COMMUNICATING TO WIN: HOW TERRORISTS GAIN ADVANTAGE IN THE INFORMATION ENVIRONMENT

Joseph Mroszczyk and Max Abrahms | 10.19.21

The appeal of terrorist groups remains strong. For at least the past two decades, the United States and its allies have pursued terrorist organizations across the globe, disrupting their networks, killing or capturing their leaders, and removing their safe havens. Yet with the Taliban regaining control of Afghanistan, jihadist organizations expanding across Africa, and the threat of an Islamic State resurgence in Iraq, tactical military successes have not defeated them entirely.

Terrorist organizations remain resilient in part because they possess advantages over the US government in the information environment. The nature of the information environment—in which a statement, photo, or video is disseminated worldwide in an instant—often forces the United States into a reactive posture, allowing terrorist groups to maneuver freely toward their messaging objectives.

Terrorist groups manipulate information for a variety of goals, including to recruit new members, distance themselves from attacks that are politically costly, and issue threats that can change the behavior of their targets. In response, the United States struggles to keep pace, consistently identifying the problem while falling short of making the changes necessary to compete. Today, faced with adversaries that are far more sophisticated than any terrorist group, the United States would do well to learn from its mistakes in the information environment over the past two decades of counterterrorism operations if it hopes to compete more successfully with Russia and China.

How Terrorists Manage Their Images

Terrorism has long been understood as theater. Terrorist groups advertise their grievances with violence. The head of the United Red Army, an offshoot of the terrorist Japanese Red Army, explained: "Violent actions . . . are shocking. We *want* to shock people, everywhere. . . . It is our only way of communicating with the people." Al-Qaeda characterizes its violence with similar language. Osama bin Laden and his deputy, Ayman al-Zawahiri, described violence like the September 11, 2001 terrorist attack as "messages with no words," which is "the [only] language understood by the West." Beyond amplifying a political message, political scientists understand terrorism as a means to demonstrate resolve, coerce concessions, and attract recruits and other resources. Indeed, the informational dimension of a terrorist attack aims to cause political or religious changes, distinguishing terrorism from other types of criminal violence.

Effective militant leaders recognize that indiscriminate violence against civilian targets can cost them, especially

MOST POPULAR POSTS

Escalation to Nuclear War in the Digital Age: Risk of Inadvertent Escalation in the Emerging Information Ecosystem

Not Your Grandfather's Resistance: The Unavoidable Truths about Small States' Best

compared to more selective violence against military and other government targets. Numerous empirical studies find that terrorist attacks on civilians risk lowering the odds of government concessions while increasing political support for hardline politicians and the likelihood of punishing counterterrorism measures. Based on this insight, smart militant leaders adjust their use of the information environment to distance themselves from counterproductive civilian attacks.

Our previous analysis of terrorist propaganda videos discovered that there are incongruities between the actual targeting practices of terrorist groups and the attacks they choose to publicize in their official propaganda videos; terrorist groups are sensitive to their public images and highlight the attacks that are most politically advantageous. Militant leaders engage in a reputation-enhancing strategy in two ways: denying involvement and denying intent.

Terrorist groups deny organizational involvement in an attack to improve public perception of the group. The Taliban leadership, for example, eagerly assumed organizational responsibility for selective attacks against military targets, while distancing themselves when operatives committed indiscriminate bloodshed. For instance, the Taliban claimed responsibility when operatives ambushed Mohammad Qasim Fahim, leader of the alliance that toppled the Taliban in 2001, on a road in northern Kunduz. By contrast, the leadership denied organizational involvement when Taliban operatives were widely believed to be the ones behind a 2013 attack on the International Committee of the Red Cross in Jalalabad.

Denying involvement in politically costly civilian attacks is hardly limited to the Taliban. In June 2021, for example, jihadists slaughtered over 130 civilians in Solhan village in the Burkina Faso's Yagha province, shooting people and burning down homes and a market. Analysts fingered the al-Qaeda-linked group Jama'at Nasr al-Islam wal-Muslimin as the perpetrators, but the group's leadership released a statement denying involvement and saying that such indiscriminate acts are "not a part of the methodology of Muslims in jihad and fighting for the sake of Allah." Beyond such anecdotal evidence, large comparative studies find

Defense Against Aggression

Ten Years after the al-Awlaki Killing: A Reckoning for the United States' Drones Wars Awaits

UPCOMING EVENTS

There are no upcoming events at this time.

ANNOUNCEMENTS

Announcing the Modern War Institute'...

Call for Applications: MWI's 2021–22 Fellow...

Call for Submissions: Polar SOF Essay Contest

Without Firing a Shot: Coercion and Strategy...

that militant groups around the world are significantly more likely to claim credit for attacks against military targets rather than civilian ones.

When militant leaders cannot plausibly deny organizational responsibility, they often deny intent. Whereas denying involvement attempts to conceal that the attack was committed by the organization, denying intent attempts to demonstrate that it did not reflect the intentions of the group's leadership. Apologies are a common method of doing so. Such apologies are not necessarily insincere: operatives often engage targets in defiance of leadership preferences.

Al-Shabaab did just this in December 2019, denying senior leader intent following a massive vehicle-borne improvised explosive device attack in Mogadishu, Somalia, that killed more than eighty people. Al-Shabaab claimed responsibility for the attack but a spokesman for the group said they were "very sorry" that Somalis were killed, noting that the intended targets of the attack were Turkish mercenaries. Such apologies for harming civilians are found across militant groups, from Colombia's National Liberation Army to the Communist Party of Nepal (Maoist). As recently as July 2021, following the death of a Danish Reuters journalist embedded with Afghan special operations forces during a clash with Taliban fighters, a Taliban spokesman apologized for his death.

In these ways, militant leaders practice denial of organizational involvement and denial of intent to distance themselves from politically risky civilian attacks and thereby improve their odds of success. Terrorist propaganda videos are also carefully crafted to maximize sympathy: we find that most militant groups feature a smaller proportion of civilian attacks in their propaganda videos than the actual attack patterns of their operatives. But denials are not the only way militant groups further their efforts with information operations.

Issuing Threats and Attracting Recruits

Terrorist groups also use the information environment to threaten target populations and generate a supply of

recruits in order to sustain operations.

In contrast to a group's efforts to deny involvement in a politically costly attack, sometimes militant leaders maximize fear by threatening and broadcasting attacks that their groups do not actually carry out. For instance, in February 2015, the Somali terrorist group al-Shabaab released a video online calling for attacks against the Mall of America in Minnesota, along with other malls in the United States, Canada, and Britain. This prompted increased security measures and a scramble by retailers to assure customers of their safety. One economist noted that there was "no question" that the threat was a "disruption to economic activity." Despite the fact that al-Shabaab had no known operational capability in the United States at the time, it still provoked a response from the US public. And in October 2019, the Islamic State falsely claimed that the sniper behind the Las Vegas shooting was a "soldier of the Caliphate." Significantly, this faulty credit claim was issued while the Islamic State was suffering a string of battlefield losses in Syria, and the claim was presumably intended to signal the group's continued viability.

Terrorists also use the information environment to attract recruits. Much has been written about how terrorist groups recruit using modern communication technologies, such as social media. Though it is difficult to measure what percentage of terrorist group members were recruited online, ample anecdotal evidence suggests that terrorist groups effectively attract recruits on these platforms, both locally and internationally. For example, al–Shabaab tailors recruiting messages on social media to target recruits from within Somalia as well as from the Somali diaspora community in the United States and Europe. Similarly, the Islamic State attracted over forty thousand foreign fighters from over one hundred countries. When mainstream social media platforms are shut down, terrorist communications have gravitated to encrypted apps such as Telegram. In some cases, terrorist groups communicate with new mechanisms before they have reached peak popularity in society: the Islamic State was an early adopter of TikTok. The modern social media ecosystem offers militants countless platforms to disseminate material around the world and strengthen their brands.

Challenges in Countering the Narratives

The United States has stumbled to keep pace with terrorists in the information environment, even with the widespread acknowledgement in the wake of the 9/11 terrorist attacks that much of the new war against terrorism would be fought in this environment. This is largely due to the inherently distributed nature of the information environment in which messages can be disseminated around the world, even from a remote terrorist camp. This puts governments at a disadvantage due to difficulties such as whole-of-government synchronization, a lack of ownership of the issue, and other bureaucratic obstacles that inhibit rapid and agile maneuver. Terrorist groups make plenty of public relations mistakes, but they have demonstrated greater adaptability and innovation in the information environment than the governments tasked with countering them.

Despite various efforts by the US government in the years after 9/11 to reform its bureaucracy to counter terrorists in the information environment, the problem remains unresolved. The 2017 National Security Strategy admitted that US "efforts to counter the exploitation of information by rivals have been tepid and fragmented" while lacking a "sustained focus." The subsequent 2018 National Strategy for Counterterrorism acknowledged that the United States has still "not developed a prevention architecture to thwart terrorist radicalization and recruitment." Developing and coordinating a whole-of-government response to a rapidly changing information environment has proven stubbornly difficult.

Since the private sector owns many of the nodes through which terrorists transmit their messages, the government must work with these companies to limit the spread of extremist content and dampen its effects. Social media companies have acknowledged that terrorist groups use their platforms to spread extremist content. To address this issue, technology companies such as YouTube, Microsoft, and Twitter started the Global Internet Forum to Counter Terrorism in 2017 with the mission of preventing terrorists and violent extremists from exploiting digital platforms. More recently, Facebook announced it would begin warning

some users that they had been exposed to extremist content on its platform. Continued engagement with these technology companies is vital to limiting extremist content and its spread. But this impulse must be balanced against the knowledge that terrorists often hope to elicit overreactions from governments and that illiberal government responses are actually advantageous for terrorists. Striking the right balance between counterterrorism and free speech is among the trickiest aspects of combating terrorists.

Moving Forward

The last twenty years have shown that competing in the information environment, even against militarily inferior adversaries, is difficult. But while terrorist groups have certain advantages in the information environment, they also have vulnerabilities that can be exploited. For example, a concerted effort to highlight the carnage of terrorist attacks can chip away at a group's appeal. Attributing attacks against civilians to a group before it has a chance to deny involvement could hurt the group's image and ultimately reduce its appeal among potential recruits. And since many of these groups rely on digital platforms to disseminate their message, policymakers should continue to work with the private sector to rapidly identify and remove dangerous content and users.

As the US national security apparatus pivots away from counterterrorism, both Russia and China continue engaging in the information environment to pursue their interests. But the United States has so far struggled to adopt lessons from two decades of counterterrorism operations. "The United States is being strategically defeated in the information environment," retired US lieutenant general Michael Nagata noted in October 2020. "We're not even holding our own. We're being defeated. We're being outmaneuvered, we're being outflanked, we're being out persuaded." This sentiment appears widespread; it is not uncommon today to read opinion pieces arguing that the United States is already losing the information war with both China and Russia.

There are growing appeals for the United States to revamp its information operations efforts. For example, an April 2021 Government Accountability Office report recommended enhanced leadership and integration of information operations at the Department of Defense, noting that the Pentagon has "made little progress in implementing its information operations strategy" and confronts "challenges conducting information operations." DoD has made strides to reorganize for information warfare, but much more work still needs to be done.

So what lessons from twenty years of counterterrorism can we apply in this new era of competition in the information domain?

First, use the information domain to increase the reputational costs of adversary actions. This is particularly relevant with respect to Russian and Chinese action in the gray zone. A 2019 Rand report on how to gain competitive advantage in the gray zone argued that, since Russia and China both value their current status as legitimate and respected members of the international system, they remain vulnerable to information campaigns orchestrated to heighten the reputational costs associated with their aggressive or hostile actions. In much the same way that terrorist organizations are vulnerable to the reputational costs associated with civilian targeting, Russia and China may face similar reputational costs on the international stage if the United States is able to strategically expose their actions and draw negative attention.

Second, the United States must increase the velocity with which it operates in this domain. According to psychologists' studies of misinformation and disinformation, people are prone to accept information they are exposed to first, regardless of its veracity. False information can persist in people's minds even after they learn valid information. In fact, attempts at correcting false information may even lead to a "backfire effect" in which belief in the false information actually strengthens. Terrorist organizations have understood that speed of dissemination is key, as demonstrated by their rapid release of propaganda videos designed to frame an event or an attack to their advantage. The United States must recognize that in the global

competition against Russia and China, the velocity with which it can disseminate information could provide advantages.

Third, US policymakers must become more tolerant of risk when operating in the information environment. Effects in this domain are not governed by the laws of physics, and US commanders and leaders need to recognize that some operations will not always achieve the intended effects. The Joint Concept for Operating in the Information Environment admits that, in contrast to US forces, adversaries "are bolder and accept more risk operating in this changing [information environment]. As a result, they create political, social, and military advantages that exceed their traditional combat power." Low risk tolerance prevents the United States from engaging in the types of rapid and distributed responses needed to shape the environment to its advantage.

Today, the United States faces competitors with more robust, sophisticated, and synchronized capabilities than any terrorist organization. It would do well not to dismiss some of the hard-earned lessons of the past two decades.

Dr. Joseph Mroszczyk is a defense contractor at the US Naval War College and also serves as an officer in the US Navy Reserve, where he has mobilized in support of Combined Joint Task Force – Horn of Africa. He has previously worked at the Department of Homeland Security, with the US Army's Human Terrain System program in Iraq, and in various private sector intelligence-related roles.

Dr. Max Abrahms is an associate professor of political science and public policy at Northeastern University and senior fellow at the Institute for Peace & Diplomacy. He has published extensively on terrorism with articles in International Organization*,* International Security*,* International Studies Quarterly*,* Security Studies*,* Comparative Political Studies*,* Harvard Business Review*,* Foreign Affairs*,* Foreign Policy*, and the* New York Times*. Abrahms has been a fellow at the Center for International Security and Cooperation at Stanford University, the Dickey Center at Dartmouth College, Johns*

Hopkins University's Department of Political Science, and the Washington Institute for Near East Policy, among other places.

The views expressed are those of the authors and do not reflect the official position of the United States Military Academy, the US Naval War College, Department of the Navy, Department of the Army, or Department of Defense.

LEAVE A REPLY

Your email address will not be published. Required fields are marked *

COMMENT

NAME * EMAIL * WEBSITE

☐ Save my name, email, and website in this browser for the next time I comment.

POST COMMENT