role in, the world of counterterrorism and how specific counterterrorism actions or responses take place. Today's CT environment is more compound, as responses to modern terrorism threats often involve inputs and actions taken from commercial and public actors, from coalitions, and coordination and collaboration across and between a range of different types of partners.

The compound era of U.S. CT framing provides multiple benefits. At a high level, describing the moment in this way would explicitly acknowledge that terrorism and CT efforts are part of a much more complex and intersectional security landscape, what Isaiah Wilson and Scott Smitson have described as the compound security environment.[7] The term "compounded," as Wilson and Smitson explain, "refers to the increased interaction – interconnectedness and collision – of otherwise separate policy issues," an environment characterized by "the interaction effect at play between simultaneous and overlapping sources of instability."[8] This view of the environment, which embraces complexity and multi-dimensionality as a foundational starting point, is useful as it requires that U.S. responses to global security challenges be integrated and multi-dimensional as a starting point as well. As Wilson has highlighted separately, today's security environment "demands nothing less than a working at the nexuses and between the boundaries and seams of our own created divisions between matters of 'defense and security' from the traditional and nontraditional 'water's edge' that separates the foreign from the domestic."[9] Thus, instead of counterterrorism and great power competition being bifurcated as two separate issues, a compound view would examine how counterterrorism could be leveraged not only as a tool for threat mitigation (which is how it is primarily viewed) but also as a form of influence to help the United States more effectively compete, develop important relationships, or be a better partner in priority areas around the globe, such as the Sahel, the Levant, or the Philippines.[10]

The compound security environment framing that Wilson and Smitson outline is also beneficial as it reflects the often-messy ways in which counterterrorism and great power competition interact, blend, or influence one another in the real world, especially in key conflict theaters where the United States has strategic interests. Take Syria and Iraq, for example. While the conflicts in those two countries have always been multidimensional—and have been influenced by a range of actors and factors from

7 Isaiah Wilson III and Scott A. Smitson, "The Compound Security Dilemma: Threats at the Nexus of War and Peace," *Parameters* 50:2 (2020).

8 Ibid. The U.S. government and Department of Defense are already focused on interactions, and the interconnectivity, between different threats. As the 2022 National Defense Strategy stated: "Now and over the next two decades, we face strategic challenges stemming from complex interactions between a rapidly changing global balance of military capabilities; emerging technologies; competitor doctrines that pose new threats to the U.S. homeland and to strategic stability; an escalation of competitors' coercive and malign activities in the 'gray zone'; and transboundary challenges that impose new demands on the Joint Force and the defense enterprise. These developments and the threats they present are interconnected — in part because our competitors deliberately link them to erode deterrence, exert economic coercion, and endanger the political autonomy of states." "2022 National Defense Strategy of the United States of America," October 2022.

9 Isaiah Wilson III, "Rediscovering the Value of Special Operations," *Joint Forces Quarterly* 105, April 2022.

10 In commenting on the Islamic State case, and the future of U.S. special operations forces, Ike Wilson had the following to say: "The fact that the U.S. Government did this with such minimal investment, while assuming acceptable risk, must be understood and appreciated, even lauded, for what it was: a new paradigm in which the use and utility of SOF goes well beyond its two decades of direct action merely in the *context* of counterterrorism, but instead where direct action and counterterrorism are integral use-of-force activities endemic to, and not separate or separable from, GPC." Wilson. There are limits to the compound view approach, as CT and great power competition efforts or initiatives are not always going to nest or align. But where areas of synergy exist, or CT efforts can be leveraged to advance GPC initiatives and goals, those should be pursued.

terrorism to sectarian strife and regional power dynamics—during the height of the Islamic State's power and territorial holdings, concerns about terrorism were at the forefront, at least for the United States. But regional and great power competition dynamics also underpinned the Syrian civil war and the Assad regime's ability to survive, as Iran and Russia both had a lot to lose if that were to transpire.[11] As Wilson has noted, other factors shaped the conflict and the trajectory of its importance to the United States:

> What began as an effort to destroy the physical manifestations of the caliphate through direct action, raids, and strikes, many times in concert with state and nonstate actors committed to defeating the so-called Islamic State (IS), quickly became a mission to deter further Russian (and Turkish) territorial provocation, assure new partners (Syrian Kurds), deny freedom of action to Iran and its surrogates and proxies, defend critical resources and infrastructure, deny any resurgence of IS as an existential threat to friendly regional governments, and maintain U.S. access and influence where the East and West truly converge.[12]

The compound nature of the security environment in Syria is also reflected by the threats U.S. and partner forces currently face in the region.[13] U.S. forces who are in Syria to maintain pressure on and coordinate actions against Islamic State remnants, for example, have had to worry less about attacks from that group recently and more about rocket, mortar, and drone attacks by Iranian proxy forces.[14]

A different set of intersectional dynamics have been at play in Ukraine. In that conflict, the state-to-state level fight between Russia and Ukraine has been at the forefront. But the issue of extremism has been an undercurrent, a more micro-level issue, that has complicated the conflict on both sides and its potential longer-term tail. This has included extremist views expressed by pro-Russia Wagner elements, the history of Ukrainian units like the Azov Regiment that have openly embraced extremist ideas on the Ukrainian side, and the risks associated with the flow of foreign war volunteers to the conflict zone. While concerns rightly remain focused on the state-level fight, and Ukraine's defense, the issues of extremism and terrorism linger as factors that could shape the conflict's outputs over the longer term.

In key countries in Southeast Asia and Africa, terrorism remains a core intersectional issue that is deeply relevant to great power competition. There is no better case than the Philippines. For more than 20 years, defense cooperation between the United States and the Philippines has primarily been anchored by counterterrorism. U.S.-Philippine partnering across that span of time has helped to bolster the capabilities of the Armed Forces of the Philippines (AFP)—and the AFP's legitimacy—to degrade key terror networks, develop mil-to-mil relationships, build trust, and enhance interoperability. The announcement in February 2023 that Washington and Manila had agreed to create four new Enhanced Defense Cooperation Agreement (EDCA) sites in the Philippines, which will allow the United States to access those sites, store equipment, and conduct additional training with Philippine forces, happened because of the trust and close working relationship that DoD and AFP forged over more than two decades. Given the Philippines' geostrategic location, it is not hard to see how EDCA site expansion (from the previously agreed upon five to nine) benefits both countries and is a U.S. great power competition win that came about because of longstanding counterterrorism cooperation.

---

11 Wilson and Smitson used a different example to describe how the Islamic State's rise in the Levant evolved into a compound security issue. In their words: "On June 9, 2014, the self-declared Islamic State breached and erased the international boundary separating Syria and Iraq, making the crises in Syria and in Iraq compound into one so-called Syraq. The vital national security interests of the United States did not necessarily fall within one or both nation-states, rather it fell across their nexus." Wilson and Smitson.

12 Wilson.

13 As CENTCOM Commander General Michael "Erik" Kurilla testified in March 2023, the CENTCOM region is "a landscape of increasing complexity." See "Senate Armed Services Committee Hearing on Posture of USCENTCOM and USAFRICOM in Review of the Defense Authorization Request for FY23 and the Future Years Defense Program," March 16, 2023.

14 For example, see Phil Stewart and Idrees Ali, "US strikes Iran-backed facilities in Syria after drone kills American," Reuters, March 24, 2023.

There is a similar dynamic at play in Africa. While the United States has strategically moved on from terrorism being its leading national security concern, terrorism remains a primary and ongoing strategic threat for several countries on the continent, such as Mali, Burkina Faso, and Somalia. And so, even though it might not be the top U.S. priority, terrorism, not great power competition, is what many African partners—and potential partners—care about. In countries where that remains the case, counterterrorism can and should be used as a mechanism through which the United States can develop ties, build trust, enhance partner capabilities, and share and gain access to localized security data. For the United States, this type of activity can be leveraged to better understand the local and regional environment, to include how the actions, influence, and presence of China and Russia—and their own partners—are evolving. It would be foolish and counterproductive for the United States to overlook how counterterrorism, an area where the United States has developed considerable experience, capabilities, and currency, can be used to help develop or enhance security ties with partners (and potential partners) across the region. Indeed, as Christopher Faulkner, Raphael Parens, and Marcel Plichta, have noted: "Near-peer competition in Africa and counterterrorism cannot, and should not, be decoupled. In order to compete with other powers, the United States will have to conduct security assistance well, especially in the counterterrorism space."[15]

Another key benefit of framing the current moment of CT as the compound era of U.S. counterterrorism is that it reflects the complex and evolving set of terrorism and extremism-related threats that the United States now faces. Long gone are the days when the United States needed to worry primarily about one group or network like al-Qa`ida, headquartered abroad that sought to conduct spectacular attacks against the "far" enemy. This is because today's terrorism and extremism landscapes are more diffuse and compound; they are more intersectional, blended, interactive, and organizationally complex than they have been in the recent past. For example, today the United States needs to monitor the enduring threats posed by al-Qa`ida and the Islamic State and their regional partners; navigate a complex domestic extremism environment comprised of individuals, distributed networks, and militias that are motivated by varied ideologies and goals, and that leverage misinformation and/or conspiracy theories; and deter and contend with armed non-state proxies, or surrogates, supported by Iran and Russia that are either directly hostile to the United States or that, like the actions of the Wagner Group in Africa, principally complicate security environments. The ways in which commercial technologies and systems have been revolutionizing how actors—from non-state to state and hybrid entities—communicate, organize, and conduct operations is another core, cross-cutting challenge.

To minimize the risk of surprise and the likelihood that terrorism will distract U.S. great power competition efforts, the United States needs to pay close attention to how terrorism and extremism dynamics—and the character of each of these problems—are evolving. Over the past several years, a lot has been written about this topic. Thanks to that corpus of work, the counterterrorism community has a good appreciation for what those trends are[16] and what they may mean for the future of terrorism and extremism. But in reviewing this literature, the author found that the conversation about this topic suffers somewhat from being disjointed and not well aggregated, as written examinations of the issue either placed emphasis on one or two trends only or were 'light' and designed to be short, higher-level overviews.

As a result, the goal of this report is to better structure this research and examine the identified trends

15 Christopher Faulkner, Raphael Parens, and Marcel Plichta, "How Smarter U.S. Counterterrorism in the Sahel Can Pay Dividends for Great Power Competition," *CTC Sentinel* 16:4 (2023).

16 For example, see Colin P. Clarke, "Trends in Terrorism: What is on the Horizon in 2023?" Foreign Policy Research Institute, January 3, 2023. Five trends impacting white supremacist violence that Elizabeth Yates has highlighted are also quite useful, and this report leverages some of the trend framing that Yates identified. These include: an "increase across five dimensions of the movement: 1) Decentralization and accessibility; 2) Ideological fluidity; 3) Transnationality; 4) Speed in radicalization; 5) Mainstreaming." For background, see Elizabeth Yates, "Domestic Extremism in America: Examining White Supremacist Violence in the Wake of Recent Attacks," Testimony Before the United States Senate Committee on Homeland Security and Governmental Affairs, June 9, 2022.

in an organized way so that key terrorism trends and illustrative data or examples are available in one place. In doing so, this report calls additional attention to how these trends are shaping the behavior of terrorists and extremists, and how, to meet and stay at pace with these changes, the United States and its partners are going to need to respond in a more collaborative and integrated way.

Today's extremist, terrorism, and counterterrorism landscapes are being principally shaped by three cross cutting themes: complexity, diversity, and fluidity—interrelated characteristics that make it hard to conceptually bound, or draw neat borders around, key trends. The first section of this report highlights the geographic span of terrorism today, and the range of threats and national security considerations that this issue presents for the United States as it seeks to devote less time, attention, and resources to CT efforts around the globe. The second section focuses on structure and highlights how extremist and terrorist organizational modalities and preferences have been shifting, an issue that presents observation, monitoring, and disruption challenges for counterterrorism analysts and practitioners. The third and fourth sections explore the interactive, fluid, and intersectional dynamics that have been driving aesthetic/cultural, motivational, informational, organizational, and, to a more limited extent, operational changes across extremists and terrorist milieus. Section three focuses on participatory dynamics and the interactive and customizable nature of specific forms of terrorism today, while section four explores the fluid and intersectional ways in which individuals and extremist ecosystems have been interacting and learning from one another. Section five examines issues of speed and potential scale, and how—at least in the U.S. context—political violence over the last several years appears to have become more normalized. The last section explores how technology continues to serve as a key locus of competition between terrorists and counterterrorists, and how technology has been reshaping the landscape of CT stakeholders. The report then concludes with key implications of these trends for U.S. and partner-nation counterterrorism strategies and efforts and includes a set of 11 priorities that can help to guide the next chapter of U.S. counterterrorism.

1. Span: A Diverse, Geographically Diffuse, and Complex Array of Threats

"Compared to 20 years ago, the threats facing us today are more ideologically diverse and geographically diffuse."[17] – Dr. Liz Sherwood Randall

The terrorism threat has metastasized considerably since 9/11, and especially over the past decade.

Instead of needing to understand and combat one or two primary terror networks, today the United States and its partners need to confront and figure out ways to proactively manage the threat posed by a more diverse, diffuse, and complex array of extremists. This includes the ongoing threat posed by mainstay terror networks like al-Qa`ida and the Islamic State—which although not as powerful or capable as they once were, remain committed, enterprising, and dangerous—a collection of smaller and more regionally or locally focused jihadi groups; a cohort of capable proxies supported by states like Iran and Russia; a diverse and ever-evolving ecosystem of violent far-right,[18] far-left, anti-inclusion, anti-government, anti-technology, single-issue, and 'overthrow the status quo' extremists; and individuals motivated by other grievances.[19] Many of these 'actors' have existed, and presented different types of terrorism threats, before; the mere existence of these threats is not new. But what is new is how active each of these threat streams are and the ability of each to conduct attacks, present credible threats, or create operational or other security challenges to U.S. national security interests.

17 "Remarks as Prepared for Delivery by Assistant to the President for Homeland Security, Dr. Liz Sherwood-Randall on the Future of the U.S. Counterterrorism Mission: Aligning Strategy, Policy, and Resources," White House, September 9, 2021.

18 For a good overview of the complex far-right extremist landscape, see Mark Pitcavage, "Surveying the Landscape of the American Far Right," George Washington University Program on Extremism, August 2019.

19 How the Federal Bureau of Investigation has chosen to categorize the domestic terrorism landscape in the United States provides another window into the different types of domestic terrorism threats streams. For backgrounds, see "Domestic Terrorism: Definitions, Terminology, and Methodology," FBI, November 2020.

Multiple layers, or levels, of complexity make monitoring and evaluating this broad universe of actors hard, especially during an era when the United States needs to devote more time, resources, and strategic attention to threats posed by near-peer adversaries like China. Geographic diversity, and the diffuse nature of today's terror landscape, is one important layer of complexity with which practitioners must grapple. For example, there are more than 20 established terror organizations active in the Afghanistan-Pakistan region alone.[20] And even though there is a considerable amount of interaction between jihadi groups based in that area, each of those entities has its own identity, attributes, priorities, and set of capabilities, which have a bearing on what type of threat they may pose. Additionally, we have seen these groups cooperate and compete with one another under different circumstances, making it hard to simply look at the 'biggest' threat in any one area.[21]

The jihadi threat environment in Africa represents a similar, and arguably more profound, challenge, as there are multiple seasoned organizations loyal to al-Qa`ida and the Islamic State—as well as other non-state armed groups and mercenaries—active on the continent that complicate local, regional, and international security.[22] Filter in the mix of armed proxies active in places like Iraq and Syria (and other areas) that embrace terrorism, and it becomes clear that terrorism remains a key issue in a lot of places where the United States either has key interests and/or preexisting security concerns.

The geographic diversity and diffusion of the terrorism threat is not just an international problem. It has domestic characteristics as well. As Nicholas Rasmussen, the Department of Homeland Security's counterterrorism coordinator, recently observed about America's domestic terror threat environment:

> I don't think of it now as being attached to major urban or suburban areas. If you think back to most of the post-9/11 periods, the plots we would have disrupted … tended to be in large American cities … Now, as you can see just by reading the news, all 50 states, rural, suburban, urban, there is no environment that you can point to across the United States where we aren't at risk of, some form of extremism of one or another narrative flavor. So that feels different than in past years.[23]

2. Structure: A Spectrum of Organizing Forms and Modalities

"Unlike 21 years ago, the American public today is more likely to experience a terrorist attack by an individual attacker than a highly structured terrorist organization. Today's lone-actor threats can mobilize in unpredictable ways based on a variety of motivations. These individuals almost certainly mobilize to violence independently without direction from specific groups."[24] – Christine Abizaid

Another core complicating factor is that today's terrorism threats manifest in different organizational forms and derive their support—and in some cases capabilities—by leveraging different approaches, such as attacks that are remotely encouraged, or enabled, from afar, approaches that are not static but evolving. These dynamics make it hard for counterterrorism practitioners to gain analytical or operational efficiencies across threat streams, as how a group, network, or ecosystem function, and how an individual can interact with each form, can vary from one threat type to the next.

20 For background, see the State Department's Foreign Terrorist Organization (FTO) list at "Foreign Terrorist Organizations," Bureau of Counterterrorism, U.S. Department of State, n.d.

21 The author would like to thank Daniel Milton for highlighting and recommending this point.

22 For background, see Tricia Bacon and Jason Warner, "Twenty Years after 9/11: The Threat in Africa – The New Epicenter of Global Jihadi Terror," *CTC Sentinel* 14:7 (2021).

23 Rasmussen.

24 "Statement for the Record: Ms. Christine Abizaid Director, National Counterterrorism Center, United States Senate Committee on Homeland Security and Government Affairs Annual Threat Assessment to the Homeland," November 17, 2022.

An ongoing debate among terrorism and extremism researchers is just how much organization, or organizational structures, matter today. This debate is deeply intertwined and influenced by the effect and increasingly important role that digital ecosystems play in helping to facilitate real-world violence.[25] Some researchers, for example, have argued that we are in a post-group or post-organizational phase of extremist violence – "where the fluid boundaries between organisations and movements, direction and inspiration, and online and offline are becoming more and more ambiguous."[26] As noted by Amarnath Amarasingam, Marc-André Argentino, and Graham Macklin, the academic literature has "highlighted this post-organizational shift in the REMVE [Racially and Ethnically Motivated Violent Extremist] space, whereby membership in and support for different groups have become less clear, and online activity has made it easier for transnational movements to grow and change. Attacks are carried out by people who have very weak or no ties to specific groups. Instead, violent extremists draw on a shared culture and set of beliefs."[27] But, even though some extremist communities and networks rely much less on groups and organizational structures, especially categories of domestic extremists active in the United States,[28] hierarchy and organizational form still matters a great deal to other threat networks. What organizational aspects matter to networks or threat ecosystems these days, and how we can think about the evolving relevance of organizational structures and form, is an area where more developed conceptual work by terrorism studies scholars and specialists from other academic disciplines is needed.

Given the variance, today's terrorism threats are best understood as occurring across a spectrum of organizational forms and modalities,[29] whereby just how much organizational attributes matter, or networks rely on them, is dependent on local and situational context. Al-Qa`ida and the Islamic State, for example, have generally embraced hierarchy and organizational structures, likely because these types of groups operate and are predominately based in countries where they enjoy some form of safe haven or where the local environment is permissive enough for them to embrace organizational forms. Internal documents produced by the Islamic State illustrate how it was obsessed with meticulously cataloging the personal details of its recruits.[30] One spreadsheet it created, for instance, contained details on more than 50,000 members, with each individual entry organized by the division and sub-tier military unit that individual had been assigned to.[31] So, for an entity like the Islamic State, organization and organizational form still matters a great deal, and in many respects remains 'core' to how it operates. The same goes for an entity like Lashkar-e-Taiba and its partner organization Jamaat ud-Dawah, which for more than two decades have developed and operated a network of physical locations in Pakistan where recruits and members can learn, organize, and train.

25 As Cynthia Miller Idris has noted: "Violence is mostly perpetrated by lone actors who are influenced by ideas online rather than by plots hatched by group leaders in secret gatherings." See Cynthia Miller-Idriss, "Extremism has Spread Into the Mainstream," *Atlantic*, June 15, 2021. For additional context, see Heather J. Williams et al, "The Online Extremist Ecosystem: Its Evolution and a Framework for Separating Extreme from Mainstream," RAND, 2021. For a good example of how offline meet-ups and encounters can still matter for those extremists who are connected online, see H.E. Upchurch, "The Iron March Forum and the Evolution of the 'Skull Mask' Neo-Fascist Network," *CTC Sentinel* 14:10 (2021).

26 Milo Comerford, "Confronting the Challenge of 'Post Organizational' Extremism," Observer Research Foundation, August 19, 2020. For additional perspectives, see Alex Newhouse, "We are in the post-group, post-ideological, post-political phase of extremist violence …," Twitter, July 6, 2022, and Jacob Davey, Milo Comerford, Jakob Guhl, Will Baldet, and Chloe Colliver, "A Taxonomy for the Classification of Post-Organisational Violent Extremist & Terrorist Content," Institute for Strategic Dialogue, January 2022.

27 Amarnath Amarasingam, Marc-André Argentino, and Graham Macklin, "The Buffalo Attack: The Cumulative Momentum of Far-Right Terror," *CTC Sentinel* 15:7 (2022).

28 Bruce Hoffman and Colin Clarke, "The Next American Terrorist: The Growing Irrelevance of Organizational Structure for U.S. Domestic Terrorism," Cipher Brief, July 2, 2020.

29 The author would like to give a hat tip to Ethan Spangler for highlighting that it is helpful to view "things across a spectrum of organizations." See Ethan Spangler, "I think it's necessary to view things across a spectrum of organization. On the explicit side …," Twitter, July 7, 2022.

30 Daniel Milton and Don Rassler, *Minor Misery: What an Islamic State Registry Says about the Challenge of Minors in the Conflict Zone* (West Point, NY: Combating Terrorism Center, 2019).

31 Ibid.

This is not to say that a group like the Islamic State does not embrace other forms, that organizational diversity does not exist within and across the jihadi community, or that views within the jihadi milieu on this issue have not been evolving. How al-Qa`ida and the Islamic State have approached external operations is an important case in point. For a long period, al-Qa`ida's approach to external operations was generally driven in a top-down, hierarchical, and more structured manner. Part of what set the Islamic State apart from al-Qa`ida was that the former embraced and encouraged a more crowdsourced approach to external operations, an approach that sought to inspire remote online enthusiasts to conduct local attacks in their home countries on its behalf so that the group could complement its own top-down driven efforts (which it also pursued).[32]

Differences in organizational approaches, and the level of reliance on organizational structures, are even more diverse and profound in other threat areas. The domestic extremist ecosystem in the United States, for example, is comprised of an array of entities motivated by different ideals and goals that embrace varied, and in some cases blended, organizational approaches. For example, some nodes of the far-right extremist network, like anti-government militia groups (i.e., Oath Keepers), still rely more on hierarchical leadership models and physical in-person interactions among members, and in that way, they 'look' and generally act more like organizations with easier to identify forms of infrastructure. Then there is an entity like the Proud Boys, which has "a national apparatus with local chapters that operate on a semi-autonomous level" but whose activity at a local level can often be more "dynamic and diffuse," or less centrally controlled.[33] And then there are other threat streams such as accelerationism-motivated or -minded networks and types of racially and ethnically motivated extremists that are designed to be or appear 'center-less' and operate in an even more decentralized, distributed, and self-organized way.

The mix of individuals and networks that have been charged in relation to the siege of the U.S. Capitol on January 6, 2021, and how those networks came together, also highlights the diversity that is at play. According to a January 2022 analysis of court filings conducted by the Chicago Project on Security and Threats, of the 861 individuals who have been arrested and/or charged with a crime related to January 6th, 86% were "unaffiliated with pre-existing militias/extremist organizations and groups."[34] This mix of individuals who were not affiliated with a specific network or group, such as the Proud Boys or Oath Keepers, ended up coalescing and operating alongside those groups as a diversified mob that shared common interests and objectives. For practitioners, the events of January 6th highlight how they need to understand the system or collective, mob-like dynamics that brought a diverse collection of individuals and groups together and the individual, more micro level pieces of the whole. This type of analysis is more complicated than analysis of more hierarchically structured groups, in part because membership is not as clearcut, and because the influence of the networks often far exceeds what a standard link-chart might show.

The broad availability of secure forms of communication and rise in the communicative power of the individual—the ability for an individual to express themselves and make their own mark in the digital age—has certainly compounded the shift from organization-centric terror approaches to individual-based and more loosely defined ones. Some have argued that the shift is even more profound, and that "contemporary extremism" does not emerge from groups but instead "arises out of swarm dynamics in deep internet subcultures, where identities are rapidly fused and violence is used as a revolt against

32 For background, see Daveed Gartenstein-Ross and Madeleine Blackman, "ISIL's Virtual Planners: A Critical Terrorist Innovation," War on the Rocks, January 4, 2017.

33 Matthew Kriner and Jon Lewis, "Pride and Prejudice: The Violent Evolution of the Proud Boys," *CTC Sentinel* 14:6 (2021).

34 Robert Pape, "American Face of Insurrection: Analysis of Individuals Charged for Storming the US Capitol on January 6, 2021," Chicago Project on Security and Threats, January 5, 2022. As of July 6, 2023, the number of individuals charged in relation to events at the Capitol on January 6, 2021, has risen to more than 1,069. For background, see "30 Months Since the Jan. 6 Attack on the Capitol,"United States Attorney's Office District of Columbia, U.S. Department of Justice, July 6, 2023.

the fabric of society."[35] The ongoing shift toward more decentralized structures and 'form' creates significant observation and detection challenges for the government and the private sector.

The next two sections examine how the fluid, interactive, and intersectional nature of today's extremism and terrorism landscapes is reshaping how individuals pursue and frame their acts of violence and how extremist subcultures connect with and learn from one another. Section 3 places emphasis on the individual and an emerged set of participatory dynamics that helps radicalized individuals to commit and associate their acts of violence as part of a broader cause or movement. Section 4 looks at the intersections across extremist networks, and examines how different, and what appeared to previously be divergent, extremist online ecosystems and ideologically oriented camps have been interacting, learning from one another, and discussing how and where they have common ground.

3. Participatory Dynamics: Interactive, Momentum-Based, and Customizable

Key quarters of today's terror landscape are more interactive[36] and gamified,[37] where momentum and the ability for an individual to customize—to tailor and frame their attack on their own idiosyncratic terms—and link their effort as part of a broader collective are also helping to drive the pace and impact of threats, and push threats in new directions. These dynamics have been amplified by the development and more regularized use of an operational framework, a playbook, or "cultural script"[38] that allows individuals to associate their own personalized attack as part of a broader movement, or corpus, of similarly minded incidents. And in this way, with the operational framework functioning as a type of glue and the online environment serving as network and information- and knowledge-sharing ecosystem, the individual and their act can become part of a broader movement or distributed collective.

Various researchers have highlighted the connectivity that exists between individual far-right terror attacks, and how they have functioned as part of a momentum-based, but distributed, threat stream. Here, it is worth quoting Amarasingam, Argentino, and Macklin at length:

> The Christchurch attack had a catalytic effect upon extreme-right actors, sparking a chain reaction of mass shootings. Shortly after the Christchurch attack, extreme-right terrorist attacks took place in Poway, California (April 2019); El Paso, Texas (August 2019); Bærum, Norway (August 2019); and Halle, Germany (October 2019). By the end of 2019, five individual extreme right terrorists had killed a total of 78 people, in four countries, on three separate continents.
>
> Each of these attacks, and dozens of smaller instances of violence and attempted violence, followed what sociologist Ralph Larkin called (with regard to school shootings referencing Columbine) a "cultural script." In each instance, this crop of extreme-right terrorists who claimed inspiration from the Christchurch attack have sought to exceed its death toll, incite further violence, and honor the attacks with their own violence. The Buffalo terrorist attack conformed to all three of these aspirations.[39]

35 See Alex Newhouse, "We are in the post-group, post-ideological, post-political phase of extremist violence …," Twitter, July 6, 2022.

36 "The Violent White Supremacy Issue," Current 2, n.d.

37 As noted by Jigsaw: "This gamification of violence by white supremacists online is common, and is incentivized either top down - where group leaders offer members badges, titles, or other affordances for hateful acts - or bottom up - where individual forum members create online competition around a distributed virtual scoreboard tallying deaths or other acts of violence." "The Violent White Supremacy Issue." See also Firas Mahmoud, "The Gamification of Jihad: Playing with Religion," DIIS Report, September 27, 2022, and Robert Evans, "The El Paso Shooting and the Gamification of Terror," Bellingcat, August 4, 2019.

38 Ralph W. Larkin, "The Columbine Legacy: Rampage Shootings as Political Acts," *American Behavioral Scientist* 52:9 (2009): pp. 1,309-1,326.

39 Amarasingam, Argentino, and Macklin. For an additional view on the gamified nature of these attacks, see Jigsaw's "The Violent White Supremacy Issue," which noted: "Their online communities described the death tolls of each attack as 'high scores,' comparing the attacks as events in the same apocalyptic live action role-playing video game."

The chain reaction in attacks, as separately noted by Macklin, has been "fomented within the violent sub-cultural online milieus of right-wing extremism. This digital eco-system is fueling a cumulative momentum, which serves to lower 'thresholds' to violence for those engaged in this space, both in the United States and elsewhere, as one attack encourages and inspires another, creating a growing 'canon' of 'saints' and 'martyrs' for others to emulate."[40] And as "more and more people participate, the thresholds (both social and moral) for partaking in violence begin to lower. And as they do, increasing numbers of people are able to contemplate and indeed have situated their own actions within a continuum of violent activity that has preceded their own, giving the phenomenon a depth of meaning that the word 'copycat' fails to convey."[41]

The presence and repeated use of common aesthetic, performative, and operational attack features[42] highlight the general playbook that is being used. While customized to each person, this playbook often involves the use of specific visual aesthetics; a semi-automatic or automatic firearm, or a handgun; the targeting of an ethnic, racial, or religious minority; and at times the livestreaming of the attack and public release of a personal manifesto.[43] Amarasingam, Argentino, and Macklin use the case of Payton Gendron, the Buffalo shooter, to put these features into context:

> Instead of using Facebook Live, as [Christchurch attacker Brenton] Tarrant had, Gendron transmitted his killings via Twitch, the online gaming platform that the Halle terrorist had also utilized to broadcast his attack. The Buffalo terrorist's visual aesthetic mirrored Tarrant's, however. He too painted his weapons with the key ideological reference points, individual inspirations, and racial slurs, while, in the commission of his violence, he dressed, like Tarrant, in combat gear as part of his self-delusion that he was a military "partisan" fighting against an occupying force.

Another common feature, or binding agent, in key far-right attacks have been mobilizing concepts such as the "Great Replacement" conspiracy theory,[44] a theory that—given its broad-based nature—"in essence [functions as] an empty vessel that its adherents can fill with their own particular racial animus." This provides a pathway for radicalized individuals to customize or personalize their own attack, specifically target selection, but also link their unique operational contribution to a broader movement that leverages and shares the Great Replacement as a more common frame. As noted by Amarasingam, Argentino, and Macklin:

> This explains the heterodox nature of the racist target selection seen during this 'wave' of extreme-right terrorist attacks since 2019. Gendron targeted Blacks; Tarrant chose Muslims. A decade earlier, Breivik had drawn upon his own anti-Muslim racism to target government officials and teenage Labour party activists instead, believing them to be "traitors" for facilitating Muslim immigration and multiculturalism in the first place. Tarrant's own

40 Graham Macklin, "The El Paso Terrorist Attack: The Chain Reaction of Global Right-Wing Terror," *CTC Sentinel* 12:11 (2019).

41 Ibid. A helpful framework that Macklin highlights is "Mark Granovetter's 'threshold model of collective behavior,' which has recently been used to interpret the prevalence of high school massacres, is useful. Put simply, Granovetter's model enjoins analysts to consider these violent acts not simply as resulting from individual decision-making, each considered in isolation from one another, but as part of a broader social process in which violence is enacted in reaction to, and in combination with, other actors."

42 As noted by Jigsaw, "Not only were Tarrant and Crusius not 'lone wolves,' they were part of the same distributed online network. Both wrote similar warning messages to their online community before their attacks. They used similar rhetoric and ingroup language to broadcast their intent. They both posted manifestos on 8chan describing similar supremacist ideals of a white ethnostate. They both described a perceived existential threat to whites from a conspiracy theory - a 'great replacement' by immigrants. They both described their automatic weapons used in the attack as 'gear,' as though they were players in a video game. See "The Violent White Supremacy Issue."

43 Ibid. "In a study of lone actor extremists, which was not confined to violent white supremacists, the National Center for the Analysis of Violent Crime found that 96% of lone actor extremists 'produced writings or videos intended to be viewed by others' including videos, blogs, or manifestos online."

44 For background on how the Great Replacement Theory served as a motivator for various far-right attacks, see Yates. See also Jacob Davey and Julia Ebner, "'The Great Replacement': The Violent Consequences of Mainstreamed Extremism," Institute for Strategic Dialogue, July 7, 2019, and "The Insurrectionist Movement in the United States: Professor Robert Pape," Intelligence Matters podcast, October 2022.

> acolytes targeted a similarly diverse array of ethnic and religious minorities: Jews (Poway), Mexicans (El Paso), and Muslims (Bærum), each of whom, in the idiosyncratic worldview of the individual killer in question, fulfilled the role of occupier and usurper. The Halle attacker had initially targeted Jews but having failed to gain entry to a synagogue, turned to targets of opportunity—murdering a female passerby and a man eating lunch in a kebab shop instead.[45]

An additional concerning feature of these developments is that the distributed community of individuals who have conducted these recent attacks, and the online networks of individuals who have encouraged and canonized them, have embraced learning as way to increase the impact and lethality of attacks across time. Indeed, as Amarasingam, Argentino, and Macklin also point out, just days prior to his attack, Gendron posted the following message on Discord:

> I need you guys to do a deep analysis of all mistakes I made and how to fix them … mistakes will be made. [Halle, Germany, synagogue shooter] Stephen [sic] Balliete and [Poway, California, synagogue shooter] John Earnest are examples. They had the right intentions but still it went wrong for them. What's important is to honor these men who at least tried, and to learn from their mistakes.[46]

While the playbook discussed above helps to facilitate, or provide voice and enhanced forms of recognition for, more idiosyncratic terror attacks conducted by individuals often motivated by far-right extremist ideas, the Islamic State's creation of its own do-it-yourself operational template had a similarly disruptive, and impactful, effect. That template, which encouraged Islamic State sympathizers from around the world to conduct terror attacks in their home countries or countries of residence as a way to contribute to and advance the group's mission and vision, successfully inspired various individuals to act.[47] The planning for those remote Islamic State-motivated attacks varied from person to person. When possible, Islamic State operatives tried to 'coach' and/or provide resources to enable those external attacks where the group was more hands on. But the Islamic State's calls for remote action, which often included recommendations for weapons, tactics, and potential targets, also led to several individually driven and customized local attacks executed by enthusiasts who had no known direct contact with the group or its representatives.

While different in form and character, both playbooks have provided opportunities for individuals to associate their acts of violence with either a broader movement, group, or ideological objective.

The next section builds on this one and explores how interactions within and across different extremist milieus have been complicating the world of extremism and the type of threats that might manifest in the future.

4. Fluidity and Intersections: A Driver of More Complex and New Threats

"The mainstreaming of extremism has itself led to the second trend: a scrambling and recombination of extremist groups and ideas … These changes have rendered violent extremist movements less coherent and more unpredictable than ever before."[48] *– Cynthia Miller-Idriss*

Over the past 20 years, there have been profound changes to how individuals communicate and receive information and the scale of data an individual can access with a connected device. These dynamics

45 Amarasingam, Argentino, and Macklin.

46 Ibid.

47 For background, see Alexander Meleagrou-Hitchens and Seamus Hughes, "The Threat to the United States from the Islamic State's Virtual Entrepreneurs," *CTC Sentinel* 10:3 (2017). See also Gartenstein-Ross and Blackman, "ISIL's Virtual Planners: A Critical Terrorist Innovation."

48 Cynthia Miller-Idriss, "How Extremism Went Mainstream: Washington Needs a New Approach to Preventing Far-Right Violence," *Foreign Affairs*, January 3, 2022.

have also been changing the way individuals and networks interact with, adopt, and communicate extremist ideas, and how extremists can actualize their plans, federate, and enable others. The net effect is that extremism and terrorism are both more fluid and intersectional than they have been in the past, a trendline that has led to a rise in more blended, individually customized, and composite[49] or coalitional-based threats,[50] and that holds the potential to lead to more change and some unique collaborations.[51] The impact of this trendline varies across threat streams and the preferences of individuals, as while some networks are less boundary-adhering, and are more accepting of acts of violence that blend or incorporate different ideological inputs, other networks, such as the Islamic State, still place important stock in maintaining clearer ideological and organizational boundaries.

The 'terrorism is fluid' trend is far from new,[52] but our understanding of where, how, and why this trend has been occurring, its full significance, and how we can explain and conceptualize it has been evolving. There is still a lot we do not know, but two high-level observations seem clear. First, the fluid and intersectional trendlines, and their significance, are being influenced by other trends. For example, the fluidity observed across extremism landscapes today is likely being deeply enabled by the ongoing trend toward decentralization that this paper also discusses, a trendline that has been supercharged by online forms of networking and the "hyper mobilizing" power of social media.[53] These factors have all provided individuals with more opportunities to be selective, customize, and individualize their own extremist path. Second, the fluid and intersectional patterns are an integrated phenomenon, as the conditions that enable and make it more acceptable for individuals and networks to bound across and move in a more fluid way between different extremist 'spheres' also end up enhancing and diversifying the areas and ways that extremists intersect and influence each other. Or put more simply, the more fluid and boundary-crossing an ecosystem is, the more intersectional it is also likely to be.

There are reasons to be concerned about the fluidity and intersectionality that has taking place in the extremism world. On a practical level, it is hard to track activity across an environment and ecosystem that is more fluid, as prior indicators, or signs, of concerning activities and behavior may be less relevant and/or more difficult to spot. The potential for innovation and surprise are also important concerns. A book published in 2004 by entrepreneur Franz Johansson, *The Medici Effect: What Elephants and Epidemics Can Teach Us About Innovation*, highlights one of the core reasons why. In his book, Johansson argues that "many key primary innovations arise as a result of intersectionality."[54] The book specifically makes the case that "increased creativity and innovation occurs through diversity" and that the most powerful innovations happen "at the 'Intersection,' where ideas and concepts from diverse industries, cultures, and disciplines collide."[55] Johansson's book does not focus on extremism, but the general idea that he conveys stills has analytical utility, even if only as a frame of reference, for the potential outputs and risks that may emerge from the intersectionality that has been taking place across the extremism world.

For practitioners, the interactivity between different networks who embrace violence and hate, is likely to spur new innovations and lead to surprises in the future. As a result, it is important that attention is focused on those points of intersection, as they are going to offer clues and early signs of how threat

49 For background on composite dynamics, see Daveed Gartenstein-Ross et al, "Composite Violent Extremism: A Radicalization Pattern that is Changing the Face of Terrorism," Lawfare, November 22, 2022.

50 Jade Parker, "Accelerationism in America: Threat Perceptions," GNET, February 4, 2020; "Accelerationism and the Threat to American Democracy," Loopcast, January 29, 2020.

51 Miller-Idriss, "How Extremism Went Mainstream."

52 For example, five years ago in 2018, the U.S. National Security Strategy for Counterterrorism recognized how "today's terrorism landscape is more fluid and complex than ever."

53 See Michael Jenson's comments in Nick Shifrin, Sam Lane, and Ali Rogan, "Mainstream presence of Proud Boys, other extreme groups creates mass radicalization fears," PBS News Hour, January 4, 2022.

54 "The Medici Effect: A Simple Introduction," World of Work Project, n.d.

55 Ibid.

networks are evolving, and how different extremist nodes are learning from each other.

The fluid and intersectional character of today's extremist environment has been taking place, and can be observed, across ideological, informational, organizational, and to a more limited extent operational areas. For example, misinformation and conspiracy theories play an important role in motivating and/or radicalizing many domestic extremists active in the United States, and other extremists abroad. The importance and role played by misinformation is reflected by its mention in the United States' first strategy to counter domestic terrorism, which identified the issue as a "crisis."[56] Given the broad accessibility of misinformation and the popularization of various conspiracy theories, such as the QAnon movement,[57] and how integrated and intertwined misinformation and extremism can be these days, it can be hard to neatly separate, or draw some type of meaningful boundary between where one problem starts and the other ends, especially since the amount of 'bleed over' is case dependent and can vary from person to person.

To help spotlight, unpack, and ground these trends, this subsection examines some of the fluid and intersectional characteristics that are occurring, and have been shaping, the world of extremism and terrorism. Emphasis is placed on two areas: 1) the interplay, including learning, admiration, and search for common ground, between online subcultures of hate and division; and 2) how the decentralized and highly individualized nature of today's extremist environment fuels the ability of individuals to operate in more fluid ways across ideological and organizational categories.

Common Ground at the Fringes: Interplay between Online Subcultures of Hate and Division

One useful window into the intersectional nature of today's extremist landscape that researchers have highlighted is learning, the sharing of content, and cultural transmission that has taken place between far-and-alt-right networks and jihadi- and Gen-Z-salafi online milieus. As Meili Criezis and Brian Hughes have noted, "interaction across ideological spectrums is not a new phenomenon"[58] but is instead being facilitated and enabled by the accessibility and interactivity that digital environments and communication platforms are designed to foster.

The interest that these different online communities have for one another extends beyond general curiosity, as there is evidence that it is also driven by a certain level of admiration for or glorification of what the opposing ideological camp has achieved.[59] For example, as reported by Ben Makuch and Mack Lamoureux in 2019, "the neo-Nazi group Atomwaffen Division [AWD], and its Canadian propagandist 'Dark Foreigner', created an image eulogising al-Qaeda's former leader Osama Bin Laden."[60] In a post "titled 'The Islamic Example'" that AWD put out that same year, AWD explained "that the culture of martyrdom and insurgency within groups like the Taliban and ISIS is something to admire and reproduce in the neo-Nazi terror movement."[61]

56 "National Strategy for Countering Domestic Terrorism," June 2021.

57 Marc-André Argentino, Adnan Raja, and Aoife Gallagher, "She Drops: How QAnon Conspiracy Theories Legitimize Coordinated and Targeted Gender Based Violence," Institute for Strategic Dialogue, October 10, 2022.

58 Meili Criezis and Brian Hughes, "Erstwhile Allies and Community Convergence: A Preliminary Study of Online Interactions Between Salafi-Jihadists and White Supremacists," GNET, August 31, 2021.

59 "Moustafa Ayad on jihadist and white nationalist fusion," Theory of Change podcast #024, November 2, 2021.

60 Ben Makuch and Mack Lamoureux, "Neo Nazis are Glorifying Osama bin Laden," Vice, September 17, 2019.

61 Ibid.

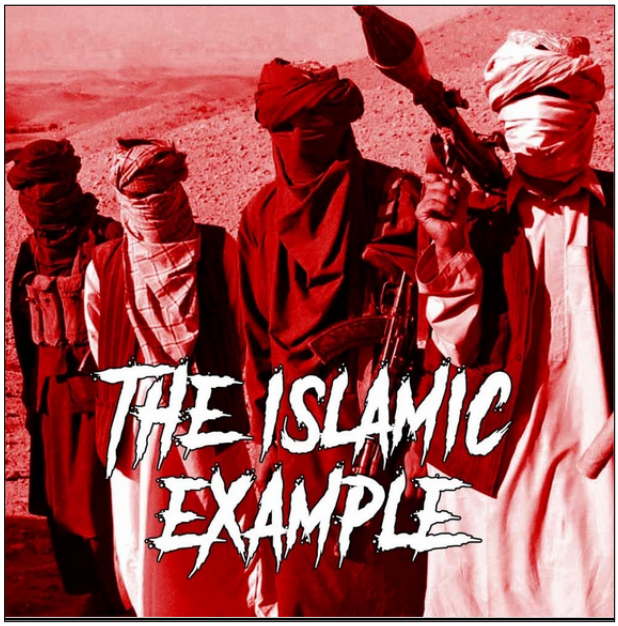

Figure 1: "An Image from AWD website" (Source: Vice News)[62]

The two communities have taken strategy and operational cues from one another as well. The manifesto that Anders Breivik—the "right-wing, anti-Islam terrorist" that killed 77 people in Norway in 2011—left behind, noted how "lone acts of jihadist terrorism were a main source of his inspiration."[63] As Petter Nesser has observed, in that document, Breivik wrote that "solo-cell systems in combination with martyrdom is the most efficient and deadly form of modern warfare. This strategy was adapted by jihadist groups. And now we will be using it as well."[64] There are other more recent examples that demonstrate how far-right extremists have awareness of, and have learned from, jihadis. In 2018, for instance, The Base, a neo-Nazi extremist group, "recommended *The Management of Savagery* to its online followers. The book, written by al- Qaeda strategist Abu Bakr Naji in 2004, is regarded as one of the most influential texts for ISIS strategists who oversaw the establishment of the Islamic State in Iraq and Syria."[65]

There is also evidence that members active in each community have shared tactical and training materials, and that individuals active in far- and alt-right and Gen-Z-salafi circles visit some of the same online spaces—and in more limited cases, have had direct ties. For example, in 2019, "ISIS-bomb making videos were circulated on Telegram channels associated with Feuerkrieg Division, an international neo-Nazi movement popular with Americans, and part of the wider online white supremacist Siege movement."[66] That same year, neo-Nazi Jack Reed, was convicted by a U.K. court "of plotting attacks including firebombing synagogues."[67] As part of his plot preparation, he "consulted

62 Ibid.

63 Petter Nesser, "Individuals Jihadist Operations in Europe: Patterns and Challenges," *CTC Sentinel* 5:1 (2012). It is also important to point out other types of groups have espoused the idea of leaderless resistance. For example, as noted by Jigsaw, "In 1983, white supremacist Louis Beam argued that like-minded individuals should operate independently, without central coordination, in order to evade law enforcement and create, 'an intelligence nightmare.'" See "The Violent White Supremacy Issue."

64 Nesser.

65 Bennet Clifford and Alexander Meleagrou-Hitchens, "Imitators or Innovators: Comparing Salafi-Jihadist and White Supremacist Attack Planning in the United States," Program on Extremism, April 2022.

66 Ibid.

67 Clifford and Meleagrou-Hitchens. See also "Terror plot: Durham teenage neo-Nazi named as Jack Reed," BBC, January 2021.

al- Qaeda and ISIS bomb making guides."[68] Extremism researcher Meili Criezis has also observed that "users with distinctly Salafi-jihadist or white supremacist usernames cohabiting in the same online chat space."[69] "In another instance," Criezis observed that "a Salafi-jihadi channel admin" admitted to being "friends with the admin of a well-known far right channel."[70]

A separate 2022 study of the "narrative syncretism" between accelerationists and salafi-jihadis authored by Marc-André Argentino, Amarnath Amarasingam, and Emmi Conley found that both communities were targeting similar recruitment demographics and were using "comparable digital recruitment tactics" focused on overlapping online spaces.[71] The authors of that study also concluded that the two communities were following a "pragmatic engagement approach that prioritises outreach over content," which in their view demonstrated "how accessing key recruitment demographics" was "likely more important than the misused content itself."[72]

One of the more interesting developments has been "cultural transmission" between these different digital communities, and how they have appropriated, or blended, visual and cultural aesthetics from one another. In a landmark study of Gen Z salafi 'Islamogram'[73] influencers, Moustafa Ayad found that members of that network were "using a set of tropes originally espoused by the alt-right and far-right" and were "appropriating the power of exclusionary language and imagery as a means to define themselves."[74] A key example of this phenomenon is the avatar that the Islamogram "subculture's most notable influence: Abu Anon" decided to use. As noted by Ayad, Abu Anon's "signature avatar is a 'Groyper', a fat cartoon frog associated with white nationalist and alt-right trolls, dressed in a dishdasha, the traditional garb of the Arabian Gulf."

68 Clifford and Meleagrou-Hitchens.

69 Criezis and Hughes.

70 Ibid.

71 MarcAndré Argentino, Amarnath Amarasingam, and Emmi Conley, "'One Struggle': Examining Narrative Syncretism between Accelerationists and SalafiJihadists," ICSR, 2022. See also Firas Mahmoud, "From Atari to Allahu Akbar: Comparing White Supremacist and Jihadist Uses of Gamified Extremism," GNET, February 8, 2023.

72 Argentino, Amarasingam, and Conley.

73 As defined by Moustafa Ayad: "Ideologically heterogenous, Islamogram is a network of young Salafi propagators who use the Instagram platform but draw heavily on the visual and linguistic culture of 4Chan, Reddit and Discord. The rise of these Islamogram influencers closely resembles the rise of the alt-right in 2016, in that it feeds off other noxious trolling subcultures online." See Moustafa Ayad, "Islamogram: Salafism and Alt-Right Online Subcultures," Institute for Strategic Dialogue, November 16, 2021.

74 Ibid.

Figure 2: "The avatar used by Abu Anon, an Islamogram influencer with thousands of followers across multiple platforms, such as Instagram, Twitter, Discord and Reddit."[75]

Other images, like the mashup of the Confederate flag with the Islamic State's below, highlight how Islamogram members have blended key visual symbols used by the two communities. This blending of visual aesthetics is not one-sided; far-right extremists have engaged in similar activity.[76]

Figure 55 In a Telegram channel linked to Islamogrammers, a user posted a series of mashup flags, which include this flag that contains elements of the Islamic State "flag," the Nazi flag, and the Confederate flag used in the Civil War.

Figure 3: A "mashup of flags, which include this flag that contains elements of the Islamic State "flag," the Nazi flag, and the Confederate flag used in the Civil War" that was posted "to a Telegram channel linked to Islamogrammers."[77]

75 This image, and the associated description, was featured and published in Ayad, "Islamogram: Salafism and Alt-Right Online Subcultures."

76 As noted by Julian Bellaiche: "In June 2021, a hyper-stylised image of a jihadi fighter pointing a finger upward, representing *tawhid* – the unity of God in Islam, customised with neo-Nazi symbols circulated in channels identified with the group [the neo-nazi group Pax Aryana] … The jihadist is represented harbouring the group's symbol on a headband and wearing a skull mask, an accessory that became popular in far-right circles in 2016. He is also surrounded by *Wolfsangels*, an ancient runic symbol that was part of several divisional insignias of Nazi Germany's Waffen-SS and that is very popular among neo-Nazis today." See Julian Bellaiche, "Connecting the Fringes: Neo-Nazi Glorification of Salafi-Jihadi Representations Online," GNET, August 24, 2021.

77 This image, and the associated description, was featured and published in Ayad, "Islamogram: Salafism and Alt-Right Online Subcultures."

While these online sub-cultures are enemies in many ways, there are also areas where their hate overlaps or they have common ground, an issue that members of both communities (and researchers) have recognized.[78] At a high level, far- and alt-right extremist networks and the Islamogram subculture that Ayad profiled both have strong 'in' and 'out' group dynamics,[79] some shared values, common enemies (i.e., Jews/Zionism, pluralism, multiculturalism, liberals, LGBTQ+ communities, etc.). As noted by Ayad: "There is a shared hatred that runs through both circles. And that essentially is where the convergence is happening. It is not necessarily a wholesale embrace of the other, but there is a bleed where it's cool to borrow from each other's shared hate and responses, and sort of vilification of others."[80] The fact that this type of overlap, or cross-learning, between these different extremist networks is taking place is not in and of itself surprising, but the search for common bonds, or common causes, is a 'watch out' and broader cause for concern.

The two camps also have distinct but overlapping conceptions of the need to create 'pure' communities as part of their vision for the future.[81] In the Islamic State case, the creation of a physical caliphate is viewed as a key, strategic, and necessary step toward religious purity. For a collection of white supremacists active in the United States, the creation of racially pure territories or 'homelands' has long been viewed as an imperative.[82]

Some members of these online communities have even suggested—at least in a playful way—that maybe there is room for the two networks to collaborate. A meme posted by an Islamogram member that features an Ottoman soldier and a Christian Crusader standing side by side in front of an array of common enemies, with the two fighters asking each other whether they should fight together against communities they both hate, highlights this view.

78 For example, as noted by extremism researcher Meili Criezis, "one Telegram white nationalist group member commented, "There are also more shared values, specifically 'the collapse of the current system,' with IS (Islamic State) than with normies." See Meili Criezis, "Intersections of Extremisms," *Journal of Education in Muslim Societies* 2:1 (2020).

79 J.M. Berger, *Extremism* (Boston: Massachusetts Institute of Technology, 2018). A 2020 study of the promotion of violence within chan cultures found that "several boards appear to be facilitating the 'in-group' status centred around the shared consumption of extremist content." Florence Keen, Blyth Crawford, and Guillermo Suarez-Tangil, "Memetic Irony and the Promotion of Violence within Chan Cultures," CREST, December 15, 2020.

80 Theory of Change podcast #24.

81 Ibid. Also, as noted by Julian Bellaiche: "These movements are also characterised by their extreme violence and have revolutionary aspirations, seeking to replace existing regimes with new orders based on religious or racial particularities. They are highly structured around clearly defined in-groups and out-groups and both Salafi-Jihadism and neo-Nazis display a profound and virulent hatred toward Jews, which often appear through antisemitic conspiracy theories accusing them of controlling world governments. Moreover, both currents strictly enforce gender roles, which often appears as a central concern." Bellaiche.

82 Casey Michel, "Want to Meet America's Worst Racists? Come to the Northwest," Politico, July 7, 2015; Wayne King, "Neo Nazis Dream of a Racist Territory in Pacific Northwest Refuses to Die," *New York Times*, July 5, 1986.

Figure 41 An Islamogram account posts a drawing of an Ottoman soldier and a Crusader agreeing to fight the "hoards" of liberals, such as Black Lives Matter, LBGTQ+ community members, as well as feminists in this meme used by Islamogrammers and the far right.

Figure 4: An "Islamogram meme depicting the uniting of a Muslim soldier and Crusader-era knight to fight worldwide culture wars" shared by Malang Khostay.[83]

The willingness of extremists to look beyond their differences and focus on areas of common ground, or how they can help one another, is even more profound in the U.S. context. And it is being driven by practical considerations. For example, as Michael Jensen has observed:

> The most concerning thing that we've seen in the last couple of years is that competition [on the far right] is actually eroding to some extent, and there has been more of an effort for these groups to link and to cooperate with each other. We're starting to see neo-Nazis and Proud Boys adopt some of the language of the QAnon community—talk about pedophilia and a "satanic cabal"—as a way of forming a bridge.[84]

When asked why this was the case, Jensen added:

> I think it's the recognition that they feel like they have a common enemy—the "left" and liberal America—and they're willing to look past differences to unify against that common enemy because it's more effective than going alone. They're stronger together. They can push their narratives more [effectively]. They can have demonstrations with a show of force. If it's just the Proud Boys showing up, it's probably not going to be the most amazing demonstration, but if they can get the Oath Keepers and "sovereign citizens" and QAnon supporters to show up, it ends up being a fairly significant display for the movement.[85]

Intersectionality and Fluidity at the Individual Level, and Operational Crossover

The interplay and cultural cross-pollination that has occurred across the far- and alt-right ecosystems and online jihadi- and Gen-Z-salafi networks has also influenced the unique ideological journeys of individuals. For example, in his study of the Islamogram community, Ayad noted how his research pointed "to an emerging global ecosystem of young Salafis defined not by ideological rigidity, but rather an ideational elasticity that allows these communities to draw on seemingly oppositional alt-right and far-right tropes."[86] In their study of fringe fluidity, Daveed Gartenstein-Ross and Madeleine Blackman examined cases where "some people who come to accept and act on an extremist ideology

83 This image, and the associated description, was featured and published in Ayad, "Islamogram: Salafism and Alt-Right Online Subcultures."

84 Zack Stanton, "The Problem isn't Just One Insurrection. It's Mass Radicalization," Politico, February 11, 2021.

85 Ibid.

86 Ayad.

transition from the embrace of one form of violent extremism to another."[87] As part of their effort, Gartenstein-Ross and Blackman identified "over half a dozen" recent cases of "individuals who either made the transition from neo-Nazi beliefs to militant Islamism, or else worked to advance both causes simultaneously."[88] They also argued that fringe fluidity was a broader phenomenon not limited to movement between those two communities, and that fringe fluidity should be viewed as a distinct radicalization pathway.[89]

As many scholars have pointed out, the internet has lowered, and continues to lower, barriers to entry for individuals to access extremist content and extremist networks. This has made it easier for "supremacists [or individuals more broadly] to pick and choose which aspects of supremacist [or extremist] ideology resonate and engage selectively with those ideals."[90] And the effect, as Jigsaw has noted, is that "supremacists no longer have to find a group with which they fit; there is less friction to joining the distributed movement because they can retain idiosyncratic beliefs."[91] This in turn, as Cynthia Miller-Idriss has highlighted, has resulted in the creation of new, unique, and unexpected extremism forms.[92] For example, this has included "a self-described 'Bolshevik' white supremacist group … [calling] for the liquidation of the capitalist class, far-right groups … [praising] the Taliban and the Unabomber, QAnon … [spreading] through yoga studios and alternative medicine communities, and antigovernment militias … [joining] forces with left-leaning antivaccine groups to protest restrictions and mandates related to the COVID-19 pandemic."[93]

Terrorism researchers have been using different terms to explain this phenomenon. This includes terms such as idiosyncratic terrorism,[94] "salad bar" ideology extremism,[95] mixed and unclear ideology extremism,[96] and composite violent extremism.[97] The latter term, compositive violent extremism, was coined by Daveed Gartenstein-Ross, Andrew Zammit, Emelie Chace-Donahue, and Madison Urban.[98] These authors developed a helpful typology to unpack the term and describe it. That typology includes four different types of composite violent extremism: ambiguous, mixed, fused, and convergent.[99] The fact that there was a need for such a typology demonstrates how idiosyncratic terrorism or composite violent extremism has become much more of a 'thing.' And that 'thing,' given the other interrelated trends described above that are helping to enable and 'feed' this individual-level ideological fluidity, is likely to remain a steady feature of extremism and terrorism in the years ahead.

Ideological crossover, or bounding, from association with one extremist belief system to another, or the blending of influences from different views, is clearly happening but at a limited scale thus far. Furthermore, up until this point, operational crossover or convergence between alt- and far-right networks and jihadi networks has not been as common. A comparative study of salafi-jihadi and white supremacist attack planning in the United States, for example, found that "similarities between jihadist

87 Daveed Gartenstein-Ross and Madeleine Blackman, "Fluidity of the Fringes: Prior Extremist Involvement as a Radicalization Pathway," *Studies in Conflict and Terrorism* 45:7 (2022).

88 Ibid.

89 Ibid.

90 "The Violent White Supremacy Issue."

91 Ibid.

92 Miller-Idriss, "How Extremism Went Mainstream."

93 Ibid.

94 Jesse J. Norris, "Idiosyncratic Terrorism: Disaggregating an Undertheorized Concept," *Perspectives on Terrorism* 14:3 (2020).

95 "IntelBrief: The Counterterrorism Challenge of 'Salad Bar' Ideologies," Soufan Center, March 29, 2021.

96 Alexander Meleagrou-Hitchens and Moustafa Ayad, "The Age of Incoherence? Understanding Mixed and Unclear Ideology Extremism," Program on Extremism, June 15, 2023.

97 Gartenstein-Ross et al.

98 Ibid.

99 Ibid.

and white supremacist attack planning in the U.S. from 2014 to 2019 were few and far between."[100] That is not to say that these two camps have not learned from how the other conducts operations or borrowed tactical approaches. Data on terrorism in Europe, for example, "suggests that the threats [posed by Islamist and right-wing extremists] have become more similar over time."[101] One area where there has been some tactical overlap is the livestreaming of attacks. In 2013, al-Shabaab live-tweeted its attack against the Westgate Mall in Kenya.[102] And then several years later in 2016, during an attack in France, an individual inspired by the Islamic State used a livestream "to broadcast and justify his actions."[103] Since that time, the livestreaming of attacks has been a more regular feature in attacks conducted by far-right extremists, and less so by jihadis.[104]

Vehicle ramming is another area where there has been operational convergence. As noted by Argentino, Amarasingam, and Conley, "although IS pioneered and agitated for vehicle ramming attacks, this is now a common far-right, or Racially and Ethnically Motivated Violent Extremist (REMVE) tactic to target protestors/civilians in peaceful demonstrations."[105] While the Islamic State certainly played an important role in popularizing vehicle ramming as an attack modality, research on the use and evolution of the tactic by Ari Weil, Brian Michael Jenkins, Ryan Scott Hauser, and others has highlight how Palestinian nationalists were the first to repeatedly use the tactic.[106] So there have been waves of vehicle ramming as a tactic by at least three different types of groups: Palestinian nationalists, jihadis, and far-right extremists[107]—a point which only further emphasizes how extremists motivated by different goals have learned and borrowed operational ideas from one another.

Thus, given the fluid and intersectional dynamics that are, and that will likely remain, in play, it is reasonable to assume that the future of extremism will look even more complicated and unique, not less. The rise of interstate strategic competition between great powers, and the incentives nations have to keep hostilities below the threshold of direct state-to-state armed conflict, also makes it likely that states will turn to and rely more on armed proxies to act on their behalf in the future, too. And if that ends up taking place, one potential, and arguably probable, outcome is that it will lead to a rise in state-sponsored terrorism or at least greater cooperation between state and armed non-state proxies.[108] This is another key intersection area that has the potential to further complicate, what is already a complex, dynamic, and fluid terrorism threat picture.

---

100 Clifford and Meleagrou-Hitchens.

101 "Islamistisk terrorisme er mest dodelig," FFI, December 5, 2022.

102 J.M. Berger, "Hug a Mole," Substack post, November 30, 2022.

103 For background, see Maura Conway and Joseph Dillon, "Future trends: Live-Streaming terrorist attacks," VOXPol, 2016; Amarasingam, Argentino, and Macklin; and Graham Macklin, "The Christchurch Attacks: Livestream Terror in the Viral Video Age," *CTC Sentinel* 12:6 (2019). While not an act of terrorism, the live on-air assassination of a U.S. television journalist during a broadcast in 2015 may also be relevant to the broader context of the development of livestreaming as a phenomenon. For background, see Cassandra Vinograd, "WDBJ7 Reporter Alison Parker, Photographer Adam Ward Killed on Live TV," NBC News, August 26, 2015.

104 Macklin, "The Christchurch Attacks: Livestream Terror in the Viral Video Age;" Amarasingam, Argentino, and Macklin.

105 Mahmoud, "From Atari to Allahu Akbar."

106 Kriston Caps, "Why Vehicle Attacks Against Protestors are Rising," Bloomberg, June 3, 2020; Ryan Scott Houser, "Democratization of Terrorism: an Analysis of Vehicle-Based Terrorist Events," Trauma Surg Acute Care Open, 7, 2022; Brian Michael Jenkins and Bruce R. Butterworth, "'Smashing into Crowds:' - An Analysis of Vehicle Ramming Attacks," Mineta Transportation Institute, November 2019.

107 Caps.

108 The Office of Director of National Intelligence is also aware of this possibility and has flagged it as a concern. As noted in its Global Trends 40 report: "In this more competitive global environment, the risk of interstate conflict is likely to rise because of advances in technology and an expanding range of targets, a greater variety of actors, more difficult dynamics of deterrence, and weakening or gaps in treaties and norms on acceptable use. Major power militaries are likely to seek to avoid high-intensity conflict and particularly full-scale war because of the prohibitive cost in resources and lives, but the risk of such conflicts breaking out through miscalculation or unwillingness to compromise on core issues is likely to increase." "Global Trends 2040: A More Contested World," ODNI, March 2021.

5. Speed and Potential Scale: Radicalization Faster and Political Violence More "Normalized"

Today's terrorism landscape has also been shaped by the accessibility of extremist content, and the greater normalization or 'mainstreaming' of such content in the United States.[109] These dynamics have contributed to two important and troubling effects.

First, the internet has sped up the time it takes an individual to radicalize. For example, according to an empirical analysis of individuals radicalized in the United States led by researcher Michael Jensen, "over the past roughly 15 years, the average time span of radicalization in the U.S. has shrunk from 18 months to 7 months."[110] This is because the "internet lowers barriers for those curious about a supremacist idea to anonymously learn about it, lurk in supremacist spaces online, and eventually interact with others as part of loose, informal networks."[111] As noted by Jensen: "Think about somebody in the 1980s or 1990s radicalizing into the 'white power' movement. You had to know somebody in your real-world life who was involved in it. They had to recruit you in or introduce you to the ideas. That tended to be a pretty slow process—a process that, for a lot of individuals, didn't happen. Now, it's a click away. It's really easy to find."[112]

The content moderation actions of large social media and technology companies like Meta and YouTube have helped to push extremist content to different and smaller platforms, and more boutique corners of the internet, but extremist networks have also adapted and continue to figure out ways to circumvent content moderation tools and tradecraft.[113] For practitioners, these developments mean that they have less time to identify individuals operating across a wider and more distributed array of digital platforms who have radicalized *and* less time to navigate through the messy and complex business of evaluating which individuals do, and do not, pose a threat. This type of situation advantages the potential individual attacker, and not governments. Commercial companies, which need to make content moderation decisions at scale, also operate from a disadvantaged position, as extremists continue to adapt their tactics and figure out ways to evade or circumvent detection in the first place.

Second, extremism researchers have been sounding the alarm for years that hate and bigotry have become a more regular feature of public discourse, and that extremist discourse has become increasingly 'mainstreamed' in the United States.[114] There is an abundance of anecdotal evidence that supports this view. There are also various reasons that help to explain why this phenomenon, and trendline, is occurring.[115] For example, white supremacists and other far-right extremists have a steady track record of leveraging mainstream causes to expand their appeal, recruit, and grow their membership.[116] That type of approach is not happenstance, but instead part of an intentional strategy to better package and market their radical views.[117] As Rachel Kleinfeld has observed, "in the aftermath

109 For a general overview on the mainstreaming of extremism, see Milo Comerford and Sasha Havlicek, "Mainstreamed Extremism and the Future of Prevention," Institute for Strategic Dialogue, September 30, 2012.

110 Stanton.

111 "The Violent White Supremacy Issue."

112 Stanton.

113 For background, see Moustafa Ayad, Anisa Harrasy, and Mohammed Abdullah A., "Under-Moderated, Unhinged and Ubiquitous: Al-Shabaab and the Islamic State Networks on Facebook," Institute for Strategic Dialogue, June 14, 2022, and Brody McDonald, "Extremists are Seeping Back into the Mainstream: Algorithmic Detection and Evasion Tactics on Social Media Platforms," GNET, October 31, 2022.

114 Shifrin, Lane, and Rogan; Barbara Perry, "Blurring the Boundaries of Mainstream and Extreme: Contexts and Contours of Right-wing Extremism in Canada," in *Right-Wing Extremism in Canada and the United States* (New York: Springer International Publishing, 2022).

115 For example, see Miller-Idriss, "How Extremism Went Mainstream."

116 Kleinfeld; Roderick Graham, "Inter-ideological mingling: White extremist ideology entering the mainstream on Twitter," *Sociological Spectrum* 36:1 (2016).

117 Kleinfeld; Graham.

of the January 6 insurrection, daily internet monitoring showed right-wing violent extremists were encouraging members to use mainstream conservative causes and local rallies to increase recruitment while flying under the radar of national news."[118]

Much has also been written about the role and influence political leaders, prominent media personalities, and other celebrities in creating, or fostering, an enabling context that has made support for hate and the demonization of opponents more okay. One only needs to look at the statement former President Trump made about the racist 'Unite the Right' rally in Charlottesville, Virginia,[119] or his public comments about the Proud Boys[120] (a group that has been formally designated as a terrorist organization by the Canadian government),[121] Tucker Carlson's platforming of the Great Replacement Theory,[122] or Ye's praise of Adolf Hitler on InfoWars[123] to see the pattern. In today's context, division sells and attracts, an issue that only creates incentives for individuals to engage in the same type of behavior. As Michael Jensen has astutely noted, it is "more politically lucrative for individuals to play up polarization, to play up their tribe vs. the other tribe" instead of being "the old-style leader who tries to find a bridge and a middle ground."[124] This 'us' versus 'them' dynamic and the embrace—even if only casual—of discourse that frames individuals associated with an out group as enemies lie at the core of modern conceptions of extremism.[125]

The abundance of misinformation and disinformation that exists online has also been another critical, and evolving challenge, as it has created an informational environment that can be hard or confusing for individuals to navigate. A RAND study focused on the online space puts the issue into context:

> Research on the spread of misinformation and conspiracy theories suggests that most people struggle to distinguish between true, false, and misleading content online and are therefore susceptible to unintentionally sharing incendiary or propagandic material. This problem, as behavioral scientists David Rand and Gordon Pennycook have written, is "likely exacerbated on social media, where people scroll quickly, are distracted by a deluge of information, and encounter news mixed in with emotionally engaging" content.
>
> Similarly, internet users may not recognize that they are engaging with propaganda or other manipulative content intended to radicalize and recruit adherents.[126]

For the U.S. national security enterprise, this issue is a strategic, cross-cutting intersectional problem that extends well beyond extremism and terrorism, as it creates vulnerabilities and opportunities for actors—both foreign and domestic—to sow, stoke, and exploit fractures, cultural flashpoints, distrust, and political tensions to achieve specific objectives. For foreign adversaries like China and Russia, the violent siege of the U.S. Capitol building—and how the United States arrived at that moment—shows how misinformation can be used to mobilize,[127] how it can be weaponized, and how it can be used to fracture societal trust over the longer term.

---

118 Kleinfeld.

119 "Full Text: Trump Comments on White Supremacists, 'Alt Left' in Charlottesville," Politico, August 15, 2017.

120 Kathleen Ronayne and Michael Kunzelman, "Trump to far right extremists: 'Stand back and stand by,'" Associated Press, September 30, 2020.

121 See "Currently listed entities," Public Safety Canada, Government of Canada, February 3, 2021.

122 Graig Graziosi, "Video of Tucker Carlson Promoting 'Great Replacement' Theory Surfaces Again," *Independent*, May 16, 2022.

123 Azi Paybarah, "Kanye West Draw Fresh Denunciation for Hitler Praise in Alex Jones Interview," *Washington Post*, December 1, 2022.

124 Stanton.

125 Matteo Pugliese, "J.M. Berger on Extremism," European Eye on Radicalization, November 14, 2018.

126 Williams et al.

127 For example, "Even though the January 6 insurrection was a mass gathering, it included thousands of individuals mobilized through online disinformation campaigns and propaganda. Just 14 percent of those arrested to date are members of extremist groups." Miller-Idriss, "Extremism has Spread Into the Mainstream."

The concerns and changing views Americans have about politically motivated violence and terrorism reflects how the environment has been shifting and how the ongoing normalization of hate is likely to lead to more real-world violence. According to a *Washington Post*-ABC News poll conducted in late 2022, a "wide and bipartisan majority of Americans worry there is increased danger of politically motivated violence in the United States."[128] The poll specifically found that nearly "9 in 10 Americans (88 percent) are concerned that political divisions have intensified to the point that there's an increased risk of politically motivated violence in the United States, including over 6 in 10 who are 'very concerned.'"[129] A separate poll conducted by NORC and the Associated Press in 2021 found that more Americans are concerned about domestic extremism than they are about terrorist threats from abroad, which is quite a statement considering that the United States spent billions upon billions of dollars abroad to degrade al-Qa`ida, the Islamic State, and related networks for more than 20 years.[130]

Even more concerning is longitudinal data from another key poll led by academics Lilliana Mason and Nathan Kalmoe, which has highlighted how Americans' "acceptance of political violence has been rising sharply over the past five years."[131] According to results from their poll, in 2017 between 7-8% of poll respondents approved of political violence.[132] In 2021, "one in five Republicans (20%) and 13% of Democrats claimed that political violence was justified 'these days.'"[133] For Republican respondents, support for political violence has doubled across the five-year 2017-2022 span of time; for Democrats acceptance has also grown, but not by as much.[134] The bump-up across both groups of partisans is not just noteworthy; its historical parallel is chilling.[135] As Kleinfeld noted, to "put this level of support into context: In 1973 during the most violent period of Northern Ireland's Troubles, 25% of Catholics and 16% of Protestants agreed that 'violence is a legitimate way to achieve one's goals. The U.S. is fast approaching these numbers.'"[136]

128 Guskin.

129 Ibid.

130 Mychael Schnell, "More Americans worried about domestic extremism than threat abroad: survey," Hill, September 7, 2021.

131 Kleinfeld.

132 Sheilah Kast and Maureen Harvie, "Radical American Partisanship," On the Record, November 1, 2022.

133 Kleinfeld

134 Ibid.

135 For an empirical and comparative look at terrorism trends across ideologies, see Katarzyna Jasko et al, "A comparison of political violence by left-wing, right-wing, and Islamist extremists in the United States and the world," *Proceedings of the National Academy of Sciences*, July 18, 2022. For a more detailed look at anarchist and left-wing extremism in the United States, see "Anarchist/Left-Wing Violent Extremism in America: Trends in Recruitment, Radicalization, and Mobilization," Program on Extremism, November 2021. See also Teun van Dongen, "We Need to Talk About Left Wing Extremism. Or Do We?" ICCT, November 24, 2021.

136 Kleinfeld. As she notes in her testimony: "Some experts believe that these numbers are emotional or philosophical statements and thus overstate the acceptance of actual violence. Abstract questions with no definition of violence opens surveys to that claim, and no doubt a percentage of respondents are not serious. Yet there is reason to believe a significant number of respondents mean what they say."

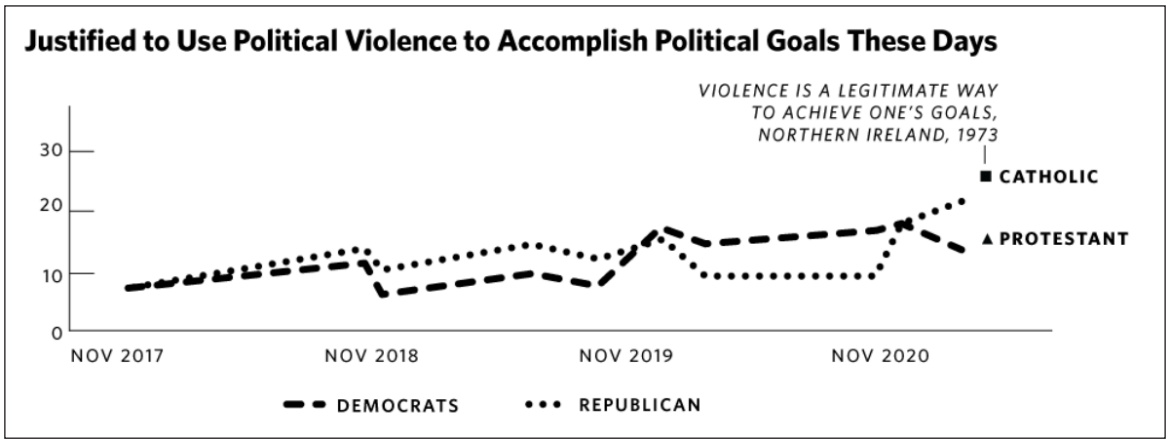

Figure 5: Views on political violence in the United States. Data compiled by scholars Lilliana Mason and Nathan Kalmoe[137]

For those more skeptical, it is tempting to dismiss the results from these various polls as abstract numbers that represent views, not real-world activity. But other incident trends highlight how, and why, there are real reasons to be concerned. Kleinfeld calls attention to rises in two key data points: the number of threats made against members of Congress and hate crimes. In 2016, the Capitol Police investigated 902 threats against members of Congress.[138] In 2021, that number was 9,600; a 964% jump up in the number of threats over a five-year period.[139] That rise was not a one-year outlier, but instead the result of a steady year-over-year increase across the entire 2016-2021 time period.[140] In 2022, the number of threat investigations by the U.S. Capitol Police decreased to 7,501 cases, but as noted by U.S. Capitol Police leadership, "the caseload remains historically high."[141] While the majority of threats made against members of Congress do not materialize, or translate into, real-world harm, some—such as the physical attack against Paul Pelosi, the husband of Nancy Pelosi (then Speaker of the House) inside their personal residence in October 2022 or the armed attack against a Republican Congressional baseball practice in 2017—do. And the dramatic rise in the number of threats made suggests that more real-world acts of violence against members of Congress are also likely to increase.

The trajectory of hate crimes in the United States has followed a different trendline, but still a concerning one that also reflects how the 'hate to hate-motivated action continuum' has been shifting. According to data released by the FBI, the high-water mark year for hate crimes in the United States was 2001 with 9,730 hate crime incidents reported that year.[142] After 2001, the number of hate crimes "declined, hitting a low of 5,479 in 2014."[143] But after 2014, hate crimes have started to climb upward again, and have started growing even faster starting during the 2016-2017 time period.[144] In 2020, the FBI reported 8,263 hate crimes having occurred in the United States, "the highest number since 9/11."[145] So instead of the United States continuing to see declines in the number of hate crimes, the number of hate crimes—after moving along a downward trajectory for more than a decade—

137 Cited in Kleinfeld.

138 Kleinfeld.

139 Ibid.

140 Ibid. See also "USCP Threat Assessment Cases for 2022," United States Capitol Police, January 17, 2023.

141 "USCP Threat Assessment Cases for 2022."

142 Ibid.

143 Ibid.

144 Ibid.

145 Ibid.

experienced a multi-year upward climb.

The FBI's most recent annual report of hate crime statistics, which provides an overview of hate crimes that occurred in 2021, has been criticized and is the subject of controversy. According to the FBI, in 2021 "law enforcement agencies reported 7,262 total [hate crime] incidents," which would represent a decline in the total number of hate crimes in the United States from 2020 to 2021.[146] But, the FBI's 2021 hate crime report has been criticized by specialists as being "meaningless"[147] as during 2021 there was a significant reduction in the number of agencies that provided localized hate incident data to the FBI. The FBI acknowledged this problem, plainly stating how this change meant that "data cannot reliably be compared across years."[148]

The general takeaway, despite the shift in FBI-received data between 2020 and 2021, is that more U.S. residents are more inclined to conduct acts of hate than they were a decade ago. So instead of making progress toward minimizing hate, actionized hate is becoming more common in the United States.

This trendline has several national security implications. The level of divisiveness and broader acceptance of hate is a vulnerability that external actors can stoke and exploit, as it is easy to understand how keeping the United States and its populace focused on internal disagreements, strife, and division would be a useful way or strategy to distract and weaken the United States' ability to remain as competitive or as capable abroad.[149] Looking at the United States' own strategies and approaches to counterterrorism is illustrative in this regard, as one key approach the United States used to degrade and 'defeat' al-Qa`ida and the Islamic State has been to expose and attempt to acerbate internal fractures, rifts, and disagreements within the jihadi community. It seems obvious that America's state-level adversaries would recognize the benefits of working to advance, even if slowly and in creative ways, a similar approach (as Russia has already been doing).[150]

6. Technology Continues to Enable and Constrain—and It Remains a Key Locus of Competition

"Never in history have violent non-state actors been so globally connected, resourceful, dynamic, well-funded, and technologically savvy."[151] *– Christina Schori Liang*

Technology and access to innovative and disruptive technologies, equipment, and systems have always been a core driver of terrorism and efforts to prevent and/or mitigate terror threats.[152] As scholars David Rapoport and Audrey Kurth Cronin have highlighted, the invention of dynamite and the AK-47 assault rifle both had a profound and strategic effect on a terrorist's ability to inflict harm.[153] Twenty-four-seven cable news coverage, the invention of the internet, and the more recent proliferation of

146 See "FBI Releases Supplement to the 2021 Hate Crime Statistics," U.S. Department of Justice, updated March 28, 2023.

147 Cynthia Miller-Idriss, "The FBI's 2021 Hate Crime Data is Worse than Meaningless," Lawfare, December 16, 2022.

148 See "FBI Releases Supplement to the 2021 Hate Crime Statistics."

149 For one perspective on this and its impact on military readiness, see Brooke Singman, "China is 'laughing' as US culture war erodes combat readiness, says former defense secretary," Fox News, February 2, 2023.

150 Mark Galeotti, "Active Measures: Russia's Covert Geopolitical Operations," *Security Insights* 31 (2019).

151 Christina Schori Liang, "Global Terrorism Index: Emerging Technologies and Terrorism," Global Terrorism Index, 2022.

152 As noted by Brian A. Jackson: "Since the beginnings of modern terrorism in the 1970s, technological change has caused major shifts in the means applied by terrorist organizations and the context in which they must act to carry out their violence. With shifts in technology, the destructive potential of the weapons available to the terrorists has increased. With changes in the infrastructure and technologies integral to the functioning of modern societies, the targets they have available to choose from have shifted as well." Brian A. Jackson, "Appendix F: Technology and Terrorism," in *The Global Technology Revolution 2020, In-Depth Analyses: Bio/Nano/Materials/Information Trends, Drivers, Barriers, and Social Implications* (Santa Monica, CA: RAND: 2006), pp. 209-214.

153 Audrey Kurth Cronin, *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists* (Oxford: Oxford University Press, 2020); David C. Rapoport, "The Four Waves of Modern Terrorism," June 5, 2006.

digital technologies and platforms that allow individuals to network, communicate, and make their voice heard have also revolutionized how extremists operate. Technological advancements, from armed drones to image recognition software and natural language processing tools, have likewise transformed how the United States and its partners engage in the practice of counterterrorism.

Access to technology has the power to create new opportunities and challenges for all actors, and as a result, it remains a key area where extremists and counter-extremists compete to identify weaknesses and/or gain an advantage. The existence of this competitive 'space' is not new, but as Cronin and others have highlighted, the characteristics of the space have been changing, and changing in ways that enhances the ability of non-state actors to develop new advantages, overcome power imbalances, and to innovate. A core part of the reason why is because over the past several decades there has been a shift away from a 'closed technological revolution', a system under which innovation and lethal power is heavily controlled, regulated, and accessible to nation states, to an 'open technological revolution' where technologies and lethal power are less controlled by states and more broadly accessible to the public.[154] The scale and type of data that is publicly available today, combined with free and/or accessible tools that allow individuals to harness it, have also enhanced the ability of individuals and networks to use those new tools and technologies in more unique and impactful ways.

Another way of framing the impact of the open technological revolution that Kurth Cronin describes is that the more open system reduces barriers to entry, and facilitates access, for more parties. In practical terms, this means that individuals, organizations, and networks have access to not just a broader array of equipment, technology, and information, but that they also have better access to more advanced and sophisticated technologies than they did previously. Overall, this type of access provides countless benefits to society and has a positive net effect. But there are also downsides and risks to this type of access as "changes in technology, and the deployment of new technologies in society, can result in new vulnerabilities and targets for terrorist attack," as well as create opportunities for other malign actors.[155]

It is not hard to find examples. During its heyday and before mainstream platforms engaged in more encompassing crackdowns, the Islamic State was able to leverage Twitter and Facebook to spread its hate and influence, and mobilize thousands of recruits from around the world.[156] Shortly thereafter, the Islamic State also shocked the world by creatively transforming commercial quadcopters so they could drop explosive weapons from the air, a terrorist group's version of a Do-It-Yourself (DIY) air force.[157] Over the past decade advances in additive manufacturing have made it easier for individuals and companies to make their own parts or items, including 3D printed guns, a weapon that some extremists have tried to use in attacks and that other extremists have sought to make or acquire.[158] Advances in other technologies and fields, such as synthetic biology, present other longer-range risks and concerns, too.[159]

The accessibility of technology today has also been shaping the type of systems and weapons that proxies and state adversaries have been able to make. For example, a recent investigation of Iranian-made UAS used by Russia in Ukraine by Conflict Armament Research found that 82% of the components found in the recovered UAS were "manufactured by companies based in the United States."[160] The CAR team traced the components of four UAS, from three different Iranian UAS variants. The core

154 Cronin.

155 Jackson.

156 J.M. Berger and Jonathan Morgan, "The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter," Brookings Project on U.S. Relations with the Islamic World, Analysis Paper No. 20, March 2015.

157 Don Rassler, *The Islamic State and Drones: Supply, Scale, and Future Threats* (West Point, NY: Combating Terrorism Center, 2018).

158 Yannick Veilleux-LePage, "CTRL, HATE, PRINT: Terrorists and the Appeal of 3D-Printed Weapons," ICCT, July 13, 2021; Rajan Basra, "The Future is Now: The Use of 3D-Printed Guns by Extremists and Terrorists," GNET, June 23, 2022.

159 For background, see the April 2022 and May 2022 special issues of *CTC Sentinel*.

160 "Dissecting Iranian drones employed by Russia in Ukraine," Conflict Armament Research, November 2022.

and concerning implication of CAR's discovery is that the Iranian government was able to source and acquire the components made by U.S. based companies and use and rely on them to operate different UAS systems in a regularized way. Or put more simply, several key UAS produced by the Iranian government appear to rely in large part on technology and components produced by U.S. companies to operate.

As many researchers have pointed out, despite the broad access to technology and equipment that extremists and terrorists have these days, low-tech and tried-and-true methods—like the gun and bomb, which are "sufficient, accessible, and reliable"[161]—still dominate.[162] While it still happens, the use of novel equipment and weapons in terror attacks does not occur frequently. This is because terrorists have to grapple with adoption, operational, and security tradeoffs when deciding whether the use of a new technology, system, approach, or piece of equipment is worth the risk.[163] And given that most terrorist groups already operate in contested environments where pressure is being placed against them, most decide that the risk of introducing something new usually is not worth it—so they utilize methods like the gun and the bomb that are reliable.

This does not mean that there are not risks associated with the access to technology and systems that extremists and terrorists have today—there are plenty. One of the key areas of risk, as the Islamic State's experience with drones illustrates, is that there is a plethora of opportunities for extremists to combine and creatively cobble together 'high' and 'low' end systems and components in ways that can surprise and/or make an impact. The case of 9/11, where al-Qa`ida upended hijacking norms and did the unexpected by using commercial airliners as a weapon to attack, also demonstrates how sometimes new threats are generated not by the introduction of a new technology but by a reimagining of how existing resources, equipment, and systems can be used together. To minimize the risk of these type of surprises, it is important that the United States and its partners pay close attention to unique outlier cases where terrorists have innovated; learn from areas where terrorists have attempted to innovate but failed; think about how terrorists might asymmetrically mirror image capabilities used against them; and pay close attention to commercial product enhancements and how hobbyists innovate.[164]

The open technological revolution that Kurth Cronin describes has also been reshaping the worlds of counterterrorism and intelligence. Not only has it broadened the array of commercial technologies and capabilities to which security practitioners have access, it has also been shifting the number, type, and diversity of actors or stakeholders operating in the counterterrorism space, and the dynamics of who designs, manages, owns, and has access to, or influence over, specific platforms and approaches. One of the more profound changes over time has been the rise in what might be called commercial counterterrorism, or commercial counter violent extremism, which has given more influence and power to companies whose service or platform intersects with extremism or terrorism to drive responses.[165]

This change, which is being shaped by the world's increasing reliance on digital tools and technologies, has slowly been complicating and reducing the amount of control and influence that governments

161 "Global Trends 2040: A More Contested World."

162 As Bruce Hoffman astutely noted in 1994, "Terrorists, therefore, seem to prefer the assurance of modest success to more complicated and complex--but potentially higher pay-off (in terms of casualties and publicity)--operations." Bruce Hoffman, "Responding to Terrorism across the Technological Spectrum," USAWC Press, 1994.

163 Jacob N. Shapiro, *The Terrorists Dilemma: Managing Violent Covert Organizations* (Princeton, NJ: Princeton University Press, 2013); Gabriel Koehler-Derrick and Daniel Milton, "Choose Your Weapon: The Impact of Strategic Considerations and Resource Constraints on Terrorist Group Weapon Selection," *Terrorism and Political Violence*, March 2017.

164 For more background on these categories, see Don Rassler and Muhammad al-'Ubaydi, "Anticipating Future Directions of Tech-Enabled Terror," Lawfare, December 12, 2021.

165 Language included in the U.S. government's domestic counterterrorism strategy highlights how the U.S. government is aware of this trend. As noted in the strategy: "The widespread availability of domestic terrorist recruitment material online is a national security threat *whose front lines are overwhelmingly private– sector online platforms*…" [Emphasis added]. "National Strategy for Countering Domestic Terrorism."

have over digital areas where extremists find refuge and/or operate. The establishment of the Global Internet Forum to Counter Terrorism (GIFCT), an NGO created by Twitter, Facebook, Microsoft, and YouTube in 2017 to "prevent terrorists and violent extremists from exploiting digital platforms,"[166] provides one window into how the number, type, and diversity of actors operating in, or who have stake, influence, or an ability to initiate actions directly relevant to counterterrorism, has grown. Since its creation in 2017 GIFCT has evolved from its four founding members to 22 tech companies by the end of 2022.[167] While GIFCT serves as a key collaborative coordinating body for its members, each of its 22 members have their own terms of service and processes that guide how they respond to extremism and/or terrorism on their sites or platforms. To enhance the collective response of GIFCT members to a terror or extremism incident, the organization has established a centralized communications mechanism and a content incident protocol that enables GIFCT to share information and coordinate actions.[168] The ways in which GIFCT interacts with governments is nuanced, however. It regularly engages with governments and has established formal structures and processes that guide how the organization interacts with government representatives. But there are also aspects of GIFCT's work, such as its hash-sharing database, to which governments do not have access, likely due to security and privacy considerations.[169]

The livestreaming of terror attacks highlights how the landscape of counterterrorism stakeholders, and who or which entities can action or tactically respond to an incident, has been evolving. When an extremist decides to livestream an attack or incident, the company that owns the platform being used initiates a response, a response that is bolstered by the network and protocols that GIFCT and other stakeholders have developed. While a government can notify the livestream platform of the incident/attack and support that company's investigation (and legally request data and/or information about the incident), the initial response to a livestreamed attack is managed and led by the company, or companies, that are involved, as they work to stop the stream and prevent the spread of the video and longer-term access to it. Most of this activity takes place outside the realm of government action.

The ongoing rise and proliferation of digital platforms also has the potential to complicate counterterrorism investigations and responses and/or make them less productive. This is because while most of the large, mainstream digitals platforms are run by U.S. companies, over the past decade there has been a growth of other digital platforms and tools created by companies based elsewhere. For example, if a provider or platform is not a U.S. company, and is a foreign entity, that can make it harder for U.S. authorities to secure cooperation from that entity or obtain access to legally requested data.[170] Extremist networks are security conscious and as a result spend time evaluating which platform or service will afford them the most amount of privacy and protection with special attention placed on who might be able to gain access to their data and communications. These concerns and other considerations like which platform will enable access to potential recruits and sympathizers shape their preferences and is part of the reason why extremists have sought out platforms like Telegram and Rocket Chat, which both offer end-to-end encryption and are respectively based in the United Arab

166 "The Global Internet Forum to Counter Terrorism (GIFCT) is an NGO designed to prevent terrorists and violent extremists from exploiting digital platforms. Founded by Facebook, Microsoft, Twitter, and YouTube in 2017, the Forum was established to foster technical collaboration among member companies, advance relevant research, and share knowledge with smaller platforms." For background on GIFCT, see "About," GIFCT, n.d.

167 "2022 GIFCT Transparency Report," GIFCT, December 15, 2022.

168 For background, see "Incident Response," GIFCT, n.d. and "Content Incident Protocol," GIFCT, n.d.

169 For background, see "FAQs," GIFCT, n.d.

170 When it comes to cooperation with the U.S. government, there are also nuances for U.S.-based companies, too. Apple's approach is an important example in this regard. For background, see Lauren Feiner, "Apple Refuses Government's Request to Unlock Pensacola Shooting Suspect's iPhones," CNBC, January 14, 2020, and Matt Apuzzo, David E. Sanger, and Michael S. Schmidt, "Apple and Other Tech Companies Tangle with US Over Access to Data," *New York Times*, September 7, 2015.

Emirates and Brazil.[171] As digital platforms and tools continue to proliferate, these types of issues are likely to become more commonplace in the future, and potentially further complicate or constrain the United States' ability to forge constructive partnerships with digital providers.

The trends discussed above have other implications for counterterrorism practitioners. The growth in the size and diversity of the commercial counterterrorism sector means that partnerships between government and industry will be more important, and require more government attention, resources, and expertise, then they have in the past. This is because there are more commercial counterterrorism actors and stakeholders with which governments need to dialog with and establish productive partnerships. As a result, in the future the U.S. government will need to establish more and higher quality partnerships with commercial entities. If the U.S. government does not place strong emphasis on partnerships, there is a risk that the seams between public and private entities could become an area that extremists target or manipulate, even more so than they already do. Since many of the digital tools and platforms utilized by individuals today are used to help them communicate and/or share information, individual privacy and security concerns and considerations are a second core implication that has the potential to become more pronounced and create new dilemmas for companies and governments in the future. Indeed, as Kathleen McKendrick has noted, certain technologies, such as AI, have the potential make "invasion of privacy at scale much easier,"[172] which may only deepen the security versus privacy tradeoffs that governments already face, and at times struggle with.

The existing challenges are already notable. But since the pace and scale of technological change is projected to only increase over the next several decades, it is likely that these issues will become even more profound and complicated, which will have implications for a wide range of security issues, including terrorism. For example, as noted by the Office of the Director of National Intelligence's (ODNI) *Global Trends 2040: A More Contested World* assessment:

> During the next two decades, the pace and impact of technological developments are likely to increase, transforming and improving human experiences and capabilities and offering the potential to tackle challenges such as aging, climate change, and low productivity growth, while creating new tensions and disruptions within and between societies, industries, and states … By 2040, the world will have orders-of-magnitude more devices, data, and interactions, linking together all aspects of modern life and crossing political and societal boundaries.[173]

The assessment went on to add that while "emerging technologies are rapidly improving a broad range of human experiences and capabilities … at least in the short term, these same technologies may disrupt longstanding systems and societal dynamics, forcing individuals, communities, and governments to adjust and find new ways of living, working, and managing."[174]

A key implication of these likely developments is that "some will thrive whereas others will struggle, potentially facing increasing inequalities and imbalances"[175]—ingredients that can help fuel extremism, terrorism, and other forms of conflict.

171 For a period, Telegram was viewed by extremists as attractive, as it was seen as being less friendly to law enforcement investigations and governmental requests for data. While it still offers chat features like 'Secret chats' that provide end-to-end encryption (which makes the chat data not accessible unless a government entity has access to one of the physical devices involved in the chat), Telegram's policies on cooperation with law enforcement has changed in recent years. For background, see "Telegram Privacy Policy," Telegram, n.d. and Sven Taylor, "Is Telegram Sharing User Data with Government Agencies?" Restore Privacy, June 15, 2022. See also David Meyer, "Telegram starts to play nice with security agencies over user data, but not in Russia," ZDNet, August 29, 2018.

172 Kathleen McKendrick, "Artificial Intelligence Prediction and Counterterrorism," Chatham House, August 2019.

173 "Global Trends 2040: A More Contested World."

174 Ibid.

175 Ibid.

Conclusion

"Now, if you are thinking and talking about counterterrorism, you are doing so in an environment where you may not have first claim on resources, you may not have the ability to resource your way out of particular problems and it is requiring our counterterrorism enterprise … to make harder choices." – Nicholas Rasmussen[176]

The trends and dynamics discussed in this report highlight how the terrorism and extremism landscapes are dynamic, complex, and increasing intersectional, and how they are evolving in unique ways. These changes present several challenges and implications for the U.S. and international counterterrorism communities. For the United States, one core challenge is how it can keep pace with changes in the environment *and* better anticipate how those changes are likely to enhance or amplify known threats—as well as lead to the creation of new ones—that have the potential to surprise. And how it can do so during an era of enhanced complexity dominated by less U.S. government attention and resources devoted to counterterrorism. That is going to involve some tradeoffs and careful consideration given to, or a reimagining of, the ways in which the United States' approach to counterterrorism should evolve.

The compound and additive[177] makeup of the terrorism and extremism landscapes underlies the challenge. Today, the United States needs to be aware of and evaluate the intentions and capabilities of more types of actors, not less, and to do so with less people and resources. Mainstay networks like al-Qa`ida and the Islamic State endure, as prior experience has demonstrated that without ongoing forms of pressure to suppress them these groups will regenerate and seek to target the United States, its partners, and its interests. The threats posed by mainstay networks have been complemented by the rise of a complex and interactive mix of domestic and transnational extremists motivated by a range of ideologies and goals, *and* threats that state-supported proxies and surrogates, like Iranian militias and the Wagner Group, present to the U.S. personnel and interests abroad. Given the diversity of terror threats, a key consideration for the U.S. CT enterprise is developing frameworks and approaches that help guide when the United States needs to be aware of, and monitor, a threat, and when it needs to "worry" and take that threat more seriously. Some of this prioritization work is already being done, but it still appears to be an area, at least for some threats, that requires more thinking and analysis.

The compound terrorism environment the United States faces is further complicated by how terrorism can be integrated with, and serve as a key driver or sustainer of, conflict in key countries around the globe. For this reason, terrorism and counterterrorism remain core, strategic interests for many of the United States' partners across the Middle East, Africa, and South and Central Asia, and in places like the Philippines. While the United States, given the concerns it is has about China, wants to continue moving on from terrorism, the United States should recognize counterterrorism, and specifically counterterrorism assistance, for the three-fold opportunity that it is: 1) a core mechanism for the United States to be a good partner to, and build trust with, allies; 2) a form of influence and tool to compete in the great power competition sphere to gain insight, access, and placement; and 3) a more cost-effective, longer-term way to continue to monitor and put pressure on priority terror threats.[178]

The U.S. government understands—in some quarters, begrudgingly—that counterterrorism still

176 Rasmussen.

177 In his remarks to the Washington Institute in May 2023, Nicholas Rasmussen used the term "additive" to describe the threat environment. See Ibid.

178 As Brian Michael Jenkins has noted: "Counterterrorism assistance is a currency." See Brian Michael Jenkins, "The Future Role of US Armed Forces in Counterterrorism," *CTC Sentinel* 13:9 (2022). Matt Levitt has expanded on this point, adding: "That currency buys goodwill and partnership on a wide array of other interests, including Great Power competition. The flipside is also true: if the United States declines to help other countries address their counterterrorism needs, it creates a vacuum that will be filled by states like Russia and China, or Iran and Turkey. These states will not intervene in helpful ways, and they will use limited power to outsize effect." See Levitt. See also Jacob Ware, "The Enduring Importance of Tactical Counterterrorism for Strategic Competition," Irregular Warfare Initiative, March 31, 2023.

matters and must remain a persistent priority.[179] It also knows that it needs to meet today's complex threat environment with less,[180] and it has been working to manage that challenge by prioritizing threats, missions,[181] and workflows and navigating where it believes it can prudently assume more risk. Remarks by Rasmussen about the complexity of today's terrorism environment and the implications for the United States' approach place the tradeoffs and dilemmas America confronts into context: "That puts us in a place where we are adopting … a risk management model, rather than an aggressive direct action model for engaging in [terrorism] threat mitigation."[182] That shift, as Rasmussen noted, "puts a tremendous amount of pressure on our intelligence community to be looking over the horizon. To be identifying the particular indicators and warning signs that thy would expect to see if a threat that has been suppressed is at risk of reemerging."[183]

As the U.S. government adjusts to meet the moment and build-out the next chapter of U.S. counterterrorism, it would be wise to develop approaches that mirror the intersectional and compound nature of today's terrorism and extremism threats in ways that are possible. Several priorities can help guide the community's transition. First, the United States should strategically frame the current counterterrorism moment. This report has put forward a suggestion to frame the current CT period as the compound era of U.S. counterterrorism, a framing that would arguably help the United States to place and position counterterrorism less as a stand-alone pursuit and more as a domain that needs to be optimized and leveraged to advance U.S. state-level influence and competition goals.[184] This could be done through counterterrorism being utilized to create or maintain 'space' for the United States to pursue those goals, or for counterterrorism, where and when appropriate, to put in service of them. The United States should not let terrorism fatigue, and the desire to move on from terrorism, cloud how counterterrorism assistance can be useful as a tool and mechanism for the United States to accomplish or advance its other objectives.

Second, the United States should be honest and transparent about its counterterrorism track record, including the successes, failures, and limitations of prior CT strategies and approaches, and the extremist and terrorism threats it faces. Over the past two decades, U.S. counterterrorism strategies have been suppressive[185] and played an important role in minimizing, and in various ways substantively degrading, the threats posed by al-Qa`ida and the Islamic State. But those two movements are resilient and still endure. U.S. efforts to stabilize Iraq and Afghanistan have also come at great human and financial cost, and U.S. initiatives to develop the capabilities of local security force partners also have a mixed track record, and in some cases were arguably a general failure. It is important that the U.S. national security enterprise learn from these challenges, and its mistakes, so it can improve and not repeat them.

There is also a need for honesty and candor on the domestic front. The United States has a serious

179 This is reflected by U.S. strategy and in testimony of national security leaders to Congress.

180 "Counterterrorism Chief Christy Abizaid on Top Terror Threats to the U.S.," Intelligence Matters podcast, May 11, 2022.

181 For example, see Cragin et al, "11. Counterterrorism and the United States in a New Era of Great Power Competition," in "Strategic Assessment 2020," National Defense University, November 4, 2020. In this contribution, Cragin and her co-authors argue "that the military should prioritize preventing external operations, directed or virtually planned by foreign violent extremist organizations (VEOs), against the U.S. homeland and minimizing the ability of foreign VEOs to inspire attacks by sympathizers in the West, commonly referred to as homegrown violent extremists."

182 Rasmussen. For additional background, see Matt Levitt, Katrina Mulligan, and Christopher Costa, "Rethinking U.S. Counterterrorism Two Decades After 9/11," in *U.S. Counterterrorism Reimagined: Tracking the Biden Administration's Effort to Reform How America Addresses Violent Extremism*, Washington Institute for Near East Policy, September 2022.

183 Rasmussen.

184 Kevin Bilms and Doug Livermore have also advocated for the United States to frame a new CT approach, and shared some helpful thoughts for how that approach could be executed by placing more emphasis in three areas: prioritization, load sharing across the CT enterprise, and burden sharing with partners and allies. See Kevin Bilms and Douglas A. Livermore, "Resource-Sustainable Counterterrorism in an Era of Great Power Competition," Small Wars Journal, October 20, 2020.

185 Rasmussen.

domestic extremism/terrorism problem. That fact is recognized in some quarters, but much less embraced in other quarters—an issue that has a bearing on how America's domestic extremism problem is resourced, approached, and proactively monitored.

Third, the United States needs to evaluate whether it is appropriately postured and structured to meet today's complex and composite terrorism threats, and that it has the tools it needs to confront a range of threats, especially those posed by domestic and homegrown extremists. This will require navigating some difficult legal issues and organizational questions. For example, two key issues that have been raised are whether the United States needs, or would benefit from, a domestic terrorism statute,[186] and whether the National Counterterrorism Center's mission should be broadened so it can play more of a role countering domestic and homegrown extremism.[187] Both of these ideas have their merits. Those ideas, alongside the constitutional, civil liberty, and data projections issues associated with collecting, storing, and analyzing data on or about U.S. persons, should be considered and publicly debated.

Fourth, due to the complexity of today's terrorism environment, the United States should take steps to preserve expertise and institutional memory on key terror groups and movements that it has worked hard to develop over the past two decades. The downgrading of terrorism as a priority is the right call, but the associated loss, or longer-term erosion, of deep experience and knowledge on key terror networks is not without its share of risk. Attrition in any enterprise is normal, but there is a danger that terrorism as a problem set could, over time, evolve into being a 'backwater,' or a not or less-well desired career path for U.S. government professionals—as it was during the 1990s. The complexity of the moment requires that the United States seek out and gain efficiencies across all areas, and so as part of its risk mitigation[188] plan, U.S. leaders should develop mechanisms to leverage the knowledge of experienced terrorism 'hands' who have transitioned, to create incentives to keep talented and experienced people engaged on the counterterrorism problem set, and to attract new talent.

Fifth, to do more with less and better understand and navigate the complexity of the terrorism landscape, the United States should invest more in partnerships.[189] This is imperative because the more fluid and interactive character of extremism today creates more seams, and as a result more gaps. Enhancing the quality of existing partnerships and investing in and developing new ones with non-governmental entities is part of the way that the U.S. government can work to observe and minimize those gaps and reduce the likelihood of surprise. Over the past two decades, academic and non-governmental research communities who focus on, and specialize in, terrorism, extremism, data analysis, open-source investigations, and related areas have matured. Across that same span of time, due to the proliferation of online forms of data and communication, the digital and commercial counterterrorism sphere has also grown—in both influence and importance, as well as the number of stakeholders. There exists a considerable amount of talent and specialized expertise within these communities. And while the interests of these different communities and those of the U.S. government do not always align, there is still room for these communities to learn from one another and enhance how they can team up or collaborate.

Thus, a key part of the way forward for U.S. counterterrorism during this period is for it to increase and enrich its touchpoints with academia, private industry, technologists, civil society, and other specialist communities—such as hobbyists—who either have something meaningful to add or who

186 Mary B. McCord and Jason M. Blazakis, "A Roadmap for Congress to Address Domestic Terrorism," Lawfare, February 27, 2019; Eric Halliday and Rachael Hanna, "How the Federal Government Investigates and Prosecutes Domestic Terrorism," Lawfare, February 16, 2021; "Notes: Responding to Domestic Terrorism: A Crisis of Legitimacy," Harvard Law Review, 136:7, May 2023.

187 Bruce Hoffman and Jacob Ware, "The National Counterterrorism Center Must Expand to Better Fight Domestic Terrorists," Defense One, May 26, 2023.

188 For additional views on how the U.S. CT enterprise can do more with less, see Stephen Tankel, "Doing More with Less: How to Optimize U.S. Counterterrorism," War on the Rocks, May 22, 2018, and Bilms and Livermore.

189 Levitt; Nathan Sales, "Counterterrorism and Great Power Competition," Atlantic Council, September 7, 2021.

think creatively about complex problems. It is important that these partnerships are centered on trust and oriented around value for all parties. For the U.S. government, this is likely going to require that it identify how it can either be more inclusive or get more comfortable sharing data, knowledge, and know-how as a way to build trust *and* provide reciprocal forms of value to partners whose expertise, technology, or capabilities are important to advance U.S. CT objectives. At a strategic level, there is also a need for the United States to look across where and how different government departments invest in the work of counterterrorism research institutes, or initiatives, to identify where efficiencies can be gained or how those disparate efforts could be harmonized or build toward overarching goals.

Sixth, given the persistence of terrorism and the diversity of the terrorism landscape, identifying and understanding risk is a central feature that the United States needs to get 'right' if it wants to maintain strategic focus on great power threats.[190] The United States has various programs and efforts to evaluate terrorism threats and to model terrorism risk. But it remains unclear how well the tools and methods the U.S. government have been using to model and navigate terrorism risks capture, or account for, the changes that have been occurring across the terrorism and extremism landscapes. As a result, it also is not clear what gaps, assumptions, or blinders the United States might have. Key U.S. CT community stakeholders know that risk, and better understanding risk, underpin the shift in the United States' counterterrorism posture. But it is not clear who is guiding this issue at a strategic level, and which government entity/entities are working to update and modernize how the U.S. government assesses terrorism risks—and the indicators that can help the government track its evolution.

U.S. government approaches to terrorism risk, as one would expect in a large bureaucracy, appear to be mainly oriented around more static, and less dynamic, conceptions of data whereby risk evaluations are updated not in a 'living' type-of-way using algorithms or automated tools, but through a less regular and often more manual (and time-consuming) process. There are likely a lot of opportunities for collaboration and knowledge sharing in this space, as it is an area where parallel expertise exists outside of government, from actuaries who model terrorism risk for private companies to financial institutions to field-based organizations that navigate risks in conflict zones every day—expertise that could be leveraged to either validate or update U.S. terrorism risk evaluation approaches.

Seventh, the future of U.S. counterterrorism will be driven by data and technology and how the country is able to leverage those two key inputs in a combined way.[191] Indeed, the United States' ability to evaluate risk, and shift toward a counterterrorism posture more focused around indicators and warning,[192] will be underpinned by its ability to navigate—and make sense of—an increasingly complex, voluminous, and compound data environment. As many commentators have already noted, this is going to require that the U.S. CT enterprise make smart investments in technology, artificial intelligence, and automation; that it develop tradecraft and tools that allow analysts and operators to structure, aggregate, harness, and quickly develop insights from an exponentially growing lake of diverse types of data; and that it provide data upskilling opportunities for its current workforce while it simultaneously builds out the infrastructure, systems, and teams needed to support the data-driven CT workforce of the future.

Eighth, to meet the moment, the United States should also be more intersectional in how it studies and approaches problems, and the options it develops to respond to those challenges. For example, if not already being done, the National Counterterrorism Center should consider embedding a liaison at

190 For background on terrorism risk assessments, see Karl Robert's and John Horgan's foundational article "Risk Assessment and the Terrorist" in *Perspectives on Terrorism* 2:6 (2008).

191 As Russ Travers noted in 2019: "If we're going to get the intelligence right, we need to get the electrons right. Data is everything: whether looking for strategic trends, or conducting tactical level analysis associated with individuals and networks; data is the life blood of the CT community." See Travers.

192 As Matt Levitt has noted: "In facilitating a shift away from a military-focused counterterrorism posture and toward one focused on indicators and warning, policymakers and strategic planners must disentangle the funding for intelligence collection from the larger military budget bins within which they currently reside to prevent the loss of key support to downstream counterterrorism activities." See Levitt.

the CIA's new China Mission Center. The person assigned to that role would be tasked with learning more about the priorities of the Center; the ways in which NCTC—its data holdings, expertise, and tools—could support the work of the Center; how U.S. counterterrorism assistance in key locales could help advance the Center's mission; how China is leveraging counterterrorism to compete; and in understanding and projecting how U.S.-China rivalry could manifest as, or intersect with, terrorism through issues like proxy warfare in the years ahead. The U.S. government effort, led by U.S. Special Operations Command, to counter small unmanned aerial systems 'prior-to-launch' is also an intersectional problem that requires interdisciplinary and diverse expertise, from supply chain experts and intelligence analysts to individuals who understand how products are acquired and moved.

Ninth, authorities are another area where the United States needs to continue its efforts to be more intersectional. The evolution of the Department of Defense's 'Build, Train, Equip' authorities—from 1206 to 2282 then 333—over a nearly 15-year period provides an important case in point. Across that span of time, the language associated with this set of build, train, and equip authorities has been expanded and made more encompassing to account for a wider range of partners and activities beyond counterterrorism. The United States should look for ways in key locations to design build partner capacity programs that would allow foreign partners to use the specific skills and capabilities for cross-functional purposes. For example, a program focused on intelligence network development could help a country like the Philippines to better leverage data to deepen its knowledge of Islamic State networks in Mindanao and understand their structure, map out patterns of behavior of China's maritime militias and fishing fleets, and better explore networks responsible for harmful cyber activity that have targeted Philippine government institutions and public infrastructure.

Despite the U.S. government's best efforts, terrorism attacks will unfortunately happen. And so, a tenth area that the United States should invest in and further develop are efforts to bolster the American public's resilience to terrorism through messaging, strategic communication, and other outreach efforts. This area has been a central, stated U.S. counterterrorism priority for more than a decade.[193] It includes support for efforts that are preventative in nature, which aim to "diminish terrorists' efforts [and ability] to radicalize and recruit people in the United States" by working with, and providing support to, community and civil society organizations,[194] and initiatives that in a broader sense seek to "build societal resilience to terrorism."[195] As the United States' 2021 National Strategy for Countering Domestic Terrorism highlights:

> Resilience can take many forms. It can mean raising public awareness of how terrorists deliberately seek overreaction, which can help to avoid precisely that overreaction and instead thwart terrorists' own strategies. And it can mean, broader still, cultivating the type of digital literacy that can empower the American public to resist those who would use online communications platforms and other venues to recruit, radicalize, and mobilize to violence.[196]

One of the ways that the United States can help to raise "public awareness of how terrorists deliberately seek overreaction" is by being more proactive, thoughtful, and calculated in terms of how it responds to terror attacks and potential terror attacks. For example, the National Counterterrorism Center should consider creating a position for an official spokesperson. The person selected to serve in that role would be trained in crisis communication and be able to serve as a bona fide terrorism and extremism subject matter expert to news outlets. They would also coordinate public messaging or outreach campaigns to raise awareness of today's complex terrorism threats. The work of the spokesperson could be informed, and shaped, by approaches other countries such as Israel or Canada have taken to build societal

193 Reflections of this can be found by how the issue of resilience is treated in the 2011 and 2018 U.S. National Counterterrorism Strategies.

194 "2018 U.S. National Strategy for Counterterrorism of the United States of America."

195 Ibid.

196 "National Strategy for Countering Domestic Terrorism."

resilience to terrorism.

Finally, during this period of transition, the U.S. CT community should embrace experiments and create mechanisms and structures to enable them. One small way this could be done is by holding an annual project concept day, a mechanism for CT community members regardless of level to pitch project ideas, designed to solve a problem or advance a specific U.S. CT priority, to senior CT leaders. A similar event could be run to generate ideas for how new or existing CT programs and policies could be measured and better evaluated, as a way to further U.S. CT prioritization goals.

The current moment is a tough and unique time for U.S. counterterrorism, but it is also an exciting one filled with a lot of opportunities to innovate, evolve, and forge a better and more sustainable path.

Combating Terrorism Center

AT WEST POINT

JSOU PRESS

JOINT SPECIAL OPERATIONS UNIVERSITY