Counterterrorism in an Era of More Limited Resources

By Sarah Bast

THE ISSUE

- With the National Security Strategy and National Defense Strategy lowering the prioritization of terrorism, the U.S. government will need cost-effective options to continue to diminish the terrorist threat.

- Nonkinetic efforts can be a cost-effective way to reduce terrorist groups’ ability to radicalize, disseminate messages, use the internet, facilitate foreign fighters, fundraise, and exploit poor governance. Undercutting these intertwined terrorist enablers weakens the groups writ large.
Over the past 17 years, the U.S. government and its allies have made tremendous progress detecting and preventing catastrophic terrorist attacks like 9/11. The intelligence community improved collection, analysis, and information sharing; law enforcement got better at arresting terrorist supporters and potential attackers; and the U.S. military mastered finding, fixing, and finishing terrorists. Unfortunately, even with all those improvements and resources, terrorism has gotten more pervasive and terrorist groups have gotten more resilient. Even removing key leaders and taking away physical strongholds, while great and necessary victories, have not defeated the groups. With the National Security Strategy and National Defense Strategy lowering the prioritization of terrorism compared to other threats, the U.S. government will need to rely more on the cost-effective nonkinetic efforts—in addition to limited kinetic strikes—to continue making progress against this global and generational issue. This commentary will examine different cost-effective ways to counter some of the intertwined necessary terrorist enablers, including terrorists’ radicalization, messaging, use of the internet, foreign fighters’ facilitation, financing, and exploitation of poor governance. It will also offer opportunities to alter, expound, and enhance ongoing initiatives to address these factors.

RADICALIZATION

Terrorists do not have a single recruitment strategy. Radicalization is based on personal, group, community, sociopolitical, and ideological factors, according to a National Counterterrorism Center (NCTC) study.¹

Terrorists recognize this and offer an array of pull and push factors to gain recruits, with more local recruits likely pushed into joining for practical reasons and recruits coming from a further distance likely more ideologically driven to support the fight. The so-called Islamic State (ISIS)—which has succeeded in getting the most recruits of a Sunni terrorist group—is full of digital natives who use social media to share their stories and make themselves available to answer questions from potential recruits.²

ISIS’s open recruitment to all Muslims, including females,
to join the caliphate led to a relatively large membership compared to al Qaeda, which was more exclusionary and required references.

Preventing radicalization is not one size fits all. Terrorism prevention has been woefully under supported and underfunded and has over-relied on online messaging efforts. Community and civic leaders are at the forefront of challenging violent extremism by addressing root causes, but they require much greater funding, support, and encouragement, according to a 2016 CSIS report.

Terrorism prevention receives less than 0.01 percent of the U.S. government’s counterterrorism (CT) budget. It needs significantly more resources to empower locals who are best positioned to identify those most vulnerable to recruitment. While initial studies on effectiveness are ongoing by the Department of Homeland Security (DHS) with its 2017 grants, anecdotal success stories exist and should encourage the risk of investing the time and political will to try on a larger scale.

Example of Terrorism Prevention

Between 2007 and 2012, the U.S. Agency for International Development (USAID) Office of Transition Initiatives implemented a pilot program aiming to counter the drivers of violent extremism in Kenya. This program provided small grants for livelihood training, cultural events, community debates on sensitive topics, and counseling for posttraumatic stress disorder. The Integrity Research and Consultancy evaluated the program at the end of the trial and found considerable qualitative evidence to suggest that the program achieved a positive impact in dissuading certain individuals from following the violent extremist path, though the evaluators found areas to improve the execution of the program. This five-year program cost an average of $353,200 a year.

MESSAGING
Messaging and recruitment are often conflated. While they are related—and a lot of messages are geared toward recruitment—they are not synonymous. Terrorists tailor messages to different audiences—including potential supporters, existing sympathizers, enemies, and the general public—to encourage different responses—like providing passive or active support, inspiring action, providing threats, or encouraging a change in policy. ISIS messaging has been the most prolific and sophisticated of any Sunni terrorist group. Even with ISIS’s lost territory—which reduced the group’s media output—it still produced 1,373 unique media products between August 1, 2017, and February 28, 2018, according to terrorist messaging scholars Charlie Winter and Haroro J. Ingram. ISIS is not just prolific, it is compelling. Its messaging is successful because it proactively combines positive and negative themes tailored to its different audiences. Simon Sinek famously explained that in marketing and leadership it is not what you do, but why you do it. ISIS mastered this lesson and has successfully promoted its caliphate vision to a mass audience—something that al Qaeda always struggled to do.

The United States and the defeat-ISIS coalition, on the other hand, mostly reacts to ISIS messages, focusing on content removal and responding to terrorist messages rather than providing a compelling alternative message. As last year’s unanimously adopted UN Security Resolution 2354 (2017) says, “many States and experts in the field believe that focusing attention only on countering terrorist narratives is unlikely to succeed, in part because this only targets one facet of narratives that are often multilayered and complex. It is thus necessary, it is argued, also to offer alternative or positive narratives, especially when terrorists seek to exploit genuine grievances.” Furthermore, social-media research has shown that messages from friends and peers are more persuasive than general advertising. Therefore, in addition to traditional counterterrorism messaging that provides a tailored message to a specific audience, we also need to share a better vision that could inspire the masses to proactively take a stand against terrorism, thereby increasing engagement and providing a more tailored response to local situations. By crowdsourcing part of the messaging effort, we would have an inspiring movement of our own that counters the terrorist movement rather than a handful of individuals countering it. This comes with risk though, most notably the inability to control the counter message.

Example of Messaging Efforts
The U.S. Embassy in Abuja and the U.S. State Department supported Equal Access International’s efforts to create a radio program to counter Boko Haram’s ideology and messaging with positive local narratives that reduce vulnerability to violent extremism in northern Nigeria. When Equal Access International surveyed listeners about the impact on their behavior or attitude around issues such as nonviolence, gender inclusion, and supporting youth because of listening to the shows, 90 percent reported a positive change in their behavior, according to a report by Equal Access. After a radio episode on radicalization, one community noted that almost 20 radicalized youth surrendered weapons to local authorities and almost 70 people created a group named after the show to offer advice, counseling, and guidance to young people. Equal Access estimates that around 80 percent of its target populations in the 19 northern states of Nigeria where it broadcasts are familiar with or have listened to at least one of its programs. With a broadcast audience in the tens of millions, the cost of reaching one person with their message is just a few cents.

USE OF THE INTERNET
Terrorist use of the internet is intertwined with messaging and radicalization, as it is a platform to do both. Terrorists also use the internet for communication, command, control, and attacks. Terrorists are communicating on encrypted applications to circumvent intelligence collection and private-sector disruption. According to the FBI website, encryption blocked the bureau from accessing the content of about 7,800 devices in fiscal year 2017—which was more than half of the devices it attempted to access during that timeframe—even though there was legal authority to do so. Director of National Intelligence Daniel Coates has testified that terrorists also have the capability to do denial of service attacks against under protected servers, web defacements, and personally identifiable information disclosures. While terrorists evolve at the speed of the internet, the U.S. government bureaucracy has not. The last U.S. government strategy to combat terrorist use of the internet is from 2007, when Twitter was still in its infancy and before WhatsApp, Snapchat, Telegram, and many other
popular applications and sites were created. It is time for a new CT cyber strategy that looks at both defensive and offensive capabilities. While public-private partnerships exist between government agencies and tech industries, further strengthening these partnerships could enhance efforts to counter terrorists’ use of the internet. However, the government needs to act in a unified manner, rather than each agency reaching out independently, and it needs to understand the private sector’s goals, capabilities, and limitations. Leveraging existing private-sector platforms and technologies saves the government from having to develop some of these capabilities.

**Example of Efforts to Limit Terrorist Use of the Internet**

Tech Against Terror is a UN-mandated public-private partnership between the tech sector, civil society, and governments to tackle terrorist exploitation of their technologies while respecting human rights. Tech Against Terror has engaged over 150 companies and launched a knowledge-sharing platform and a data science network to develop and share tools to help small tech platforms protect themselves from terrorist exploitation, according to Tech Against Terror’s website.

**FOREIGN FIGHTERS’ FACILITATION**

Foreign fighters move from one conflict to the next. Since September 11, 2001, the United States has confronted the phenomenon of foreign fighters in Afghanistan, Pakistan, Iraq, the Philippines, Yemen, Libya, and Syria—to name a few. As those foreign fighters who fought in Iraq and Syria move on to new conflicts, that list of countries likely will grow. At its height, ISIS attracted 40,000 foreign fighters from 120 different countries to its so-called caliphate. For comparison, the First Chechen War attracted 200–300 fighters; the Second Chechen War attracted an additional 700; and al Qaeda attracted 10,000–20,000 foreign fighters to Afghanistan between 1996–2001, according to a CSIS study of foreign fighters.

Of those 40,000 foreign fighters, only about 300 were Americans, which means that our partner nations will be doing most of the heavy lifting when it comes to returning foreign fighters. Those partners and the United States need to put in place the plans, legal frameworks, and institutions necessary to interdict, arrest, prosecute, incarcerate, and eventually rehabilitate and reintegrate returning fighters. Without rehabilitation and reintegration programs, law enforcement may end up rearresting those same individuals. Rehabilitation, mental health support, and social support will be especially relevant for the children of returning foreign fighters.

**Example of Rehabilitation**

Since 2009, The Unity Initiative (TUI)—a specialist intervention consultancy based in the United Kingdom that focuses on rehabilitating individuals convicted of terrorist offenses—has rehabilitated more than 50 individuals convicted of terrorism offenses in the United Kingdom and an additional 180 individuals considered extreme by authorities, family members, or peers. TUI has worked with almost two dozen returning foreign fighters, according to a West Point interview with Dr. Angela Misra, the deputy chief executive and co-founder of TUI.

TUI’s model includes providing the individuals with an alternative, positive activism, something that gives their life purpose.

**FINANCING**

While Sunni terrorists may gloat that a particular attack was relatively cheap compared to the impact that it has, terrorist groups require significant finances to operate. They need to be able to train and equip operatives. They pay member salaries and sometimes death benefits. When they occupy territory, they are responsible for the basic services. They simply cannot operate without money. Al Qaeda gained a lot of its finances from donations. The New York Times recovered ledgers, monthly budgets, and receipts from formerly ISIS-held territory, which revealed that the group self-funded and diversified its resources and monetized every inch of territory, making hundreds of millions of dollars on agriculture alone. Tax revenue far exceeded oil sales. The group peaked at an estimated $40 million per month in 2015, according to the International Centre for the Study of Radicalisation and Political Violence. With the loss of territory, ISIS lost most of its funding streams.
After 9/11, the United States, United Nations, and our allies created laws, policies, and institutions to track terrorist financing. However, as former deputy national security adviser for combating terrorism Juan Zarate testified to Congress earlier this year, “For a financial pressure campaign to work, it must be applied and enforced constantly.” Building international consistency is one of the areas where we can have the biggest impact on terrorism finance. A 2015 report by the Financial Action Task Force (FATF)—an international body concerned with combating financial crimes—found that while most countries had comprehensive legal frameworks against terrorist financing, two-thirds of the countries did not implement them.

Counter-finance efforts should entail further training, advising, and assisting foreign intelligence and law enforcement to increase the consistency of the pressure on terrorists’ financial resources.

Example of Counter-Finance Efforts

After 9/11, the U.S. Treasury Department initiated the Terrorist Finance Tracking Program (TFTP) to identify, track, and pursue terrorists. The TFTP has provided thousands of valuable leads to U.S. agencies and other governments, which have helped prevent and investigate attacks. This program provided lead information that helped thwart attacks, including a plot to bomb transatlantic aircraft in 2006, a plot to attack New York’s John F. Kennedy Airport in 2007, and a plot to assassinate the Saudi Arabian ambassador to the United States in 2011, according to the U.S. Treasury Department. It also helped aid the investigations of several of the most visible and violent attacks, like the November 2015 Paris attack and the 2013 Boston Marathon bombing.

GOVERNANCE

While we press forward with an integrated kinetic and nonkinetic plan, we must impress upon our partners the importance of human rights and good governance. Some states use terrorism as a convenient justification to stifle dissent, which ultimately plays into terrorist messaging. A study that examined nine types of repression on domestic terrorism in 149 countries over a 24-year period found that forms of repression that close off nonviolent avenues of dissent and boost group grievances increase the amount of domestic terrorism a country faces. The Office of the UN High Commissioner for Human Rights has reported that repressive counterterrorism measures have been used to stifle the voices of human rights defenders, journalists, minorities, indigenous groups, and civil society. As the U.S. government works with its partners, it must encourage responsible governance at national, state, and local levels that upholds human rights.

Simultaneously, it is important for credible local governments to hold areas cleared of ISIS and other violent extremist organizations and to restart basic local services. If there is a power vacuum, those same groups—or Iranian proxies—will step in. Iran, for example, has trained associated groups—such as Hizballah, Asaib Ahl al-Haq, and Kataib Hizballah—to exploit disorder by providing services and security, according to a New York Times article. As Mark Mitchell, acting assistant secretary of defense for special operations/low-intensity conflict, testified in December, “to achieve enduring results, we must ensure that our successes on the battlefield are complemented by well-resourced post-conflict stabilization efforts. These efforts, principally led by the Department of State and USAID, are critical to cementing military gains and preventing terrorist organizations from reestablishing themselves.”

KINETIC

All the while, we need to continue to put kinetic pressure on terrorists. Some terrorists have skill sets that need to be removed from the battlefield, and in other cases, removing a terrorist from the battlefield sends a message that helps get us closer to a peaceful end state. Kinetic action can also deny terrorists control of territory, from which extremist groups would plan attacks, train, raise funds, and recruit.

Kinetic operations are expensive. Annual spending peaked at $164 billion in Iraq in FY 2008 and $122 billion in Afghanistan in FY 2011, according to a report by the Center for Strategic and Budgetary Assessments. For FY 2019, DoD requested $1.4 billion to work by, with, and through the government of Iraq’s security forces and vetted Syrian opposition forces to secure territory liberated from ISIS and counter any future ISIS threats.

CONCLUSION

Focusing on enabling elements of terrorism—like radicalization, messaging, foreign fighter facilitation, funding, and exploitation of poor governance—can provide cost-effective ways to lower the terrorist threat, which would reduce the need for more expensive kinetic options.

The U.S. government also needs to better integrate our kinetic and nonkinetic efforts. Military or law-enforcement operators should meet with leaders of nonkinetic efforts before acting, so that the corollary
messaging, cyber, prevention, and counter-finance plans are in sync and complementary.

It’s time to focus on the rest of the tools and invest the time, political support, and resources into nonkinetic options, so we can fully utilize all the tools of national power to limit the terrorism threat. It is also critical to use these tools consistently and to be patient; truly altering the environment that enables terrorists is a formidable task, but one that the United States and its allies can rise to.

**RECOMMENDATIONS**

- Provide community and civic leaders with greater funding, support, and encouragement to **prevent radicalization**.
- In addition to traditional counterterrorism messaging that provides a tailored message to a specific audience, we need to share a **positive alternative message** that could inspire the masses to proactively take a stand against terrorism.
- We need a new **CT cyber strategy** that looks at both defensive and offensive capabilities.
- The United States needs to help allies put in place the plans, legal frameworks, and institutions necessary to interdict, arrest, prosecute, incarcerate, and eventually rehabilitate and reintegrate returning fighters.
- The United States should increase training, advising, and assisting foreign intelligence and law enforcement to help allies maintain consistent pressure on terrorists’ financial resources.
- We must impress upon our partners the importance of human rights, good governance, and providing basic local services, which would mitigate potential grievances that terrorists could exploit.
- We need to continue to use **limited kinetic action** to remove key terrorists and deny them safe haven.

Sarah Bast is a visiting fellow with the International Security Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C.
ENDNOTES


3. Ibid.


8. USAID, “Kenya Transition Initiative.”


15. Ibid.


22. Donnelly, “History of Foreign Fighters.”


26. Barrett, Beyond the Caliphate.


28. Ibid.


31. Ibid.


39. Ibid.


