COMBATING TERRORISM CENTER AT WEST POINT

CTC SENTINEL

OBJECTIVE · RELEVANT · RIGOROUS | AUGUST 2025 · VOLUME 18, ISSUE 8

FEATURE ARTICLE

Tehran's U.S. Options

Terror pathways for Iran to strike in the United States

MATTHEW LEVITT

A VIEW FROM THE CT FOXHOLE

James Stack

DIRECTOR, GREAT PLAINS DIAGNOSTIC NETWORK

Contents

FEATURE ARTICLE

INTERVIEW

COMMENTARY

ANALYSIS

FROM THE EDITORS

In our cover article this month, Matthew Levitt examines potential retaliation by Iran against the U.S. homeland following its 12-day war with Israel and U.S. airstrikes against three of its nuclear facilities. "Iran may seek to carry out reprisal attacks in the United States, as it already has tried to do in Europe, targeting U.S. officials, Iranian dissidents, Israelis, or Jews," he writes. "If there were ever a time Iran would want to activate its homeland option, this would be it." Drawing on past cases of Iranian plots in the United States and elsewhere, Levitt outlines "the primary pathways available to Iran to conduct or enable an attack inside the United States," including "deploying Iranian agents, criminal surrogates, terrorist proxies, or actively seeking to inspire lone offenders to carry out attacks within the homeland."

Our interview is with James Stack of Kansas State University and director of the Great Plains Diagnostic Network, who we asked about vulnerabilities to the U.S. agricultural sector following news earlier this summer that several individuals had been arrested for smuggling "a potential agroterrorism weapon"—*Fusarium graminearum*—into the United States. "I didn't think that was a great pathogen to use as a bioweapon," he explains. "But that event may be less about *Fusarium graminearum* and more about finding the best way to sneak an organism into the country."

In this month's commentary, Nicholas Clark considers the appropriate role for generative artificial intelligence (AI) in the counterterrorism mission. He argues that rather than relying too heavily on generative AI in CT efforts, the focus should shift "toward enhancing education in probabilistic reasoning … and building robust data governance infrastructures." "In an environment where adaptability, innovation, and judgment can determine life or death," he writes, "overreliance on generative AI may do more harm than good. … In many cases, generative AI is a distraction and should only be used within a disciplined, use-case-driven approach, one that leverages narrow efficiencies while preserving the uniquely human strengths that remain irreplaceable in counterterrorism work."

Finally, Jason Warner examines China's new counterterrorism ambitions in Africa. He finds that whether engaging in U.N. peacekeeping operations, establishing overseas bases, conducting bilateral and multilateral training drills, or providing police training, China has proceeded with "caution, amity, respect, non-interference, and deference to African partners." Warner writes that China's "risk-averse, economic-first approach to CT may well prove to be too meager—all carrot and no stick—to deal with the brutality of the current African terrorism scene. At a certain point, China will likely have to cross a perilous bridge: take bolder, riskier, and more muscular and militarized approaches to CT, or stay the course, be perceived as weak, and ultimately, likely be ineffective." Either way, "for the United States, China's rise as an aspiring counterterrorism force in Africa should cause concern," he concludes.

Don Rassler and Kristina Hummel, *Editors-in-Chief*

CTCSENTINEL

Editors-in-Chief

Don Rassler

Kristina Hummel

CONTACT

Combating Terrorism Center
U.S. Military Academy
752 Thayer Road, Mahan Hall
West Point, NY 10996
Phone: (845) 938-8495
Email: ctc@westpoint.edu
Web: www.ctc.westpoint.edu/ctc-sentinel/

SUBMISSIONS

The *CTC Sentinel* welcomes submissions.

Contact us at ctc@westpoint.edu.

The views expressed in this report are those of the authors and not of the U.S. Military Academy, the Department of the Army, or any other agency of the U.S. Government.

Cover: On August 11, 2025, an Iranian flag hangs on a building that had been targeted during Israeli strikes in Tehran, Iran. (Morteza Nikoubazl/NurPhoto via AP)

Tehran's Homeland Option: Terror Pathways for Iran to Strike in the United States

By Matthew Levitt

The 12-day Iran war may be over, but the threat of Iranian reprisal attacks now looms large, and will for the foreseeable future. European authorities exposed plots in Sweden and Germany even as the war was being waged, and Israeli authorities issued a warning over potential attacks in the United Arab Emirates a couple of weeks later, specifically citing heightened concerns in the wake of the war with Iran. Iranian operatives or their agents could also attempt to carry out attacks inside the United States, leveraging what U.S. counterterrorism officials have describe as a "homeland option" developed over years. Given the U.S. role in bombing the Fordow nuclear complex, it should not be a surprise that U.S. authorities quickly issued a terrorism advisory warning of potential Iranian plots in the homeland. Drawing on past cases of Iranian plots in the United States and elsewhere, this article explores the primary pathways available to Iran conduct or enable a terrorism act in the United States. These include deploying Iranian agents, criminal surrogates, terrorist proxies, or actively seeking to inspire lone offenders to carry out attacks within the homeland.

The 12-day Iran war may be over, but the threat of Iranian reprisal attacks now looms large, and will for the foreseeable future. Authorities in Europe have already exposed two plots linked to Iran, one targeting Israeli and American interests in Sweden[1] and another targeting Jewish institutions and specific Jewish individuals in Germany.[2] But Iran and its proxies have spent years investing in a "homeland option"[3] here in the United States as well. In just the past five years, U.S. authorities have disrupted at least 17 Iranian plots in the homeland, including those involving Iranian operatives as well as terrorist and criminal proxies.[4] Other cases that fell short of plotting for a specific attack include a Hezbollah operative in Texas who purchased 300 pounds of ammonium nitrate,[5] an explosive precursor, and another who carried out surveillance missions in New York and Canada.[6] U.S. law enforcement and intelligence authorities remain on high alert for potential revenge attacks by Iranian agents or proxies arising out of the 12-day Israel-Iran war and the June 21 U.S bombing of Iranian nuclear facilities. The FBI increased its monitoring of Iran-backed operatives in the United States in advance of the U.S. strikes[7] and then, in June 2025, reassigned counterterrorism agents recently tasked to work on immigration cases back to the counterterrorism mission.[8] Federal officials advised their state and local government counterparts to be vigilant for potential domestic plots in the United States,[9] and the Department of Homeland Security issued a National Terrorism Advisory System bulletin warning that the "Iran conflict is causing a heightened threat environment in the United States."[10]

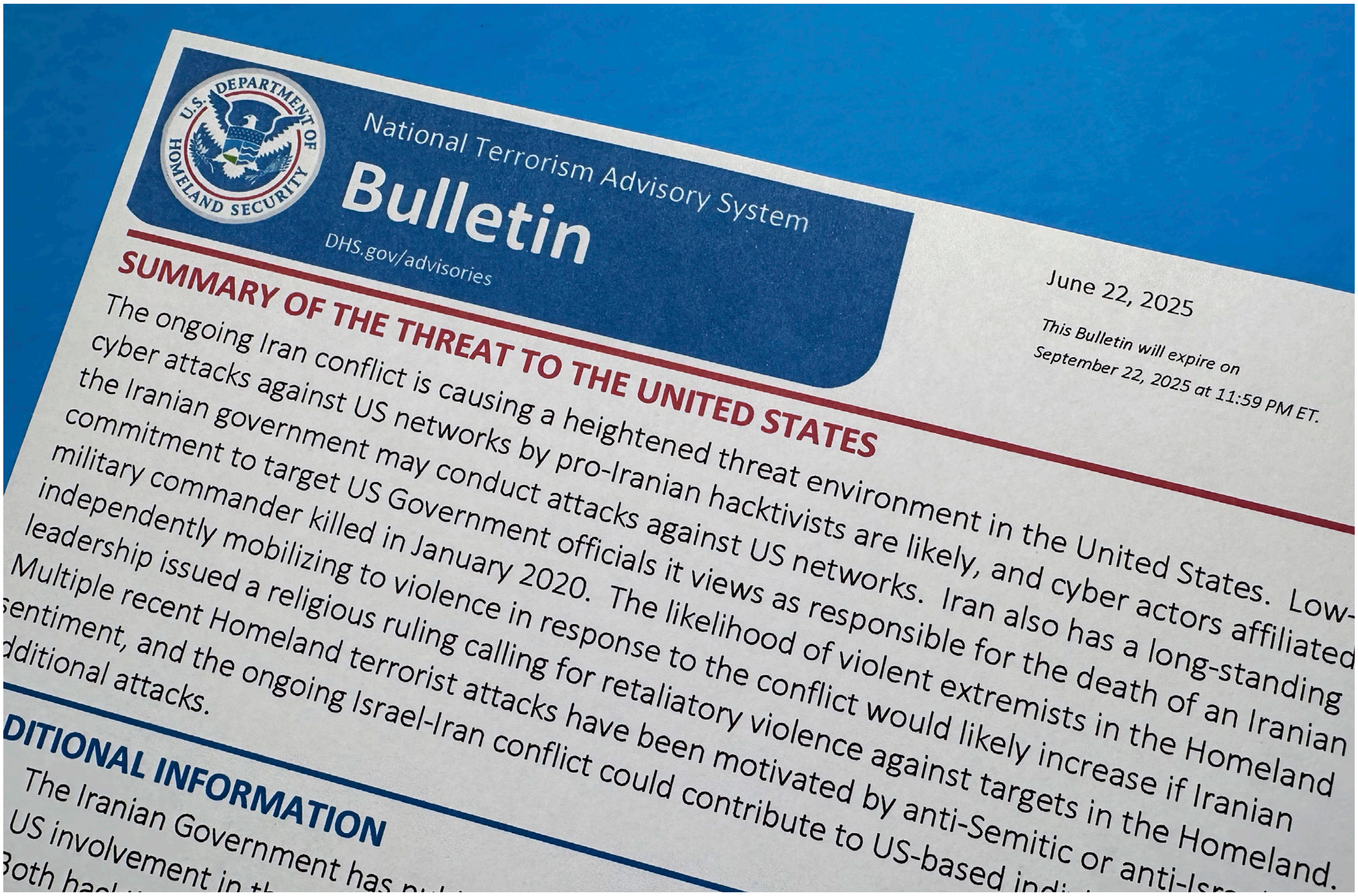
Dr. Matthew Levitt is the Fromer-Wexler senior fellow and director of the Reinhard program on counterterrorism and intelligence at the Washington Institute for Near East Policy. Levitt teaches at Georgetown and Pepperdine Universities. He is the author of Hezbollah: The Global Footprint of Lebanon's Party of God *and the creator of interactive, open-access online maps of Hezbollah and Iranian worldwide operational activities. He has written for* CTC Sentinel *since 2008. X: @Levitt_Matt*

With a ceasefire in place, Iran is likely wary of being tied to any successful plot for fear of inviting further reprisal attacks for any acts of terrorism abroad. Iran may even be less capable of executing sophisticated plots of its own right now, in light of the severe damage to Iran's Islamic Revolutionary Guard Corps (IRGC)—such as the killing of IRGC intelligence organization chief, Mohammad Kazemi, as well as his deputy.[11] Near-term plots are therefore more likely to come from criminal proxy groups or lone offenders operating at arm's length from Tehran (like the plots in Sweden and Germany), or from homegrown violent extremists inspired to carry out attacks to avenge Iran's humiliating losses. But in the long term, there can be no doubt that Iran will turn to foreign plots of various kinds to avenge the loss of so many senior officials[12] and the damage to Iran's nuclear and ballistic missile programs, much as Iran has sought to avenge the January 2020 killing of Quds Force leader Qassem Soleimani in a U.S. airstrike. Iran certainly has the capacity to do so.

Iranian Threats in Context

In the days leading up to the U.S. strikes against three Iranian nuclear facilities, Iran reportedly sent a message to President Donald Trump threatening to "activate sleeper-cell terror inside the United States" if the U.S. military attacked Iran.[13] Such threats should not be taken lightly, given the sharp uptick[14] in Iranian external operations[15] around the world—including in the United States—over the past decade, as well as the history of Hezbollah operatives carrying out surveillance of potential targets in the U.S. homeland.[16]

Iran sees terrorism as an extension of foreign policy—an asymmetric means of reaching its adversaries beyond its borders despite their military superiority. According to CIA reporting in the mid-1980s, "Tehran has used terrorism increasingly to support Iranian national interests," not only as a means to export its revolution.[17] That said, in a 1987 report, the CIA underscored that "the [Iranian] constitution gives the Revolutionary Guard responsibility for exporting the revolution, in addition to its



U.S. DEPARTMENT OF HOMELAND SECURITY

National Terrorism Advisory System

Bulletin

DHS.gov/advisories

June 22, 2025

This Bulletin will expire on
September 22, 2025 at 11:59 PM ET.

SUMMARY OF THE THREAT TO THE UNITED STATES

The ongoing Iran conflict is causing a heightened threat environment in the United States. Low-
cyber attacks against US networks by pro-Iranian hacktivists are likely, and cyber actors affiliated
the Iranian government may conduct attacks against US networks. Iran also has a long-standing
commitment to target US Government officials it views as responsible for the death of an Iranian
military commander killed in January 2020. The likelihood of violent extremists in the Homeland
independently mobilizing to violence in response to the conflict would likely increase if Iranian
leadership issued a religious ruling calling for retaliatory violence against targets in the Homeland.
Multiple recent Homeland terrorist attacks have been motivated by anti-Semitic or anti-Isr
sentiment, and the ongoing Israel-Iran conflict could contribute to US-based ind
dditional attacks.

DITIONAL INFORMATION

The Iranian Government has pu
US involvement in th
Both ha

A National Terrorism Advisory System bulletin issued by the U.S. Department of Homeland Security warning of a "heightened threat environment" following U.S. strikes on Iranian nuclear sites, is photographed on June 23, 2025. (Jon Elswick/AP Photo)

[domestic] security functions."[18] Indeed, while Iran's support for terrorism was meant to further its national interest, it also stemmed from the clerical regime's perception "that it has a religious duty to export its Islamic revolution and to wage, by whatever means, a constant struggle against the perceived oppressor states."[19] There can be no question that Iran today sees Israel and the United States in that light, and its revolution challenged as never before.

The revolutionary regime in Tehran has carried out plots abroad targeting dissidents, journalists, foreign officials, and others since just months after the 1979 revolution.[20] One of the first targeted a former Iranian official turned dissident in Bethesda, Maryland, in July 1980.[21] But for years, the U.S. intelligence community assessed that Iran and its proxies were unlikely to carry out attacks within the United States. Then came the 2011 IRGC plot to assassinate the Saudi ambassador to the United States in a popular Washington, D.C., restaurant,[22] which forced the U.S. intelligence community to reassess its assumptions. The result was a new assessment, expressed by then-Director of National Intelligence James Clapper in congressional testimony, that the plot "shows that some Iranian officials — probably including Supreme Leader Ali Khamenei — have changed their calculus and are now more willing to conduct an attack in the United States in response to real or perceived U.S. actions that threaten the regime."[23] Since then, Iranian agents or their proxies have been tied to 27 plots in the United States, according to a dataset maintained by the Washington Institute for Near East Policy.[24] Around the world, over the past five years, the dataset tracks 157 cases of Iranian foreign operations, including 75 involving Iranian agents, 22 involving criminal proxies, and 55 terrorist proxies.[25] "U.S. law enforcement has disrupted multiple potentially lethal Iranian-backed plots in the United States since 2020," DHS reported in June 2025. "During this timeframe, the Iranian government has also unsuccessfully targeted critics of its regime who are based in the Homeland for lethal attack."[26]

In its 2025 threat assessment, the DNI assessed that Iran "will continue to directly threaten U.S. persons globally and remains committed to its decade-long effort to develop surrogate networks inside the United States,"[27] harking back to the 2011 plot. The DHS Homeland Threat Assessment concurred, reporting "we expect Iran to remain the primary sponsor of terrorism and continue its efforts to advance plots against individuals—including current and former US officials—in the United States."[28]

Such plots have been on the rise in recent years,[29] and could involve Iranian operatives, criminal surrogates, or terrorist proxies. Authorities also worry that inspired lone offenders could decide to carry out less sophisticated but still deadly attacks of their own in support of Iran.[30]

Iranian Agents

In the past, Iran has both dispatched agents to the United States and tasked persons residing in the country to act as their agents. In

November 2003, New York City police spotted two Iranian guards employed at the Iranian Mission to the United Nations filming subway train tracks. Then, in May 2004, two different Iranian Mission security guards were observed videotaping infrastructure, public transportation, and New York City landmarks.[31]

Iranian agents have also conducted surveillance of Iranian dissidents and institutions inside the United States. Consider the case of Ahmadreza Mohammadi-Doostar, a dual U.S.-Iranian citizen living in Iran, and Majid Ghorbani, an Iranian citizen who resided in California. In 2017-2018, Ghorbani carried out surveillance of Iranian dissidents and dissident rallies in the United States and provided that information to Doostar. Doostar conducted surveillance of Jewish student organizations in Chicago.[32] In 2020, the two were sentenced to prison "in connection with work on behalf of Iran."[33]

Threats of Iranian plots in the United States spiked after the January 2020 targeted killing of Iranian general Qassem Soleimani. Within days of the U.S. airstrike that killed Soleimani, U.S. intelligence and law enforcement agencies released a joint intelligence bulletin warning of the need "to remain vigilant in the event of a potential [Government of Iran] GOI-directed or violent extremist GOI supporter threat to US-based individuals, facilities, and [computer] networks."[34]

Over the course of 2020 and 2021, a group of Iranian operatives based in Iran used an Iranian-American in California and unwitting American private investigators to collect information about the movements of Iranian-American human rights campaigner Masih Alinejad in support of a plot to kidnap her and transport her by sea from New York to Venezuela and from there to Iran.[35] This Iranian foreign operations network was run by Iranian intelligence operative Alireza Shavaroghi Farahani whose operatives targeted victims in the United States,[36] Canada, the United Kingdom, and the United Arab Emirates, according to the U.S. Department of Justice.[37] The plot was foiled when authorities issued an indictment of members of the Iranian intelligence network in July 2021.[38]

Meanwhile, in February 2021, a Belgian court convicted Assadollah Assadi, an Iranian diplomat based in Vienna, of organizing a July 2018 plot to bomb the annual convention of the National Council of Resistance of Iran—the political wing of the Mujahedeen-Khlaq, MEK—near Paris.[39] Three accomplices, all Iranian-Belgian dual citizens, were also sentenced for their roles in the plot.[40] According to German and Belgian prosecutors, Assadi was no run-of-the-mill diplomat but rather an Iranian intelligence officer operating under diplomatic cover.[41] In a statement, prosecutors tied Assadi to Iran's Ministry of Intelligence and Security (MOIS), whose tasks "primarily include the intensive observation and combating of opposition groups inside and outside Iran."[42]

"Iran maintains its intent to kill US government officials it deems responsible for the 2020 death of its Islamic Revolutionary Guards Corps (IRGC)-Qods Force Commander and designated foreign terrorist Qassem Soleimani," DHS reported earlier this year.[43] And Iran appears to have the potential capability to do so as well. In late May of this year, shortly before the Israel-Iran war began, FBI agents arrested Sharon Gohari, a naturalized U.S. citizen from Iran living in New York, on his return from a trip to Iran on charges of allegedly receiving child sexual abuse material.[44] According to the Department of Justice, Gohari is also a "professional alien smuggler" who is suspected of soliciting and receiving payment from Iranian nationals and others to smuggle people into the United States.[45] In one case, Gohari allegedly smuggled an Iranian national into the country who admitted that he had "previously completed tasks in Iran and Malaysia" for the IRGC.[46] The case, first reported by Court Watch,[47] led law enforcement to request that Gohari be detained pending trial.[48]

Recognizing the potential threat, President Trump posted to social media after the June 2025 U.S. airstrikes that "ANY RETALIATION BY IRAN AGAINST THE UNITED STATES OF AMERICA WILL BE MET WITH FORCE GREATER THAN WHAT WAS WITNESSED TONIGHT."[49] In an effort to distance Iran from plots against the United States and its allies, and mitigate the risk of retaliatory attacks against Iran, Iranian agents have taken to hiring criminal proxies to carry out attacks at Tehran's behest.

Criminal Surrogates

Following the failed 2018 Iranian bomb plot outside of Paris and the arrest and conviction of its organizer, Assadollah Assadi, Iranian operatives pivoted away from relying on Iranian nationals to carry out attacks in favor of hiring criminals to carry out attacks at Tehran's behest.[50]

In 2022, the U.S. Department of Justice indicted[51] IRGC operative Shahram Poursafi for running a murder-for-hire plot targeting former senior U.S. officials John Bolton[52] and Michael Pompeo.[53] Poursafi appears to have planned a series of attacks, telling the person he recruited to carry out the murders—someone he thought was a criminal for hire but who was actually working for the FBI—that he should first focus on killing Bolton but "then there would be other jobs" and the two "had years of work to do together."[54]

European officials expressed grave concern over Iran's use of criminal proxies to carry out attacks there, as well. The director of MI5 in the United Kingdom revealed in October 2024 that over the previous two and a half years, U.K. authorities had tracked 20 Iranian-backed plots targeting U.K. citizens and residents.[55] "Iranian state actors make extensive use of criminals as proxies – from international drug traffickers to low-level crooks," he added.[56] "The Iranian regime's use of criminal networks as terrorist proxies in Europe poses a grave threat to our internal security," the European Commission reported that same year, following accounts from Swedish authorities that Iran had contracted Swedish gangs to carry out attacks there.[57]

U.S. officials noticed a similar trend. In early 2024, the U.S. Department of the Treasury designated Iranian narcotics trafficker Naji Ibrahim Sharifi-Zindashti for operating a "network of individuals that targeted Iranian dissidents and opposition activists for assassination at the direction of the Iranian regime," specifically at the behest of Iran's Ministry of Intelligence and Security (MOIS).[58] For example, Zindashti's network recruited two Canadian Hell's Angels bikers to assassinate individuals in the United States who had fled Iran, including an Iranian defector.[59] According to the Treasury Department, "the MOIS and Iran's Islamic Revolutionary Guard Corps (IRGC) have long targeted perceived regime opponents in acts of transnational repression outside of Iran, a practice that the regime has accelerated in recent years," including in the United States.[60] In the wake of the Israel-Iran war, the European Union designated Zindashti and members of his network for serious human rights violations and transnational repression linked to these plots around the world.[61]

Undeterred by the exposure of the network that planned to kidnap Masih Alinejad, Iranian Revolutionary Guard general Ruhollah Bazghandi hired members of an Eastern European organized crime group to murder Alinejad in Brooklyn, New York.[62] One operative was arrested in July 2022 near Alinejad's home with a loaded automatic weapon in his car shortly after conducting surveillance of her and her home.[63] He later testified against two other members of the organized crime group who were convicted in the murder-for-hire case in March 2025.[64]

Last year, Asif Merchant, a Pakistani operative working for Iran, tried to hire hitmen who were actually undercover law enforcement officers[65] to assassinate then-presidential candidate Trump, among other political or government officials.[66] This was not intended to be a one-off relationship, Merchant told a confidential law enforcement source, but would be ongoing and involved other criminal activities, such as planning protests and stealing documents or USB drives from a target's home.[67]

Even in the midst of the 12-day Israel-Iran war, Iran reportedly reached out to organized crime groups in Europe, such as Foxtrot in Sweden, pressing them to quickly carry out attacks targeting Israeli and American interests there.[68] But the cost of taking on such contracts increases for organized crime groups as authorities around the world focus their intelligence and law enforcement agencies on potential Iranian threats. Terrorist proxies, however, are more likely to be motivated to act in Iran's interests given that their interest is ideological, not just financial.

Terrorist Proxies

Historically, Iran has used terrorist proxies to carry out attacks at its behest—on their own, or working together with Iranian agents—around the world.[69] While Hezbollah has never carried out an attack within the United States, the group has long had networks of operatives and supporters living across the country, some of whom carried out preoperational surveillance for potential future attacks in the homeland.[70]

"Hezbollah has maintained a presence in the United States since at least 1987," according to the FBI.[71] In 1994, the FBI reported that a Hezbollah cell in New York was divided into teams to protect operational security and Hezbollah matters could not be discussed outside of a member's team.[72] It further noted that members of a Hezbollah cell on the West Coast initiated a neighborhood watch program to alert cell members if law enforcement officers came around.[73] Hezbollah leadership in Lebanon would likely be wary of jeopardizing the relatively safe environment its operatives enjoy in the United States—where they primarily engage in illicit financial activities—by carrying out an act of terrorism in the homeland, the FBI assessed at the time.[74] But it then added this caveat: "However, such a decision could be initiated in reaction to a perceived threat from the United States or its allies against Hezbollah interests."[75] In 2002, the FBI went further still, reporting that "FBI investigations to date continue to indicate that many Hezbollah subjects in the United States have the capability to attempt terrorist attacks here should this be a desired objective of the group."[76]

Over time, Hezbollah cells in major American cities—places such as New York, Houston, Detroit, Los Angeles, and Boston—became aware of FBI surveillance of their activities.[77] In response, a former head of the FBI's Iran-Hezbollah unit explained, "Hezbollah started placing operatives in areas such as Portland, Oregon; Louisville, Kentucky; and these operatives were to blend into the community and establish, essentially, sleeper cells to be activated, to conduct whatever activities Hezbollah may want of them."[78]

Fast forward to June 2017, when the FBI arrested two Hezbollah operatives—Ali Kourani in New York and Samer el-Debek in Michigan—both members of Hezbollah's Islamic Jihad Organization terrorist unit.[79] One of the FBI agents who met with Kourani recalled that the then-suspect "sat back in his chair, squared his shoulders and stated, 'I am a member of 910, also known as Islamic Jihad or the Black Ops of Hezbollah. The unit is Iranian-controlled.'"[80]

At his Hezbollah handler's instruction, "Kourani carried out a variety of pre-operational intelligence-gathering missions in New York City, including conducting surveillance of FBI and U.S. Secret Service offices, as well as a U.S. Army armory."[81] "Kourani described himself as a Hezbollah sleeper agent, and carried out other operational activities in New York, such as identifying Israelis in New York who could be targeted by Hezbollah and finding people from whom he could procure arms that Hezbollah could stockpile in the area. Kourani told the FBI he believed his [Islamic Jihad Organization] IJO handler tasked him with identifying Israelis currently or formerly affiliated with the Israeli army 'to facilitate, among other things, the assassination of IDF personnel in retaliation for the 2008 assassination of [IJO leader] Imad Mughniyeh.'"[82]

Kourani also carried out surveillance at New York's JFK and Toronto's Pearson international airports and provided Hezbollah with detailed reports regarding "airport security procedures, the uniforms worn by security officials, and locations of cameras, security checkpoints, and other security barriers. At trial, prosecutors concluded that Hezbollah wanted this information because the group was 'thinking about how to get terrorists, and weapons, and contraband through airports, from Lebanon into Canada, from Lebanon into the United States.'"[83] In 2019, Kourani was convicted and sentenced to 40 years in prison for his covert terrorist activities on behalf of Hezbollah.[84]

For his part, el-Debek appears to have pleaded guilty and cooperated with U.S. authorities and was never put on trial.[85] Described as a Hezbollah bomb maker, el-Debek carried out Hezbollah missions around the world, including cleaning up precursor explosives at a bomb-making safe house in Thailand and carrying out surveillance of U.S. and Israeli embassies and other potential targets in Panama.[86]

A few years later, another Hezbollah operative, Alexei Saab, would be convicted of receiving military-type training from Hezbollah and other crimes.[87] According to the Department of Justice, he too carried out extensive preoperational surveillance of potential targets, including the United Nations headquarters, the Statue of Liberty, Rockefeller Center, Times Square, the Empire State Building, and local airports, tunnels, and bridges, and provided detailed information on these locations to Hezbollah.[88] "In particular," authorities noted, "Saab focused on the structural weaknesses of locations he surveilled in order to determine how a future attack could cause the most destruction."[89]

Kourani, as mentioned, described himself as a sleeper agent and informed the FBI in 2016 that "there would be certain scenarios that would require action or conduct by those who belonged to the cell."[90] Kourani said that the U.S. sleeper cell would expect to be called upon to act if the United States ever went to war with Iran, or if the United States were to target Hezbollah, Hezbollah leader

> **"Iran took its time preparing plots to avenge the death of Soleimani, and while all such plots have so far been thwarted, Iran continues to pursue plots to avenge his killing. The damage Israel and the United States inflicted on the regime in Tehran in the context of the recent war overshadows even the loss of Soleimani."**

Hassan Nasrallah, or Iranian interests. Kourani added, "in those scenarios the sleeper cell would also be triggered into action."[91] All these lines have now been crossed.

One case suggests Hezbollah may have already come close to triggering such action. In 2015, a Hezbollah operative in Houston was caught stockpiling ice-packs for the ammonium nitrate they contain, accumulating 300 pounds of the explosive precursor at the behest of the group.[92] Robert Assaf pleaded guilty to lying to investigators about this activity and agreed to cooperate with investigators.[93] The case suggests that Hezbollah sought and obtained hundreds of pounds of explosive precursor materials capable of producing multiple explosive devices in the United States.

All these cases, however, were thwarted by authorities, which suggests that Iran may increasingly seek to mobilize inspired lone offenders—who are much harder for law enforcement agencies to detect[94]—to carry out attacks, especially in the near term.

Inspired Lone Offenders

Authorities are concerned that individuals with no actual ties to Iran or its criminal or terrorist proxies could be radicalized by events abroad, for which they hold the United States responsible, and carry out acts of violence in the U.S. homeland.

In the terrorism advisory bulletin issued about the potential for Iranian reprisal strikes, DHS noted that Iran "publicly condemned direct U.S. involvement in the conflict," adding that the Iran war could "motivate violent extremists and hate crime perpetrators seeking to attack targets perceived to be Jewish, pro-Israel, or linked to the US government or military in the Homeland."[95] This would become more likely, DHS assessed, in the event that Iranian leadership were to issue a religious ruling calling for retaliatory violence against specific targets in the U.S. homeland.[96]

In fact, according to U.S. law enforcement authorities, Iranian information operations targeting the homeland are not new. "Over the last year," the Department of Homeland reported in October 2024, "Iranian information operations have focused on weakening US public support for Israel and Israel's response to the 7 October 2023 HAMAS terrorist attack. These efforts have included leveraging ongoing protests regarding the conflict, posing as activists online, and encouraging protests."[97] New York City police went on heightened alert in the context of the war with Iran, despite the lack of any specific threat to the city, because—in the words of Mayor Eric Adams—"you always want to be conscious of lone wolves."[98]

U.S. authorities have been concerned about the prospect of Shi`a militant homegrown violent extremism (HVE) for several years now, predating even the January 2020 killing of Soleimani and the many Iranian plots targeting current and former U.S. officials that followed.[99] Already in October 2018, the National Counterterrorism Center produced an unclassified analytical report on the subject, entitled "Envisioning the Emergence of Shia HVE plotters in the U.S."[100] The report noted there had been no confirmed cases of Shi`a HVE plots in the United States, but identified several catalyzing events—most of which have already come to pass—that would increase the likelihood of Shi`a HVE mobilization to violence:

- U.S. military actions abroad against Iran, Hezbollah, or Shi`a militants
- Shi`a leaders and clerics call for violence in the United States
- Israeli government or Sunni killing of Shi`a individuals
- Anti-Shi`a activity in the United States

While the United States has thankfully not experienced significant anti-Shi`a activity (though there has been some[101]), the other catalyzing events have all come to fruition. The United States killed Soleimani in January 2020,[102] and Iranian leaders responded with threats of "severe revenge"[103] for his death with plots targeting current and former senior U.S. officials, including President Trump.[104] Israeli forces killed Hezbollah leader Hassan Nasrallah[105] in 2024 and many other senior Hezbollah leaders,[106] as well as Iranian officials in strikes in Syria[107] and more recently in Iran.

A year after Soleimani's death, several U.S. traffic controllers in New York heard a threat over aviation frequencies in which unknown persons warned, "We are flying a plane into the Capitol on Wednesday, Soleimani will be avenged."[108] While the threat was deemed not credible, and it is not clear if the breach of aviation frequencies was the work of Iranian agents or lone offenders, it underscored the threat posed by Iran and its proxies and supporters.

Indeed, online digital ecosystems run by domestic Shi`a extremists already exist here in the United States with the aim of inspiring and mobilizing lone offenders to carry out acts of violence in the U.S. homeland. Such outlets are nurtured by the Iranian government, attack regime opponents, and are "openly seeding Tehran-approved tropes across a range of platforms,"[109] as Mustafa Ayad and this author concluded in a study on the subject.[110] One such network, dubbed Pure Constellation, has managed 20 websites supportive of Iran and its proxies. Administered by an LLC registered at different times in Michigan and Georgia, the websites link to Telegram channels, WhatsApp groups, and social media sites such as Facebook and X.

A key theme in Pure Constellation's online presence is the veneration of "martyrs," many of them linked to the IRGC and its Middle East proxies. Pure Constellation aggressively helps spread English-language messages, wills, books, and biographies through a website dedicated to martyrs.[111] The site describes itself as making "a humble attempt" to introduce martyrs because "a martyr is a true inspiration for all and, through his/her martyrdom, is capable of reviving a dead and decaying society from dark[ness] just like a candle that burns itself in order to provide light to those around it."[112]

In January 2023, Iranian officials marked the anniversary of

Soleimani's death with a series of public statements threatening retaliatory attacks. Iran's state-affiliated media released a list of 51 Americans accused of playing some role in the Soleimani operation, warning that they were "under the shadow of retaliation."[113] Speaking on the occasion, however, Maj. Gen. Mohammad Bagheri—then-chairman of Iran's Armed Forces General Staff, who was killed in an Israeli airstrike during the recent war[114]—focused not on what Iranian agents might do, but on how angry youths inspired by the regime might act on their own. "Revenge against the masterminds and perpetrators of General Soleimani's assassination will never be removed from the agenda of the youths of the Muslim world and his devotees across the world," Bagheri asserted.[115]

A Multilayered Threat with a Long Tail

Iran may seek to carry out reprisal attacks in the United States, as it already has tried to do in Europe,[116] targeting U.S. officials, Iranian dissidents, Israelis, or Jews. U.S. authorities assess the war with Iran created a "heightened threat environment in the United States,"[117] and warned[118] of potential cyber or terrorist attacks in light of calls[119] by foreign terrorist organizations for attacks and Iran's own threat to activate sleeper cells in the United States. If there were ever a time Iran would want to activate its homeland option,[120] this would be it. But even if the next few weeks pass without any attack, the threat will persist.

Iran took its time preparing plots to avenge the death of Soleimani, and while all such plots have so far been thwarted, Iran continues to pursue plots to avenge his killing. The damage Israel and the United States inflicted on the regime in Tehran in the context of the recent war overshadows even the loss of Soleimani. Many senior Iranian officials and nuclear scientists were killed, Iran's nuclear and ballistic missile programs were bombed extensively, and the standing of Iran's security services was severely undermined by their very public penetration by Israeli intelligence. It would be dangerous and hubristic to underestimate the anger Iranian regime figures must be experiencing now, and their commitment to retaliate for their embarrassing losses.

As a window into the regime's commitment to retaliatory action, a slick propaganda video Iran's security services produced to mark the third anniversary of Soleimani's death in January 2023 is telling. Posted on the Sepahcybery Telegram account (Sepah is a reference to the IRGC), the video opens with a view of a small office and zooms in on a file on Soleimani's death along with photo, and a magnifying glass sitting on the desk next to a cup of coffee.[121] The date of the airstrike that killed him, January 3, is circled and marked with an 'x' in red on a desk calendar. Next, the camera hones in on a corkboard with photos and reports connected with red string attached to thumbtacks. The effect is to depict a network exposed in some investigation as being behind the Soleimani strike. The camera first zooms in on a photo of President Trump, the red string connecting his photo to those of other former U.S. government officials, including former National Security Advisor Robert O'Brien, former Chairman of the Joint Chiefs of Staff General Mark Milley, and about a dozen others. The picture fades, the music crescendos, and text appears on a black screen: "The perpetrators of general Soleimani's martyrdom will be punished for their actions."

The threats are clear as a series of images appear against a background of staccato music.[122] An Iranian drone, followed by Trump golfing. A sniper rifle, then Robert O'Brien in front of a government building. An explosive detonator, then a clip of former Deputy National Security Advisor Matthew Pottinger. Clips of a knife, a syringe, a handgun with a silencer, a vile of poison, are interspersed with pictures of General Mark Milley, Keith Kellogg, General Richard Clarke, General Andrew Poppas, Lt. Gen Joseph Guastella, Gen. James Slife, Gen. James Holmes, Victoria Coates, and Lt. Gen. Scott Howell.

"We will determine how and when to punish," reads a text that follows, followed by crime scene tape, images of various crime scenes, first responders in hazmat suits, blood-stained chairs, and ambulances.[123] The camera zooms in on the corkboard, where the faces on each of the photos are now crossed out in red ink. The words "coming soon…" appear on a black screen, followed by the logo[124] of the IRGC. U.S. authorities take the threat of Iranian retaliatory attacks very seriously, and this warning, though a few years old and propagandist, is worth heeding. If Iran fails to carry out an attack using its own agents, criminal or terrorist proxies, or inspired lone offenders, it will not be for lack of trying.

Conclusion

Tough talk aside, Iran has a stronger track record of plotting attacks than of successfully executing them. Counterterrorism agencies around the world have successfully thwarted most Iranian plots, whether targeting an Iranian dissident or President Trump, often based on tips received from Israeli intelligence. And yet, the terrorists only have to get it right once to be successful, while counterterrorism officials have to get it right every single time to avoid catastrophic failure.

In the early years after the Iranian revolution, Iranian agents boasted a nearly 80 percent operational success record, based on the author's dataset of Iranian external operations.[125] From 1979 to 1988, Iran and its agents executed 11 successful external operations out of a total of 14 (a 78.5 percent success rate). But as counterterrorism capabilities developed over the years, Iran's success rate dropped precipitously. Over the past 10 years, Iran and its agents executed 47 successful external operations out of a total of 191 (a 24.6 percent success rate).

Successful operations have deadly consequences, and even those that are unsuccessful force authorities to allocate limited resources to thwart the next one. Examples of recent Iranian plots that succeeded include the abduction and murder of Rabbi Zvi Kogan in the UAE by Uzbek assailants in November 2024;[126] a teenager firing a gun at the offices of Elbit Systems in Sweden at the behest of a criminal organization hired by Iran in 2024;[127] and incendiary devices thrown at the entrance to the National Council of Resistance of Iran (NCRI) office in Paris in 2023.[128]

While no spectacular Iranian plots succeeded in recent years, the pace of these threats has increased, and authorities remain very concerned Iranian operatives and their agents will continue to attempt attacks. In a joint statement in July 2025, 14 Western countries came together to "condemn the growing number of state threats from Iranian intelligence services" in their respective countries. "We are united in our opposition to the attempts of Iranian intelligence services to kill, kidnap, and harass people in Europe and North America in clear violation of our sovereignty," the statement reads, adding that Iranian services "are increasingly collaborating with international criminal organizations to target journalists, dissidents, Jewish citizens, and current and former officials in Europe and North America. This is unacceptable."[129]

The same day that this statement was released, the Israeli National Security Council renewed a travel warning for Israelis in the UAE, noting that Iranian and other extremists are "driven by heightened motivation to exact revenge following Operation Rising Lion," the 12-day war with Iran, and the Gaza war with Hamas.[130]

Iran will surely seek to avenge its losses in its 12-day war with Israel, and it will likely look to settle the score with the United States as well, given the U.S. airstrikes that targeted the Fordow nuclear complex. Iran's intent to do harm is clear, but its capability to successfully carry out attacks—in particular spectacular ones—is less clear. The concern is that if Iranian operatives and their agents keep up the frenetic pace of operations, some might succeed. CTC

Citations

[1] "Security Alert – U.S. Embassy Stockholm," U.S. Embassy in Sweden, June 23, 2025.

[2] "Arrest on Suspicion of Engaging in Intelligence Activities," Der Generalbundesanwalt beim Bundesgerichtshof, July 1, 2025.

[3] Elise Labott and Laura Koran, "US Officials Warn of Potential Hezbollah Threat to US Homeland," CNN, October 11, 2017.

[4] Matthew Levitt, "Iranian External Operations Interactive Map and Timeline," Washington Institute for Near East Policy, August 6, 2024.

[5] Matthew Levitt, "Robert Assaf Purchases 300 Pounds of Ammonium Nitrate," Lebanese Hezbollah Select Worldwide Activities Interactive Map and Timeline, Washington Institute for Near East Policy.

[6] Matthew Levitt, "Ali Kourani Conducts Preoperational Surveillance in New York City," Lebanese Hezbollah Select Worldwide Activities Interactive Map and Timeline, Washington Institute for Near East Policy.

[7] "Trump Administration Boosts Monitoring of Possible Iran-Backed Cells in U.S., as Trump Weighs Strikes," CBS, June 19, 2025.

[8] "FBI Returning Agents to Counterterrorism Work After Diverting Them to Immigration," NBC News, June 24, 2025.

[9] "Trump's Iran Attack Spurs Concerns of Retaliation in the U.S.," *Wall Street Journal*, June 24, 2025.

[10] "National Terrorism Advisory System Bulletin – June 22, 2025," U.S. Department of Homeland Security, June 22, 2025.

[11] "Iranian State Media Confirms Death of Iran's IRGC Intelligence Chief and His Deputy," Euronews, June 16, 2025.

[12] Francesca Regalado, Euan Ward, Farnaz Fassihi, Samuel Granados, and Lynsey Chutel, "These Are Iranian Generals and Scientists Killed by Israel," *New York Times*, June 13, 2025.

[13] "Live Updates: Iran-Israel-Trump," NBC News, updated June 23, 2025.

[14] Matthew Levitt, "Trends in Iranian External Assassination, Surveillance, and Abduction Plots," *CTC Sentinel* 15:2 (2022).

[15] Matthew Levitt, "Iranian External Operations, 1979-Present," Washington Institute for Near East Policy.

[16] Matthew Levitt, "Hezbollah Isn't Just in Beirut. It's in New York, Too," *Foreign Policy*, June 14, 2019.

[17] "State Support for International Terrorism, 1985," Directorate of Intelligence, Central Intelligence Agency, May 1986, approved for release 8/23/16.

[18] "Iran's Revolutionary Guard: Armed Pillar of the Islamic Republic," Directorate of Intelligence, Central Intelligence Agency, January 1987, declassified 5/8/12.

[19] "Iranian Support for International Terrorism, November 22, 1986 Memorandum for the DCI," Central Intelligence Agency, approved for release June 1999.

[20] Levitt, "Iranian External Operations, 1979-Present."

[21] Ibid.

[22] "Manssor Arbabsiar Sentenced in Manhattan Federal Court to 25 Years in Prison for Conspiring With Iranian Military Officials to Assassinate the Saudi Arabian Ambassador to the United States," U.S. Attorney's Office, Southern District of New York, May 30, 2013.

[23] "U.S. Intelligence Chief: Iran Is More Willing to Launch Attack on U.S.," NPR, January 31, 2012.

[24] Levitt, "Iranian External Operations, 1979-Present."

[25] Ibid.

[26] "National Terrorism Advisory System Bulletin – June 22, 2025."

[27] "Annual Threat Assessment of the U.S. Intelligence Community — Unclassified," Office of the Director of National Intelligence, March 2025.

[28] "Homeland Threat Assessment 2025," U.S. Department of Homeland Security, October 2, 2024.

[29] Levitt, "Trends in Iranian External Assassination, Surveillance, and Abduction Plots."

[30] "National Terrorism Advisory System Bulletin – June 22, 2025."

[31] Ioan Pop and Mitchell D. Silber, "Iran and Hezbollah's Pre-Operational Modus Operandi in the West," *Studies in Conflict & Terrorism* 44:2 (2021).

[32] Chuck Goudie, Barb Markoff, Christine Tressel, and Ross Weidner, "Feds Charge Man in Chicago in Bizarre Iranian Spy Plot," ABC7 Chicago, August 21, 2018.

[33] "Two Individuals Sentenced in Connection with Work on Behalf of Iran," U.S. Department of Justice, January 15, 2020.

[34] Matthew Levitt, "Contending with IRGC Plots," Washington Institute, August 16, 2022.

[35] Benjamin Weiser, "Iranian Operatives Planned to Kidnap a Brooklyn Author, Prosecutors Say," *New York Times*, July 13, 2021.

[36] "Treasury Sanctions Iranian Intelligence Network Targeting Iranian-American Activist in the United States," U.S. Department of the Treasury, Office of Foreign Assets Control, September 3, 2021.

[37] "Iranian Intelligence Officials Indicted on Kidnapping Conspiracy Charges," U.S. Department of Justice, July 13, 2021.

[38] "Manhattan U.S. Attorney Announces Kidnapping Conspiracy Charges Against an Iranian Intelligence Officer and Members of an Iranian Intelligence Network," U.S. Attorney's Office, Southern District of New York, July 13, 2021.

[39] Weiser.

[40] Ibid.

[41] Kirsten Grieshaber, "Germany Charges Iranian Diplomat Detained in Bomb Plot," Associated Press, July 11, 2018.

[42] Ibid.

[43] "Homeland Threat Assessment 2025."

[44] *United States v. Sharon Gohari* (No. 25-MJ-172), U.S. District Court for the Eastern District of New York, May 19, 2025.

[45] *United States v. Sharon Gohari*, Criminal Complaint, No. 1:25-cr-00183, Magistrate Docket No. 25-172, United States Attorney Eastern District of New York, May 21, 2025.

[46] Ibid.

[47] Seamus Hughes and Peter Beck, "#129: Buying a Flamethrower off TikTok," Court Watch, June 6, 2025.

[48] *United States v. Sharon Gohari*, Criminal Complaint, No. 1:25-cr-00183.

[49] The White House, "ANY RETALIATION BY IRAN AGAINST THE UNITED STATES OF AMERICA WILL BE MET . . .," X, July 18, 2025.

[50] Matthew Levitt and Sarah Boches, "Iranian External Operations in Europe: The Criminal Connection," International Centre for Counter-Terrorism, October 16, 2024.

[51] Matthew Levitt, "Justice Department Indicts Shahram Poursafi for John Bolton and Mike Pompeo Assassination Plot," Iranian External Operations Map and Timeline, August 10, 2022.

[52] Matthew Levitt, "Shahram Poursafi Plots to Assassinate John Bolton," Iranian External Operations Map and Timeline, October 21, 2021.

[53] Matthew Levitt, "Shahram Poursafi Plots to Assassinate Mike Pompeo," Iranian External Operations Map and Timeline, April 13, 2022.

[54] *United States v. Poursafi*, "Affidavit in Support of Complaint," August 5, 2022.

[55] "Director General Ken McCallum Gives Latest Threat Update," MI5, October 8, 2024.

56 Ibid.

57 Tomas Tobé, "Iran's Use of Criminal Networks as Terrorist Proxies in Europe," European Parliament, October 14, 2024.

58 "The United States and United Kingdom Target Iranian Transnational Assassinations Network," U.S. Department of the Treasury, January 29, 2024.

59 "One Iranian and Two Canadian Nationals Indicted in Murder-for-Hire Scheme," U.S. Department of Justice, January 29, 2024.

60 "The United States and United Kingdom Target Iranian Transnational Assassinations Network," United States Department of the Treasury, January 29, 2024.

61 "Iran: Council sanctions eight individuals and one entity over serious human rights violations and transnational repression," Council of the European Union, July 15, 2025.

62 "Two Eastern European Organized Crime Leaders Convicted of Murder-for-Hire Targeting U.S.-Based Journalist on Behalf of the Iranian Government," U.S. Attorney's Office, Southern District of New York, March 21, 2025; *United States v. Amirov et al*, "Superseding Indictment," October 2024.

63 "Justice Department Announces Charges and New Arrest in Connection with Assassination Plot Directed from Iran," U.S. Department of Justice, January 27, 2023.

64 Luc Cohen, "At US Trial, Gunman Admits to Trying to Kill Iranian Journalist," Reuters, March 11, 2025.

65 "Pakistani National with Ties to Iran Charged in Connection with Foiled Plot to Assassinate a Politician or U.S. Government Official," U.S. Department of Justice, August 6, 2024.

66 Aaron Katersky and Jack Date, "Pakistani National Charged with Alleged Plot to Assassinate Donald Trump, Other Public Officials: DOJ," ABC News, August 6, 2024.

67 "Pakistani National with Ties to Iran Charged in Connection with Foiled Plot to Assassinate a Politician or U.S. Government Official."

68 "Uppgifter: Rawa Majid hårt pressad av Iran att utföra dåd mot Israel och USA," SVT Nyheter, June 22, 2025.

69 Matthew Levitt, "Lebanese Hezbollah Select Worldwide Activities Interactive Map and Timeline," Washington Institute for Near East Policy, August 1, 2020.

70 Matthew Levitt, "Breaking Hezbollah's 'Golden Rule': An Inside Look at the Modus Operandi of Hezbollah's Islamic Jihad Organization," *Perspectives on Terrorism* 14:4 (2020): pp. 21-42.

71 "International Radical Fundamentalism," Investigative Project on Terrorism, November 1994.

72 Ibid.

73 Ibid.

74 Ibid.

75 Ibid.

76 "Hearing Transcript on Current and Projected National Security Threats to the United States," Senate Select Committee on Intelligence, August 2024.

77 Matthew Levitt, "Episode 4: Hezbollah Support Networks in America, Breaking Hezbollah's Golden Rule," Washington Institute for Near East Policy, March 2, 2022.

78 Ibid.

79 "Bronx Man and Michigan Man Arrested for Terrorist Activities on Behalf of Hizballah's Islamic Jihad Organization," U.S. Department of Justice, June 8, 2017.

80 Levitt, "Breaking Hezbollah's 'Golden Rule.'"

81 Ibid.

82 Ibid.

83 Ibid.

84 "Hizballah Operative Sentenced to 40 Years in Prison for Covert Terrorist Activities on Behalf of Hizballah's Islamic Jihad Organization," U.S. Department of Justice, December 3, 2019.

85 Levitt, "Breaking Hezbollah's 'Golden Rule.'"

86 "Bronx Man and Michigan Man Arrested for Terrorist Activities on Behalf of Hizballah's Islamic Jihad Organization."

87 "New Jersey Man Sentenced to 12 Years in Prison for Receiving Military-Type Training From Hezbollah, Marriage Fraud and Making False Statements," U.S. Department of Justice, May 23, 2023.

88 "Manhattan U.S. Attorney Announces Indictment of New Jersey Man for Terrorist Activities on Behalf of Hizballah's Islamic Jihad Organization," U.S. Department of Justice, September 19, 2019.

89 Ibid.

90 Levitt, "Hezbollah Isn't Just in Beirut. It's in New York, Too."

91 Ibid.

92 Levitt, "Robert Assaf Purchases 300 Pounds of Ammonium Nitrate."

93 Ibid.

94 "Jewish Museum Killings Show How Hard It Is to Stop Radicalized Lone-Wolf Attacks," NBC News, May 22, 2025.

95 "National Terrorism Advisory System Bulletin – June 22, 2025."

96 Ibid.

97 "Homeland Threat Assessment 2025."

98 "Live Updates: Iran-Israel-Trump," NBC News, June 23, 2025.

99 Matthew Levitt, "Contending With IRGC Plots," Lawfare, August 16, 2022.

100 Moustafa Ayad and Matthew Levitt, "Is Iran Looking to Inspire Shia Homegrown Violent Extremist Attacks?" Washington Institute, Policy Notes 134, June 2023.

101 "Confronting Anti-Shia Hate Is Necessary to Prevent Killings Like Albuquerque's," Interfaith America, August 22, 2022.

102 Ben Hubbard, Farnaz Fassihi, and Michael Crowley, "U.S. Strike in Iraq Kills Qassim Suleimani, Commander of Iranian Forces," *New York Times*, January 2, 2020.

103 "Qasem Soleimani: Iran Vows 'Severe Revenge' for Top General's Death," BBC, January 3, 2020.

104 Ryan Lucas, "What We Know About Iran's Alleged Threats to Assassinate Trump," NPR, September 25, 2024.

105 "Hezbollah leader Hassan Nasrallah killed by Israeli airstrike in Lebanon's capital Beirut," CBS News, September 28, 2024.

106 Kareem Chehayeb, Jack Jeffery, and Associated Press, "Who Were the 7 Hezbollah Leaders Killed Over the Past Week?" PBS NewsHour, September 30, 2024.

107 "Israeli Strike on Iran's Consulate in Syria Killed Two Generals and Five Officers, Iran Says," Associated Press, April 1, 2024.

108 "Chilling Threat Made Over Air Traffic Control Frequencies Vowing to 'Avenge' Soleimani," CBS News, January 3, 2021.

109 Moustafa Ayad and Matthew Levitt, "Is Iran Looking to Inspire Shia Homegrown Violent Extremist Attacks?" Washington Institute for Near East Policy, Policy Note 134, June 12, 2023.

110 Ibid.

111 Ibid.

112 Ibid.

113 "Iran President Vows Vengeance Three Years After General's Death," Associated Press, January 3, 2023.

114 Ross Adkin, Tamar Michaelis, and Nadeen Ebrahim, "Israeli Strikes Kill Some of Iran's Most Powerful Men, Including Military and Nuclear Leaders," CNN, June 13, 2025.

115 "Top Iranian General: Muslim Youths Determined to Avenge Death of Soleimani," *Times of Israel*, January 2, 2023.

116 "Arrest on Suspicion of Engaging in Intelligence Activities."

117 "National Terrorism Advisory System Bulletin – June 22, 2025."

118 Ibid.

119 Ibid.

120 Labott and Koran.

121 "Iranian Video Threatens Trump and Defense Officials With Revenge for Soleimani Assassination," MEMRI Jihad and Terrorism Threat Monitor, January 9, 2023.

122 Ibid.

123 Ibid.

124 "Pasdaran (IRGC) Logo," Militant Imagery Project, Combating Terrorism Center at West Point.

125 Matthew Levitt, "Iranian External Operations, 1979-Present," Washington Institute for Near East Policy. The first round of findings based on this dataset was first reported in Levitt, "Trends in Iranian External Assassination, Surveillance, and Abduction Plots."

126 "UAE Rabbi Killed Following Abduction" in Matthew Levitt, "Iranian External Operations, 1979-Present," Washington Institute for Near East Policy.

127 "Shots Fired by Teen at Israeli Firm's Office in Sweden" in Matthew Levitt, "Iranian External Operations, 1979-Present," Washington Institute for Near East Policy.

128 "Two Individuals Throw Explosives into National Council of Resistance to Iran Building North of Paris" in Matthew Levitt, "Iranian External Operations: 1979-Present," Washington Institute for Near East Policy.

129 "Joint Statement on Iranian State Threat Activity in Europe and North America," U.S. Department of State, July 31, 2025.

130 "Message from the National Security Council Reiterating the Travel Warning for Israelis in the United Arab Emirates," Israeli National Security Council, July 31, 2025.

A View from the CT Foxhole: James Stack, Director, Great Plains Diagnostic Network

By Don Rassler and Kristina Hummel

James Stack, Ph.D., is an internationally recognized leader in the field of plant biosecurity. A professor in the Department of Plant Pathology at Kansas State University since 2003, Dr. Stack provided leadership in the development of the National Plant Diagnostic Network (NPDN) and became regional director of the Great Plains Diagnostic Network (GPDN), one of the five regional networks, soon after it was formed. From 2006 to 2008, he served as the director of KSU's Biosecurity Research Institute, a biocontainment facility for plant, animal, and human health.

Dr. Stack's research focuses on genome-informed diagnostics for plant-pathogenic bacteria to the subspecific and population levels of discrimination, as well as research on the epidemiology and ecology of toxigenic fungi and bacteria. He speaks regularly on plant biosecurity topics, to include at the U.S. Naval War College and the National Academy of Sciences, among other forums.

CTC: You are an internationally recognized leader in the plant biosecurity field. If you had to characterize the evolution of the plant biosecurity field, how would you describe where it has been and where it is currently?

Stack: Biosecurity in the plant world is not new. It didn't begin at 9/11. It has a history of well over 100 years, going back to the time when cherry trees were first imported into Washington, D.C. That first attempt was a total failure because the trees were heavily infested with fungi and insects, and most of the trees died or were burned. Most of the crops we grow in the U.S. are not native to North America; they were introduced by food explorers. An entomologist named Charles Marlatt was cautioning the plant explorers that were going around the world and bringing plants back to the United States. He worked with the USDA [U.S. Department of Agriculture] and was responsible for initiating the legislation around 1915 to start safe-guarding against the introduction of organisms into the United States on plants and plant materials.

With respect to plant biosecurity in the context of intentional introductions for nefarious purposes, accusations have been leveled for many years between different nations, including between the United States and Cuba, one accusing the other of intentionally introducing a plant pathogen into their agricultural systems to undermine their economy. In each case, it was very difficult to assign attribution with any degree of certainty. So, whether those were intentional or natural events is hard to determine, but accusations continued for decades between several nations. Prior to 1975, many nations, including the U.S., had biological weapons programs that included plant pathogens to target crop systems in adversarial nations.[1] Over 180 nations have signed onto the treaty to ban biological weapons, but the threats persist.

9/11 changed the whole perspective on biosecurity and preparedness because of the challenge to each federal department to assess the vulnerabilities that we have in our critical systems, food being one of them. At that point, biosecurity took on an additional meaning. In the United States, it depends on which agency you ask as to what the definition of biosecurity is. There are multiple definitions of biosecurity, and oftentimes it intersects with definitions of biosafety. But if we look at biosecurity in the sense of the unintentional or intentional introduction of an organism, we have a long history on the plant side in terms of protecting food systems and natural plant systems. But 9/11 did bring a focus on the intentional side, and we've worked on that. There are reports of documented evidence that terrorist groups like al-Qa`ida were planning to use plant pathogens to target crops.[2] We've partnered with the FBI to develop tools to help discriminate between natural and intentional introductions of pests and pathogens. However, no completely satisfying system exists.

The bottom line is that agricultural environments and natural environments have *a lot* of noise, and that background noise makes investigation and attribution a real challenge. We've actually had organisms introduced to the United States on hurricanes from South America and the Caribbean, on dust storms from Africa. Many plant pathogens and pests have been introduced through trade of plants and plant products as well as on wooden packing crates. Global trade is at astronomical levels, and we currently inspect about one percent of what comes across our borders. You're not going to find everything. USDA APHIS [Animal and Plant Health Inspection Service] does a great job; Customs and Border Protection, they do a great job. It's just that if you've ever spent time at a port of entry, you know that the volumes coming across preclude inspection at any high rate. It's just not possible. APHIS PPQ [Plant Protection and Quarantine] puts up a report every year about what they're intercepting, and the numbers of detections are very high [while] inspecting only one percent. So, we know that potentially harmful organisms are being introduced.

We have the benefit of history to know that most organisms that get introduced go to extinction; they fail. That's because the environment's a pretty tough place, and organisms have to be adapted for it in order to survive and establish. But the high numbers and the recurrent introductions are what we worry about because ultimately the numbers catch up with you. It is a numbers game, and the numbers are large. We're introducing massive amounts of material every year, and we're doing it year after year. Some of them succeed, and the consequences are quite high. Some of the consequences are tainted food; we see that with foodborne pathogens in our imported foods. Some are environmental concerns. If you just look at natural plant systems, forests, trees, they're in serious trouble right now across the United States. There is not a region of the United States that is not being seriously impacted by introductions of fungi and insects.

So, what we're seeing is a destabilization of some ecosystems. An

James Stack

analogy that I use is, if you build a house, it's more than likely going to be constructed of wood. What do you worry about when you have a house with a wooden frame and infrastructure? You worry about the big threat, fire. So, you put a lightning rod on the roof. You have fire extinguishers in the house. And then a neighbor's house burns down and you're even more concerned about this one threat—fire—so you install a sprinkler system. You're focused on this one big threat—fire—all while termites are eating out your foundation.

That is the biggest problem we have with all the threat assessments in the United States: looking for that one big organism that will have a catastrophic effect. One problem with that is the lack of an adequate definition for 'catastrophic.' So, if you're trying to develop mitigation and prevention measures, you don't have a metric by which you can measure success, because you haven't defined what catastrophic means. One definition is, 'It's something that overwhelms our system.' So, what does 'overwhelm' mean? We haven't clearly defined things to the point where we know we're making progress toward security. It's the same thing in plant systems. There's no difference: plant, animal, human. We do the same thing. We focus on the big organisms that would cause a massive effect. The real challenge is that we have many organisms attacking multiple plant systems concurrently and consistently and intersecting with other societal challenges that amplify the impacts. The challenge in plant systems could easily be generalized to include human and animal systems as well.

What I use in food security assessments is an arbitrary metric based on calorie consumption in any country and the split between calories from protein, carbohydrate, fat. If you look at the consumption needs of that country, we know—from different organizations that address food security—what the differential is for calories to support a healthy adult and then the calories that would put someone into food deprivation. We know that differential is about 30 percent displacement. So, I use 30 percent as catastrophic. If you can displace the mean by 30 percent, that's a catastrophic effect. Here's the question I pose: What's the difference between a *single* organism coming in and displacing the mean by 30 percent, or *five* organisms coming in and each displacing the mean by six percent? It's the same total effect, and that's what we cannot wrap our minds around at the federal level. We're still looking for that one big thing that causes the catastrophe. That's *not* what's going to happen on the plant side. It's multiple, continuous introductions of many different pathogens and pests that threaten plant health in natural and agricultural ecosystems. It's the constant flow of many threats. An intentional introduction could be a tipping point that pushes a system over the edge.

CTC: If you were to step back and explain the intersection between your world of plant biosecurity and its intersection with national security and terrorism, how would you recommend that our readers think about that issue? At a strategic level, I think some people might have a challenge of even connecting these different worlds and how they come together.

Stack: Remember the Arab Spring in 2010? We had a situation in Tunisia where there were fundamental challenges—cultural challenges, social challenges, political challenges. What was the proverbial last straw? The tipping point was the increase in the cost of food.[3] It was people going into the streets and waving loaves of bread that drove, in part, that food vendor [Mohamed Bouazizi] to self-immolate, that triggered the massive demonstrations that spread across North Africa into the Middle East, repercussions of which we're still facing today. It destabilized a whole region of the world. How about 2008? In 2008, we had increasing demand from China to import maize; we had the diversion of maize into biofuels; and we had the increase in cost of petroleum-based fuels that affected distribution. It spiked the price of grains. There were food riots in over 35 nations in 2008. It led to the destabilization of governments in two countries, one overthrown.[a] The food and plant systems are global networks. There are many nodes in global food distribution networks, and when you remove a node in a network, connections quickly start switching. That drives the cost of food up significantly, making it unaffordable to poverty-stricken communities in some countries. And that's what happened in 2008 and subsequently.

Fast forward, and what began just a few years ago? The Ukraine-Russia war. Many countries depend on Ukraine, a major exporter

[a] Editor's Note: The governments of Haiti and Cameroon experienced significant political turmoil as a result of surging global food prices in 2007 and 2008. Haiti's then prime minister, Jacques-Édouard Alexis, was forced to resign in April 2008 following riots in Port-au-Prince, and anti-government riots took place in Cameroon's capital and elsewhere in the country in late 2008. See "Haiti Senate fires prime minister over food riots," Reuters, April 12, 2008, and "Antigovernment rioting spreads in Cameroon," *New York Times*, December 7, 2008.

of agricultural products. Somewhere [around] 30-35 percent of Egypt's import of wheat comes from Ukraine. Same with Tunisia; same with Spain. People all of a sudden started looking for a source somewhere else. There are consequences to that. It drives the price up, which makes it difficult for low-income nations to import. Another consequence is when you need to move food quickly, you no longer have the same risk assessments. You're moving pests and pathogens with these products because it becomes urgent and you don't have time to do an in-depth risk assessment. We have a long history of introducing pests and pathogens in food aid, Africa being the major recipient of those.

Those are examples of how plants impact our world and intersect with national security. It's not that the introduction of one organism into the United States is going to trigger some massive crisis. But they become the tipping point in some nations. And in the United States, we need to be concerned about the multiple introductions to multiple systems simultaneously and repeatedly. To believe that what we have seen happen in other nations could not happen in the United States would be an epic mistake.

"It's not that the introduction of one organism into the United States is going to trigger some massive crisis. But they become the tipping point in some nations. And in the United States, we need to be concerned about the multiple introductions to multiple systems simultaneously and repeatedly. To believe that what we have seen happen in other nations could not happen in the United States would be an epic mistake."

CTC: It seems that one of the things that can make plant biosecurity threat detection and forecasting hard is that agrosecurity threats exist in a complex environment where there can be, as you just noted, a lot of 'noise' and a lot of dynamism. Similarly, terrorism threats can also be hard to identify and forecast, as they're usually embedded in a dynamic and messy information environment. In your view, when it comes to indicators and warnings and evaluation of risk, what can the counterterrorism community learn from the field of plant biosecurity, given that they both share ecosystems where there's a lot of noise?

Stack: We know from a long history in human, animal, and plant systems that early detection is really critical as is effective response, which is dependent upon early detection. You need to have a full signal-to-solution system in place, and the critical components need to be well integrated, not independent of each other. A plant disease outbreak site is initially messy, and often becomes more messy before forensic analyses begin. That is because response to minimize impacts will come first. We need rapid and effective response to contain and eradicate, if possible. In general, the greater the time between the introduction and the detection, the greater the impacts. One major weakness in the U.S., and globally, is the lack of effective plant surveillance systems to effect early detection.

We've been working on this for 23 years, and to date, we—USDA, the academic environment, FBI—have not collectively come up with a set of criteria that would allow one to say, 'This was intentional.' Unless somebody takes credit for it, which they might, you can never be 100 percent certain. I teach a one-week course in plant biosecurity every year at our biocontainment facility, and on the last day, we do a forensic desktop exercise where the group is split into four teams and I give them an evidence packet of a scenario based on a real event. The scenario is an outbreak of an organism that produced a really serious toxin. The challenge for the teams is to investigate to determine whether it was natural, accidental, or intentional. We give them an evidence packet to look at after they've seen this scenario and come back with questions for the experts. Then we give them the second set that has DNA fingerprint data, aerial photographs, and a guide to help decide whether it was intentional or not. And in the 10 years I've been doing this, only two teams have ever come back and said, 'It was intentional.' The challenge of assigning attribution in an agricultural environment with enormous background noise is exceptionally difficult.

What we've learned is that you need to get on it right away because the system's going to get *more messy* afterwards as you're trying to contain and perhaps eradicate. The current protocol is that the USDA APHIS Plant Protection and Quarantine respond and contact the FBI when they believe it was intentional; then the investigation begins. It's *the reality* that it's exceptionally difficult. Law enforcement and regulatory agencies as well as academic subject matter expert labs may all be involved to varying degrees. Having a fully integrated biosecurity system in place so that you can respond quickly is essential to positive outcomes. If you let the system or the situation evolve, it's going to be nearly impossible to determine whether it was intentional or not.

We commonly think of the biological threats at the species level, but often, the real concern is at subspecific levels of taxonomic discrimination. We're talking strains. We saw this with COVID. Whether that was a natural or manipulated strain still hasn't been fully resolved. It can be exceptionally difficult to do. The best you can do is have a fully integrated system that is going to detect it as quickly as possible and allow you to get in there before it gets even more messy. We know this with COVID, we know this with the Ebola outbreaks in West Africa. During an epidemic, the strains are evolving, and so the genotype composition at the end of the epidemic is not the same as the genotype composition at the beginning of the epidemic. It's the same thing with some pathogens in plant systems. Unless you get in there very quickly, it's going to be difficult to assign attribution. As mentioned earlier, we need to address the lack of effective plant surveillance systems to enable early detection.

CTC: You were instrumental in setting up the National Plant Diagnostic Network, "a consortium of diagnostic labs in the U.S. and its territories to protect plant health through timely diagnostics of plant pests and pathogens."[4] The NPDN was established in 2002 to address vulnerabilities in the U.S. agricultural sector following the attacks of September 11th.[5]

Can you tell us more about what the NPDN does, what entities it works with, and how it supports the U.S. government's agrosecurity efforts?

Stack: Our mission is to provide high-quality diagnostics to support plant health, whether that be in a natural plant system like a forest ecosystem or whether it's agriculture or horticulture. We serve agriculture industries, producers, regulatory agencies at both the state and federal levels, and even homeowners. The success of this has been that we have provided diagnostic services to over 97 percent of the over 3,000 counties in the United States. That's a reach that not a single state or federal regulatory agency or defense agency has. We have approximately 72 labs across all 50 states and the territories in the Caribbean and Pacific. We span seven time zones. When we have our national meeting, we typically have between 150 and 200 diagnosticians and support personnel. NPDN has its finger on the pulse of plant health in the United States.

Any of the systems that we've put in place for protecting our natural and human resources, depend upon a highly trained, educated workforce. And so that's one of the things NPDN does. We have an NPDN professional development program, and we link with USDA for advanced training for our diagnosticians. We keep them trained, and we keep them aware of what's happening and what's on the horizon.

NPDN regularly interacts with regulatory agencies. For example, during multiple incursions of the select agent *Ralstonia Solanacearum* Race 3 Biovar 2 into the United States, NPDN provided diagnostic support because when those introductions happened, many states were involved; the last one affected 26 states. When APHIS needs sample surge support, they connect with NPDN. We provide that support. We are not, nor do we wish to be, a regulatory agency. We have no regulatory authority. We have *responsibility* to provide services to our state or the nation as needed.

CTC: When you think about vulnerabilities and threats—to the extent that you can share—of plants being weaponized or used to create harm or instability intentionally, what concerns you? Can you paint a bit of that picture just so then we can drill into a case here?

Stack: One vulnerability in the plant sector, and I suspect in others as well, is that we establish programs and build infrastructure to achieve biosecurity, but then under-resource those programs to the point where they cannot fully achieve their mission. We check the box that we have done something, but we do not follow-up to ensure that the programs are at operational levels adequate to the challenges. The National Plant Diagnostic Network is an excellent example of an outstanding program that is tremendously under-resourced relative to the challenges it is being asked to address.

We talked a little bit about tipping points. There are many ways to do that. We look at Ukraine, and the disruption was war. But *anything* that disrupts that network is a potential for a national security event. We have policies that regulate trade and the safety of that trade regarding organisms that might move from one country to another. That's the International Plant Protection Convention. The World Trade Organization requires any nation that wants to enter into the global marketplace to abide by these regulations. So, if an organism is detected in a shipment, a country has a right to refuse entry and may stop trading with that nation. Whatever the disrupter, it's often the same eventual impact, and that's the way we need to look at this: Anything that disrupts those trade channels has the potential to destabilize a locale, a region, or even a nation. It only takes an organism being detected. You don't even have to be sophisticated enough to know how to cause an epidemic to disrupt trade; it can be just a detection.

If you are a terrorist and you want to make the evening news, you put a bomb on a bus. You cause some impactful event that is immediate and shocking. But if the goal is to undermine a nation, you go after more subtle targets. We have a history of what happens when you impact the cost of food or you disrupt trade. And again, if your goal is to cause an epidemic, to put an organism in place, that's *really* hard to do. It's hard to do in human systems, but it's really hard to cause an epidemic in a plant natural or agro-ecosystem; the environment is a significant regulator and quite variable. One of the most frightening things for me from the COVID experience was not the illness that it caused, but that it demonstrated we now have a really great vector, SARS-CoV-2, that will spread like wildfire around the planet. That's frightening.

From a plant health perspective, we have some high consequence pathogens we're worried about right now, including the wheat blast pathogen. It's a fungus called *Magnaporthe oryzae* Triticum that emerged in Brazil in the 1980s. It spread in Brazil, then into Bolivia, Paraguay, and now most recently Uruguay. But the big deal was in 2016, it was introduced into Bangladesh and caused a major epidemic. The following year, it was introduced into Zambia in East Africa. These are areas of the world with inherent instability vulnerable to tipping point consequences; South Asia as we just saw with Pakistan and India,[6] which are two nuclear nations, and near neighbor Bangladesh that is dependent upon wheat to maintain food security. Zambia is at the southern end of the eastern wheat belt in Africa. This organism spreads, and these are staple crops at risk. What does it take to cause civil unrest? Actually, not much. Plant health issues are perfect as tipping points, when people don't have food, they migrate or they protest. The resulting consequences can be short-term and contained (e.g., food riots of 2008) or long-lasting, disseminated, and destabilizing as in the case of the Arab Spring of 2010.

CTC: There also might be an interesting takeaway here about the types of actors that we need to be concerned about. With that 'bomb on the bus' example, for certain groups, that tactic will be 'appealing' because it's loud and has an immediate impact. But it sounds like one of the core aspects of agrosecurity threats is the danger of a quieter, more strategic, longer-term action, which might impact the types of violent extremists or terrorist groups that could be attracted to this type of activity, and which might be different than a lot of the terrorists we think about today. I also think about proxy groups and then nation-states, too, as you mentioned. Would you agree with that?

Stack: I would agree with that, most definitely. We're talking about 'intentional.' What's the first part of that? Intent. And that's the most difficult aspect to wrestle with. When thinking about intent, the nature of the event is as important as the magnitude of the event. For example, blowing up a seed factory resulting in one death and all the seed destroyed in the fire. The magnitude of the event was relatively small, one death and one destroyed building. But the

"That organism, *Fusarium graminearum*, exists all over the United States and all over the world ... Unless they figured out some way to increase its aggressiveness, virulence, and/or dispersal capability, or very specifically, enhanced its toxin production (nivalenol, deoxynivalenol), then I don't think it would make a great bioweapon ... But that event may be less about *Fusarium graminearum* and more about finding the best way to sneak an organism into the country; that could be an equally important concern."

nature of the event was to eliminate the crop seed for 50 percent of a nation's farmers—enormous impact. You want to know what keeps me up at night? Anarchists. They keep me up at night because so far, the true terrorist groups are more concerned with the bomb on the bus. Anarchists, on the other hand, are super difficult to predict, and they have multiple motivations. They're not really ideologically driven. It's hard to calculate what's going on in that community. Their common denominator seems to be disruption and destabilization.

CTC: This June, the U.S. Department of Justice announced that it had charged two Chinese nationals with smuggling "a potential agroterrorism weapon" into the United States (a fungus called *Fusarium graminearum*)—among other charges.[7] And one week later, it was announced that a third Chinese national had been charged for smuggling biological materials into the United States—among other charges.[8] Recognizing that few details from these cases are publicly available, which limits what can be known about them specifically, what did you make of that news when you first heard it? Were you surprised or concerned?

Stack: Concern that it was going to cause a major problem in the United States? No, not so much. With the caveat that few details about the case are available, it seemed if that's the best they've got, just let them keep going down that road because it's not likely to lead to something significant. That organism, *Fusarium graminearum*, exists all over the United States and all over the world; a lot of expertise exists on the pathogen and its management. Unless they figured out some way to increase its aggressiveness, virulence, and/or dispersal capability, or very specifically, enhanced its toxin production (nivalenol, deoxynivalenol), then I don't think it would make a great bioweapon. It would have to displace the pathogen populations that are already widely prevalent in the environment; that would likely take a long time without a substantial ecological advantage. In addition, there are reasonably effective mitigation measures for this pathogen (e.g., fungicides), and we have an excellent forecasting system in place developed and deployed by a scientist at Kansas State University. I didn't think that was a great pathogen to use as a bioweapon. But that event may be less about *Fusarium graminearum* and more about finding the best way to sneak an organism into the country; that could be an equally important concern. However, the most likely explanation in this case is a few scientists disregarding the established regulations on the legal movement of pathogenic organisms. Perhaps, in time we will know.

What I did worry about is putting that idea/suggestion into the minds of people or groups with intent to disrupt or cause harm: 'Isn't that interesting? I wonder if we could that type of thing.' This event drew a lot of attention, at least in the press. I worry that it raises this idea that 'maybe that's something we should be thinking about doing.' We need somebody or some entity keeping track of all these events. Following any introduction of a plant pathogen, we do two things, trace-forward and trace-back (i.e., where is going from the introduction site and where did it come from?). We need to be doing that for all of these events and have a database that we can refer to and learn from. I'm sure that this is being done.

CTC: How are advancements in technologies such as artificial intelligence lowering the barriers to entry for those less specialized individuals to engage in agroterrorism or create novel threats?

Stack: Artificial intelligence is a very big deal. Even with AI programs as simple as ChatGPT, you can ask it to write the algorithm that you need to accomplish some task. You don't need to know how to code anymore. It's the same with DNA or RNA sequencing. There are many specialized companies that do that for you. You request a sequence, and one or two days later, you receive that sequence—maybe the sequence for a virus of concern. It can be alarming without proper context.

There's a saying that 'what kills you, cures you.' It's the same in reverse. The technologies that we are developing and the research that we are conducting to make things better, of course, could be misused, but that's almost true with everything. A spoon in the wrong person's hand could be lethal. So, I think this is about anticipation. It's about preparedness in a true sense. It's about evaluating all the scenarios, the red teaming, and identifying what could be done to mitigate the consequences of an introduction of a biological agent whether that be disruption of trade or an epidemic that disrupts food production. This is where we have the challenge of this notion that certain types of research shouldn't be allowed. Do you think criminal organizations and terrorists are going to abide by those rules and regulations? This is about whether people are responsible in the way they do research. That's true for any kind of research. It's why we have biosafety protocols, why we have biosecurity protocols, why every academic institution has an Institutional Biosafety Committee, an Institutional Review Entity, and an Institutional Review Board that looks at every program to evaluate what the implications of that research are. All those are in place and functioning well from both safety and security perspectives.

CTC: What it sounds like is that while obviously there are

concerns about how advances in technologies are lowering the barriers to entry for nefarious actors to do bad things, there are opportunities to leverage those same technologies within government and across private-public partnerships to help us get ahead to monitor these threats for good. And there's a real parallel on the counterterrorism side, which has been very good at preventing different threats, but a next challenge for the counterterrorism community is how we leverage these technologies and integrate them into our ability to do things at greater speed and at scale. It sounds like there's a similar challenge in your field as well.

Stack: Absolutely. Utilizing these technologies in response offers several advantages, the computing power, the speed is just astounding. When you're dealing with the detection of something unknown, you have to make decisions on the next best steps, most often with incomplete information. And this is where some of these tools like AI modeling can really help generate your options much more quickly than with pen and paper, literature searches, and endless database queries. One important element that is not fully in place yet is the integration of networks and database systems that contain relevant information important to deriving effective solutions to unknown pathogen introductions. Even in the sequencing era, it can take time to identify an organism and its origin with the level of certainty that gives confidence to response efforts.

CTC: Is there anything else that we haven't talked about that you think would be important for our readers to know and understand?

Stack: I'll finish where I started, and that is, most people are unaware of the benefits they receive from plant systems. Plants are the foods that we consume directly and the feeds that we provide to the animals that we consume. Approximately 20-25 percent of the medicines that we depend upon come from plants. The chemistries that other medicines are built on came from plants. If you look at the history of medicine, it started with plants. While many benefits from plants are obvious (e.g., food and nutrition), some benefits are very subtle. For example, there's solid data that the more greenery you have in an urban setting, the less crime you have.[9] Psychologists did a study a number of years ago, and even people in urban center settings that don't get to travel much have psychological benefit in knowing there are national parks.[10] There's something calming about an interaction with a natural setting. Plant health underpins human health and well-being. People have not lost their connection to plants; however, most people have lost their awareness of that connection. The consequence of that is that it doesn't enter into how we formulate plant health policy nor how we fund programs that support plant health, like the National Plant Diagnostic Network. We need to recognize that just because you're not thinking about plants, doesn't mean your life isn't dependent upon them. CTC

Citations

[1] Editor's Note: W. Seth Carus, "A Short History of Biological Warfare: From Pre-History to the 21st Century," Occasional Paper, No. 12, Center or the Study of Weapons of Mass Destruction, National Defense University, August 2017; Paul Rogers, Simon Whitby, and Malcolm Dando, "Biological Warfare against Crops," *Scientific American* 280:6 (1999); Simon Whitby and Paul Rogers, Anti-crop biological warfare - implications of the Iraqi and US programs," *Defense Analysis* 13:3 (1997); L.V. Madden and M. Wheelis, "The threat of plant pathogens as weapons against U.S. crops," *Annual Review of Phytopathology* 41 (2003).

[2] Editor's Note: Dean Olson, "Agroterrorism: Threats to America's Economy and Food Supply," FBI Law Enforcement Bulletin, February 1, 2012.

[3] Giulia Soffiantini, "Food insecurity and political instability during the Arab Spring," *Global Food Security* 26 (2020).

[4] "K-State honors faculty with university distinguished professor title," Kansas State University, April 17, 2024.

[5] "History of NPDN," National Plant Diagnostic Network, n.d.

[6] Editor's Note: See Christopher Clary, "Four Days in May: The India-Pakistan Crisis of 2025," Stimson Center, May 28, 2025.

[7] "Chinese Nationals Charged with Conspiracy and Smuggling a Dangerous Biological Pathogen into the U.S. for their Work at a University of Michigan Laboratory," U.S. Attorney's Office, Eastern District of Michigan, June 3, 2025.

[8] "Alien from Wuhan, China, Charged with Making False Statements and Smuggling Biological Materials into the U.S. for Her Work at a University of Michigan Laboratory," U.S. Attorney's Office, Eastern District of Michigan, June 9, 2025.

[9] Editor's Note: See, for example, Michelle C. Kondo, SeungHoon Han, Geoffrey H. Donovan, and John M. MacDonald, "The Effect of Trees on Urban Crime: Evidence from the Spread of the Emerald Ash Borer in Cincinnati," Department of Criminology, University of Pennsylvania, Working Paper No. 2015-12.0, 2015; Austin Troy, J. Morgan Grove, and Jarlath O'Neil-Dunne, "The relationship between tree canopy and crime rates across an urban-rural gradient in the greater Baltimore region," *Landscape and Urban Planning* 106 (2012): pp. 262-270; and Geoffrey H. Donovan and Jeffrey P. Prestemon, "The Effect of Trees on Crime in Portland, Oregon," *Environment and Behavior* 44:1 (2012): pp. 3-30.

[10] Editor's Note: See, for example, Kirsten Weir, "Nurtured by nature," *Monitor on Psychology* 51:3 (2020).

Commentary: The Dangers of Overreliance on Generative AI in the CT Fight

By Nicholas Clark

The explosive rise in generative artificial intelligence (AI) use has sparked debate over its applicability in military domains such as counterterrorism (CT). This article critically evaluates the role of large language models (LLMs) in CT, arguing that their utility remains limited and potentially detrimental when applied indiscriminately. After providing a high-level overview of the mathematical foundations of LLMs, the article demonstrates how these tools can produce misleading or confidently incorrect outputs. Through case studies and empirical findings, this article underscores the cognitive risks of overreliance on AI in CT planning and intelligence operations, including reduced analytical engagement and inhibited creativity among operators. While generative AI may assist in automating routine tasks, it lacks the capacity for nuanced judgment, uncertainty quantification, and dynamic responsiveness critical to effective CT work. The article concludes by advocating for a shift in focus toward enhancing education in probabilistic reasoning, such as Bayesian inference, and building robust data governance infrastructures. Such foundational improvements are prerequisites for any effective or responsible integration of AI into CT domains.

According to Brad Lightcap, OpenAI's chief operating officer, the number of weekly users of ChatGPT has now surpassed 400 million, up from 30 million only two years ago.[1] Given this reality, coupled with the drum beat of constant news stories extolling the virtues of artificial intelligence (AI), it is natural to question whether the counterterrorism (CT) community should expand its use of generative AI in general and large language models (LLMs) in particular. Indeed, the common thought is that the use of these tools will allow organizations such as U.S. Special Operations Command (SOCOM) to gather and analyze large amounts of data.[2]

Yet, in practice, the actual utility of AI remains narrow, especially in high-stakes or variable environments. In operational planning and intelligence analysis, overreliance on algorithms risks thwarting creativity and hindering the intellectual growth that is a hallmark of organizations within SOCOM. This is not to say that generative AI does not have a role in these types of organizations; however, this article argues for a recalibration of AI deployment: focusing on narrow, clearly beneficial, public-interest uses while resisting the temptation to adopt AI indiscriminately or unquestioningly. Rather than a vast investment in generative AI tools, the CT community would benefit more from an increased educational investment in probabilistic reasoning and data governance.

This article provides a high-level overview of the math behind LLMs that will highlight the limitations of these algorithms. The article then discusses how LLMs could potentially be employed in CT operational planning and intelligence analysis, arguing that the tools may not be beneficial in many cases. The article concludes by discussing other areas that would be more beneficial for the CT community to focus on than generative AI.

High-Level Overview of the Math Behind LLMs

While readers may be tempted to avoid the mathematics behind the algorithms, it is only through having a basic understanding of what these models are doing that allows users to understand the limitations of the tools. The more mathematically inclined reader will note that what follows is certainly not a full treatment of the algorithms, but it is very easy for even those who have advanced degrees in computer science, statistics, or mathematics to get lost in the full architecture of the algorithms.

The key to understanding LLMs is that they are built off autoregressive models; that is, the models provide probabilistic output based off the words that are provided into the prompt. Each word in the English language is a potential next word and the algorithm assigns probabilities to all of the corpus. The algorithm then returns the word with the highest probability. The whole process then restarts to generate the second word and so on.

As a toy example, consider the prompt to an LLM to "Provide the next word in the statement 'The quick brown fox jumps over the lazy…'". What the algorithm does is takes the statement and first converts it into a vector.[a] This is what is referred to as tokenization.[3] The algorithm then assigns each token a weight and uses the weights to provide a probabilistic output. For instance, if we ask ChatGPT to complete the statement "The quick brown fox jumps over the lazy",

[a] While technically the tokenization occurs on syllables or smaller aspects of a word, what follows is still generally correct and serves as a high-level example of what the black box is doing 'under the hood.'

COL(R) Nicholas Clark, Ph.D., is an Associate Professor in the Department of Mathematics at the University of St. Thomas (Minnesota). Prior to joining St. Thomas, COL(R) Clark served as an Associate Professor at the United States Military Academy at West Point from 2016 to 2024, where he founded and led the Applied Statistics and Data Science Program. In 2021, he created a curriculum in data literacy that is now the widest adopted program in the U.S. Army. Prior to his academic appointments, COL(R) Clark served as an intelligence officer for multiple units with U.S. Special Operations Command (SOCOM).

it would state that the word with the highest probability is 'dog' and give us this word as the answer. However, we note that 'under the hood,' the algorithm is evaluating all possible words and assigning each a probability. For instance, if instead we ask the algorithm to provide the top-five most likely words and associated probabilities, we would get:

Rank	*Word*	*Estimated Probability*
1	dog	~85%
2	cat	~5%
3	boy	~3%
4	man	~2%
5	cow	~1%

However, we are often looking for more than a single word response. This is where the idea of auto-regression comes into play. If, instead, we wanted the algorithm to provide the next three words that would come after the statement "The quick brown fox jumps over the lazy", we would get:

Rank	*Next Three Words*	*Estimated Probability*
1	dog. The	~65%
2	dog and ran	~10%
3	dog without stopping	~7%
4	dog, then	~6%
5	cat. The	~3%

Here, the algorithm first predicts the first word; the second word, then, is conditional upon the first word that the algorithm provided. That is, first the algorithm says that the most likely word is 'dog', then it pretends that we passed in the prompt, "provide the next two words that come after the statement 'The quick brown fox jumps over the lazy dog'", and it determined that the most likely next word would be "." It then repeats this and says that since we are starting a sentence, we would next expect to get "The" for the final word.

To see how these probabilities are calculated, we consider the first prompt, "Complete the statement 'the quick brown fox jumps over the lazy'". To provide a probabilistic output, the model has to know what 'right' looks like. To do this, the algorithms are trained on Common Crawl; books (fiction and nonfiction); Wikipedia; WebText (Reddit, forums, etc.); technical content, manuals, and examples from real-world use.

That is, the model essentially looks across these examples and sees what most people would put as the next word in this prompt. Here, essentially the model shows that around 85% of the times people type the words "the quick brown fox jumps over the lazy" the next word is 'dog'.

So, what can go wrong? Let's say we type in "The quick brown fox jumps over the lazy cat" into a Google search. Google's AI tool will state:

> *The phrase "The quick brown fox jumps over the lazy cat" is a common English pangram, meaning it includes all letters of the English alphabet. It is often used for testing typing and fonts.*

The problem is, this is just wrong. The statement is not a pangram; however, the algorithm stated that it was because overwhelmingly most of the time people type out "The quick brown fox jumps over the lazy", they are using the pangram. Therefore, the strength of those words overwhelms the word 'cat', essentially ignoring the fact that we prompted it with 'cat' rather than 'dog.'

To see what else can go wrong, consider the prompt "Provide the next 10 words after the statement, 'the quick brown fox jumps over the lazy'". We would get "dog and ran swiftly across the green grassy field." The issue is, without having user knowledge on what we expected, we would have no idea whether this was correct. The algorithm, though, does not provide any warning that it is much more certain that the one-word completion is 'dog' than it is the 10-word completion is 'dog and ran swiftly across the green grassy field.'

One final potential issue is in the training data itself. Often, when developers are dissatisfied with the output from the algorithm, they will up-weight, or down-weight, certain datasets. For instance, recently xAI felt that its algorithm was providing responses that were too 'politically correct.'[4] The developers, subsequently, gave more weight to training data that was not seen as 'politically correct.' This resulted in their algorithm overweighing conspiracy theories and provided vile, antisemitic responses.[5] The ability to fine-tune is a double-edged sword: It enables customization but also opens the door to dangerous distortions.

LLMs in CT Operational Planning

One potential use for LLMs in CT would be for an operational planner to use the tool to generate courses of action. One immediate concern, as discussed above, would be that the algorithm would provide nonsense. However, there are other reasons that this may not be beneficial for the CT community. Perhaps the largest concern is embodied in the quote by President Dwight Eisenhower, "Plans are worthless, but planning is everything."[6] The use of generative AI for operational planning may, in fact, make our planners worse by removing the real benefits of the planning process and limit the CT forces' ability to respond dynamically to branches and sequels.

To understand the risk, we must look at the recent study by Kosmyna et al. on what happens to the human brain when individuals use AI assistance such as ChatGPT for writing papers. The study took three groups and asked them to write essays using ChatGPT, Google search, and nothing at all. They then examined the brain activity of the users and found that those that used ChatGPT had the lowest brain engagement and consistently underperformed the other groups. Perhaps most disturbingly, over the course of the study, ChatGPT users got lazier with each subsequent essay, often resorting to copy-and-paste.[7]

While special operations forces are extremely selective, perhaps less appreciated is the growth of the operator or support personnel while they are assigned to a special operations unit. One of the tenants of special operations is that competent SOF cannot be created after an emergency.[8] This is due to the training and growth that is required by individuals after they have been selected. Reliance on generative AI may impede this growth and limit the intellectual development of both operator and support personnel.

Operational plans in CT, in particular, require creativity that likely would not be produced through generative AI. A hallmark of special operations is that they are granted greater license to innovate during ongoing operations.[9] While it certainly is possible to create an LLM that integrates domain specific knowledge into an algorithm through fine-tuning existing tools,[10] a lesser appreciated aspect of human planning in special operations is that a planner knows when and where to be creative and when to rely on conventional military methodology. Further, recent research has shown that the creativity employed by generative AI is predictable rather than truly being innovative.[11]

Where generative AI may be of use in operational planning is through automating the routine tasks of order production. For example, within a CT operations order (OPORD), there are typically paragraphs that an operations officer may find themselves cutting and pasting from previous OPORDs. Paragraph completion and other tools that rely on generative AI may be of use in these instances, however the wholesale adaptation of LLMs inside of operations planning is likely to impede both individual and unit growth and also lead to adverse outcomes.

LLMs in Intelligence Operations

The military domain that is often seen as rife for improvement by the use of generative AI is intelligence. Articles such as the joint report by UNICRI and UNCCT on "Countering Terrorism Online with Artificial Intelligence" seem to highlight a multitude of ways that AI can assist in CT.[12] However, as the article mentions, here the term AI is misleading and, in fact, most of the algorithms discussed are widely known and rely on structured data that often is missing in CT operations. Where AI has the most potential in intelligence is automating the processing of raw information into structured data, commonly referred to as data engineering. Generative AI may assist intelligence analysts who have a background in programming, however this, too, may be problematic.

Articles on using AI in intelligence operations often cover everything from basic regression models to more advanced topics such as neural networks or generative adversary networks. However, it is important to note that these are not examples of generative AI. While algorithms such as those that underlie ChatGPT are based off neural networks, saying a neural network is a form of generative AI would be like saying an engine is a form of a car.

One of the difficulties, though, in using more advanced analytical techniques in intelligence operations is that they rely on having high-quality, curated datasets. If there are issues with the data, then we cannot create algorithms to fix this. When data is messy or observed imperfectly, then an advanced algorithm may just be providing a false level of certainty.

As an example, we recently created an algorithm to assist in automating the process of creating a gridded reference graphic, or GRG.[13] This relied on using a set of satellite images to predict where buildings and key road intersections would be. In training the algorithm, we discovered that depending on where in the world we were observing, the model would require very different weights. That is, if we relied on data from Europe, the model would perform horribly in North Africa. The difficulty, then, became in creating such a robust set of training data that the algorithms could be useful in multiple areas. However, the algorithm used here was not generative AI. Where an LLM, perhaps, could be useful would be in the coding up of the convolutional neural network (CNN)[14] that we used in this instance. This, though, is far from certain. Recent research suggests that in some instances, generative AI may actually slow down developers.[15]

One final caution for CT intelligence analysts tempted to use generative AI as part of their work process is that the algorithms do not quantify uncertainty. That is, while traditional statistics allow researchers to yield a range of plausible values, generative AI typically provides a single output, or multiple outputs, but does not quantify how certain they are in their response. This is problematic for intelligence analysts who typically get asked how certain they are in their analysis and are asked to provide likelihood assessments for a variety of outcomes.

"Instead of focusing on generative AI, the CT community would benefit from focusing on learning and applying statistical tools to data and to ensure that good data governance exists in order to standardize aspects of data engineering."

If Not Generative AI, Then What?

In general, LLMs excel in three broad categories: quickly creating coding demonstrations,[b] translating between different coding languages, and explaining and critiquing coding. However, these are not the areas where intelligence or operations experts within CT typically need help. In fact, creating demonstrations that are not necessarily scalable often are distractions from the day-to-day work that these professionals need to accomplish. Rather, where intelligence professionals need to better leverage data is in creating predictive analytics and quantifying uncertainty in their predictions. Therefore, instead of focusing on generative AI, the CT community would benefit from focusing on learning and applying statistical tools to data and to ensure that good data governance exists in order to standardize aspects of data engineering.

Of the multitude of potential quantitative methods that CT professionals might focus on, the community would benefit from an increased awareness of Bayesian methodologies. Unlike purely data-driven models, Bayesian approaches allow analysts to formally incorporate prior knowledge, whether derived from field experience, historical data, or expert judgment, into probabilistic frameworks. This capacity to combine prior beliefs with new evidence enables more nuanced and interpretable assessments of uncertainty, especially in complex, evolving, and highly fluid environments where data may be sparse or noisy. Such probabilistic reasoning should not be treated as a niche tool but rather integrated into the broader analytic training of intelligence professionals. Teaching Bayesian inference alongside more traditional statistical and algorithmic methods would empower analysts to make more transparent and defensible judgments about future risks.

Operations experts and leaders inside the CT community would also benefit from increased instruction in probabilistic reasoning including Bayesian techniques. A basic lack of understanding of the meaning of probabilities often results in command teams asking

[b] For example, writing Python code to automate a task or creating a dashboard to allow users to interface with data.

intelligence professionals to either quantify that which cannot be quantified or to adjust the data in order to meet prespecified conclusions. A stronger understanding of how probabilities can be used to weigh data with subject matter expertise would allow planners to better quantify risk and also help to focus reconnaissance tasks on refining uncertainty rather than on areas of highest threat. For example, we recently demonstrated that dynamically re-tasking unmanned aerial surveillance (UAS) to areas of higher uncertainty rather than to areas of highest threat, or flying in a predetermined pattern, allowed users to more quickly map out the entire region of nuclear contamination.[16]

Still, regardless of the algorithm or framework employed, one fundamental truth remains: High-quality, consistent data is indispensable. Even the most sophisticated methodologies will falter—potentially catastrophically—when applied to flawed or incomplete data. Thus, investments in data infrastructure and governance are not ancillary but central to any successful analytic strategy. Everyone within an organization should understand how data is structured, shared, and stored. Data standardization is instrumental for any organization to successfully operate, and far too often it is a lack of clearly enforced rules that limit an organization's ability to successfully incorporate data into their decision-making processes. Recent research has shown that even after hiring AI experts (and paying them well), organizations fail to gain insight from data as a result of not having a data-driven culture—a key component of which is a common understanding of data standards and organizational goals.[17]

Conclusion

Generative AI holds clear appeal for the CT community. But beneath the surface lies a host of unresolved concerns: opaque reasoning, unreliable creativity, biased training, and the erosion of essential human competencies. The promise of AI must be weighed against its risks, however—not just technical ones, but cognitive and operational as well. Prior to any use of AI, organizations should upskill their population in probabilistic reasoning and basic data governance. It is only after these are properly understood that an organization can fully recognize whether tools such as generative AI are appropriate for their formation.

A final concern for the CT community is that AI development is dominated by a handful of U.S. tech corporations: Microsoft (partnered with OpenAI), Google (DeepMind, Gemini), Amazon (Bedrock, CodeWhisperer), Meta (Llama), and a few smaller players. These firms leverage their access to data, compute infrastructure, and talent pipelines to consolidate market share, extract rents, and shape public policy. In order to use their tools, they likely will request access to the most sensitive CT data possessed by the U.S. government and seem unlikely to share the underlying architecture for their algorithms. This will create a situation where the U.S. government will continue to need to purchase products and services for algorithmic maintenance in order to use tools that the corporations hope will become integral components of both the intelligence and operational planning cycles. While this issue is not unique to AI technology, this is particularly pronounced with generative AI as once organizations have access to CT data, the relationship between the U.S. government and corporations will become one-sided as the U.S. government will have to rely on the computational resources provided by the corporations. Future data acquisition that the government may attempt to use as leverage in contract discussions will be of little value once the initial tranche is provided to train the models. To potentially mitigate this, acquisition professionals will need to ensure that contracts stipulate that models are firewalled off from the corporations and prevent the models from learning from the unique sources of data that have been ingested. However, this still requires an increase in education grounded in basic data analytic skills that are largely missing from military curricula.

In an environment where adaptability, innovation, and judgment can determine life or death, overreliance on generative AI may do more harm than good. Instead, this article advocates for an increase in education in Bayesian reasoning and data principles. In many cases, generative AI is a distraction and should only be used within a disciplined, use-case-driven approach, one that leverages narrow efficiencies while preserving the uniquely human strengths that remain irreplaceable in counterterrorism work. CTC

Citations

[1] Allison Morrow and Lisa Eadicicco, "Grok antisemitic outbursts reflect a problem with AI chatbots," CNN, July 10, 2025.

[2] Allyson Park, "Just In: SOCOM Using AI to Speed Up Acquisition Workflows," National Defense Magazine, May 6, 2025.

[3] Pranjal Kumar, "Large language models (LLMs): Survey, technical frameworks, and future challenges," *Artificial Intelligence Review* 57:10 (2024).

[4] Morrow and Eadicicco.

[5] Ibid.

[6] "Remarks at the National Defense Executive Reserve Conference," U.S. Presidency Project, n.d.

[7] Nataliya Kosmyna et al., "Your brain on ChatGPT: Accumulation of cognitive debt when using an AI assistant for essay writing task," arXiv.org, June 10, 2025.

[8] Bryan D. Brown, "U.S. Special Operations Command – Meeting the Challenges

of the 21st Century,” *Joint Forces Quarterly* 40 (2006).

[9] Robert G. Spulak, “Innovate or Die: Innovation and Technology for Special Operations,” *JSOU Report* 10:7 (2010).

[10] Zirui Song et al., “Injecting domain-specific knowledge into large language models: A comprehensive survey,” arXiv.org, *2025.*

[11] Mark A. Runco, “AI can only produce artificial creativity,” *Journal of Creativity 33*:3 (2023).

[12] See “Countering Terrorism Online with Artificial Intelligence: An Overview for Law Enforcement and Counter-Terrorism Agencies in South Asia and South-East Asia,” United Nations Interregional Crime and Justice Research Institute and United Nations Office of Counter-Terrorism, 2021.

[13] Samuel Humphries, Trevor Parker, Bryan Jonas, Bryan Adams, and Nicholas J. Clark, “A dual U-Net algorithm for automating feature extraction from satellite imagery,” *Journal of Defense Modeling and Simulation* 18:3 (2021): pp. 193-205.

[14] “Convolutional neural networks,” IBM, n.d.

[15] Joel Becker, Nate Rush, Elizabeth Barnes, and David Rein, “Measuring the impact of early-2025 AI on experienced open-source developer productivity,” arxiv.org, July 12, 2025.

[16] Daniel Echeveste, Andrew Lee, and Nicholas Clark, “Using Spatial Uncertainty to Dynamically Determine UAS Flight Paths,” *Journal of Intelligent* & *Robotic Systems* 101:76 (2021).

[17] Thomas H. Davenport and DJ Patil, “Is data scientist still the sexiest job of the 21st century?” Harvard Business Review, July 15, 2022.

Understanding China's New Counterterrorism Ambitions in Africa

By Jason Warner

China has recently been pursuing a much more aggressive stance in African security affairs, including playing a more engaged role in counterterrorism (CT). Where is China engaged in CT in Africa, and by what means? What challenges would China face in engaging more robustly in African CT? Most importantly, why is China newly expressing interest in engaging in the African CT landscape at this particular moment? In the main, this piece argues that despite ostensible rationales related to self-defense of economic interests and solidarity with African states, at its core, Beijing's primary motivations for entering the African CT space are to diversify its means of influence in Africa beyond its historical "economics-first" approach. Recognizing that engaging in African CT is a high-risk but potentially high-reward activity (which other global powers have recently engaged in with mixed results), Beijing likely believes it has a new genre of CT assistance—less kinetic, more economic, and rooted in equitable partnerships—that represents a fundamentally new and productive means of gaining influence in Africa. Yet, China faces challenges in its African CT pursuits, including reconciling whether its cautious ethos can stomach the turbulent landscape of African terrorism; how to deal with a saturated African CT space; and how not to fall victim to the same pitfalls as other global powers that have recently engaged in African CT. Nevertheless, if China can prove that its cautious non-military-first approach is fundamentally different from existing CT value propositions from external states, Beijing could deeply rival, and potentially replace, Washington as the partner of choice for security cooperation in Africa.

Over the past 20 years, external states have sought to gain influence in Africa by assisting African countries in fighting terrorist groups.[1] Beginning with the United States' entrance into the Sahara and Sahel in the years after 9/11 to stem the tide of al-Qa`ida's presence there, Washington would soon also become involved in trying to tamp down al-Shabaab's presence in Somalia.[2] By 2011, France had begun to intervene seriously in African counterterrorism (CT) in Mali with its Operation Serval mission in the country against a combination of al-Qa`ida affiliates and separatists,[3] a mission that would expand to see it creating an ill-fated pan-Sahelian counterterrorism organization, the G-5 Sahel,[4] all while its own Operation Barkhane tried and failed to stem the exponentially rising tide of terrorism in Mali, Burkina Faso, and Niger.[5] By 2019, Russia too had entered the African CT space in a bid to gain influence on the continent, deploying elements of its state-run Wagner Group to address terrorist threats affiliated with al-Qa`ida or Islamic State groups in Mozambique, Mali, Burkina Faso, and Niger, all with highly variable results.[6]

Yet, fast forward to the present day, and each of these states has been met with a general lack of success[7] in African CT, with reputations being tarnished, not burnished, as a result. Most notably, after more than a decade of serious engagement, in the 2020s, France began having its counterterrorism forces ridiculed and accused of supporting terrorist elements in the countries they were present in—notably Mali, Niger, and Burkina Faso—by both host governments[8] and civil society[9] alike. Due to a combination of the perceived failures of its CT efforts as well as its treatment of local partners, France has of late ignominiously had its security cooperation agreements annulled by state after African state (including Mali,[10] Niger,[11] Burkina Faso,[12] Senegal,[13] Côte d'Ivoire,[14] Chad,[15] and others), resulting in its lowest degree of influence in Africa in half a century.

For its part, the United States, while not faring as poorly as France and still generally the partner of choice for African militaries, notably saw its primary counterterrorism bases—Bases 201 and 202, on which it had spent hundreds of millions of dollars over a decade—revoked by the Nigerien government in 2024.[16] Even Russia, which has, for the past several years, been the CT partner of choice for many of the most terrorism-beset African regimes, saw its own stock plummet recently: Beyond the constant reports of human rights abuses perpetrated by the Wagner Group/Africa Corps,[17] the Wagner Group recently announced it was leaving Mali after apocryphally claiming a "completed mission."[18] In the midst of this scramble by current, former, or aspiring great powers for influence via CT in Africa, one global heavyweight has historically been notably quiet: China.

But 2024 marked a turning point. In that year, more than any other before, China shed the illusion that it sought to remain a primarily economic partner for African states and made clear that it was instead ready to jump more ardently into the security realm in Africa. The most telling example of this was the fact that at the September 2024 Forum on China-Africa Cooperation (FOCAC)

Dr. Jason Warner is the Director of Research and the Senior Africa and Senior Terrorism/Transnational Crime Analyst at Foreign Military Studies Office (FMSO), part of the U.S. Army's Training and Doctrine Command (TRADOC) G2. He is also a Senior Non-Resident Fellow at the Africa Program at the Center for Strategic and International Studies (CSIS), and serves as an adjunct professor at American University and Penn State University.

Summit, China was unabashed about its desire to become a major security actor on the African continent, giving what some called "unprecedented Chinese emphasis on its role in security on the continent."[19] In the opening speech of the summit,[20] "Chinese President Xi Jinping promised to provide Africa with approximately $140 million in grants for military assistance; training for 6,000 military personnel and 1,000 police and law enforcement officers; participation in joint military exercises, training, and patrols; and invitations for 500 young African military officers to visit China."[21]

More broadly, since 2024, observers have recognized and underscored China's growing military role in Africa. To that end, they have focused on the growing militarization of China's Africa policy,[22] the growing role of private Chinese security firms in Africa,[23] and China's increased use of military diplomacy[24] and arms sales in Africa,[25] with one analyst underscoring that "Africa now represents the PRC's largest persistent military deployment outside of its periphery."[26] And yet, one specific dimension of China's broader push has, to date, received relatively little attention: counterterrorism.[27]

To that end, this article asks: Where is China engaged in CT in Africa, and by what means? What challenges would China face in engaging more robustly in African CT? Most importantly, why is China newly expressing interest in engaging in the African CT landscape at this particular moment? In the main, this piece argues that despite ostensible rationales related to self-defense of economic interests and solidarity with African states, at its core, Beijing's primary motivations for entering the African CT space are to diversify its means of influence in Africa beyond its historical "economics-first" approach. Recognizing that engaging in African CT is a high-risk but potentially high-reward activity (which other global powers have recently engaged in with mixed results), Beijing likely believes it has a new genre of CT assistance—less kinetic, more economic, and rooted in equitable partnerships—that represents a fundamentally new and attractive means of gaining influence in Africa. Yet, China faces challenges in its African CT pursuits, including reconciling whether its cautious ethos can stomach the turbulent landscape of African terrorism; how to deal with a saturated African CT space; and how not to fall victim to the same pitfalls as other global powers that have engaged in African CT. Nevertheless, if China can prove that its cautious non-military-first approach is fundamentally different from existing CT value propositions from external states, Beijing could deeply rival, and potentially replace, Washington as the partner of choice for security cooperation in Africa.

This article proceeds in four sections. First, it lays out the evolution of Chinese understandings of "terrorism" and "counterterrorism" in both domestic and international spheres. Next, it describes the specific genres of activities that China is currently engaged in within the African CT space. In the third section, it articulates the rationales as to why China has chosen the current moment to pursue this new interest in African CT. In the fourth, it lays out some of the challenges that China will grapple with if it does elect to become a more forceful player in African CT. Finally, the conclusion synthesizes the above discussions, drawing out the implications for Africa, the United States, and the world if China succeeds in becoming the new major CT provider in Africa.

Part I: Evolution of the Chinese Conceptualization of CT

The notion of 'terrorism' in China is a relatively new phenomenon, which primarily has roots in China's domestic politics but has, over time, evolved to become a concern and an area of policy engagement for China internationally. In Imperial China, the notion of 'terrorism' did not exist; political violence was instead conceived of as actions threatening to the emperor and leading to "chaos."[28] However, as China began to liberalize in the 1980s, dissident groups in the country became more vocal, and China saw a rise in separatist and religiously fervent groups. Most specifically, this pseudo-opening and liberalization led to the rise of increased threats posed to national unity by its Uyghur Muslim minority in the western Xinjiang province, and its militant arm, the Uyghur East Turkmenistan Islamic Movement (ETIM). Arising in the 1990s, ETIM sought a separate "East Turkistan" state. ETIM has undertaken attacks on police,[29] bombed a train station,[30] assassinated local officials,[31] undertaken a widescale knife stabbing attack in Kunming in 2014,[32] and plotted to attack the U.S. embassy.[33] Germanely, ETIM has also been shown to have links to al-Qa`ida, the Taliban, and their allies, including the Islamic Movement of Uzbekistan and Tehrik-i-Taliban Pakistan.[34]

In light of its experience with ETIM, China would eventually come to conceive of terrorism in the context of combating the "three evils"—ethnic separatism, religious extremism, and violent terrorism.[35] Importantly, China's view of terrorism is rooted in its domestic experience, in which Islamist terrorists not only threatened disruptive violence but more fundamentally endangered the very territorial integrity of the Chinese state.

The year 2001 also served as a fundamental turning point in China's understanding of threats of transnational terrorism. Though China never served as a steadfast or particularly important partner in the United States' Global War on Terror,[36] given its experience with al-Qa`ida-linked ETIM, the 9/11 attacks did, nevertheless, lead China to take such threats from al-Qa`ida much more seriously.

> **"China faces challenges in its African CT pursuits, including reconciling whether its cautious ethos can stomach the turbulent landscape of African terrorism; how to deal with a saturated African CT space; and how not to fall victim to the same pitfalls as other global powers that have engaged in African CT. Nevertheless, if China can prove that its cautious non-military-first approach is fundamentally different from existing CT value propositions from external states, Beijing could deeply rival, and potentially replace, Washington as the partner of choice for security cooperation in Africa."**

Supporters of Niger's National Council of Safeguard of the Homeland (CNSP) wave the Chinese flag and a flag bearing a logo of private military company Wagner in Niamey on September 16, 2023. (Democracy News Alliance/news aktuell via AP Images)

Domestically, China increased its use of language about terrorism in national documentation and, throughout the early 2000s and 2010s, consistently grew its own counterterrorism legislative agenda,[37] including passing its wide-ranging Counterterrorism Law in 2015. Among other provisions, the law laid out definitions of "terrorism" (which have been critiqued as broad and vague); expanded state authority to prevent terrorism (including granting wide-ranging powers for intelligence gathering, surveillance, detention, and the use of armed forces); put new demands on companies and individuals to assist the government in counterterror efforts (including rendering communications records and demanding citizen assistance); and defined the root causes of terrorism (which include a lack of economic development and a desire for social justice).[38] Germanely, the law also outlined the international dimensions of China's counterterrorism outlook. These included stipulations that China would seek to develop CT cooperation with other states and organizations (Article 68); would undertake exchanges of intelligence, cooperative enforcement, and financial monitoring (Article 69); and could assign members of the People's Liberation Army (PLA) and police forces to leave the country on CT missions (Article 71).[39] While the 2015 Counterterrorism Law would come to serve as the bedrock for China's domestic and international counterterrorism outlook, it received wide-ranging criticism for the exceptional powers it granted to the state, and the potential abuses such powers could engender.

Perhaps the wide-ranging powers of the Counterterrorism Law were no more evident than concerning China's Uyghur communities. China's enduring concerns about its Uyghur minority led it to undertake "preventive counterterrorism" strategies, which included extreme surveillance measures, widespread arrests, and the placement of these members in so-called "re-education camps," all of which have been widely critiqued by human rights groups.[40] In response, with the rise of the Islamic State in 2014, Chinese Uyghurs came to serve as a non-negligible presence of foreign fighters in Iraq and Syria.[41] The Islamic State leader, Abu Bakr al-Baghdadi, singled China out in April 2014 as a state that repressed Muslims.[42] Indeed, China's treatment of its Uyghur minority has come to serve as a troubling shibboleth of its approach to CT. As of 2020, reporting suggested that some one to three million people—including Uyghurs, but also Kazakhs and Kyrgyzs—had been detained in an array of some 1,200 "re-education" camps in China, while members of the Uyghur diaspora had been put under intense surveillance.[43]

Outside of its domestic sphere, also beginning in the aftermath of the 9/11 attacks, China began engaging in counterterrorism assistance with nearby countries to safeguard its own borders. Working primarily under the auspices of the Chinese-established Shanghai Cooperation Organization (SCO), China began extensive bilateral and multilateral counterterrorism cooperation with countries in its near-abroad, including Russia and especially in the '-stans': Pakistan,[44] Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan. This cooperation normally focused on joint exercises and intelligence-sharing. For instance, in 2021, in the face of the resurgence of the Taliban and worries about the impact on its economic projects, China signed a deal to finance a counterterrorism military base in Tajikistan,[45] with which it conducted counterterrorism drills in 2019,[46] 2021, and 2023, and with which it has agreed to host joint counterterrorism exercises every two years.[47]

When it comes to Africa more acutely, China's concerns about the effects of terrorism on its economic interests coincided with the 2013 launch of its Belt and Road Initiative (BRI), and the need to protect its overseas economic investments. While Chinese "private" security companies (though with state funding and attached to international state enterprises) were some of the first deployments that intended to safeguard Beijing's investments, these were generally perceived to be far more anodyne than traditional PMCs. For instance, by law, Chinese nationals cannot carry weapons abroad,[48] and the Chinese government only grants a limited number of companies the authority to serve in such security roles.[49]

As BRI projects expanded on the African continent, particularly in terrorism-afflicted states—Mali, Burkina Faso, Niger, Chad—or simply unstable states—Sudan, Guinea, Gabon[50]—so too did China's concern about the economic impacts of terrorism. By 2014, Chinese analysts began referring to "an arc of instability caused by terrorism" in Africa that included Mali, Nigeria, Tunisia, Libya, Egypt, and Somalia,[51] while simultaneously, Chinese workers on the continent began facing violence from non-state armed actors. Anecdotally, nine Chinese goldmine workers were killed in the Central African Republic in 2023 by rebels, just days after another three Chinese workers were kidnapped in another part of the country.[52] In both the DRC and Nigeria, Chinese nationals have been kidnapped by members of violent extremist organizations; in the latter, Chinese workers are referred to as "sweet pastries" due the substantial ransom payments they could expect to generate.[53] Thus, China's early engagement in defensive African anti-terrorism efforts—to be distinguished from offensive counterterrorism efforts—began with an economic impetus, and for good reason: One think-tank shows that from 2014-2024, Chinese citizens were subject to some 150 violent incidents in sub-Saharan Africa, though numbers on terrorism-specific incidents are not known.[54] And indeed, this is logical, as many of Beijing's economic investments occur precisely in conflict-prone spaces. For instance, in its 2019 defense white paper, China noted that "China's overseas interests are endangered by immediate threats such as international and regional turmoil, terrorism, and piracy" and that one of the missions of the PRC's armed forces is to "safeguard China's overseas interests."[55]

However, China's clearest definition of its current understanding of terrorism and counterterrorism has been incrementally articulated via its Global Security Initiative (GSI) framework, intended to serve as an alternative international security effort to that of the Western and NATO-led world order. While its initial unveiling in 2022 addressed terrorism in the context of China's near-abroad regions of Southeast and Central Asia,[56] it said little about the GSI's view of terrorism in other world regions, including Africa.[57] However, in February 2023, China released "The Global Security Initiative Concept Paper," which elucidated global and regional priorities of the GSI, giving stark evidence of its prioritization of CT in Africa. To that end, the report was notable in two regards. First, while it made broad references to global terrorism, the only *region* in which terrorism was mentioned explicitly was Africa. Second, and perhaps more tellingly, China's commitment to assisting in counterterrorism efforts in Africa was arguably the *primary lens* through which China articulated its value proposition to the continent. The full text of the Africa section of the GSI Concept Paper (below) underscores this centrality of its role in African security generally, and counterterrorism specifically, both in explicit mentions of CT as well as allusions to the most volatile terrorism-afflicted regions of the continent. In it, China pledges to:

> *Support the efforts of African countries, the AU and sub-regional organizations to resolve regional conflicts, fight terrorism and safeguard maritime security, call on the international community to provide financial and technical support to Africa-led counter-terrorism operations, and support African countries in strengthening their ability to safeguard peace independently. Support addressing African problems in the African way, and promote peaceful settlement of hotspots in the Horn of Africa, the Sahel, the Great Lakes region and other areas. Actively implement the Outlook on Peace and Development in the Horn of Africa, promote the institutionalization of the China-Horn of Africa Peace, Governance and Development Conference, and work actively to launch pilot projects of cooperation.*[58]

The GSI Concept Paper's focus on "Africa-led counterterrorism" via a variety of instruments—conflict resolution, conferences, security-focused pilot projects, and global cooperation—speaks to the breadth of approaches in its toolkit. This Chinese focus on African counterterrorism was followed by a March 2023 U.N. speech by Liu Yuxi, special representative of the Chinese government on African affairs at the United Nations, whose statements focused exclusively on the need for more global action to combat terrorism in Africa.[59] Collectively, these actions set the stage for the recent Chinese CT push that has been evident for at least the past several years.

Part II: Means of Chinese Engagement in African CT

Having laid out how China thinks about terrorism and counterterrorism domestically, internationally, and increasingly, in Africa, just how is China engaging in counterterrorism-related activities in Africa?

A Deferential, Cautious Approach

At the broadest level, and beyond any individual means of engagement, the hallmark of China's engagement in military and security cooperation—and, inter alia, counterterrorism cooperation—in Africa is one of caution, amity, respect, non-interference, and deference to African partners. As this author has suggested elsewhere, China's military ambitions in Africa have tremendous potential to upend the status quo precisely because they appear to be non-threatening. In opposition to others, China's military engagement in Africa has been marked by being "quiet, nonviolent, boringly technical, and profoundly, delicately measured," focusing on "technical—not combat—training; police—not military—training; and more broadly on economic—and not security—phenomena."[60] Thus, as an organizing principle, *how* China frames its CT, not merely *what* it does, is one of the most important dimensions of its engagement.

Bilateral and Multilateral Terrorism-Related Diplomacy, Outreach, and Agreement Making

Across the continent, China's recent push for counterterrorism-related influence has been evident. Stories have emerged of counterterrorism-focused discussions between senior Chinese and African officials in Algeria (February 2025[61]), Benin (September 2023[62]), Burkina Faso (June 2021,[63] December 2023[64]), Cameroon (September 2024[65]), Djibouti (September 2024[66]), Egypt (January 2023,[67] June 2024,[68] October 2024,[69] April 2025[70]), Gambia (February 2024[71]), Mali (June 2025[72]), Niger (March 2025[73]), Tunisia (May 2024[74]), and Togo (September 2024[75]). China has also signed formal counterterrorism-related agreements with various African countries, including Nigeria (December 2020,[76] February 2025[77]), and, arguably, depending on interpretations,[a] Egypt (November 2024[78]). It has donated material to African states to combat terrorism in Benin (March 2023 and August 2024[79]), engaged in counterterrorism intelligence-sharing in Egypt,[80] and conducted joint counterterrorism drills with Tanzania and Mozambique in July and August 2024.

Outside of these bilateral counterterrorism agreements, China has also sought to inform the contours of the United Nations' means of addressing terrorism through its funding of U.N. counterterror mechanisms. China frequently espouses the need for greater counterterrorism cooperation for Africa within the United Nations[81] and led the creation of the UN Peace and Development Trust Fund,[82] which funds counterterrorism efforts and argues for more resourcing and empowerment of African international organizations, including the African Union, and regional economic communities, including the Economic Community of West African States.[83]

Elsewhere, China has sought multilateral CT influence in organizations including the BRICS, FOCAC, and China-Arab States Cooperation Forum (SASCF),[84] but especially in the context of the Chinese-led SCO, which has, at its core, a focus on regional counterterrorism cooperation. It has also offered its rhetorical support for African-led counterterrorism research and capacity-building through continued assistance to the African Centre for the Study and Research on Terrorism (ACSRT), based in Algiers.[85] Beyond the discussions that happen in and on the sidelines of these multilateral events, an imperative feature of its engagement in multilateral fora is China's infusion of its *modus operandi* of CT into global normative counterterrorism culture.

Engagement in U.N. PKOs

As a major player in funding and participation in U.N. peacekeeping missions, the majority of which are in Africa and involve some dimension of terrorism presence, China has quietly gained experience via U.N. peacekeeping operations (PKOs) while also burnishing its image as a responsible and altruistic rising 'great power.' Indeed, some analysts have described its peacekeeping efforts as "the most significant platform of Chinese security engagement in Africa."[86] Since 1990, China has deployed over 30,000 peacekeepers to Africa-based missions, equaling approximately 80 percent of its total global peacekeeping deployments.[87] Most notably, China once had a somewhat significant presence in the terrorism-centric U.N. peacekeeping operation in Mali (MINUSMA),[88] which had been interpreted by some observers as demonstrating "China's willingness to further engage in [counterterrorism] operations."[89] Indeed, underscoring the continued trope of Africa as a proving ground for China, one PLA officer described Africa as a "test lab" for China, where it can "get military experience without giving up on its non-interference principle,"[90] with all military activities occurring under the far more innocuous U.N. banner.[91] As some analysts have noted of China's one-time approach in Mali, "rather than [Beijing] contributing to a comprehensive CT strategy in Mali, participants found that 'keeping a low profile' has thus far been crucial in China's CT efforts."[92]

However, it is worth noting that while many observers view China's role in U.N. PKOs as helping bolster its overall security profile on the continent, as has been the case with other international actors in U.N. PKOs, China has also been barred from counterterrorism hotspots in Africa, especially Mali, thus limiting its influence via counterterrorism cooperation generally. For instance, according to the latest available numbers (as of May 31, 2025), of the 1,776 U.N. PKO troops China had deployed, the vast majority were part of the UN Mission in South Sudan (UNMISS) (1,031 troops), Lebanon (UNIFIL) (475), and the disputed Abyei region between Sudan and South Sudan (UNISFA) (270), none of which features terrorism as a primary source of conflict. Instead, it has only 18 personnel—a combination of experts, police, and staff officers—in the two terrorism-centric African PKOs in the Central African Republic (MINUSCA) and the DRC (MONUSCO).[93] Put otherwise, while China uses PKOs to learn about the African security environment, it is limited in how much these can be used to get an up-close look at the dynamics of terrorism, given the exodus of foreign actors from such missions today.

Basing

While China's military base in Djibouti is rarely considered for its potential counterterrorism-related role, it should not be overlooked. China opened its first overseas base in Djibouti in 2017, promising that it was intended solely for economic purposes to support its growing international investment portfolio, asserting in 2010 that "the idea that the Chinese would establish overseas bases was groundless"[94] and the location in Djibouti was a "support facility intended to help logistics resupply for Chinese PLA Navy (PLAN) vessels."[95] Yet after opening, the rationale shifted to include roles in counterpiracy missions, assisting the PLA in its role in African PKOs, and humanitarian missions. It would soon also go from being referred to as a "support facility" to a "support base."[96] Between 2017 and 2020, the PLA was then shown to be conducting numerous live-fire exercises in Djibouti, and by 2020, the PRC announced that the PLANMC (People's Liberation Army Navy Marine Corps) had deployed a special operations force (SOF) unit to Djibouti.[97] Intuitively, a SOF presence was a logical next step for counterterrorism operations. Indeed, as recently as April 2025, Djibouti and China conducted joint counterterrorism exercises.[98]

Outside of Djibouti, China is looking to establish another military base, likely with a smaller footprint, likely in the Gulf of Guinea.[99] Reports have emerged of its talks with Equatorial Guinea and Gabon.[100] While neither of those states faces counterterrorism crises, their authoritarian governance structures combined with their proximity to the terrorism-beset Sahel would lead Beijing to have an ideal launching pad for CT operations if it so chose. Moreover, in the Sahel, China has been shown to have some degree of

[a] In this instance, Egypt and China signed a security cooperation protocol, focusing on regional security and "crimes in all their forms," which include mutual security concerns that generally involve terrorism.

interest in the lesser-considered coastal West African states of Benin and Togo, which are currently battling to stem the tide of al-Qa`ida (JNIM)-related threats from entering their northern borders. In addition to documented discussions on counterterrorism in both countries,[101] China has been shown to have donated four Norinco PMR-50 reconnaissance drones to Benin (March 2023) to monitor terrorist groups' movements and four howitzers (August 2024) to help bolster the country's defenses against the groups.[102]

As concerns the search for new bases in proximity to the Sahel, some analysts have surmised that the PRC may actively look for African partners that allow multiple foreign partners to base there,[103] suggesting either that it seeks to partner with other international powers, or, conversely, that it seeks proximity to other international military presence to gather additional intelligence, which the FBI has emphasized is a concern.[104]

Bilateral and Multilateral Training Drills

Perhaps the most visible moves that China has taken to bolster its CT credentials in Africa as of late have been its leading of bilateral and multilateral counterterrorism drills between African countries, akin to what it has been doing in Central Asia for years. The banner events in this regard were the trilateral Peace-Unity Drills between China, Tanzania, and Mozambique. Running in July and August 2024 in Tanzania, the Peace-Unity Drills of 2024 were focused on joint counterterrorism military operations and enhancing participating countries' ability to conduct counterterrorism operations. The 2024 drills were the fourth iteration of China's Peace-Unity Drills with Tanzania, with previous iterations having been held in 2014, 2019/2020, and 2023.[105] Of note, the 2014[106] and 2023[107] iterations stated a focus on counterterrorism.[b]

The 2024 exercises were comprised of two phases of training. The first was the sea phase, which consisted of nine operations, including port joint defense; counterterrorism tactics; visit, board, search, and seizure (VBSS) operations; anti-terrorism and anti-piracy; and joint maritime patrols. Aside from the military operations, the PLA held open vessel days for the public in Tanzania to come aboard the ships, intending to promote its cultural diplomacy efforts and demonstrate its "blended approach" to military diplomacy.[108] The second, land phase, focused on counterterrorism. As one analyst describes:

> *The land phase took place at the PRC-built combined training center in Mapinga, Tanzania. It centered on counterterrorism operations and was divided into four stages: joint specialty training …, combined command, tactical training, and live-fire drills. During the joint specialty training component, units from the TPDF and the PLA 82nd Group Army participated in an equipment-instruction module. PLAA soldiers displayed and provided instruction on more than 23 different types of weapons and equipment, including small arms, micro unmanned aerial vehicles, and various engineering, reconnaissance, communication, and infantry vehicles. As part of this event, both sides trained together on counterterrorism concepts and modern battlefield tactics, techniques, and procedures.*[109]

This phase consisted of exercises such as joint combat planning, infiltration and reconnaissance, stealth assault and rescue, and decapitation and arrest.[110] It also showcased a variety of light arms, many different infantry fighting vehicles, assault vehicles, command vehicles, communications vehicles, explosive ordnance disposal vehicles, and drones.[111] Indeed, the drills, which were hailed as representing a "significant increase in scope and scale" of Chinese engagement,[112] are perhaps the clearest signal yet of China's bid to establish itself as a CT player in Africa.

Finally, it is worth stating that the two partner countries of choice—Tanzania and Mozambique—were reasonable ones. With shared socialist and communist affinities, Tanzania has been one of China's most important African military allies, having been a training partner with China in three other iterations of the drills, as described above. In an upcoming study from the U.S. Army's Foreign Military Studies Office, China receives a relatively rare "high" degree of military influence in Tanzania.[113] For its part, Mozambique, Tanzania's resource-rich but terrorism-troubled southern neighbor, is an intuitive collaborator. With an enduring but contained threat of terrorism in Mozambique from the Islamic State-affiliated Al-Sunnah (also known as Islamic State-Central African Province - Mozambique, or ISCAP-M), Mozambique could be an ideal laboratory for China to test out counterterrorism tactics in a generally under-considered theater.

Police Training

Another primary means by which China is inserting itself into the African CT space is via police training, which Beijing uses as yet another means to avoid being seen as overly aggressive instead of more traditional military training. As Paul Nantulya has described, China has taken a wide-ranging interest in training African police. Informed by China's understanding of the nature of terrorism and the aforementioned "Three Evils," China's police training in African states is similarly based on these ideals: curbing "terrorism," separatism, and religious extremism.[114] But indeed, more than merely aligning on understandings of the *nature of terrorism*, China's inroads in African CT are abetted by the similar *structures* that mark the role of police in fighting counterterrorism. As Nantulya describes:

> *African police entities are centralized under the executive and overseen by an interior, police, or public security minister like in China. Most African police are also part of the national security architecture and tend to be highly militarized in their basic organization, ranking system, and work methods. Many African police jurisdictions, furthermore, are organized into "commands," and it is common for police to deploy into the military and vice versa.*[115]

Indeed, between 2018 and 2021, some 2,000 African police received Chinese training from across 21 police academies associated with China's Ministry of Public Security.[116]

Intelligence and Surveillance

One of the hallmarks of China's domestic counterterrorism strategies in Xianjing has been its focus on surveillance and monitoring of Uyghur and other populations. Another understudied phenomenon of China's engagement in African CT relates to its provision of similar surveillance techniques to African states. Most notably, China's eagerness to provide "Smart City" technology to African states[117]—which improves urban security

[b] Open-source research did not reveal a CT focus for the 2019/2020 "Sincere Partners" exercise. Instead, it is referred to as an event to upgrade military capabilities and build on China and Tanzania's partnership. See Chen Lufan, "China, Tanzania conclude 'Sincere Partners 2019' joint military training," Ministry of National Defense of the People's Republic of China, January 21, 2020.

"A primary boon for China in African CT is that it does not have the same burden of history as other actors: It has only a minimal reputation as a security actor on the continent, and most of that reputation is generally positive and uncontroversial."

and efficiency, but which can also be used to closely track citizen movement—speaks to its future CT ethos. For instance, reports have emerged of African governments using Chinese technologies specifically to surveil dissenters,[118] track political opponents, and suppress protests, particularly in Ethiopia, Uganda, and Zambia.[119] China has elsewhere been shown to have controversially engaged in intelligence-sharing with Egypt, including Chinese intelligence officers collaborating with the Egyptian state to interrogate Chinese students at an Egyptian prison in 2022.[120] More broadly, China's outsized role in African information and communications technology (ICT) namely through its state-owned Huawei telecommunications company, is consistently one of the primary instruments that this author and colleagues have found that China uses to exert military influence in Africa.[121] On the use of smart technologies for CT purposes explicitly, in July 2021, China's EXIM bank launched the $94 million "Smart Burkina Faso" project (in conjunction with Huawei Technologies and China Communications Construction Group Co. Ltd.,) to install a 650km fiber optic network and 150km metro access network in the country,[122] which also included the installation of around 900 surveillance cameras to curb urban crime and, importantly, improve counterterrorism efforts.[123]

Economic Development

Finally, while not traditionally conceived of as a counterterrorism measure, for Beijing, its broader ethos of prioritizing economic development is part and parcel of a bid to reduce terrorist threats. Conceptually, China's view of terrorism is that it is undergirded by poverty and underdevelopment.[124] As a result, one of Beijing's underlying approaches to counter radicalization and deradicalization[125] is economic development.[126] Remarks in November 2022 from China's Ambassador, Xhang Jun, at a U.N. Security Council High-Level meeting on counterterrorism in Africa underscore this vision:

> *We should address both the symptoms and the root causes of terrorism. Military and security means alone cannot fully and completely eliminate the threats of terrorism. We must focus on the reality on the ground in Africa, with a view [to] adopting a systematic governance approach to implement integrated measures. The Sahel and the Lake Chad region are highly representative. The local economies [are] comparatively underdeveloped, and the people there have difficulties in making [a] living. So terrorist forces take advantage of the situation, and target unemployed poor youth from underprivileged background[s] for recruitment. The international community should take measures to support Africa's development with a greater sense of urgency. The UN should listen to Africa and give more prominence to the importance of the development agenda, and raise favorable environment to enable Africa's development.*[127]

Notably, in the speech above, Ambassador Jun made clear that China views the antidote to the rise of African terrorism as economic development, which China can provide via the BRI.[128] In practice, China has claimed that it would not levy tariffs on most incoming goods from the Least Developed Countries (LDCs), like Burkina Faso, linking the tariff reduction to combating terrorism.[129] China would make similar linkages in a March 2023 speech at the United Nations.[130]

Part III: Examining Rationales for Chinese Interest in African CT

Having understood the evolution of how China thinks about CT and the real-world instances of how it is increasingly engaging in African CT, the question bears asking: What rationales undergird China's newfound interest in African counterterrorism efforts?

At its core—and despite varying other proffered rationales such as protection of investments and citizens on the continent[c]—China's burgeoning new engagement in African CT is primarily about diversifying pathways to influence in Africa. To date, China's means to gain influence in Africa have been heavily economically focused. Indeed, even among the tools that it could use to gain *military* influence, data from the M-DIME Research Project, which this author co-leads, underscores China's lopsided emphasis on using economic ("E") tools in attempts to gain military influence in third-party states (through investment in strategic minerals and materials, strategic infrastructure development, and foreign military sales). In contrast, by far, this research shows that China's least-used tools of military influence are the most typically military ("M") tools, (such as formal defense treaties and joint bilateral and multilateral training exercises.) Having broadly cornered the market on external economic influence, Beijing is now seeking new pathways to cement its presence via more traditional, though tempered, military means.

However, beyond the need to diversify its means of influence in Africa, other rationales are likely at play. First, and related to the above, one can understand China's push for CT influence through the lens of its geopolitical rise and its desire to see itself serve as an alternative pole of power in the international security sphere. As articulated in the GSI, China is explicitly trying to carve out a leadership role for itself in the realm of international security. To that end, it could well be the case that, as an aspiring global power, it views itself as being unable to continue to effectively sit on the sidelines on one of the thorniest international security issues—African terrorism—if it truly wants to assert itself as a global security leader. In other words, while its demure approach to engagement in lower-level African security has worked to this point, Beijing may now view it as necessary to take bolder action than it has to date in order to show that it is truly listening to African concerns and working in earnest to address them. Simultaneously, a primary boon for China in African CT is that it does not have the same burden of history as other actors: It has only a minimal

[c] Yet, it should not be overlooked that China does have real economic concerns: Its workers and projects are genuinely vulnerable to certain violent African non-state actors, though in no place is the threat so significant that national-level counterterrorism engagement would be imperative.

reputation as a security actor on the continent, and most of that reputation is generally positive and uncontroversial.

Second, one might understand China's desire for African CT engagement through a military planning lens. China, considering an invasion of Taiwan, needs quick, on-the-ground combat experience, and Africa's conflict-prone pockets offer relatively low-stakes training grounds. Indeed, as China has set its sights on a potential invasion of Taiwan by 2027 or 2030,[131] it has notably little real-world combat experience outside of the Indo-Pacific. As Beijing considers its capacity to operate kinetically in the future, having experience is important. As noted earlier, observers have already pointed to the fact that Africa has long served as a sort of Chinese military laboratory,[132] with some suggesting that China's deployments in U.N. peacekeeping missions as well as its increased air drills with Egypt[133] serve as pathways for it to gain experience in new theaters.

Third, China might also be compelled to enter the African CT fight as a matter of opportunistic timing. A confluence of geopolitical realities may be signaling to Beijing that the time is ripe for new action. As terrorism rises to unprecedented levels in the Sahel and continues strong elsewhere,[134] it is also the case that the stalwart external actors assisting African countries in their counterterrorism efforts—the United Nations, France, the United States, and, newly, even Russia—are now being ousted. While the challenges of African counterterrorism lamentably grow by the day, especially related to the increased movement of actors associated with JNIM into coastal and western West Africa, any continuity of external actor involvement to help aid in CT efforts is in chaos. Therefore, China may have strategic calculations related to timing. Indeed, as AFRICOM Commander General Michael Langley said in May 2025 of China's military presence in Africa in response to the current moment of U.S. retrenchment: "They're stepping it up and trying to replicate every type of thing, whether it be advise-and-assist type of training and specialized military domains, or putting on exercises like they did in the fall."[135] Simultaneously, Langley has also implored allied partner nations to help fill in the gaps the United States has left.[136] Indeed, as this author has argued elsewhere, China, not Russia, is the next greatest military partner likely to threaten U.S. presence in Africa.[137]

Part IV: Challenges for Chinese Engagement in African CT

Despite some of the reasons presented above that indicate the rationality of a more forceful Chinese entrance into African CT, many challenges remain. First, and most broadly, is the question of just how deeply China seeks to wade into the fraught waters of African counterterrorism in the pursuit of an alternate, non-economic avenue of influence. With truly deep engagement, at some point China will be forced to reconcile its cautious approach with the brutal realities and difficult decisions incumbent in the African terrorism space. Indeed, China has historically shown clear reluctance for deep kinetic CT engagement in other partner nations, even when its interests are directly affected. For instance, in Pakistan, where Chinese nationals working as part of China's BRI have been attacked and killed in sundry instances, China has shown an unwillingness for a direct kinetic response, akin to its ethos in sub-Saharan Africa.[138] Instead, Beijing has responded by paying ransoms to violent non-state actors; pressuring leaders to provide better security; and offering surveillance technology.[139] It thus remains a question as to how it would prove itself a forceful, prevalent player while also remaining cautious and non-controversial: Its risk-averse, economic-first approach to CT may well prove to be too meager—all carrot and no stick—to deal with the brutality of the current African terrorism scene. At a certain point, China will likely have to cross a perilous bridge: take bolder, riskier, and more muscular and militarized approaches to CT, or stay the course, be perceived as weak, and ultimately, likely be ineffective.

"It thus remains a question as to how [China] would prove itself a forceful, prevalent player while also remaining cautious and non-controversial: Its risk-averse, economic-first approach to CT may well prove to be too meager—all carrot and no stick—to deal with the brutality of the current African terrorism scene. At a certain point, China will likely have to cross a perilous bridge: take bolder, riskier, and more muscular and militarized approaches to CT, or stay the course, be perceived as weak, and ultimately, likely be ineffective."

Beyond the *depth* of engagement, there is also the question of the *breadth* of engagement: Would China be willing to take on a major degree of responsibility for a given operational environment—akin to the United States in Somalia or France in the Sahel—or would it seek to be a more present partner among many different theaters? To date, it has shown little deep commitment to any particular African country or theater beset by terrorism.

Second, even if China does decide that it seeks much deeper and broader engagement in Africa, does China have a model of CT that could actually be effective, and what exactly would be its novel value proposition for African states? To be clear, despite its engagement in training, in reality, China has limited experience in CT outside its borders. To the extent that China has any real background in CT, it is in dealing with the Uyghur minority, both within its own borders and in neighboring states. It has a smattering of engagement in the proximity of terrorism in U.N. peacekeeping missions in Mali, for instance. Apart from that, it has scarce real-world CT experience akin to that of the United States, France, or Russia. That said, what seems to be the most likely case scenario is that if China does become involved in African CT, there will somehow be an "economics-first" approach, akin to what it has done elsewhere in its engagement in African security.

Third, if China does become involved in African CT, will there be a China-Russia clash in terms of CT? An emerging organizing principle of the analysis of contemporary geopolitics focuses on the analytical unit of the so-called CRINK alliance, between China, Russia, Iran, and North Korea. At its core, this nominal alliance is worrisome precisely because it puts the four major U.S. state adversaries in a cooperative relationship with one another. While some commentators have referred to the CRINK Alliance as a new "axis of disorder," "Axis of Evil 2.0," "axis of autocracy," "unholy alliance," or even "Legion of Doom,"[140] others have emphasized the tenuousness of the alliance,[141] underscoring that, depending on the issue area, cooperation between the countries constitutes a convenience of interests rather than abiding alignment of priorities.[142] Thus, in African CT, where Russia has become the influencer *du jour* in places such as Mali, Niger, and Burkina Faso, its agenda could theoretically come into conflict with that of China. However, despite that potential scenario, in the work that this author and colleagues have undertaken investigating Chinese and Russian military influence globally via the M-DIME Research Project, there is no clear evidence of any real discord or competition between China and Russia in the military or counterterrorism space. This may be a non-issue.

Fourth, will China engage with pariah countries on CT? One of the most vexing counterterrorism issues in Africa at the moment is the fact that the most terrorism-afflicted countries, in the Sahel, are also run by a consortium of antagonistic military juntas. These juntas, operating under the aegis of the Alliance of Sahelian States (AES), have ousted the United Nations, France, and the United States, and broadly welcomed in Russia and the Wagner Group/Africa Corps as replacements, to poor results for civilians and overall security. One challenge that China would face if it were to become more deeply involved in African CT would be just how far, if at all, it would engage with these pariah regimes. China has thus far played a cautious, even-handed, non-controversial security role on the continent. If it were to engage in CT, at least in a serious way, it would have to make a hard choice: Engage with these pariah regimes and go after terrorism in a serious way, or skirt collaboration and thus operate on the margins of the continent's real security problems. If history is any guide, this might not be as fraught a prospect as it might seem. Historically, China has proven to be agnostic to state regime; intuitively, it has little desire or space to critique autocrats. Indeed, in the aftermath of Western withdrawals of Sahelian states of late, China has been quick to step in, appointing its first defense attaché to Niger in February 2025.[143]

Conclusion and Implications

This article has shown that despite its historically overwhelming focus on economic influence, China is quietly and increasingly pursuing a role as the primary external security actor in Africa, including in the often-fraught space of counterterrorism assistance. But what are the potential impacts of this push for actors outside China?

For African citizens and states, the impact of China's CT push remains unclear. Certain observers have suggested that the PRC's expanding military presence in Africa more generally risks "negatively affecting African nations' sovereignty by weakening areas of governance, human rights, and regional cooperation."[144] However, China's CT approach has thus far exhibited none of the more worrisome dimensions of Russia's approach and could indeed accrue benefits for African citizens at risk of violence. A more responsible, less-militarized Chinese presence may well serve to offer increased protection to African citizens.

Globally, perhaps one of the greatest impacts of China's push to become a major CT player in Africa is that Beijing will increasingly dictate how the world conceptualizes the appropriateness of various CT paradigms and actions. In line with the broader ethos of the GSI, China is solidifying an alternative paradigm for 21st-century global security relations to replace the ever-sclerotic post-WWII order once led by the United States and NATO allies. Though its engagements in African CT are but a microcosm of this push, China's desire for an all-encompassing approach to the use of whole-of-state tools to shape the civilian environment for China's overall national interests is what Paul Nantulya describes as "military political work" (*jundui zhengzhi gongzuo*).[145] While he investigates this phenomenon through China's provision of professional military education, it is clear enough that this strategy pervades every Chinese interaction, including in international fora.

For the United States, China's rise as an aspiring counterterrorism force in Africa should cause concern.[146] China is the primary U.S. military pacing threat,[147] largest economic global competitor, and the state most likely to unseat the United States from its role as the global leader. China's rise in African CT could allow it to replace the United States as a preferred security partner; to minimize U.S. access to markets; and more broadly chip away at the global security posture and normative agenda of the United States.[148] Moreover, an increased Chinese presence in African CT has the potential to serve as a logical inroads for China to expand the activities at its current base in Djibouti; to make the case further for the base it is ostensibly pursuing in Equatorial Guinea or Gabon; or to compel terrorism-afflicted states, especially in the Sahel, that they should allow Beijing to open a base there. More generally, for better or worse,[149] one of the primary ways that the United States has retained some degree of military influence in Africa over the past two decades has been via counterterrorism assistance. A deeper Chinese CT presence in Africa could fundamentally undermine U.S. security relationships on the continent.

While it is clearly the case that the United States should be concerned since this Chinese push is indicative of its pursuit of global ambitions,[150] Washington's own self-retrenchment from international affairs, especially in Africa, is serving to facilitate Beijing's ambitions of influence. Washington cannot have it both ways. It cannot both seek to retrench from Africa militarily and diplomatically but also openly fret about losing influence to China globally. Either the United States needs to commit to a serious and sustained military and counterterrorism assistance presence or make peace with the fact that it is ceding counterterrorism influence to China in Africa, and pursue other means of African alliance building. The latter may not be a bad option.

To conclude, what is perhaps the most interesting phenomenon to observe at the current moment is the flip-flopping of the historical approaches to African counterterrorism: China, historically the economic juggernaut, is now trying to get into CT, while the United States, historically the CT-first external power, is now taking an economics-first approach. Meanwhile, Russia, which had been the CT player *du jour*, is now on the outs, as is France, all while Turkey surges in its own efforts. Whether China will succeed—whatever 'success' looks like—in establishing itself in African counterterrorism, a historical folly for external powers, remains to be seen. CTC

Citations

1 Jason Warner, "The Counterterrorism-as-Influence Competition in Africa," Lawfare, October 5, 2024.

2 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).

3 Nathaniel Powell, "Why France Failed in Mali," War on the Rocks, February 21, 2022.

4 "Last remaining members of G5 Sahel move to dissolve the anti-jihadist alliance," News Wires, June 12, 2023.

5 "Sahel dominates top 10 countries most impacted by terrorism," Vision of Humanity, March 4, 2025.

6 Christopher Faulkner, "Undermining Democracy and Exploiting Clients: The Wagner Group's Nefarious Activities in Africa," *CTC Sentinel* 15:6 (2022).

7 Jason Warner, Stephanie Lizzo, and Julia Broomer, "Assessing U.S. Counterterrorism in Africa 2001-2021: Summary Document of CTC's Africa Regional Workshop," Combating Terrorism Center, West Point, February 4, 2022.

8 "Mali accuses France of training 'terrorists' in the country," Al Jazeera, October 8, 2021; "Niger coup leaders accuse French forces of destabilising the country," Al Jazeera, August 9, 2023.

9 Matthew Kirwin, Lassane Ouedraogo, and Jason Warner, "Fake News in the Sahel: 'Afrancaux News,' French Counterterrorism, and the Logics of User-Generated Media," *African Studies Review* 65:4 (2022): pp. 911-938.

10 Tony Chafer, Eloise Bertrand, and Ed Stoddard, "France's Strategic Failure in Mali: A Postcolonial Disutility of Force," Royal United Services Institute, February 7, 2024.

11 Paul Melly, "Niger coup leaders expel French, but not US, troops fighting jihadists," BBC, December 20, 2023.

12 Thiam Ndiaga, "Burkina Faso marks official end of French military operations on its soil," Reuters, February 20, 2023.

13 "French troops to exit Senegal by end of 2025," Al Jazeera, February 12, 2025.

14 Shola Lawal, "Frexit: Why Ivory Coast is joining African campaign to expel French troops," Al Jazeera, January 3, 2025.

15 Moki Edwin Kindzeka, "Chad officials say French troops have finally left after 70 years' presence," VOA News, January 31, 2025.

16 Haley Britzky, "US military completes withdrawal from Niger," CNN, September 16, 2024.

17 Jason Burke, "Russian mercenaries behind slaughter of 500 in Mali village, UN report finds," *Guardian*, May 20, 2023; Tim Lister, Sebastian Shukla, and Clarissa Ward, "Russian mercenaries accused of atrocities in the Central African Republic," CNN, June 15, 2021.

18 Nkechi Ogbonna, "Wagner Group to withdraw from Mali after 'completing mission,'" BBC, June 6, 2025.

19 Carla Freeman and Bates Gill, "China's Bid for a Bigger Security Role in Africa," United States Institute of Peace, September 12, 2024.

20 "Full text: Xi's speech at opening ceremony of 2024 FOCAC summit," CGTN, September 5, 2024.

21 Jason Warner, "China's Counterterrorism Ambitions in Africa," Lawfare, December 22, 2024.

22 Paul Nantulya, "The Growing Militarization of China's Africa Policy," Africa Center for Strategic Studies, December 2, 2025; Jason Warner, "China, Not Russia, Is the Next Major U.S. Military Competitor in Africa," Lawfare, December 22, 2024; Freeman and Gill.

23 Alessandro Arduino, "China-Africa Military and Private Security," GIS Reports Online, December 6, 2024.

24 Alessandro Arduino, "China's Cautious Expansion of Military Diplomacy in Africa," ThinkChina, August 21, 2024.

25 Alessandro Arduino, "China's Expanding Security Footprint in Africa: From Arms Transfers to Military Cooperation," ISPI, September 30, 2024.

26 Timothy Ditter, "Africa is China's Testing Ground for Overseas Military Missions," CNA, October 10, 2024.

27 While scholars have not written on this topic as widely as one might imagine, notable pieces include Corbus Van Staden, "Chinese Counterterrorism in Africa," Stimson Center, July 31, 2024, and Jean-Pierre Cabestan, "China's Involvement in Africa's Security: The Case of China's Participation in the UN Mission to Stabilize Mali," *China Quarterly* 235 (2018): pp. 713-734.

28 "Chinese Social and Political Thought," Stanford Encyclopedia of Philosophy, last modified January 21, 2024.

29 "E. Turkistan group 'behind' terror attack," China Daily, August 6, 2008.

30 Sui-Lee Wee, "Chinese Police Blame Separatist Group for Urumqi Bombing: Xinhua," Reuters, May 18, 2014.

31 Jonas Bernstein, Vladimir Socor, and Stephen Foye, "Uighur 'International Terrorists' Sentenced in Bichkek," Jamestown Foundation, January 10, 2002.

32 Carrie Gracie, "The knife attack that changed Kunming," BBC, July 16, 2014.

33 Beina Xu, Holly Fletcher, and Jayshree Bajoria, "The East Turkestan Islamic Movement (ETIM)," Council on Foreign Relations, last updated September 4, 2014.

34 Zachary Abuza, "The Uyghurs and China's Regional Counter-Terrorism Efforts," Jamestown Foundation, *Terrorism Monitor* 15:6 (2017).

35 "China 2019 International Religious Freedom Report," U.S. Department of State, 2019.

36 "U.S.-China Counterterrorism Cooperation: Issues for U.S. Policy," Congressional Research Service, July 15, 2010.

37 For history of the evolution of China's legal approach to counterterrorism, see "Full text: China's Legal Framework and Measures for Counterterrorism," State Council Information Office of the People's Republic of China, January 23, 2024.

38 For the full text of the Chinese Counterterrorism Law, see "Chinese Counter-Terrorism Law (as amended in 2018)," China Law Translate (website), April 27, 2018.

39 Ibid.

40 Sheena Chestnut Greitens, Myunghee Lee, and Emir Yazici, "Counterterrorism and Preventive Repression: China's Changing Strategy in Xinjiang," *International Security* 44:3 (2020): pp. 9-47.

41 Colin P. Clarke and Paul Rexton Kan, "Uighur Foreign Fighters: An Underexamined Jihadist Challenge," International Centre for Counter-Terrorism, November 2017.

42 Abuza.

43 Greitens, Lee, and Yazici.

44 Abhishek Mishra, "From Xinjiang to the Frontier: China's Evolving Counterterrorism Strategy," ORF Online, February 20, 2025.

45 Dante Schulz, "China Advances Security Apparatus in Tajikistan in the Aftermath of the Taliban Takeover," Caspian Policy Center, November 5, 2021.

46 Lu Peng and Wu Shike, "China, Tajikistan conclude joint counterterrorism drill," Chinese Ministry of Defense, August 16, 2019.

47 Edward Lemon and Ruslan Norov, "How China Is Adapting to Tajikistan's Demand for Security Cooperation," Carnegie Endowment for International Peace, March 20, 2025.

48 Kate Bartlett, "How Chinese Private Security Companies in Africa Differ from Russia's," VOA News, March 31, 2023.

49 Ibid.

50 Ditter, Haney, Tsai, and Reid, p. 4.

51 Jean-Pierre Cabeston, "China's Involvement in Africa's Security: The Case of China's Participation in the UN Mission to Stabilize Mali," *China Quarterly* 235 (2018).

52 Jean-Fernand Koena and Krista Larson, "Gunmen kill 9 Chinese at mine in Central African Republic," Associated Press, March 19, 2023.

53 Kate Bartlett, "Chinese Working in Africa Face Threat of Kidnapping," VOA News, May 24, 2022.

54 Ditter, Haney, Tsai, and Reid, p. 4.

55 "China's National Defense in the New Era," State Council Information Office of the People's Republic of China, July 24, 2019.

56 Adina Masalbekova, "How China is Leveraging Security Cooperation in Central Asia," United States Institute of Peace, September 9, 2024.

57 Warner, "China's Counterterrorism Ambitions in Africa."

58 "The Global Security Initiative Concept Paper," Embassy of the People's Republic of China in Costa Rica, February 22, 2023.

59 Liu Yuxi, "Statement by Liu Yuxi, Special Representative of the Chinese Government on African Affairs, at the High-Level Open Debate on 'Countering terrorism and preventing violent extremism through strengthening cooperation between the UN and regional organizations,'" Permanent Mission of the People's Republic of China to the UN, March 28, 2023.

60 Warner, "China, Not Russia, Is the Next Major U.S. Military Competitor in Africa."

61 Hana Saada, "Chinese Police Delegation Visits Algeria's Elite Special Operations Command," Dzair Tube, February 6, 2025.

62 "Xi Jinping Holds Talks with President of Benin Patrice Athanase Guillaume Talon," Ministry of Foreign Affairs People's Republic of China, September 1, 2023.

63 Xinhua, "China hopes to ink BRI cooperation documents with Burkina Faso soon: Chinese FM," State Council Information Office, People's Republic of China, June 11, 2021.

64 "Xi Jinping Holds Talks with President of Benin Patrice Athanase Guillaume

Talon.”

65 “Xi Jinping Meets with Cameroonian President Paul Biya,” Ministry of Foreign Affairs, People’s Republic of China, September 4, 2024.

66 “Djibouti Strengthens Unique Strategic Partnership with China, Renegotiates Military Agreement,” Dawan Africa, September 11, 2024.

67 “President El-Sisi Meets China Minister of Foreign Affairs,” State Information Service, January 15, 2023.

68 “Egyptian Interior Minister, Chinese security delegation discuss cooperation,” State Information Service, June 6, 2024.

69 Xinhua, “China vows to deepen counterterrorism, law enforcement cooperation with Egypt,” State Council, People’s Republic of China, October 30, 2024.

70 “China and Egypt Hold the Third Counter-Terrorism Consultations Between Their Ministries of Foreign Affairs,” Ministry of Foreign Affairs People’s Republic of China, April 23, 2025.

71 “The Gambia: Govt initiates security talks with Russia to address rising terrorism threats,” West Africa Democracy Radio, February 1, 2024.

72 “Mali, China affirm commitment to FOCAC 2024 pledges,” APA News, June 19, 2025.

73 “China strengthens military ties with Niger amid western withdrawal,” Tactics Institute for Security and Counter Terrorism, March 23, 2025.

74 “Tunisia, China: reviewing security cooperation,” Ministry of Interior in Tunisia, May 26, 2023.

75 “Togo: des échanges avec le secteur de la défense chinois,” Togo First, September 9, 2024.

76 “Terrorism: FG Signs MOU with China on Military Aid,” Ministry of Defense of Nigeria, December 3, 2020.

77 Claire Mom, “China to help Nigeria fight money laundering, terrorism financing,” Cable, September 4, 2024.

78 “Egypt, China sign protocol to enhance security cooperation,” State Information Service, November 1, 2024.

79 “China boosts Benin’s Counter-Terrorism Efforts with Military Equipment Donation,” Ecofin Agency, August 26, 2024.

80 Paul Nantulya, “China’s Policing Models Make Inroads in Africa,” Africa Center for Strategic Studies, May 22, 2023.

81 Yuxi.

82 Carla Freeman, Bates Gill, and Alison McFarland, “China and the Reshaping of Global Conflict Prevention Norms,” United States Institute of Peace, September 12, 2023.

83 Warner, “China’s Counterterrorism Ambitions in Africa.”

84 Layla Ali, “Opportunities and Limits of the China-Arab States Cooperation Forum,” Gulf Research Center, June 2024.

85 “Remarks by China’s Permanent Representative to the UN Ambassador Fu Cong at the UN Security Council High-Level Open Debate on African-led and Development-focused Counter-terrorism,” Ministry of Foreign Affairs, People’s Republic of China, January 21, 2025.

86 Monika Krukowska, “China’s security relations with Africa in the 21st century,” *Security and Defence Quarterly* 46:2 (2024): pp. 4-23.

87 Ibid.

88 Cabeston.

89 Frans-Paul van der Putten, “China’s Role in Peacekeeping and Counter Terrorism in Mali,” Clingendael, April 30 - July 21, 2025.

90 Zhou Bo, “How Africa became a test lab for China’s approach to global peacekeeping,” *South China Morning Post*, August 8, 2019; Krukowska.

91 Krukowska, pp. 4-23.

92 Van der Putten.

93 “Troop and Police Contributors,” UN Peacekeeping, n.d.

94 Ditter, Haney, Tsai, and Reid, p. 7.

95 Ibid., p. 8.

96 Ibid., p. 8.

97 Ibid.

98 “China, Djibouti conducts joint military training on counter-terrorism,” Bastille Post, May 2, 2025.

99 Ditter, Haney, Tsai, and Reid, p. 10.

100 Maureen Farrell, “SOF Effectiveness in Strategic Competition: Insights for West Africa and Beyond,” JSOU Press, January 6, 2025.

101 “Xi Jinping Holds Talks with President of Benin Patrice Athanase Guillaume Talon;” “Togo: des échanges avec le secteur de la défense chinois.”

102 “China boosts Benin’s Counter-Terrorism Efforts with Military Equipment Donation.”

103 Ditter, Haney, Tsai, and Reid.

104 “The China Threat,” Federal Bureau of Investigation, n.d.

105 Guy Martin, “Joint Military Exercise Between China, Mozambique and Tanzania Underway,” Defence Web, August 2, 2024.

106 “China and Tanzania conclude historic naval exercise,” Defence Web, November 18, 2014.

107 Lin Congyi, ““Transcend–2023” China-Tanzania joint training concludes,” China Military Online, September 18, 2023; “Chinese and Tanzanian Marine Corps Engage in Hand-to-Hand Combat Training,” China-Arms, September 21, 2023.

108 “China’s drills with Tanzania and Mozambique show ‘blended approach’ to military diplomacy,” *South China Morning Post*, August 4, 2024.

109 Jake Vartanian, “Peace and Unity: China’s Growing Military Footprint in Tanzania,” Strategic Studies Institute, U.S. Army War College, October 9, 2024.

110 Liu Xuanzun and Guo Yuandan, “China-Tanzania joint military drill kicks off, ‘reflects Chinese continental power projection capabilities,’” Global Times, July 30, 2024.

111 Ibid.

112 Vartanian.

113 Lucas Winter, Jason Warner, and Alexander Tsioutsias, “Instruments of Chinese Military Influence in Tanzania,” U.S. Army, Foreign Military Studies Office (forthcoming).

114 Nantulya, “China’s Policing Models Make Inroads in Africa.”

115 Ibid.

116 Ibid.

117 Jason Warner and Toyosi Ajidbade, “China’s Smart Cities in Africa: Should the United States Be Concerned?” CSIS, November 18, 2024.

118 Mohammed Yusuf, “China’s Reach Into Africa’s Digital Sector Worries Experts,” VOA News, October 22, 2021.

119 Warner and Ajidbade.

120 Nantulya, “China’s Policing Models Make Inroads in Africa.”

121 See, for instance, Lucas Winter, Jason Warner, and Benjamin Katz, “Instruments of Chinese Military Influence in Uganda,” U.S. Army Foreign Military Studies Office, May 2025.

122 DU Xiaohui, “The #SMARTBurkina project was officially launched recently . . .,” X, July 12, 2021.

123 Rebecca Arcesati, “China’s rise in digital governance: Deploying technology to deliver public goods at home and abroad,” Mercator Institute for China Studies, March 2022.

124 Van der Putten.

125 Ibid.

126 Warner, “China’s Counterterrorism Ambitions in Africa.”

127 “Remarks by Ambassador Zhang Jun at the UN Security Council High-Level Debate on ‘Counter Terrorism In Africa,’” Permanent Mission of the People’s Republic of China to the UN, November 10, 2022.

128 Ibid.

129 Ibid.

130 Warner, “China’s Counterterrorism Ambitions in Africa.”

131 Kyle Amonson and Dane Egli, “The Ambitious Dragon: Beijing’s Calculus for Invading Taiwan by 2030,” Air University, April 24, 2023.

132 Ditter, Haney, Tsai, and Reid.

133 Darek Liam, “China, Egypt Begins Inaugural Joint Air Exercise ‘Civilization Eagle 2025,’” Military Africa, April 20, 2025.

134 “Global Terrorism Index 2025,” Institute for Economics and Peace, 2025.

135 Meghann Myers, “AFRICOM asks for help deterring terrorism, after Trump pulls aid to allied countries,” Defense One, May 29, 2025.

136 Ibid.

137 Warner, “China, Not Russia, Is the Next Major U.S. Military Competitor in Africa.”

138 Neeraj Singh Manhas, “Amid Geopolitical Tensions, Baloch Militant Attacks Undermine Sino-Pakistan Projects,” Jamestown Foundation, *Terrorism Monitor* 23:4 (2025).

139 Cullen Hendrix, “Chinese nationals have become targets for violence as China deepens its international reach,” Peterson Institute for International Economics, June 15, 2022.

140 Lucas Winter, Jemima Baar, and Jason Warner, “The Axis Off-Kilter: Why an Iran, Russia, China Axis Is Shakier Than Meets the Eye,” War on the Rocks, April 19, 2024.

141 Ibid.

142 Lionel Beehner, “U.S. Adversaries’ Trilateral Naval Exercises Reflect Convenience, Not Convergence,” U.S. Army Foreign Military Studies Office, July 2025.

143 “China strengthens military ties with Niger amid western withdrawal.”

144 Ditter, Haney, Tsai, and Reid.

145 Paul Nantulya, “China’s ‘Military Political Work’ and Professional Military Education in Africa,” Africa Center for Strategic Studies, October 30, 2023.

146 Carla P. Freeman and Alex Stephenson, “Xi Ramps Up Campaign for a Post-Pax

Americana Security Order," United States Institute of Peace, May 4, 2023.

147 "How China Fights in Large-Scale Combat Operations," TRADOC G-2, May 1, 2025.

148 Nantulya, "China's Policing Models Make Inroads in Africa."

149 Warner, Lizzo, and Broomer.

150 Ibid.