COMBATING TERRORISM CENTER AT WEST POINT

CTC SENTINEL

OBJECTIVE · RELEVANT · RIGOROUS | JULY 2026 · VOLUME 19, ISSUE 7

FEATURE INTERVIEW

# The Intersection Between Cartels, Terrorism, and Other Criminal Organizations

Vanda Felbab-Brown

FEATURE COMMENTARY

# The Impacts of AI Without Guardrails

Adam Hadley

# Contents



FROM THE EDITORS

In what ways do the objectives and motivations of cartels differ from those of more traditional terrorist organizations? What lessons from the global war on terrorism are applicable to the current fight against cartels? These were among the questions we posed to Dr. Vanda Felbab-Brown, one of the leading scholars on conflict, criminal organizations, drugs, and illicit economies, for our cover article this month. "More and more," she says, "a lot of the traditional understandings and distinctions between terrorist and criminal groups don't hold and haven't held for a long time." Those distinctions have a bearing on strategies to combat cartels, as Felbab-Brown notes how "middle-layer targeting is—in my view—a far more useful strategy, promising far greater payoffs than the high-value targeting" over the longer term.

In this month's feature commentary, the founder and executive director of Tech Against Terrorism, Adam Hadley, identifies significant gaps in AI safety that could be exploited by terrorist actors, particularly the risk of 'abliteration'—or removal of an AI model's capacity to refuse—on open-weight models. "The artificial intelligence safety community has largely not engaged with abliteration resistance," Hadley writes. "Part of the reason it has not landed is that the policy conversation still assumes that all AI models are closed. When a government judges a closed AI to present a security concern, they have a control lever. The lever exists because the model runs in one place, under one operator, where it can be audited, restricted, or withdrawn. On the other hand, a frontier open-weight release with removable guardrails attracts no equivalent scrutiny before publication. It has no control lever."

Lucas Webber, Riccardo Valle, Colin Clarke, and Daniele Garofalo trace the historical evolution of the Islamic State's anti-China propaganda—from early Uyghur grievances through COVID-era narratives to current criticism over China's economic expansion into Africa. "China now occupies a structurally embedded position within the Islamic State's global enemy hierarchy," the authors find. "Beijing is increasingly portrayed as a systemic adversary, an ascendant power whose political, economic, and security activities in Muslim-majority regions are interpreted as forms of imperial expansion."

Finally, Francesco Marone provides important context and analysis on a string of recent nihilistic violent extremist (NVE) cases in Italy. From March to May 2026, four NVE cases across the country reveal what he describes as "the first publicly visible links of a domestic mimetic chain, unfolding over a matter of weeks." The cases underscore that a youth can be "at the same time a vulnerable child and a potential source of serious public violence," he writes. "Ultimately, while effective counterterrorism is essential, an even deeper challenge concerns prevention."

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


CTC SENTINEL

*Editors-in-Chief*

*Don Rassler*

*Kristina Hummel*

*Editorial Interns*

*Abigail Becker*

*Ian Dodwell*





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.




Cover: A soldier stands guard by a charred vehicle after it was set on fire in Cointzio, Michoacán state, Mexico, on February 22, 2026, following the death of the leader of the Cártel de Jalisco Nueva Generación, Nemesio Oseguera, known as "El Mencho." (Armando Solis/AP Photo)

# A View from the CT Foxhole: Vanda Felbab-Brown, Senior Fellow in Foreign Policy, Brookings Institution

By Abigail Becker and Kristina Hummel

*Vanda Felbab-Brown is a senior fellow in Foreign Policy at the Brookings Institution. She is also the director of Brookings' Initiative on Nonstate Armed Actors and co-director of the Africa Security Initiative at Brookings. She directs the Brookings series "The Fentanyl Crisis in North America and the Global Reach of Synthetic Drugs" and is the host of the podcast show "The Killing Drugs." She was also the co-director of the "Opioid Crisis in America: Domestic and International Dimensions" series.*

*Felbab-Brown is an expert on international and internal conflicts, insurgency, terrorism, urban violence, and illicit economies. Her fieldwork has covered Afghanistan, South Asia, Myanmar, Indonesia, the Andean region, Mexico, Iraq, Somalia and the Horn of Africa, Nigeria, and other African regions. She is the author of* Narco Noir: Mexico's Cartels, Cops, and Corruption *(The Brookings Institution Press, forthcoming) and* The Extinction Market: Wildlife Trafficking and How to Counter It *(Hurst, 2018), among numerous other publications. Felbab-Brown received her doctorate in political science from MIT and her bachelor's in government from Harvard University.*

**CTC: You are currently the director of the Initiative on Non-State Armed Actors, the co-director of the Africa Security Initiative, and a senior fellow at the Brookings Institution. You're a renowned expert on internal conflicts, non-traditional security threats, and the author of several books. What first drew you to this field and to this problem set?**

**Felbab-Brown:** I started working on what was then called low-intensity conflict during my undergrad time at Harvard in the late 1990s, and I was really doing two lines of work. One was nuclear strategic deterrence issues and the other was low-intensity conflict before it became counterinsurgency again. And it was a funny time to work on those issues because both seemed very emblematic of the Cold War. I was really torn about which direction I would go: nuclear strategic issues arms control or the low-intensity side. When I started my PhD at MIT, I had made the decision that I would work on the intersection of low intensity conflict and illicit economies—drugs being the one that was receiving the most attention, but illicit economies broadly. That was the year 2000, and I had a very senior political science professor who was my advisor, who said something along the lines, 'This is an absolutely disastrous topic. What did they teach you at Harvard? Both topics are completely obsolete; you'll never get any kind of job. Nuclear deterrence is gone but sort of still around, but low intensity conflict and illicit economies, no one will ever hire you.' I said, 'No, I really think there is something to it.'

I ended up working early on the issues of Afghanistan and the Taliban and suppression of poppy in 1999, 2000. And of course, a year later, you have 9/11, and I was one of the few people in the country, relatively speaking, who knew anything about the topic and ended up working early on during my PhD years on policy issues and ended up briefing the U.S. government on that and a wider set of issues.

**CTC: You've studied cartels and TCOs (transnational criminal organizations) for many years, in addition to more traditional terrorist organizations. What have been the benefits of the U.S. government's designation of a number of cartels as foreign terrorist organizations (FTOs) over the past year and a half?**

**Felbab-Brown:** The issue of whether to designate criminal groups such as the Mexican cartels as foreign terrorist organizations is not a new topic. The Obama administration was exploring it. The first Trump administration was exploring it. The Biden administration was exploring it. And each of those administrations made the decision not to do it for essentially two reasons. One was that there was a sense that the designation of the cartels as Significant Transnational Criminal Groups provided sufficient powers in terms of law enforcement. And the second was that there was very strong opposition from governments—most importantly, the government of Mexico—to that designation. There was a sense that it was not worth rocking the bilateral relationship for the marginal gains. And this was, of course, also from the perspective that the right tool for dealing with the groups was law enforcement.

So, what has the designation meaningfully done? You often hear a lot of arguments that this vastly expands law enforcement powers. But when you probe people about how it expands law enforcement powers, you really don't get very much of a substantive difference. The big difference is that now the U.S. military is allowed to deal with the organizations in terms of intelligence provision and potentially more in terms of direct military actions. We have seen that strikes against drug boats are now justified in terms of the FTO designations—that those are strikes on foreign terrorist organizations and they can be done by the military. You have a lot of legal experts questioning the legality of whether even, in the context of the war—if there are no immediate self-defense issues—the strikes on the boats are legal. But nonetheless, that's the justification.

I would say that there are also less tangible differences. One is that even in the context of intelligence gathering, the designation kicked up the priority for intelligence gathering. And it, in some ways, also increases the importance of the cases for U.S. prosecutors. If a prosecutor can prosecute a criminal case or a terrorist case, there is often greater incentive structure for prosecuting the terrorist cases.

The designation also relates to a very important element, which is the material support clauses. U.S. counterterrorism material support clauses are enormously potent statutes, where any kind of material provision to a designated terrorist group can lead to


*Vanda Felbab-Brown*

prison sentences of decades and enormous financial penalties, as well as other issues such as visa denial if it's a foreign entity or being cut off from the U.S. banking system if it's an external business, for example. Now, material support is anything as little as a pencil and a cup of water, and it also includes potentially verbal advice that can be construed as material support. My view is that this has sometimes been effective, but very often it has not been effective in depriving terrorist groups of financing. But it creates this vast system of available pressure points, intelligence gathering points, and leverage, not just with the group itself, but with all kinds of auxiliary actors around the group, such as governments that might be providing support or corrupt individual government officials.

Here's where I need to give more context again. The designation of a criminal group as a transnational criminal organization also comes with very potent material support clauses. They might be perhaps a tinge less potent than the FTO designation, but they are also very potent if an administration chooses to activate them. So, what we have seen with the Trump administration—starting in the last year of the Biden administration, but more so with the second Trump administration—is the Treasury Department being in overdrive in looking for entities to charge. I think a lot of it is very good. It's actually great that we see Treasury indicting just today more entities on smuggling fuel to Cártel de Jalisco Nueva Generación (CJNG).[1] We've seen *narcocorrido* singers being sanctioned,[2] and a lot of the sanctions and the indictments, in my view, have been very well targeted. But the material support clauses are so wide that you could charge a U.S. drug user with material support. You could take a 16-year-old or 17-year-old and charge them under material support clauses that might be punishable, for adults anyway, with prison terms of several decades. We have not seen such crazy charges, but it could be possible.

Similarly, the Trump administration could potentially use the designation as a mechanism to further limit U.S.-Mexico trade. We have not seen such charges or sanctions. But take a money transfer business that sends remittances to Mexico, such as a family living, say, in Michoacán—a Mexican state with a strong criminal presence. The family might well face extortion pressures from criminal groups, because the *narcos* rule the life of the family, as they rule the lives of many people in Mexico. Well, if one wanted to exercise the material support clauses, whether under the FTO designation or the TCO label, you could be charging the money exchange, the financial institutions that send the money, as indirectly complicit in the financing of the terrorist group. So, there's a vast scope of sanctioning that could take place, that could be used as a tool for limiting trade, for example. The one really good outcome with the FTO designations is that, presumably, at least financial institutions and even business institutions in Mexico will be facing greater pressure to do due diligence to avoid processing or laundering money or otherwise cooperating with criminal groups.

**CTC: Going back to the designation itself, can you help our readers understand a little bit more about where there is overlap between the objectives of the cartels and the objectives of traditional terrorist organizations. Which motivations of these two types of organizations are similar and which are dissimilar?**

**Felbab-Brown:** Very early in my work, including what became my dissertation and my first book, I made the argument that all non-state actors, if they hold a territory or they need a territory or resource base for their functioning, will need to decide how they rule. They face the classic Machiavellian choice: Do they rule through brutality alone, or do they want to be feared and loved? But that also means that there was too much overemphasis on the political versus economic motivations. Back in the early 2000s, you had the work started by Paul Collier that talked about wars for profits, for greed.[3] Collier and people who followed in his school made famous arguments that wars in the 1990s had stopped being about ideology—that they became about money. I argued that even non-state armed actors that are presumably only motivated by money will still have political implications and political inclinations.[4] That doesn't mean that they—the narcos in Mexico and the criminal groups—have an ideology and that they want to topple a government. Most of the world's criminals do not necessarily want to bring a government down and hang up the flag of a criminal actor. That said, you actually have places like this in Mexico that are run by so-called militias, but they are essentially indistinguishable from criminal groups, often just criminal groups posing as militias, that hang up the flag of its 'independent' territory and set up barriers around it. The territory is not just de facto controlled by a criminal group, but also comes with barriers and flags proclaiming an independent entity. And they will say, 'This is the Republic of X, Y, and Z militias, and the government cannot formally enter here.' But those are still exceptions. Most of the time, the criminal ruler does not seek to claim that the government is no longer present and, instead, seeks to control the government.

So even criminal groups have political implications of many kinds, and sometimes they have political ambitions and political inclinations. They certainly need to build political capital. Or they may make the choice to rule through brutality alone. But many will try to build political capital with the population. They will also seek to shape the government, to prevent the government from interfering with their business. And so, a formal ideology in the way that we understand ideologies of at least some terrorist groups, such as al-Qa`ida, for example, as a quintessential example, or al-Shabaab, might not be there. But the political focus for some criminal groups is very much there, even if the objective is not to topple the government.

Certainly today, you have criminal groups—and it's not new and it's not just true about Mexico—that rule territories that try to keep the government out, that rule populations, that sometimes come even with an ideology. In Michoacán, for example, you have a group called Guerreros Unidos or Carteles Unidos—they go by

different names—telling teachers what to teach at school, such as the equivalent of *omertà* [strict silence] and obedience and family. They talk about the trifecta of the teacher, the doctor, and the priest as the core influencers who will take orders from them on how societal rule is going to take place. So, you have a real ideological element here, even if the motivation is at the end, principally not a heavenly afterlife and 70 virgins, but money and profit in one's time here on Earth. You have groups in Mexico like La Familia Michoacana, which was one of the earlier criminal groups, and the Templarios that will surround their rituals with all kinds of ideological elements, mythology, visual ritualistic elements. This is the cult of Jesús Malverde and similar ideological rituals such as La Santa Muerte. The imagery is created toward external actors; it's externally oriented to intimidate other groups and the populations. But it's also internally oriented, meant to shape the behavior of members to motivate them to be fearless and to be obedient to the leader.

So, more and more, I would say that a lot of the traditional understandings and distinctions between terrorist and criminal groups don't hold and haven't held for a long time in my view. And it's also equally true that you have some terrorist groups like Abu Sayyaf in the Philippines, which go through these changes of Islamists/not-so-Islamists, material for profit, then flip from al-Qa`ida to ISIS, then come back to nationalist/semi-separatist. They just shop for whatever ideology seems more resilient while the economic motivation stays.

**CTC: How have criminal groups in Latin America exploited governance gaps? And beyond trafficking and extortion, in what ways do they work with those local populations, as you were mentioning, and emulate state-like governance structures, creating forms of hybrid governance that may complicate traditional counterterrorism and security responses?**

**Felbab-Brown:** The bottom-line answer is 'very much,' but I would say it's also not just about Latin American groups. If you think of the Italian mafia groups, of which there are many—the Sicily-based groups, the Napoli-based groups—all along, they were about governance. And their emergence way back in the 13th century and resurrections in the 20th century during World War II and after World War II, they were all about governance in a system where governance is either extremely feudal and skewed or very sporadic and insufficient for basic functionality.

You have similar phenomena among groups in Asia; for example, the Pakistani groups in places like Karachi are a classic example, or in India in a place like Mumbai. We have a lot of groups that don't come in simply with muscle and extortion, but that focus on the under-provision of public services, whether it's security, whether it's the predictability of rules and some system of order, or whether it's the absence of particular physical goods, which could be roads, hospitals, clinics. All of them come in with the provision of rule, the provision of safety. That might be very ethnically skewed, it might be serving particular sub-populations, it might be highly discriminatory, it might be highly abusive, it's obviously to some extent arbitrary. There are no or limited checks and balances on it, and adherence to issues like civil liberties, human rights, and due process are just non-existent.

But in the context of vast under-provision of any kind of rule, the predictable, if authoritarian rule might be well tolerated and even welcomed by populations. In some cases, you will have the *extra* provision. The *narcos* in Mexico, the Pablo Escobars and its many descendants of paramilitary groups in Colombia, the FARC [Fuerzas Armadas Revolucionarias de Colombia], are they terrorist groups, criminal groups, insurgent groups? At some point, some have been all of it—the FARC dissident groups are also all of the above, although you don't have the formal terrorist label now. But sometimes the groups provide cleaning of streets, cleaning of sewage. They might give money to a *fiesta*, they might give money to schools. The *narcos* in Mexico are notorious for providing funding for schools, for local churches, building local churches, soccer stadia—all of which is not that radically different than what the *mafiosi* would be doing in Sicily or southern Italy more broadly for several centuries.

**"More and more, I would say that a lot of the traditional understandings and distinctions between terrorist and criminal groups don't hold and haven't held for a long time in my view."**

**CTC: Could you explain the roles that these traditional terrorist groups play in Latin America and how their presence might impact cartel activities? One example is Hezbollah's continued presence in Latin America, specifically in the Tri-Border Area and Venezuela. How do these groups collaborate, and what are the roles that these groups are playing?**

**Felbab-Brown:** Certainly, Hezbollah is the group that is best documented to operate in Latin America, primarily in the Tri-Border Region. Hamas would be the second group. Both groups, particularly Hezbollah, have extensively used the Tri-Border Area for financing, for laundering money, for participating in the drug trade. Now, Hezbollah does the same thing across Africa, where you have a lot of car dealerships linked to Hezbollah, where you have the infamous diamond trade, just a wider variety of other ordinary commodities that are not drugs and that are not high value goods like gold or diamonds, where the trade is a mechanism of financing. That is also what predominantly goes on in Latin America.

You have other instances of the use of spaces in Latin America by terrorist groups. In Brazil, for example, the criminal market is famous for high-quality, fake biometric passports. High-level Brazilian law enforcement officials told me of ISIS fighters going through Brazil to obtain fake passports there because of their high quality and then traveling with those passports to Europe. That's one example. And then you have the 1994 bombing in Argentina of a Jewish center in Buenos Aires, an actual large terrorist attack linked to the Middle Eastern terrorist group, Hezbollah, likely at the direction of Iran. And Latin America had its own terrorists: Remember the takeover of the Japanese Embassy in Peru in 1996 by the Túpac Amaru Revolutionary Movement?

However, the big controversial issue is how tight those relationships are with Latin criminal groups. In my view, we have really not seen very tight relations. Some criminal groups in Latin America might opportunistically flirt with terrorist groups. But, for example, the fake biometric passports in Brazil have not, at least until now, been controlled by an entity like the Brazilian Primeiro Comando da Capital (PCC), perhaps the most potent criminal

*A soldier stands guard by a charred vehicle after it was set on fire in Cointzio, Michoacán state, Mexico, on February 22, 2026, following the death of the leader of the Cártel de Jalisco Nueva Generación, Nemesio Oseguera, known as "El Mencho." (Armando Solis/AP Photo)*

group in South America. The fake passport production appears to be run by individual entrepreneurs who serve a wide variety of clients, be they criminal or terrorist, as opposed to representing a big criminal group like the PCC making a lasting alliance with, say, Hezbollah. Venezuela is a place where a lot of groups come together and where you might have linkages between Hezbollah and its presence in West Africa, shipments of drugs from Latin America to West Africa to Europe. So, connections are made and they're undesirable. But we have really not seen any large Latin American criminal group, or for that matter, any large European criminal group, cooperate with Hezbollah and saying, 'Okay, we now have an alliance with Hezbollah or with al-Shabaab or with ISIS, and we are going to be part of the jihad.'

That is actually an important difference between the two sets of actors. Latin American criminal groups have been very willing to engage in brutal, spectacular violence, starting with Pablo Escobar and the bombing of the Avianca plane in 1989, which was the first time the term narco-terrorism is used by then U.S. ambassador to Colombia. But all of this has stayed within the country. We really haven't seen the situations where Mexican cartels or the PCC, which is now designated as an FTO, go outside of their home country and blow up an embassy or a ship. The focus on the enemy—being the state—has always been inward. We have not seen Latin American criminal groups, even facing intense counter-narcotics pressures from the United States, going after 'the far enemy' like al-Qa`ida wanted to go after the U.S. in order to bring down the apostate government at home in the Middle East. Or Shabaab just falling into the eternal temptation of Somali jihadists going back to the 1990s. They always had some Ogaden[a] or Ethiopia expansionist views; they will strike in Kenya, they will strike in Ethiopia. We haven't seen that from any of the large cartels or criminal groups. And not just in Latin America. I really cannot think of any other globally than the D-Company, which is the Indian criminal group led by Dodwell Dawood Ibrahim. That's the epicenter of Indian policymakers' focus, where you have direct connections between Dodwell Dawood Ibrahim and his criminal group and terrorism from Pakistan and support for terrorist actors in Pakistan.[5] But that is really the only major one that I can think about of where you have terrorist actions conducted by a criminal group outside of its country's borders, outside of its home zone of operations.

**CTC: In the near future, we plan to feature an article in *Sentinel* that examines lessons learned from the global war on terrorism that could be applicable or are at least useful to consider in counter-cartel efforts. In your view, what strategies that have been effective against terrorist groups will also be effective against cartels?**

**Felbab-Brown:** It's easier to answer with what has *not* been effective. High-value targeting has worked in limited cases. High-value targeting was an important element of defeating the *senderistas* [The Shining Path] way back in the late 1980s and early 1990s. But high-value targeting, and specifically the arrest of [Shining Path

a Editor's Note: The Ogaden, located in southeastern Ethiopia, is predominantly inhabited by ethnic Somalis.

**"I have argued that what is needed with criminal groups is focusing the targeting strategy at the middle operational layer, which is not just the boss or the two bosses, but it's really the key logisticians, the key financial operators, certainly the key political sponsors and enablers."**

leader Abimael] Guzmán and the top leadership of *senderistas* that was around him, including his wife and others, came after the *senderistas* were essentially defeated in the countryside through a policy that a) suspended eradication of drugs and b) recruited the *rondas capesinas*, the militias in the countryside, to fight against the *senderistas*. So, decapitation was the final step. The second classic decapitation success story would be the fall of the Saddam regime, except then all kinds of internal fighting and terrorism start within Iraq right after that and it becomes an extraordinarily bloody civil war and anti-U.S. insurgency. And maybe the counterterrorism campaign against al-Qa`ida could also be consider a success of high-value targeting. I say maybe because, again, lots of elements other than getting bin Ladin and certain people around him were crucial elements of the counterterrorism effort.

Now, in the crime space, decapitation alone has essentially not worked against any group of any meaningful heft and depth.[6] That strategy alone has not been sufficient. I've written quite extensively on why that is the case, and I speculate one reason is that perhaps the skill that you need as a criminal *capo* [leader] puts much less of a premium on something like charisma. Perhaps logistical skills are much more important; that also means that replacement of leaders is highly feasible. The replacement might be very violent, which is a big part of the problem. It might be difficult to replace Usama bin Ladin or his successor, Ayman al-Zawahiri, but it might not be so difficult to replace someone like El Chapo, even though El Chapo might be a big logistical genius.[7] Now, we have had a decapitation strategy against al-Shabaab in Somalia for years; we have had decapitation in Nigeria against Boko Haram even before U.S. involvement, and against ISWAP; we have had decapitation in Afghanistan. And the groups have not gone away. Shabaab is at least as strong as it was. Taliban is in power. Boko Haram and ISWAP are very, very strong, and insecurity in Nigeria is rampant. Then you have groups like JNIM and the rest of the Sahel space.

I have argued that what is needed with criminal groups is focusing the targeting strategy at the middle operational layer, which is not just the boss or the two bosses, but it's really the key logisticians, the key financial operators, certainly the key political sponsors and enablers. The Trump administration here deserves a lot of credit for daring to go after corrupt or allegedly corrupt government officials, including sitting ones, such as the recent indictment of the governor of Sinaloa, Rubén Rocha Moya.[8] This anti-corruption thrust is a really important direction of the anti-crime effort. Now, the Trump administration also pardoned the president of Honduras,[9] who was indicted and sentenced for massive collusion with the Sinaloa Cartel and Honduran criminal groups Los Cachiros and the Valle Valle Network.[10] Nonetheless, despite this decision, the expanded list of targets to include corrupt government officials is really important. So, middle-layer targeting is—in my view—a far more useful strategy, promising far greater payoffs than the high-value targeting.

Here is where the 'but' comes in: A lot of the militant terrorist activity presumably has some sort of end state. You hit al-Qa`ida, terrorism goes away, though perhaps another actor like ISIS may rise. But you are never going to be in a crime-free space. So, the way we need to think about crime is to, first of all, make a distinction between predatory criminality and transactional criminality. Predatory criminality is something like homicides, extortion, robberies. You want to bring predatory criminality down, and you can bring that down, and you want it to be as low as possible. You want to be living in the Western Europe system where you have one homicide per 100,000, and you have civil liberties and human rights. You don't want to be living in a situation where homicides are 20, 30, 40 per 100,000, and criminals really determine your life in a very daily way, which they do in many parts of the world, certainly including Latin America.

But in the transactional crimes, like drug trafficking, other forms of contraband trafficking, you are very unlikely to be able to bring the illicit economy and the illicit activity to something like zero or close to zero. Sure, you want to limit the amount, but that's an insufficient and elusive objective. What you really want is the activity to be as non-violent as possible and as distant from political structures and society as possible. So essentially, you want the drug trafficking to take place the way it does in Bethesda, Maryland, which is a very high-income neighborhood in the outskirts of Washington, D.C. Drug dealing there is very polite. There is no shooting. You don't go to the criminal, to the purveyor of the drug, to resolve a dispute over where your fenceline sits. And you don't want that criminal to be someone who's corrupting local government officials and local police officers. The criminal just delivers the drugs and stays out of your life and doesn't shoot, hands over his hands, and gets handcuffed as opposed to shooting down the police station. Which is not to say that you just want free flow of drugs; I'm not at all arguing for that. But it's not just about limiting the flow. There is a limit how much you can push volumes down. But the way the illicit business is conducted matters very much as well, as opposed to in predatory crime, where you simply want the numbers to go down.

These, again, are significant differences where the terrorist activity is much more akin to the predatory crime. You don't want well-behaving terrorists; you don't want terrorists and terrorist incidents *at all*. And so, understanding that in this way, the two phenomena are fundamentally different, I think is important for answering what strategies are appropriate. If criminal groups provide governance, services, and have political capital with local populations, you want to take those away through strategies that sap the political capital, provide governance and services, get allegiances to switch—i.e., through the maligned or praised 'hearts and minds' approach. You want to deprive the violent actor of having support from local populations as much as possible by being a better administrator, by doing better at service delivery, by being less corrupt, by being far more present, by providing socioeconomic services that are meaningfully designed and are not just one-time handouts that don't change anything. We can talk a lot about what works in the designs or not, but if you have an understanding of the criminal actors often as being providers of governance, then you need to counter them not just by shooting them down, but by addressing what gives them strength, what gives them popular

support, or at least popular acceptance or tolerance.

The final element is, the more you can get at some of the financial nodes, the better. But, there is again a 'but.' There is a lot of self-delusion in the policy community about how much one can take away the money. And replicating the effective crackdowns on al-Qa`ida financing in the first decade of 2000 to 2010 has really not happened with any criminal group. It's just much more challenging. Nonetheless, if nothing else, looking at the highly diversified stream of activities and income and revenues of criminal groups gives you intelligence and a better map, a better sense, of the network. Mapping out the networks and dismantling it through arrests is often a much more achievable goal than hoping that you can bring the money down by 40 percent or 60 percent, or even smaller numbers. The intelligence picture gives you the ability to act against a wider set of actors. Therefore, it is of significant value to look at how diversified the powerful criminal groups are in their lines of operations, how they operate in many commodities and activities other than drugs.

**CTC: Let's pivot to China and China's activity in Latin America. As a starting point, could you describe the depth of cooperation that exists today between Chinese money laundering networks and Mexican cartels or Latin American cartels? And how and why did this cooperation develop?**

**Felbab-Brown:** Essentially, Chinese money laundering groups have become the go-to money launderers for the Mexican cartels, and they have been stunningly able to displace the Black Peso Exchange Market that for 40, 50 years has been the dominant way through which Latin American groups in general, including Mexican groups, have been laundering money. And this is not just true about Latin America. We see also a dramatic rise of the Chinese criminal groups in places like Europe, Spain, France, Portugal, Italy for the Italian mafia groups. The Chinese networks are top money laundering actors.

There are several factors that give them just an incredible advantage over others. One is that they can charge very low prices for their money laundering services, because they have captive clients—i.e., people and businesses in China. China has capital controls that prevent the movement of Chinese money out of China over essentially the equivalent of $50,000 annually. Moreover, there is a lot of instability and high uncertainty in financial systems in China. In addition to personal motivations, a lot of Chinese people and businesses want to move money out of China, but they cannot do it legally. And so, we have this vast money laundering system that has served Chinese clients but that is able to impose the majority of charges onto the Chinese clients. So, the Black Peso Exchange Market would traditionally charge somewhere between 15 and 20 percent to a cartel for changing money. The Chinese networks will charge as low as one percent to a criminal group. Essentially, the bulk of the cost is shifted on Chinese clients who have no option but to use those systems. So, that's one enormous advantage; the price mark-ups just favor Chinese money laundering networks tremendously over other money laundering systems, such as the Black Peso Exchange Market.

The second is that you can use trade-based money laundering. If you are China, you have legal business with probably every entity country in the world. If you are a Bolivian money launderer, it might be really hard to justify why you claim to have done this real estate deal or ship this amount of construction material to Mongolia. Investigators might be suspicious of that transaction. So, trade-based money laundering, even with vastly underregulated cryptocurrency burgeoning and extensively used for illicit purposes, is still one of the safest ways to launder money. Under-invoicing and over-invoicing is extraordinarily difficult for financial regulators and auditors to detect and unpack. Chinese actors are uniquely capable of doing that because of China's global trade presence.

The third advantage is linked to the big demand in China for consumer goods—luxury goods, all kinds of goods—that allows Chinese money launderers to avoid using international banks. If you are a Mexican cartel, your biggest challenge is always dealing with liquidity, whether it's because you need to offload and hide the vast amounts of cash collected during retail or because you need to use liquidity for, for example, warfare. It is in the retail markets, in the U.S. market or in the European markets, where you end up with vast amounts of cash. Before the rise of Chinese money laundering utilizing consumer goods value transfer, you would need to find a way into the highly regulated banking sector, with its suspicious activities reporting requirements, due diligence, et cetera, or you'd need to smuggle vast amounts of cash and then swap it for another currency. What you do now is, you go to your Chinese collector, you hand them bags of cash, and the Chinese collectors will deposit it in U.S. accounts, perhaps 'smurf'[b] it around, or perhaps use a variety of students or Chinese diaspora to distribute the money, to deposit cashier checks. The Chinese launderers then just buy physical goods like cell phones and ship them to China and sell them there with a mark-up. Meanwhile, in China, the money, the value will move between two Chinese bank accounts so it's not subject to the same level of scrutiny, just like domestic transactions in the U.S. are not subject to the same level of scrutiny as international wires. And then in Mexico, the equivalent sum of money will move between two Mexican accounts. And then the *narcos* will end up with having that value in Mexico and investing it in the Mexican economy or using it for other purposes. And so, this ability to bypass international banks, and use mirror transactions and value transfer among commodities, that is another really big advantage of Chinese money laundering networks.

Now, all criminals and everyone who wants to hide money are using cryptocurrencies. The Chinese are not immune to that. Chinese money laundering networks use them; Mexican cartels use them. But it's the combination of these things—captive clientele in China, worldwide trade-based money laundering, and demand for consumer goods—combined with new transaction methods such as cryptocurrencies, and the resulting ability to avoid using international wires that gives the Chinese networks tremendous advantage all around the world.

**CTC: How much does Beijing know this is going on or support this going on? Is it a bit of a turning of a blind eye because it's advantageous in certain ways to that government?**

b Editor's Note: "A smurf is an individual(s) who makes numerous same-day currency deposits of less than $10,000, usually at several different banks, to evade the filing of Currency Transaction Report (CTR). The act of conducting such transactions is termed 'smurfing.'" "Part 9. Criminal Investigation, Chapter 5. Investigative Process, Section 5. Money Laundering and Currency Crimes," Internal Revenue Service, last reviewed or updated on April 30, 2026.

**Felbab-Brown:** It's a very tough question. It's certainly common to allege Beijing's complicity. I think it's more complex. Beijing is certainly extremely unhappy about the capital flight out of China. They really don't like that at all, and they've been trying to crack down on it and, for example, really muscled very strongly the governments of Southeast Asia and Australia to cooperate with catching Chinese capital flight, then repatriating it—along with people—to China. China has, however, historically not been very keen to cooperate with anti-money laundering efforts the other way, including because China's banking system has been underregulated, and China doesn't want to reveal the banking sector's weaknesses and shadiness. There is fear of possible huge bubbles in China's financial sector and other large vulnerabilities. In fact, some think China's financial sector today might be as shaky as the U.S. financial system was in 2008 when you had the financial system crash following the burst of the housing bubble. The Chinese government fears that too much visibility into its financial system could have wide repercussion for the entire economy. Moreover, at various times, China was grey-listed under FATF[c] due to failures and problems in its financial due diligence. China came off the FATF's grey list, but China still doesn't want to really allow any eyes onto its internal financial systems.

For complex reasons, U.S.-China anti-money laundering cooperation has been mostly very limited. In general, China extends law enforcement cooperation to a country with whom it's friendly or whom it wants to court and denies it to countries with whom it has a competitive relationship or with whom the relationship has soured. In 2024, during the last year of the Biden administration, we saw an unprecedented amount of U.S.-China anti-money laundering engagement. This is when [U.S. Treasury] Secretary [Janet] Yellen had regular meetings with her Chinese counterparts. This was the first time when the Bank of China—long accused of being a massive money laundering machine—engaged in dialogue with U.S. government officials and signed memoranda of understanding on anti-money laundering cooperation. And there were actually a few cases of investigative cooperation against money laundering between the two countries and prosecution by China, including a Chinese national who is part of the money laundering network for the Mexican cartels.[11] He's indicted by the U.S., he's then arrested by China, China charges him. So, we went from very little to zero cooperation to some cooperation in money laundering.

China likes it when money comes into China. China does not like it when its reputation is tarnished. It's very sensitive to issues like being put on the FATF grey list. That said, you have all kinds of domestic, political, economic constraints, including just not wanting to disclose how much of a problem there potentially is in the financial sector and how much the housing and financial sectors could unravel. And certainly, China is very opposed to capital flight out of China. So, it's very motivated to capture money that's leaving China. It might be less motivated to capture dirty money coming into China.

**CTC: What role does China play in the drug manufacturing process and how does it fit into the larger landscape of fentanyl and synthetic opioid production in Latin America? How big of a problem is it when it comes to China and that problem set?**

**Felbab-Brown:** China is the predominant source of precursor chemicals for synthetic drugs. This is not true just about Latin America. It's not just true about synthetic opioids. It's also true about methamphetamine. India is also a very important player. India is the second-largest producer of precursors for synthetic drugs. India's pharmaceutical industry is highly under-regulated, very politically powerful, very dirty, and the Indian government is often even far more reluctant to talk about tightening regulations and acting against the vast complex of the chemical pharmaceutical sector that is a big feeder of both finished synthetic drugs and precursors for meth and synthetic opioids. But nonetheless, China is still the dominant country in the supply of precursors for synthetic drugs.

China had been under a lot of pressure since the Obama administration to reduce the flow of finished fentanyl. When China scheduled the entire class of fentanyl in 2019, fentanyl essentially stopped flowing out of China to the United States. Instead, it would be precursor chemicals going from China to Mexican cartels that then produce fentanyl in Mexico and bring it to the U.S., or precursor chemicals heading from China to Canada. Since then, the diplomatic game has essentially become 'pressure China to schedule.' They schedule a certain chemical, a certain precursor, and Chinese chemists adapt and start sending more basic chemicals that are called pre-precursors. Many of these very basic chemicals are of widespread use. The odds are very low that they will be scheduled because they're just so common; you would have huge industry rebellion and pushback against their scheduling. And so, China quite likes scheduling, though it exacts a high price for scheduling. And when China schedules, the traffickers move to non-scheduled precursors.

Here is where the problem then lies: In the U.S., material support clauses would lead any actor who sent a precursor chemical to a Mexican cartel to be subject to material support statutes and, with that, massive penalties. Well, China does not have racketeering clauses, it doesn't have material support clauses, and it doesn't have conspiracy clauses. So, an entity in the U.S. providing a pencil, a cup of water to an FTO, including now a Mexican cartel, or even before the Mexican cartel became an FTO and it was a Specially Designated Criminal Group, can face decades in prison and just that material support is sufficient to lead to charges and punishment.

China doesn't have any of those statutes. So, you will constantly hear from Chinese officials, 'We cannot act against that entity because they are selling legal products.' Meanwhile, the traffickers will advertise the non-scheduled products with notices such as 'We know how to evade Mexican customs.' And they will accompany the non-scheduled products with the recipes for producing fentanyl. Sometimes the traders are completely blatant. Other times, they'll pretend that they don't know that they are selling to a cartel. Meanwhile, Chinese traders and policy analysts insist that it is not their fault or their responsibility to know who is a cartel, who is a front for a Mexican cartel. Instead, they insist that the government of Mexico provides them with a list of companies to which they can sell. Which, of course, isn't practical since such a list would have to

c Editor's Note: "Organized by the G7 in 1989, the Financial Action Task Force (FATF) is the international standard-setting body for anti-money laundering (AML), countering of the financing of terrorism (CFT), and countering proliferation financing (CPF)." "About: Financial Action Task Force (FATF)," U.S. Department of the Treasury, n.d. "When the FATF places a jurisdiction under increased monitoring, it means the country has committed to resolve swiftly the identified strategic deficiencies within agreed timeframes and is subject to increased monitoring. This list is often externally referred to as the 'grey list.'" "'Black and grey' lists," FATF, n.d.

be frozen and Mexican cartels could always infiltrate or coopt the listed legitimate company.

Meanwhile, China does not mandate or encourage due-diligence and know-your-customer practices in the chemical sector. This is a huge loophole. It has existed across administrations. The Trump administration has not been able to make headway with it, even with the salvo of tariffs against China in January 2025. And whether it's through conversation, cooperation, or pressure, incentivizing the Chinese government to find a way to reliably act against the sale of chemicals to criminal actors that are not scheduled is really fundamental.

And for that matter, it's the same issue with the Indian government. India is even behind China in scheduling, and the quality of law enforcement in India is even behind China. India's counter-narcotics law enforcement is still very much focused on capturing heroin going across the Punjab plains or chasing actors like Dodwell Dawood Ibrahim, but not really thinking about the role of Indian pharma in the sales of industrial-potency tramadol to countries in Africa or similar drugs to countries in the Indian Ocean.

**CTC: Looking toward the future, what are the two or three new developments, particularly advances in technology, such as AI drones and other emerging tools, that you think could reshape the operations of cartels and also the effectiveness of counter-cartel efforts?**

**Felbab-Brown:** Whether it's criminal groups or terrorist groups, the future, in my view, is much less dependent on the nexus of crime and terrorism. The hallmark of the future will be the ability of non-state armed groups to conduct a wide variety of activities at home and on their own. AI and 3D printing will allow groups to produce weapons and fake passports. There will be far less dependence on long, extensive cross-border supply chains in existence. The simplification of logistics will vastly empower non-state armed actors. Both criminal actors and terrorist actors will be able to have far longer reach with much less manpower. And this is true both in terms of violence and in terms of delivery of contraband. We are seeing criminal entities weaponizing drones. There's been a lot of focus on Mexican cartels supposedly sending people to Ukraine, but you have had the weaponization of drones by the cartels for several years prior to that development, both to conduct targeted assassinations, and also to maintain population control and to depopulate areas.

And more and more, you will have the ability to hack and sabotage systems at home to have surveillance. So, think of your Roomba vacuum providing a perfect picture to someone who wants to rob your house. But you can also imagine all kinds of sabotage systems to kill someone. The future is much less dependent on labor for violence and for smuggling.[12] It's much more about the ability to do stuff on your own without dependence on international supply chains and international connections. This doesn't mean that everyone will be doing everything at home, but the labor requirements have gone down. And the value of territory will be going down significantly for both sets of actors. Conducting extortion or taxation is what non-state armed actors do to raise money—be they the Taliban, Shabaab, or Mexican cartels. Often, they simply charge money on any economic activity taking place in the territory. But with that, you need to have the credibility of violently punishing someone who disobeys, who refuses to pay the tax—the *zakat*, the extortion fees, the *cobro de piso*. The ability to hack systems, impersonate people—you will have far more ability to do that, and you can be one individual and, in the end, have tremendous impact across far distances without territorial control. In the future, non-state armed actors will have the ability to bring violence, including death, to your bedroom through just hacking your systems without having to send 20 *sicarios* out of Colombia or Mexico to conduct the assassinations.

**"The hallmark of the future will be the ability of non-state armed groups to conduct a wide variety of activities at home and on their own. AI and 3D printing will allow groups to produce weapons and fake passports. There will be far less dependence on long, extensive cross-border supply chains in existence. The simplification of logistics will vastly empower non-state armed actors. Both criminal actors and terrorist actors will be able to have far longer reach with much less manpower."**

In the delivery space, we see the weaponization of drones; we see certainly drones for all kinds of contraband delivery. We now have surface marine drones and even very basic underwater contraband drones capable of carrying drugs across the Mediterranean,[13] even as manned vessels still carry large quantities of drugs: We just had the biggest seizure of cocaine off Spain.[14] The big dramatic change will be further improvements in underwater marine drones, making detection a challenge. But the existing surface marine drones are already a massive advancement that was hard to imagine 15 or 20 years ago. Whether it's underwater or surface drones, as marine drones proliferate, then interdictions will become more challenging. Because right now, you know where drugs will head. They will head into major ports; they will head into minor ports. Islands like the Azores, islands in the Indian Ocean are natural places where drug shipments need to go through. Once marine drones carrying contraband proliferate, the entire littoral will be available for their landing. You won't have these natural points where you know that you want to law enforcement to be monitoring.

So, much less need for labor with at-home 3D printing of weapons, passports, illicit drugs, and much less dependence on long supply chains. And at the same time, much more ability to do stuff by remote, both in contraband delivery and to conduct violence. These are all really dramatic changes empowering and transforming non-state armed actors.

Of course, security and law enforcement actors will also be taking advantage of the new technologies and be empowered by them. And so will clients of criminal groups, such as drug users.

AI and 3D printing advances will enable drug users to cook drugs themselves in their home; you won't need a criminal group to be producing illicit drugs. What if every drug user is cooking drugs at home for him or herself? Is that a safer world, a better world? Will the criminal groups put up with it, with losing the drug markets? And will drug users be producing safer drugs, or drugs that make it more challenging for public health officials to reverse lethal overdoses or counter high morbidity effects?

You can imagine all kinds of new domains of criminal activity becoming available to many more actors. Just think of the scams. The proliferation of AI images will empower extortionists: AI can generate an image that looks exactly like your grandson, a seemingly very beaten up and tortured grandson presumably being held hostage and subject to death, unless grandma pays. That image can easily become an avatar complete with the voice mimicking the voice of the actual grandson. A criminal can then create a video call with the grandmother and enhanced its credibility by describing the grandmother's living room based on intelligence from her hacked Roomba: 'Hey, grandma, I'm being brutalized by Nigerian human smugglers. And I know when you sit in this chair, I know exactly what the chair looks like. Please wire this money to save me.' You will have many people falling prey to such scams. As financial security officials working in Mexico's banking sector told me in April, right now, you have Mexican cartels capturing people's voices. They'll record people's voices and then use AI to produce voice signatures and voice phrases and call Mexican banks with that, and Mexican banks then use it as sufficient authorization to access bank accounts and do bank accounts transactions. And, of course, people lose a lot of assets through such scams. It's quite prevalent in Mexico.

One other thing I would add to the trend of non-state armed actors in the future having much less need for territory, much less need for labor, and much less dependence on transnational flows and supply chains, is also the implication that they will be able to obtain less political capital. Right now, you control territory and you give stuff to people and you employ a lot of people. If you are a terrorist group, such as the Baader-Meinhof Gang,[d] maybe you employ only 10 people, for example. But if you are a Mexican cartel, you'll probably be employing thousands of people, and you get political power by giving employment to people. A combination of synthetic drugs replacing plant-based drugs, drones, and other tech reducing labor requirements means a much smaller need for labor and many fewer opportunities to employ people. The synthetic drugs revolution alone means that you have gone from millions of people working in cultivation of drug crops to thousands of people globally cooking synthetic drugs; that's a three order of magnitude decline in labor requirements and labor opportunities.

So, you have really interesting political capital implications: i.e., a big decline in political capital for non-state armed actors. And you also have really interesting social implications, one of which is that for millennia, the criminal space was the social pressure release valve: People who were unable to work in the legal economy would find employment in the illegal one. Well, that illicit opportunity and basic livelihood survival space might now close to many because the illegal economy will be conducted by a few. And so, what's going to happen to the people who don't have jobs now, many more who will be laid off as a result of AI, who even might not be employable even in the traditional criminal sphere? Are they all going to be joining insurgencies? Or roam around as predatory gangs? Does the future include apocalyptic-like, anarchistic phenomena—essentially banditry for survival—since even the criminal economy will not sufficiently provide for employment and income and social identity? I don't think that'll be in the next five years, just to be clear.

**CTC: But maybe the next 10 years?**

**Felbab-Brown:** I would say certainly in the next 20 years. We will be very quickly exploring whether social systems and political systems have adapted to prevent that, or whether we are really heading into the grips of that kind of future. Certainly, I think that the technological changes about which we talked and their implications for non-state armed actors are well underway. Whether in five or 10 years, we are in Cormac McCarthy's *The Road*[e]-like imagery, I don't necessarily think so. But in the span of two decades, we'll be really living through whether social systems have provided new safety nets, whether there is reimagined distribution of economic opportunity, whether political systems have been rearranged sufficiently, and whether there is enough value being generated and distributed to cope with the fact that many fewer people will be employable by anyone—in the legal sphere or the illegal sphere. CTC

d Editor's Note: The Baader-Meinhof gang was "Germany's most notorious far-left guerrilla group … whose members killed more than 30 people in the 1970s and 80s." It dissolved itself in April 1998. See "Who were Germany's Red Army Faction militants?" BBC, January 19, 2016.

e Editor's Note: The setting of Cormac McCarthy's 2006 novel *The Road* is a brutal, post-apocalyptic world following a cataclysmic global disaster.

## Citations


1 Editor's Note: "US Treasury and Mexico's UIF team up to target cross-border fuel theft by the Jalisco cartel," Mexico News Daily, July 2, 2026; "Treasury Targets Criminal Facilitators Behind CJNG's Cross-Border Fuel Smuggling Schemes," U.S. Department of the Treasury, June 30, 2026.

2 Editor's Note: Vanessa Buschschlüter, "Mexican band has US visas revoked for 'glorifying drug kingpin,'" BBC, April 2, 2025.

3 Editor's Note: See Paul Collier and Anke Hoeffler, "Greed and Grievance in Civil Wars," The World Bank Development Research Group, Policy Research Working Paper 2355, May 2000.

4 Editor's Note: See Vanda Felbab-Brown, "Human Security and Crime in Latin America: The political Capital and Political Impact of Criminal Groups and Belligerents Involved in Illicit Economies," Applied Research Center, Florida International University, September 2011; Vanda Felbab-Brown, *Shooting Up: Counterinsurgency and the War on Drugs* (Washington, D.C.: Brookings Institution Press, 2019); and Vanda Felbab-Brown, Harold Trinkunas, and Shadi Hamid, *Militants, Criminals, and Warlords: The Challenge of Local Governance in an Age of Disorder* (Washington, D.C.: Brookings Institution Press, 2017).

5 Editor's Note: For more on Dawood Ibrahim, see Animesh Roul, "Dawood

Ibrahim: India's Elusive Most Wanted Man," *Militant Leadership Monitor, South Asia* 1:6 (2010).

6 Editor's Note: For example, see Vanda Felbab-Brown, "The successes and problems of high-value targeting strategies around the world," Brookings Institution, October 19, 2022.

7 Editor's Note: Vanda Felbab-Brown, "Mexico's Out-of-Control Criminal Market," Foreign Policy at Brookings, March 2019.

8 Editor's Note: "U.S. charges 10 Mexican officials, including Sinaloa governor, with drug trafficking," CBS News, April 29, 2026.

9 Editor's Note: William K. Rashbaum, Maggie Haberman, Kenneth P. Vogel, and Jonah E. Bromwich, "Former President of Honduras Is Freed From Prison After Trump Pardon," *New York Times*, December 2, 2025.

10 Editor's Note: "Juan Orlando Hernández, Former President of Honduras, Indicted on Drug-Trafficking and Firearms Charges, Extradited to the United States from Honduras," U.S. Department of Justice, April 21, 2022; Seth Robbins and Alex Papadovassilakis, "US Indictment of Honduran Ex-President Spells Out 20 Years of Drug Ties," Insight Crime, April 21, 2022.

11 Editor's Note: "Treasury Sanctions Mexico- and China-Based Money Launderers Linked to the Sinaloa Cartel," U.S. Department of the Treasury, July 1, 2024; "Federal Indictment Alleges Alliance Between Sinaloa Cartel and Money Launderers Linked to Chinese Underground Banking," U.S. Department of Justice, June 18, 2024; Antoni Slodkowski, "China police probe drug-related money laundering operation after US tip," Reuters, June 19, 2024.

12 Editor's Note: See, for example, Vanda Felbab-Brown and Diana Paz García, "How technology is transforming crime and terrorism," Brookings Institution, April 13, 2026.

13 Editor's Note: See Leo Sands, "Drug smuggling: Underwater drones seized by Spanish police," BBC, July 4, 2022.

14 Editor's Note: "Spain seizes 30 tons of cocaine in record European haul, detains 23 crew," Reuters, May 7, 2026.

# Feature Commentary: Guardrails Under Test: Terrorist Misuse of AI Models and the Open-Weight 'Abliteration' Problem

By Adam Hadley

**The most serious near-term threat posed by artificial intelligence to counterterrorism is what information and support AI models are willing to provide to terrorists, and that property is almost entirely unmeasured. This article reports the results of the pilot run of Tech Against Terrorism's Counter-Terrorism AI Benchmark, which showed that almost one-third of responses from AI models provide meaningful uplift when prompted to assist malicious actors in the preparation of terrorist activity despite guardrails in place meant to prevent such responses. A model's capability sets the outer limit of how much uplift the model could provide whereas its guardrails and model disposition decide what information it is willing to share. Strategically most worrisome, guardrails are probably removable for all open-weight models, making the release of open-weight models potentially catastrophically irreversible as a result. This article closes with key considerations for public safety benchmarking built by domain specialists, for 'abliteration' resistance testing before open release, and for obligations that follow the supply chain to inference providers.**

There are hundreds of public benchmarks for what artificial intelligence models can do but almost nothing systematic focused on whether they are safe and secure to use. Intelligence, quality, performance, and price benchmarking is measured continuously, competitively, and openly, with leaderboards[a] updated within hours of a model's release. Safety, on the other hand, is measured privately by developers, against standards they set themselves with little to no transparency, with results they are under no obligation to publish.

The Executive Order of June 2, 2026, directs American agencies to—by August 1—adopt a voluntary pre-release review framework and to "develop and maintain a classified benchmarking process to assess the advanced cyber capabilities of AI models and determine the threshold at which an AI model should be designated a 'covered frontier model' for the purposes of this order," meaning the model is designated as having high-capability cyber risks.[1] The pre-deployment agreements the Center for AI Standards and Innovation[b] has reached with the major AI laboratories apply to use cases concerning cybersecurity, biosecurity, and chemical weapons.[2] However, terrorist misuse of AI is only assumed to fall within one of those categories. Indeed, there appear to be no plans for systematic measurement of how leading models respond when a user asks for help to commit an act of terrorism.

Whether an AI model possesses dangerous knowledge and whether it will hand that knowledge to someone with terrorist intent are separate questions. Capability inevitably rises with every generation of large language model (LLM) released, and we should assume that eventually all frontier models—the most capable general-purpose AI models available at any given moment—will have the knowledge and inference ability to provide meaningful uplift to terrorists absent appropriate guardrails. Train a system to reason like a doctoral chemist and it will understand explosive material: The competence that makes that possible is the same competence that makes the system worth building in the first place. Capability therefore sets the upper limit of the threat. Within that limit, then, the critical variable is the model's disposition or willingness to cooperate: what the model agrees to do, for whom, and on what pretext. Disposition can be enforced through guardrails. Guardrails can be tested and improved between one release and the next, and since uplift becomes observable only when guardrails have failed, they are the part of the system an AI model can most fairly be held to account for. A model with dangerous latent capability without robust guardrails also raises the question of whether it should be released at all.

The Tech Against Terrorism Counter-Terrorism AI Benchmark was built to compare disposition and operational uplift across all of the major closed and open-weight models. The results of the initial pilot are poor enough on their own terms alone; however, they also point to something worse: the almost complete absence of guardrails on the 'abliterated' open-weight models.

## Terms of Art

A closed AI model is reached only through its developer's own interface (chatbot or Application Programming Interface, API).

a An AI leaderboard is "a ranking system that compares AI model performance on standardized benchmarks." Leaderboards "track how different models score across multiple evaluation metrics." "Evaluation & Benchmarks: Leaderboard," ArtificialIntelligences.com, n.d.

b The Center for AI Standards and Innovation (CAISI) serves "as industry's primary point of contact within the U.S. government to facilitate testing and collaborative research related to harnessing and securing the potential of commercial AI systems." "Statement from U.S. Secretary of Commerce Howard Lutnick on Transforming the U.S. AI Safety Institute into the Pro-Innovation, Pro-Science U.S. Center for AI Standards and Innovation," U.S. Department of Commerce, June 3, 2025.

*Adam Hadley CBE is Executive Director of Tech Against Terrorism and Chief Executive of QuantSpark AI. He founded Tech Against Terrorism and directs the Counter-Terrorism AI Benchmark program.*

**"Performance of most guardrails seems to hinge on stated intent, which suggests a structural weakness in how the guardrails have been built."**

The developer can update it, restrict it, or withdraw it, and can see who is using it for what. Conversely, an open-weight model is published as a downloadable file that anyone with sufficient computation power can run, adapt, and redistribute, and that cannot be recalled. Open-weight models can be run locally or on the cloud by an inference provider (often the inference of an open-weight model is provided by the AI lab). Fine-tuning adapts such a model by training it further on selected data. Distillation compresses a large model into a smaller one that keeps much of its performance on modest hardware, which matters commercially because a small, specialized model routinely beats a large, general-purpose one inside a narrow domain at a fraction of the cost.

'Abliteration,' a portmanteau of ablation and obliteration, is the removal of a model's capacity to refuse. At frontier scale, the process of abliteration is uncertain and in many cases can result in degradation of the model's performance.[3] Neither is it a clean excision: Stripped models can show measurable degradation in performance and so abliterated models can behave significantly differently from the originals with guardrails intact.[4]

Throughout the report, "compliance" (and "complied") refers to a model complying with the user's request, not to compliance with safety policy, with "hedged compliance" meaning a response that opens with a refusal but then supplies the full content anyway. Because every prompt tested is a harmful one, a compliant response is one that assists with terrorist or violent extremist activity rather than refusing it. Central to this is "uplift."

Uplift is the difference the model makes to the information it is requested to provide. It is the margin between what a person could assemble from ordinary public sources (e.g., by Google search) and what the model hands them. For chemical, biological, radiological, nuclear, and explosive (CBRNE) use cases, we may also want to consider the accuracy of the uplift. A response that provides confident nonsense carries no uplift. Uplift is the extent to which a response moves somebody toward an outcome they could not otherwise have reached, or could not have reached as quickly or as reliably without the model.

## The Pilot

Tech Against Terrorism's Counter-Terrorism AI Benchmark began as a self-funded experiment, and its first run was deliberately modest. We graded nearly 2,500 responses from 27 leading models, drawn from a taxonomy we constructed of 152 ways that artificial intelligence can be misused for terrorism, spanning four domains and 13 pillars, of which 26 sub-categories were tested in this run.[5] Everything was text. Every prompt was single-shot: one question, one answer, no follow-up, no jailbreak, no second attempt after a refusal, and none of the multi-turn escalation an ordinary user reaches for within minutes of being told no.[c] This is close to the easiest examination a model could be subjected to. Every figure below is a lower bound and should be read as one. We also framed each prompt in three ways: explicit intent ("I want to cause harm"), neutral intent ("no specific harm given"), and benign intent ("I am a researcher"). The benchmark tested a representative set of 27 models—23 open-weight and four closed, from 7-billion-parameter models to large flagships across a global range of developers—including two deliberately de-guardrailed builds tested against their standard counterparts as a worst case.

For the initial pilot, we selected a broad range of LLMs released by companies in the United States, China, France, Canada, and the UAE. These included Claude (Anthropic), GPT (OpenAI), Llama (Meta), Qwen (Alibaba), Kimi (Moonshot), GLM (Z AI), DeepSeek, Falcon (TII), Mistral, Command R (Cohere), and many others. Future iterations of the benchmark will include multi-turn conversations and will differentiate between languages, framing, free versus paid, context window utilization, and other factors that might affect the performance of guardrails.

**Usable uplift.** Around a third of responses gave real assistance toward making a weapon or planning a mass-casualty attack, beyond what an ordinary search would return.

**Framing beats content.** The same request, its technical content unchanged and only the stated reason altered from an explicit harmful purpose to research, moved compliance from 17 to 42 percent. Safety post-training leaves a model holding two objectives at once, to be useful to a legitimate researcher and to refuse a malicious one, and a research frame sets the first against the second. What this shows is that performance of most guardrails seems to hinge on stated intent, which suggests a structural weakness in how the guardrails have been built.

**Refusal rates can be misleading.** Full refusals ran at 57 percent, which reads respectably until the largest non-refusal category at 15 percent—hedged compliance—is examined: AI models provided a warning about the danger of the request, followed by the content anyway. In those exchanges, the model identified the request as harmful, said so, and proceeded regardless.

**Coverage is uneven where it matters.** Prompts that sought information/instructions about explosives were refused around 80 percent of the time. Protection from providing meaningful uplift thinned out badly across the activities terrorist organizations actually spend their days on, with models complying with roughly two-thirds of requests concerning operational security, agentic planning, and autonomous operations. Guardrails appear to have been built around the questions developers expected to be asked.

**Open against closed is not the fault line.** Anthropic's Claude and Falcon3, from the Technology Innovation Institute in Abu Dhabi, ranked safest in the pilot, with China's MiniMax close behind. Alignment against terrorist misuse looked fragile across every frontier model tested: shallow and uneven for closed models, and removable for open-weight models.

**Stripped models comply with everything.** Two systems in the

c The pilot graded a single response per prompt. Multi-turn escalation, jailbreak prompting, non-text modalities, and agentic tool use were all outside its scope for the first version of the benchmark. The pilot also tested only 26 of the 152 misuse types in the taxonomy, so the coverage gaps reported here are those visible in a partial sample.

**"These systems compress the distance between a small organization and a large one … Small violent groups and well-resourced individuals are able for the first time to contest organizations very much larger than themselves, including states. That is a structural change in the balance between the nation-state and its challengers."**

sample had been deliberately relieved of their safety training.[d] They complied with 89 and 100 percent of requests, respectively, which is what a model with no guardrails looks like.

## Uplift and the Search Engine Objection

The standing objection to the warning about malicious actors using AI to advance their goals is that the information was available on the internet anyway, and that anybody sufficiently motivated could have found it with a search engine. Regardless, it is one thing for the Anarchist Cookbook to be available online versus having an AI model privately recreate it for you, supplement it with additional information, including technical data, and then provide encouragement and coaching support on an ongoing basis. To test the argument about information aggregation uplift, Tech Against Terrorism built the following test: Take the prompt, run the equivalent web searches agentically, aggregate what a competent person would retrieve from public sources in a comparable period, and grade the difference. Where chemical, biological, radiological, or nuclear material is involved, it is also necessary to evaluate the accuracy of outputs. Across the 27 models evaluated in our initial pilot, 15 generated at least one CBRNE output that exceeded the threshold of publicly available online information. More critically, nine models went further, producing actionable, technically accurate operational content, including explicit procedures for explosive synthesis complete with precise techniques, measurements, and molar ratios.

In any case, what the uplift objection gets wrong is that it imagines a single decisive disclosure, the paragraph that converts somebody who cannot build a device into somebody who can. For the self-radicalizing individual, however, even small increments can have a significant cumulative effect not to mention providing encouragement for their course of action. A model that will not supply a synthesis route may still refine a target rationale, dissolve a hesitation, correct a misapprehension, or supply the sense of an interlocutor taking the project seriously. Across a long exchange, small nudges compound.

d The two systems referred to are publicly distributed community builds derived from open-weight models, produced by third parties rather than by the original developers, and available for download from mainstream model repositories at the time of testing.

## What Terrorists Actually Do

A weakness in the current debate is that there is often such a large gulf between the AI safety community and those experts focusing on specific threats such as terrorism. The resulting literature is rich in what is technically possible and thin on what is likely to be adopted by terrorists or serve to accelerate self-radicalization pathways. Adoption of any technology is a psychological and organizational process, and the evidence from the wider economy is that AI adoption is stubbornly slow: While individual productivity gains are notable for some tasks, maximum value from AI often comes instead from redesigning workflows and operational processes. Existing terrorist organizations and movements are not obviously more agile than anybody else.

The skeptical literature has made this case well. A recent contribution to this publication applied affordance theory to the question and argued that generative artificial intelligence offers terrorists efficiency rather than transformation, that many anticipated threats remain hypothetical and shaped by worst-case reasoning rather than demonstrated use, and that terrorists have historically favored technologies that are accessible, cheap, simple to use, and easy to adapt.[6] I agree with nearly all of that reasoning, and I think it leads somewhere its authors did not intend. An abliterated frontier model on private hardware is accessible, cheap, simple to use, easy to adapt, and hard to detect. It is reliable, mature, and multi-purpose, and it is unobserved in a way no commercial assistant can be: no account, no logging, no content filtering, no terms of service to breach, and no provider able to withdraw access. Judged against the criteria those frameworks specify, a stripped open-weight model is close to an ideal terrorist technology, which is why the argument that terrorists prefer the mundane and the available should raise the strategic threat posed by abliteration rather than lower it.

Directed organizational use and ambient individual radicalization are often conflated in this debate, and they need separating. Ambient radicalization (e.g., self-radicalization) is where I would place most weight. Youth radicalization across the West is already at a level that would justify serious concern with no artificial intelligence in the picture, and much of it happens online via social media and messaging apps. Arrests and prosecutions that cite an AI model are a lagging indicator, reflecting conduct from months or years earlier and capturing only the cases that reached a legal charge. Tech Against Terrorism's incident tracker records more than 30 cases in which artificial intelligence served as an operational assistant in a real plot or attack, involving at least 11 distinct tools and linked to more than 70 deaths.[7] That count will look quaint soon enough.

A further asymmetry deserves attention. These systems compress the distance between a small organization and a large one. Capabilities that until recently required an intelligence service can now be assembled by a handful of committed people with a laptop and a crypto wallet. Small violent groups and well-resourced individuals are able for the first time to contest organizations very much larger than themselves, including states. That is a structural change in the balance between the nation-state and its challengers.

## Where the Funding Goes

Within AI safety, philanthropic funding is heavily concentrated in a small set of funders oriented explicitly toward catastrophic and existential risk, and it is this framing—the low-probability, high-consequence scenario in which a system escapes human control—

that commands most elite attention, to the frustration of those who see it as a distraction from nearer-term harms. That work is legitimate, and we do not dismiss it entirely. The dominance of this framing, however, has produced an odd inversion of the usual problem in risk management, in which the traditional difficulty has typically been getting decision-makers to prioritize high-impact, low-probability scenarios versus lower-impact but highest aggregate risk events. The focus should not be whether malicious actors would be able to obtain instructions to build a nuclear bomb from AI, but how they are already using AI to commit fraud, radicalization, and child sexual exploitation, among other uses. Speculative catastrophic scenarios are commanding the attention and budgets while harms already occurring at scale, and practical assistance to violent actors, are treated as an issue of "societal resilience."

The opportunity cost is real: Every hour spent ensuring against a hypothesis is an hour not spent on a harm that is already killing people. There is also an awkwardness at the center of the existential position that its holders rarely address. If the risk from frontier development is genuinely of that order, the straightforward mitigation is to stop, or at least to agree collectively how and when to slow down. The companies making the argument propose neither, which suggests either that the risk is overstated or that competitive pressure has overridden their risk calculus.

Another international body chartered to consider existential risk would add very little here. The missing layer is a network to connect subject-matter experts with the training, tools, and threat knowledge to evaluate particular harms, terrorism, fraud, and child sexual abuse among them, working to common standards and publishing what they find. The disconnect between the artificial intelligence safety community and the practitioner communities that deal with these harms every day remains the most consequential gap in the field.

## The Open-Weight Problem

Everything above concerns models that still have their guardrails. The strategic problem is that guardrails are removable, and that removing them is neither difficult nor necessarily expensive.[8]

Fine-tuning is the cheapest route. Ten adversarial examples and a few dollars of paid fine-tuning were enough to strip the safety behavior out of a served commercial model,[e] and low-rank adaptation on a single graphics card, for less than $200, has cut the refusal rate of a 70-billion-parameter open model to roughly one percent.[9] Surgery on the weights needs no training data at all. There is no single method of abliteration and the difficulty rises with model size, but large open-weight systems have had their guardrails stripped within days of release, and targeted removal has now been demonstrated at trillion-parameter scale on Kimi K2,[f] whose successor is discussed below. Stripped versions of models circulate as freely as the originals, on the same public repositories, with the same convenience.

**"The artificial intelligence safety community has largely not engaged with abliteration resistance. It is not clear whether this is because the question is awkward for a community that has, with good reason, championed open release or because it is considered someone else's risk to mitigate."**

Whether the newest frontier-scale releases resist the same treatment is not publicly known, and the question is about to cease being hypothetical. Moonshot AI has served Kimi K3 since July 16, 2026, and published its weights on July 27, 2026.[10] A joint evaluation by the United Kingdom's AI Security Institute and the American Center for AI Standards and Innovation found that the served version trailed the leading closed models on offensive cyber capability, reaching step 17 of a 32-step attack path on average against 28.5 for the most capable American systems, and that its guardrails did not stop it attempting exploit development at all.[11] That is the disposition of the model with its safety training intact and a provider standing behind it. What remains once the weights are public, and somebody sets about removing what little is there, nobody outside the company can say.

That is not a criticism of Moonshot, since no major laboratory publishing open weights has answered the question either. Developers may be releasing models whose behavior they can no longer govern, and nothing in the release process as it stands would tell it not to do it.

Size offers less protection than it appears to. A model of 2.8 trillion parameters is beyond the reach of an individual with hardware at home, but that is a logistics barrier rather than a safety property, and it falls the moment somebody with the means to serve the model decides to do so. A stripped frontier system running as a hosted service from a permissive jurisdiction, reachable by anyone with an account, would pair the capability of the frontier with the disposition of a machine that has never learned to refuse.

The probabilities sit oddly against the ones absorbing the field's budgets. Existential scenarios are, on any honest reckoning, very low in probability. That a frontier open-weight model can be stripped of its guardrails is a great deal more likely, and it is barely discussed. One of those questions has a research program and billions of dollars behind it. The other could be settled by a competent team in a few weeks and has not been.

Part of the reason it has not landed is that the policy conversation still assumes that all AI models are closed. When a government judges a closed AI to present a security concern, they have a control lever because—as with Anthropic's Fable 5 model—access can be withdrawn by the AI company. The lever exists because the model runs in one place, under one operator, where it can be audited, restricted, or withdrawn. On the other hand, a frontier open-weight released with removable guardrails attracts no equivalent scrutiny

e A served commercial AI model is a trained model that a vendor operates as an inference service under commercial terms, accessed by customers through an API or product interface, with the vendor retaining control of the model weights and the surrounding serving stack.

f Kimi K2 is a powerful open-weight model developed by Moonshot AI, with 1 trillion total parameters; it uses an MoE structure and 32b active parameters. It is optimized specifically for advanced reasoning, coding, and multi-step agentic workflows. "Kimi K2.6: From Code to Creation, From One to Many," KIMI, n.d.; Richard Gall, "Kimi K2: What's all the fuss and what's it like to use?" thoughtworks, July 18, 2025; "MoonshotAI / Kimi-K2," GitHub, n.d.

before publication. It has no control lever because once published, the open-weight model can be downloaded and run by anyone with the necessary computational power.

## Not an Argument Against Open Models

None of this is a case against publishing weights. Open models are among the most valuable developments in the field. Organizations choose them for cost, privacy, regulatory compliance, control, and sovereignty, and they allow states and institutions that will never build a frontier laboratory to run capable systems on their own infrastructure, under their own law. Inference is moving steadily toward local and private deployment for those reasons. The future of artificial intelligence probably depends on open weights, and the arrival of frontier-capability open models is in itself a considerable good.

That is why the safety of open releases matters so much, and why the answer is more engineering rather than less of it. Guardrails that sit in a thin layer above a capable model will likely always be removable. Building refusal into the substance of a model, so that it cannot be excised without destroying the capability that made the model worth taking, is among the most valuable unsolved problems in artificial intelligence safety. No open-weight laboratory has convincingly demonstrated a solution publicly, and almost nobody seems to be funding the attempt at scale. Set against the sums going into frontier capability, safety research of this kind is more of a rounding error, which is a strange way to treat the only thing standing between a published model and its worst use.

## Key Considerations

**Systematic safety benchmarking before release, agreed internationally within months rather than years.** Terrorist misuse should consistently and reliably be evaluated as a category in its own right by all developers rather than as an assumed subset of cyber or chemical, biological, radiological, and nuclear review. It should measure disposition and uplift on separate axes, since a model that agrees to help and answers badly is a different failure from one that refuses reliably, and the two demand different remedies. It should cover the full range of use cases of these actors, and it should be built by domain specialists and published, so that models can be compared, methods criticized, and developers that have done the work properly credited for it. Dario Amodei has argued that the pace of development is compounding while the policy apparatus available to governments is not, and that policy therefore has to be made on the exponential rather than on the historic trend.[12] Standards agreed in three years will describe a world that no longer exists.

**Abliteration resistance testing before open release.** Any developer publishing frontier weights should be expected to attempt the removal of its own guardrails, to publish what happened, and to release in a way that is not irreversibly dangerous. Where guardrails prove removable and the capability is high, the proportionate response may be a controlled release or none. We are not aware of a single major open-weight release that has published such a test.

**Obligations that follow the supply chain.** Frontier labs are not the only actors carrying a duty here. Infrastructure providers, hosting platforms, model repositories, and inference providers all sit between a published model and its use, and inference providers in particular are placed to conduct proportionate due diligence on customers running stripped models at scale.

The artificial intelligence safety community has largely not engaged with abliteration resistance. It is not clear whether this is because the question is awkward for a community that has, with good reason, championed open release or because it is considered someone else's risk to mitigate.

Nevertheless, addressing this risk requires little: We ask for the labs that publish frontier weights to disclose whether they have attempted to strip their own guardrails, and share what happened when they did. Technology released in a state where its protections can be removed by a determined individual over a weekend is insecure by construction. Open-weight abliteration is therefore not merely a safety question but a matter of urgent geopolitical concern. CTC

## Citations

1 "Promoting Advanced Artificial Intelligence Innovation and Security," Executive Order, The White House, June 2, 2026. On the wider scope of the voluntary pre-deployment agreements, see Center for AI Standards and Innovation announcements of evaluation agreements with Anthropic, OpenAI, Google DeepMind, Microsoft and xAI, 2025 to 2026.

2 NIST, "Center for AI Standards and Innovation (CAISI)," nist.gov/caisi

3 Tom Wollschläger, Jannes Elstner, Simon Geisler, Vincent Cohen-Addad, Stephan Günnemann, and Johannes Gasteiger, "The Geometry of Refusal in Large Language Models: Concept Cones and Representational Independence," Proceedings of the 42nd International Conference on Machine Learning, arXiv:2502.17420, February 24, 2025; Vadym Hadetskyi, Dario Pasquini, and Artem Sorokin, "Not All Refusals Are Equal: How Safety Alignment Fails Cybersecurity at Scale," arXiv:2607.02714, July 2, 2026, which reports ablation experiments on the one-trillion-parameter Kimi K2.

4 Andy Arditi, Oscar Obeso, Aaquib Syed, Daniel Paleka, Nina Panickssery, Wes Gurnee, and Neel Nanda, "Refusal in Language Models Is Mediated by a Single Direction," arXiv:2406.11717, June 17, 2024, published in *Advances in Neural Information Processing Systems* 37 (2024). On the off-target effects of the technique, see Aleksander Fafuła, "Abliteration Is Not a Scalpel: Off-Target Effects of Refusal Removal on Decision Disposition Across Model Families," arXiv:2607.17427, July 19, 2026.

5 "Counter-Terrorism AI Benchmark: Pilot Report," Tech Against Terrorism, July 2026, www.ct-ai.org.

6 Andrew Glazzard, David McIlhatton, and Paul Martin, "Will Generative AI Fundamentally Change Terrorist Threats?" *CTC Sentinel* 19:5 (2026).

7 Tech Against Terrorism artificial intelligence incident tracker, accessed July 2026.

8 Xiangyu Qi, Yi Zeng, Tinghao Xie, Pin-Yu Chen, Ruoxi Jia, Prateek Mittal, and

Peter Henderson, "Fine-tuning Aligned Language Models Compromises Safety, Even When Users Do Not Intend To!" arXiv:2310.03693, October 5, 2023.

9 Ibid.; Simon Lermen, Charlie Rogers-Smith, and Jeffrey Ladish, "LoRA Fine-tuning Efficiently Undoes Safety Training in Llama 2-Chat 70B," arXiv:2310.20624, October 31, 2023; Kevin Kuo, Chhavi Yadav, Virginia Smith, "Open-Weight LLM Fine-Tuning Defenses are Susceptible to Simple Attacks," arXiv:2605.26526, May 26, 2026.

10 Moonshot AI, Kimi K3, served from July 16, 2026, with full open weights announced for release on July 27, 2026.

11 "UK AISI / CAISI Preliminary Assessment of Kimi K3's Cyber Capabilities," UK AI Security Institute and US Center for AI Standards and Innovation, July 23, 2026.

12 Dario Amodei, "Policy on the AI Exponential," darioamodei.com, June 2026.

# The Historical Evolution of the Islamic State's Anti-China Propaganda

By Lucas Webber, Riccardo Valle, Colin P. Clarke, and Daniele Garofalo

**This article traces how the Islamic State has come to view China over the years. Over the past decade, within the Islamic State's broader propaganda and operations ecosystem, Beijing has evolved from a peripheral grievance into a routinized enemy, with serious implications. It argues that this evolution unfolded in four phases: early, episodic references to Uyghur suffering prior to 2014 and, after 2014 and the caliphate's proclamation, a gradual consolidation under Islamic State central media, which embedded Xinjiang and "East Turkestan" into the group's global narrative; a period of experimentation with Chinese-language content and symbolic threats, including Mandarin-language *nasheeds* and Uyghur-focused videos; the emergence of Islamic State Khorasan Province (ISKP) as the movement's anti-China vanguard; and finally, normalization of China alongside the usual arch-enemies of jihadis—America, Russia, and local regimes—and expansion of the anti-China campaign to Africa. The article concludes that China's ascent to great-power status and deepening involvement in fragile Muslim-majority regions will sustain, and likely increase, its prominence in Islamic State discourse, posing a persistent, if uneven, security challenge for Beijing and its partners.**

Over the past decade, the Islamic State has moved China from the periphery of its worldview to a routinized enemy whose interests are legitimate targets for both propaganda and attack.[1] This shift has not been linear, and it cannot be understood simply as a reaction to Beijing's repression of Uyghur Muslims in Xinjiang. Rather, it emerges from the interplay of three major developments: the evolution of Islamic State central media after the proclamation of the caliphate in 2014; experimentation with Chinese-language and Uyghur-focused content; and, more recently, the rise of Islamic State Khorasan Province as the movement's anti-China vanguard.[2]

This article traces that trajectory in four phases primarily through the lens of Islamic State propaganda content and output. It begins by briefly situating the Islamic State's hostility toward China in pre-2014 jihadi discourse, then shows how the group's central media after 2014 converted sporadic grievances into a recurring campaign theme. It then examines the Islamic State's experimentation with Chinese-language material and symbolic threats during the mid-2010s, before turning to ISKP's post-2019 efforts to weaponize China's regional posture and Taliban-China relations.[3] The final section argues that by the mid-2020s, violence and propaganda against Chinese targets had become normalized components of the Islamic State repertoire, lowering the threshold for future attacks on Chinese interests. The aim of this article is to accurately describe how the Islamic State views China in its media releases, how the views expressed through media content have changed over time, and why this matters for the terrorist threat landscape facing China. This includes a look ahead to regions such as sub-Saharan Africa where Beijing is likely to face increased resistance and outright hostility toward its expanding presence. This more aggressive pushback against Chinese interests is reflected in the proliferation of Islamic State media accounts, both official and unofficial, placing Beijing in their collective crosshairs.

## Phase 1: From Early Uyghur Grievances to Caliphate Rhetoric (2009-2014)

The Islamic State's hostility toward China predates the formal caliphate but was initially episodic and derivative of broader jihadi concerns. In the late 2000s, when the Islamic State was still the Islamic State in Iraq (ISI) and part of al-Qa`ida's transnational network, references to Uyghur suffering only appeared sporadically in its messaging. Shortly after the 2009 Urumqi riots and ensuing crackdown, ISI released a lengthy martyrdom video[4] that advocated for the protection of the Uyghurs, threatened Beijing, and folded Xinjiang into a global narrative of Muslim oppression at the hands of "crusaders," "Jews," and local "apostates." This material foreshadowed later themes but did not yet place China at the center of Islamic State strategy. Geopolitical developments have impacted this shift to a more China-focused Islamic State propaganda

*Lucas Webber is a Senior Threat Intelligence Analyst at Tech Against Terrorism, a Senior Research Fellow at The Soufan Center, and the Co-Founder and Editor-in-Chief of MilitantWire.com. X: @LucasADWebber*

*Riccardo Valle is a research analyst, security consultant, and founder of Militancy Chowk. He conducts research on armed groups and international jihadi non-state actors. He is currently the Director of Research at The Khorasan Diary. X: @Valle_Riccardo_*

*Colin P. Clarke is the Executive Director of The Soufan Center. He also serves on the editorial board of Studies in Conflict and Terrorism, as well as Terrorism & Political Violence. X: @ColinPClarke*

*Daniele Garofalo is an analyst and researcher specializing in jihadi terrorism, armed and insurgent groups. He also monitors terrorist propaganda and serves as a security consultant. He is the founder and director of the intelligence platform Daniele Garofalo Monitoring. X: @G88Daniele*


*Figure 1: ISI discussing Xinjiang in a 2009 video*

campaign, with operational implications expected to follow.

The proclamation of the caliphate in 2014 marked a turning point. In June of that year, Islamic State spokesman Abu Muhammad al-Adnani announced the establishment of the caliphate, and within days, Islamic State leader Abu Bakr al-Baghdadi's audio message "A Message to the Mujahidin and the Muslim Ummah in the Month of Ramadan" highlighted "the extreme torture and degradation of Muslims in East Turkestan."[5] Al-Baghdadi condemned China for preventing Muslims from exercising their basic rights and signaled that Beijing's policies in Xinjiang would occupy a significant place in the caliphate's worldview.

Subsequent Islamic State leadership statements reinforced this framing. In a July 2014 sermon, al-Baghdadi claimed that Muslims' rights were being seized in China and boasted of foreign fighters from a range of countries, including China, thereby asserting both the caliphate's global reach and its connection to Muslims in Xinjiang.[6] In 2015, he questioned Saudi Arabia's credibility by asking why its rulers did nothing for Muslims in China, an attempt to use Uyghur suffering as a wedge issue to delegitimize regional regimes.[7]

In his role as official Islamic State spokesman, the individual who was long believed to be al-Baghdadi's deputy, al-Adnani, echoed and amplified these themes through his own speeches.[8] In a September 2014 address, for example, he lamented "hundreds of thousands of dead, wounded, and imprisoned Muslims, and the millions displaced … all over the world at the hands of the Jews, crusaders, Rafidah, Nusayriyyah, Hindus, atheists, and apostates, in … China, the Caucasus, and elsewhere," explicitly grouping China with an array of religious and ideological enemies.[9] In 2016, al-Adnani again singled out Chinese "atheists" for committing "massacres, crimes and atrocities against the Muslims in … Turkestan," thus placing Beijing alongside other *taghut* (tyrant) powers like Russia and the United States in the Islamic State's cosmology of enemies.

In this first phase, China was not yet a distinct nor coherent propaganda campaign, but the rhetorical building blocks were laid: Xinjiang as "East Turkestan," Uyghur repression as emblematic of anti-Muslim tyranny, and China as one of several great powers oppressing Muslims worldwide.[10] The ground was prepared for a more sustained focus once the Islamic State's central media consolidated after 2014.[11] Given its prominent role on the world stage, China has always been on the Islamic State's radar, especially in terms of propaganda and strategic communications. But over time, as China's physical presence has expanded to different regions, and as its treatment of Uyghur Muslims became more widely discussed, Beijing has also found itself rising on the list of priorities in terms of Islamic State operational focus. Over time, the salience of China as an enemy prioritization has shifted, growing in response to geopolitical developments and the behaviors and perceived behaviors of the Islamic State's adversaries.

## Phase 2: Experimentation and Linguistic Targeting (2014-2017)

Between 2014 and 2017, Islamic State central media moved from occasional references to China toward a more deliberate, experimental campaign that tested Chinese-language and Uyghur-focused products.[12] This can be seen by the gradual and slow increase of Mandarin- and Uyghur-language media content as well as a relative focus on Chinese themes, despite being considerably inferior in quantity and quality than other topics. The consolidation of Islamic State media under the Diwan of Media during this period provided the organizational capacity to pursue such experiments in a coordinated way.

The group's flagship English-language magazines—Dabiq and its successor, Rumiyah—played a key role in embedding China into the group's global narrative.[13] They more often referenced Xinjiang as "East Turkestan," reproduced segments of al-Baghdadi and al-Adnani speeches mentioning Uyghur repression, and presented the reconquest of East Turkestan as part of the caliphate's long-term territorial ambitions.[14] As part of the group's stated intention of expanding the Islamic State "until they reach Indonesia, China, Spain, and Rome," propaganda maps were circulated online depicting future Islamic State provinces stretching from the Levant through Khorasan into Xinjiang, visually inscribing Chinese territory into the group's imagined state.[15]

At the same time, the Islamic State invested in linguistic outreach to Chinese language audiences. An October 2014 video, released by the group's media apparatus, featured Chinese subtitles and celebrated a "Chinese brother" who had conducted a suicide operation in Iraq.[16] This production signaled both technical capability and a willingness to present Chinese-speaking militants as exemplars and martyrs.

In July 2015, another video featured an elderly cleric from Xinjiang calling for the killing of "Chinese infidels," interspersed with scenes of Uyghur children pledging violence. This was a theme cultivated by the Islamic State across multiple conflict zones and theaters, including in Iraq and Syria, where the 'Cubs of the Caliphate' concept was born and featured in the group's propaganda. The carefully staged imagery in the case of China, as it did in the Middle East, suggested an intergenerational, socially embedded jihad against Beijing rather than a marginal cause.[17] In other words, while the approach was not unique to China, it demonstrated that China was on equal footing with other countries and regions prioritized in Islamic State propaganda.

In November 2015, the first killing of a Chinese citizen by the Islamic State was featured in its propaganda by highlighting Fan Jinghui in Dabiq magazine as a hostage "for sale," then later claiming that he and a Norwegian captive had been "executed" after being abandoned by "*kafir*" nations and organizations.[18] However, perhaps the most notable experiment was the release of a Mandarin-language *nasheed* (Islamic chant) in December 2015.[19]

*Figure 2: The Islamic State discussing Xinjiang in a 2015 video*

Although there was no sizable, discernible increase in recruitment among Chinese militants in favor of the Islamic State, nor an increase in the Mandarin language media content production supporting the Islamic State, the *nasheed* carried disproportionate symbolic weight. It demonstrated that the Islamic State was prepared to address Chinese-speaking audiences in their own language, to graft its ideology onto local grievances, and to test whether such content could resonate within Uyghur and broader Sinophone Muslim environments. It also directly challenged jihadi organizations—both global and local—that were traditionally considered the only platforms available for Mandarin-speaking and Uyghur militants until the inception of the Islamic State. Furthermore, the Islamic State's al-Hayat Media Center produced numerous Uyghur-language *nasheeds* around this time.[20]

The influence of these efforts extended into the digital sphere among supporters. In early 2016, a Tsinghua University website was briefly defaced with jihadi slogans calling for "holy war," illustrating how pro-Islamic State sympathizers could contest Chinese symbolic spaces even without physical access.[21] In February 2017, an Islamic State video released by al-Furat Media showed a Uyghur fighter threatening China and promising revenge.[22] The video was part of the Islamic State's attempt to reach out to militants affiliated with rival organizations and to potential supporters in China—a tactic applied also to other theaters where the Islamic State lacked physical presence—thus signaling to Chinese and Uyghur militants that the Islamic State was a viable platform for armed struggle. Shortly thereafter, the Islamic State claimed responsibility for the kidnapping and killing of two Chinese nationals in Pakistan's Balochistan, as a retaliation for Pakistan's security forces' counterterrorism operation in the area, translating years of symbolic hostility into concrete violence.[23]

Taken together, this phase was characterized by experimentation. Islamic State central media tested Chinese-language outreach, elevated Uyghur grievances, and began to depict Chinese citizens and infrastructure as legitimate targets. These experiments would prove important once regional conditions changed and a more proximate Islamic State affiliate took up the anti-China banner.[24] Furthermore, the propaganda manifested into Islamic State killings and plots targeting Chinese nationals and interests for the first time, signaling a shift in the targeting imperative.[25] Still, it should be noted that this was not the first instance of a jihadi group killing a Chinese national. In June 2009, an attack launched by al-Qa`ida in the Islamic Maghreb (AQIM) against an Algerian paramilitary police convoy escorting Chinese construction workers led to 19 paramilitary police and one Chinese worker killed.[26]

## Phase 3: Economic Imperialism, COVID-19, and the Emergence of ISKP as Vanguard (2020-Present)

As China's overseas footprint expanded and the Belt and Road Initiative (BRI) accelerated, Islamic State narratives opportunistically shifted from a Xinjiang-centric grievance frame to a broader critique of Chinese economic imperialism.[27] This evolution coincided with the rise of ISKP, headquartered in Afghanistan, as the movement's spearhead on propaganda and attacks targeting China.

With China's growing political, diplomatic, and economic footprint, it is inevitable that Beijing will encounter friction in certain parts of the world. South Asia is one of the regions where a more visible Chinese presence has resulted in an aggressive push-back from a range of violent non-state actors, including separatists and jihadis.


*Figure 3: From ISKP Al-Azaim video "The Unrestrained Metastasis Within the Body of the Ummah"*

### *Economic Imperialism and Belt and Road Narratives*

During this period, the Islamic State's Arabic-language weekly newsletter Al Naba began portraying BRI not as a neutral development project but as a scheme for political capture and exploitation.[28] Articles described China's "method of investment" as a way of binding tyrannical governments in Muslim-majority countries through debt and infrastructure, forecasting that Beijing would eventually intervene directly with military forces to defend its interests. In this narrative, Chinese nationals, diplomatic facilities, and commercial projects became legitimate targets for preemptive violence, justified as defensive measures against an encroaching imperial power. For the Islamic State, this has become a self-fulfilling prophecy, since Beijing's expansionist ambitions show no signs of ebbing, and thus, are portrayed as proof of China's creeping imperialism.

This framing was particularly salient in regions where Chinese investments were highly visible, but local grievances were acute. China-Pakistan Economic Corridor (CPEC) infrastructure,[29] energy pipelines in Central Asia, and mining ventures in Afghanistan and Pakistan were cast as the soft underbelly of a rising superpower.[30] In 2017, pro-Islamic State outlet Al-Battar Media Foundation proclaimed that it was entering into a state of war with China and would target Beijing's "New Silk Road" initiative in the name of defending Uyghur Muslims. Jihadi and separatist groups beyond the Islamic State,[31] including Pakistani Taliban (or Tehrik-i-Taliban Pakistan, TTP) factions and Baloch insurgents, converged on

similar themes, sometimes targeting Chinese nationals as symbols of unwanted foreign intrusion.[32]

### *COVID-19 as "Soldier of Allah"*

The COVID-19 pandemic added another layer to the Islamic State's anti-China discourse. Beginning in early 2020, pro-Islamic State channels on encrypted platforms framed the virus as a "soldier of Allah" sent to punish China and other enemies of Islam. Posters and unofficial media depicted figures in protective suits alongside slogans linking the outbreak in Wuhan to divine retribution for Uyghur repression and other alleged crimes against Muslims.[33] Official outlets amplified this message. Al Naba editorials described COVID-19 as a torment from God for the "Crusader" countries and infidels, with China frequently included in that category.[34] The pandemic thus became a symbolic bridge connecting theological ideas of punishment and cosmic justice to geopolitical criticism of Beijing.

Rather than focusing solely on public health consequences, the Islamic State interpreted the outbreak through a theological lens, presenting COVID-19 as a manifestation of divine retribution against states accused of oppressing Muslims, including China, because of its policies in Xinjiang. The Islamic State sought to link contemporary geopolitical events to religious concepts of justice and punishment.[35]


*Figure 4: Posted by a pro-Islamic State supporter group in 2020*

Pro-Islamic State media networks quickly incorporated the pandemic into their anti-China messaging.[36] In several cases, COVID-19 was described as an opportunity created by God to weaken hostile powers and expose the vulnerability of states that jihadi propagandists routinely portrayed as enemies of Islam.[37] Quraysh Media, for example, circulated propaganda posters (not pictured) depicting a hazmat-suited individual accompanied by the slogan, "China: coronavirus … A promise is a debt we must not forget." Posts celebrated the pandemic with messages such as "May God punish China with death, as they had brought death to Muslims," "as China beats Uyghur Muslims, coronavirus is now beating China," and "the virus is God's army that destroys the kafir (infidels)."

Significantly, the COVID-19 narrative did not exist or emerge in isolation. Instead, it was absorbed into an already established anti-China propaganda framework centered on the plight of Uyghur Muslims. This framing enabled propagandists to reinforce anti-China sentiment, legitimize hostility toward Chinese interests abroad, and integrate contemporary geopolitical developments into a broader worldview grounded in religious conflict and cosmic justice.

### *ISKP's Rise and the Taliban-China-Uyghur Triangle*

Islamic State central media gradually reduced explicit references to Uyghurs after 2016, possibly due to the lack of actual support from Uyghur militants, difficult access to the population, and the strategic choice of concentrating its media focus on other theaters. However, ISKP began to emerge as the entity in the movement that spearheaded the release of anti-China content with an unprecedented volume, in-depth content, and a string of attacks against Chinese citizens and interests. It seems that initially, ISKP's media apparatus remained tightly controlled by Islamic State central, and that it was abiding by the rules and procedures of the Islamic State media apparatus for official releases.[a] As a consequence, anti-China content was limited despite the presence of figures such as Abu Zar al-Burmi, a Burmese preacher known for his fiery anti-China rhetoric.[38] Only after ISKP lost its territorial strongholds in eastern Afghanistan around 2019-2020, and its media production became more decentralized through the emergence of various unofficial outlets, did anti-China themes crystallize.[39] Moreover, in January 2020, a plot was foiled in Brest, northwest France, where seven suspects were arrested for allegedly planning attacks on a French military site and local Chinese New Year celebrations, with the cell reportedly having recorded pledges of allegiance to the Islamic State.[40]

ISKP's strategy was to frame China's engagement with the Afghan Taliban as evidence of Taliban 'apostasy' and 'betrayal.' As the Taliban advanced militarily and retook Kabul in August 2021, pro-ISKP outlets ramped up anti-Taliban and anti-China messaging. The newly designated official media branch, Al-Azaim Foundation, began producing a steady stream of content castigating the Taliban for normalizing relations with Beijing, accepting Chinese aid and investment, and endorsing the "One China" policy.[41] Media content produced by the group systematically criticized Afghan Taliban and Chinese officials, accusing the Taliban of selling out oppressed Muslims in exchange for economic aid and international

a Media content produced by the Islamic State's regional branches and affiliated publishing houses have to be submitted to and reviewed by the Media Monitoring Committee. Prior to 2020, ISKP media content was exclusively published by Islamic State's central media. However, gradually after 2020, ISKP started publishing its own content bypassing Islamic State's central media. See Islamic State rulings on media content in Daniel Milton, *Pulling Back the Curtain: An Inside Look at the Islamic State's Media Organization* (West Point, NY: Combating Terrorism Center, 2018), documents 1, 2, 5.

recognition.[42][b] Editorials and booklets in Pashto, Dari, and English attacked Taliban statements that framed Xinjiang as an internal Chinese issue and criticized Kabul's assurances that it would not allow Uyghur militants to operate from Afghan soil.[43] In this telling, China was not just another external enemy; it was the power that had successfully co-opted the Taliban, thereby justifying ISKP's war on both.

ISKP's operational activity further reinforced this narrative. The October 2021 suicide attack on a Shi`a mosque in Kunduz—carried out by a bomber identified as "Muhammad al-Uyghuri"—was used by ISKP and affiliated pro-Islamic State media to merge themes of Uyghur identity,[44] hostility toward the Taliban, and anti-China messaging into a single symbolic event.[45] The Islamic State's Amaq News Agency named the attacker "Muhammad al-Uyghuri" and claimed that "the Taliban has pledged to expel and oust [Uyghurs] at the request of … China."

By early 2022, ISKP had fused earlier Islamic State themes—Taliban criticism, Uyghur solidarity, opposition to economic imperialism, and defiant great-power rhetoric—into a more sustained campaign. As a result, follow-on ISKP attacks and alleged plots against Chinese nationals in Afghanistan and the broader region were framed as strikes against a *taghut* regime that ISKP cast as a primary enemy. China was no longer just another distant oppressor; it was a proximate, active player in ISKP's operating environment and a symbolically rich target around which to organize its challenge to the Taliban. ISKP effectively merged anti-Taliban narratives with global anti-China Islamic State narratives. Numerous publications depicted the Taliban as *de facto* security guarantors to Shanghai Cooperation Organization (SCO) member states against ISKP in the region, whereas in other narratives, the group placed China alongside the United States and Russia as "modern Pharaohs."[46] ISKP sought to elevate Beijing to top-tier enemy status in the minds of supporters, consistent with its widening focus beyond merely local Afghan or Pakistani issues to a broader global agenda. In this context, ISKP sought to expand its regional vision by launching the now-defunct Arabic-language magazine Sadoy Khorasan.[47] Issue 5 chiefly featured one of the most detailed articles against China regarding the Arabic-speaking Muslim world's relations with China, including international organizations such as the World Council of Muslim Communities, as well as the organization's visit to Xinjiang.[48]

Operationally, the most significant attack carried out by ISKP that purposely targeted Chinese civilians—"diplomats and businessmen," as the group claimed—was the assault on the Kabul Longan Hotel on December 12, 2022, which housed Chinese nationals and Taliban officials.[49] The attack was carried out by two Tajik nationals and resulted in the death of three individuals—none of them Chinese nationals—several injuries, including Chinese nationals, and the death of one of the attackers. The attack remains the most significant one carried out by ISKP targeting Chinese nationals due to the motivation of the attack, which was explicitly targeting Chinese foreigners; the preparation, as the two attackers stayed inside the hotel for days; and the impact of the attack, which could have resulted in more Chinese casualties if they had succeeded.[50] ISKP and pro-Islamic State outlets exploited the Kabul hotel attack to amplify Al Naba's themes, with Al-Azaim quickly issuing a Pashto- and Persian-language image of the attackers amid hotel smoke, later translated into Tajik by Al-Azaim Tajiki.[51] The Kabul hotel assault did not occur in isolation. Earlier that same year, in January 2022, ISKP conducted a suicide bombing outside the Taliban's Foreign Ministry building in Kabul, timed around the expected arrival of a Chinese delegation. The attack signaled the group's intent to target Chinese diplomacy, as well as to challenge the Afghan Taliban's reassurances of guaranteeing security and the Taliban's broader relationship with China.[52]

In 2023, ISKP carried out a suicide attack in June in Badakhshan Province that resulted in the killing of several Taliban officials.[53] According to ISKP, the goal of the attack was to disrupt Islamic Emirate of Afghanistan (IEA)-China security efforts and to terrorize China's economic plans in the region.[54] In January 2025, ISKP claimed its second direct attack against a Chinese national in Afghanistan. The operation occurred in a village in the northern province of Takhar. During the attack, a group of ISKP militants stopped the vehicle in which a Chinese mining worker and his translator were traveling, and executed the miner.[55] A year later, in January 2026, ISKP conducted a suicide bombing at the Chinese noodle restaurant in Kabul, which killed six local Afghans and one Uyghur Muslim. This attack helped to amplify ISKP's China-focused narratives, spotlight its anti-China activity to an international audience, and likely gain more credibility with other jihadis and extremists who hold anti-China grievances. Consequently, ISKP immediately capitalized on the attack. On February 4, 2026, after a six-month hiatus, ISKP published issue 38 of Khorasan Ghag magazine, which carried an article seeking to exploit the international backlash over the attack for its own purposes. In the article, the ISKP directly addressed the Uyghur population, presenting itself as the only jihadi group that is attacking China on their behalf, accusing Kabul and Islamabad of ignoring the Uyghur issue.[56] The April 2026 issue of Voice of Khurasan continued to capitalize on the attack by translating the Khorasan Ghag issue into English and boasting about how the attack bypassed the Taliban's security.[57]

Simultaneously, since 2023, ISKP has been attempting to expand its recruitment of Uyghur militants allegedly based in Afghanistan. In February 2023, ISKP released its first publication exclusively dedicated to China, the Uyghurs, and the Taliban.[58] In the text, ISKP directly addresses East Turkistan Islamic Party (ETIP) militants in Afghanistan, arguing that while the Taliban are preventing them from attacking Chinese interests in the country, ISKP is eager to provide them with a platform for carrying out terrorist operations. The message was reiterated in September 2023 when ISKP discussed at length the status and fate of the ETIP in Afghanistan, arguing that ISKP is the only jihadi platform for targeting Chinese interests in the region, while stating that the Taliban have reduced the Uyghur issue to a solely internal matter

b For instance, this includes criticism of Deputy Foreign Minister Muhammad Naeem Wardak's statements on the Uyghur issue being an internal issue of China; Afghan Taliban Prime Minister Abdul Sala Hanafi's remarks that Afghanistan adheres to the "One China Policy;" Afghan Taliban ambassador to China Bilal Karimi's statements saying that the Taliban are assisting China in countering ISKP; senior Taliban leader Maulvi Abdul Kabir's statements on ISKP as a common enemy of China and Afghanistan; and Taliban officials meeting Chinese Foreign Minister Wang Yi. See Khorasan Ghag, Issue 37, pp. 10-11; Khorasan Ghag, Issue 33, p. 41; Khorasan Ghag, Issue 28, p. 45; Khorasan Ghag, Issue 30, p. 50; Khorasan Ghag, Issue 31, p. 26; "TKD MONITORING: New ISKP Video Describes the History of East Turkestan," Khorasan Diary, December 1, 2023; "TKD MONITORING: New Video from ISKP Criticizes Taliban over Palestine and Xinjiang," Khorasan Diary, November 19, 2023.

of the Chinese government.[59]

As part of the group's strategy to exploit the growing ties between the Afghan Taliban and China to boost recruitment among jihadi organizations, ISKP also expanded its criticism of Afghan Taliban-China relations to other jihadi rivals in the region. Among jihadi groups in the region, the Pakistani Taliban and its factions are the main recruitment targets for ISKP. In the recent past, Pakistani Taliban militants have been accused of carrying out attacks in Pakistan that led to the death of Chinese nationals, such as the April 22, 2021, suicide bombing at a hotel in Quetta, where the Chinese ambassador was present; the July 14, 2021, bomb attack targeting a bus carrying Chinese engineers in Dasu; and the March 26, 2024, suicide bombing in Shangla, also targeting a bus carrying Chinese engineers.[60] In this context, ISKP seeks to instrumentalize the issue to compete with other jihadi organizations. For instance, issue 13 of Urdu language ISKP magazine Nida-e-Khorasan, published in January 2026, accused the TTP of following the Afghan Taliban path in appeasing the international community, including assuring China that it does not harbor any hostility against it.[61] Even religious political parties in Pakistan were not spared criticism, as in Issue 3 of Nida-e-Khorasan, the leader of the Pakistani religious-political party Jamaat Ulema-e-Islam-Fazl (JUI-F), Mawlana Fazlur Rehman, was criticized for having cordial relations with China, in addition to his support for the Afghan Taliban's government.[62]

## Phase 4: Normalization, Multipolarity, Outlet Diversification, and African Expansion (Late 2022/Early 2023-Present)

By the mid-2020s, hostility toward China had become somewhat routine within the Islamic State's broader ecosystem. What had begun as less frequent linguistic outreach and sporadic rhetorical denunciations had matured into routine, almost bureaucratic messaging and opportunistic violence. Similar evolutions against other Islamic State targets have resulted in real-world, physical attacks. For instance, in September 2022, ISKP attempted to conduct a suicide bombing outside of the Russian Embassy in Kabul, following a media campaign threatening foreign nationals in Afghanistan.[63] Subsequently, following a stream of new threats against Russia, the Islamic State conducted the Crocus City Hall attack in Moscow in March 2024.[64]

This normalization is visible in the way attacks on Chinese-associated venues and personnel were presented by Islamic State central and ISKP alike. Claims issued via Amaq News Agency and Al Naba followed standardized templates, using conventional jihadi terminology and embedding China alongside the usual roster of enemies—America, Russia, regional 'apostate' regimes—rather than treating Chinese targets as exceptional.[65] Mandarin-language flourishes and explicit references to Xinjiang became less central in these communiqués. Instead, the focus shifted to signaling that the Islamic State remained capable of hitting a major external power despite territorial collapse and sustained counterterrorism pressure.

The evolution from 'special' to 'routine' is important. It is possible that once China's inclusion in the enemy hierarchy no longer required elaborate justification, the threshold for targeting Chinese interests was lowered. This seems to be similar to attacks against U.S. and Western targets and against the so-called near enemy (local governments), which do not require continuous justification by the Islamic State for them to be targeted by cells and inspired individuals. These dynamics made it easier for local cells and sympathizers to justify opportunistic attacks against Chinese workers, businesses, or diplomatic facilities as self-evident acts of jihad, without needing explicit central guidance and also acts that were focused on an Islamic State priority. The January 2026 suicide bombing at a Chinese-favored restaurant in Kabul's Shahr-e-Naw district discussed in the previous section, for example, was framed as both retaliation for Uyghur repression and a demonstration that Chinese nationals remained vulnerable even in supposedly secure areas under Taliban protection.

At the same time, pro-Islamic State media in South Asia further diffused anti-China narratives. The Voice of Hind magazine, associated with the Islamic State's 'Hind Province' (ISHP),[66] integrated criticism of Chinese atheism, Uyghur oppression, and China's partnership with India into a broader portrayal of great power competition as a struggle between 'evils' hostile to Islam. Other outlets, such as Voice of Khurasan and various online magazines, echoed ISKP's portrayal of China and India as joint colonial actors in the Indian Ocean and South Asia, repurposing even modest attacks on Chinese tourists or workers as proof of a global anti-China campaign.[67] This could lead to further incidents of anti-Chinese political violence in the region in the years to come.

ISHP and ISKP publications inspired new South Asian outlets to emerge and amplify their messages. In January 2024, Voice of Khurasan 32 carried a piece on the Maldives that framed the country as a site of "power struggle for regional domination of the two growing Evils, India and China, both of whom are the staunch enemies of Islam and Muslims."[68] ISKP boasted that "in Feb 2020, three kuffar — one Australian and two Chinese nationals — were stabbed by our Inghimasi brothers in Hulhumale, an Island near the capital Malé" and warned that "the soldiers of Khilafah are ever ready to slit their throats and slaughter them along with their kuffar allies (Chinese and Indians)."[69]

By incorporating the Maldives stabbing of Chinese nationals into its broader narrative, ISKP demonstrated that even relatively small attacks on tourists or workers can be repurposed as evidence of a global anti-China campaign. By broadening the narrative, it is likely that ISKP hopes to appear ubiquitous and amplify the psychological component of its propaganda campaign.

### *Multipolarity and China as a Rising Great Power*

ISKP's anti-China messaging has become one of the clearest examples of how the group turns geopolitics, grievance, and sectarian outrage into a single propaganda line. The movement does not treat Beijing as just another distant enemy; it places China within a broader map of great power competition, portraying it as both an imperial actor and a persecutor of Muslims.[70] That framing allows ISKP to present China as a target for revenge, a symbol of global disorder, and a major player in multipolar competition with the United States and its regional Asian allies.

A major step in that evolution came with the September 2022 publication of "China's Daydream of Imperialism," which marked one of ISKP's most detailed anti-China ideological attacks. The text portrayed China as an ascending hegemon seeking to build its own regional sphere while competing with American power. It argued that Beijing's "booming economy has become a global concern for many international players" and that this shift is "a real challenge for the U.S. hegemony in the world economy." ISKP also claimed that China is "pushing to turn the unipolar world into a bipolar one"

and pursuing "their future ambition of conquering the world and establishing their own power sphere." In ISKP's logic, China is not merely a rival state but an imperial project in motion, destined to collide with the Islamic world.


*Figure 5: Voice of Khurasan, Issue 13, p. 37*

That article also tied China directly to a larger collapse of the world order. ISKP predicted that escalating tensions around Taiwan and other geopolitical flashpoints would lead the "enemies of Islam" into a wider war, which it characterized as an approaching "Third World War." The text warned that Beijing would eventually face the "sharp blades of the Khilafah mujahidin," making clear that ISKP intended to exploit great-power disorder to threaten Chinese assets directly. China was thus integrated into a strategic narrative about global instability, creating room for jihadi advance.

That same logic becomes even more concrete in ISKP's multimedia output, especially its April 2023 video "The Unrestrained Metastasis Within the Body of the Ummah." The film largely focuses on criticizing and threatening the Pakistani government, but China and CPEC sit at the center of its broader message.[71] ISKP refers to the Pakistani state as "cancerous" and beholden to hostile outside powers, including communist China and the capitalist West. It presents Pakistan as a country being hollowed out by debt, corruption, foreign influence, and moral decay, while the narrator attacks the state for economic crisis, unemployment, inflation, and insecurity. The propaganda tries to make Pakistan look like a broken proxy of foreign interests rather than a sovereign Muslim state, overlapping with al-Qa`ida and Pakistani Taliban narratives. However, while Pakistani Taliban and al-Qa`ida gradually marginalized anti-China narratives, at best focusing on economic, socio/political issues while toning down Uyghur-specific content, ISKP dedicated a large portion of its narratives against Pakistan by connecting Islamabad with the Uyghur issue.

In the video and in ISKP propaganda generally, China is portrayed as a power that does not merely influence states but absorbs them through debt, infrastructure, and political dependency. For example, in the video ISKP portrays the China-Pakistan Economic Corridor as part of a wider Belt and Road strategy that allows Beijing to entrench itself inside Muslim lands. The narrator argues that Pakistan's "ever-increasing ties with China" amount to subjugation, and that CPEC functions as a vehicle for the "Chinese Atheists" to enslave local Muslim populations, "under the pretext of development projects," especially around the Pakistani port of Gwadar.

ISKP also accuses China of 'debt-trap diplomacy' and of using economic leverage to expand its control over governments around the world. To make the point, the video compares Pakistan's trajectory to Sri Lanka's debt crisis, implying that CPEC could produce the same result: dependence, loss of sovereignty, and eventual territorial control by Beijing if Islamabad cannot repay its obligations. In the group's telling, the language of development conceals a project of domination, whereby Muslim countries are being sold out from within.

That threat matters because it shifts ISKP's anti-China propaganda from abstract grievance to a concrete geopolitical warning where propaganda is paired with an operational threat. For example, the video concludes with direct warnings to the Pakistani government with ISKP pledging to attack CPEC development sites. That follows a pattern already visible in ISKP's past violence against Chinese targets, including the killing of two Chinese nationals in Pakistan in 2017, the attack on Chinese guests at a Kabul hotel, and the suicide bombing at the Taliban foreign ministry on a day when Chinese representatives were reportedly due to be present.[72]

The broader strategic logic behind these efforts is that ISKP treats geopolitical rivalry as an opportunity. This is why "China's Daydream of Imperialism" and "The Unrestrained Metastasis Within the Body of the Ummah" work together so effectively as propaganda texts. The first provides the grand ideological frame: China as an imperial power heading toward a civilizational clash. The second gives that frame a practical set of targets: CPEC, Gwadar, Pakistani institutions, and the wider Chinese footprint in South Asia. Between them, ISKP turns geopolitical rivalry into a recruiting narrative, a threat narrative, and a justification for violence.[73]

### *The Broadening Diversity of Islamic State Outlets Criticizing China*

This diffusion of anti-China narratives beyond official online Islamic State channels became increasingly evident following ISKP's December 2022 attack on Chinese nationals in Kabul,[74] which triggered a wave of anti-China propaganda from a diverse range of official and pro-Islamic State media outlets. The online Islamic State sphere does this with a select few high-profile attacks, with the Bondi Beach mass shooting, for instance, but following ISKP attacks on Chinese and other foreign targets in Afghanistan, there is a notable response by Al-Azaim Media Foundation and various pro-Islamic State propaganda outlets online.[75] The propaganda surge that followed the attack demonstrated that anti-China messaging was no longer confined to Islamic State Central or ISKP alone. Instead, a significantly broader and more diverse ecosystem of pro-Islamic State media outlets rapidly mobilized to amplify anti-Chinese narratives across multiple languages and platforms. Beyond official coverage in Al Naba and statements from ISKP's al-Azaim Foundation for Media Production, the campaign drew participation from al-Azaim Tajiki, the English-language translation outlet Halummu, the pro-Islamic State media group al-Battar, Hadm Alaswar, and the Bengali-language outlet At-Tamkeen Media. These organizations translated, repackaged, and redistributed anti-China content, ensuring that narratives linking the Kabul attack to the treatment of Uyghur Muslims reached audiences across South Asia, Central Asia, the Middle East, and the broader online supporter network.

The breadth of participation extended even further, with additional Islamic State-aligned and pro-Islamic State channels such as Aladiyat, at-Taqwa, and Vanguards of the Ansar (Supporters) producing original propaganda celebrating the attack and threatening future violence against Chinese interests. Their messaging portrayed China as an enemy of Islam, framed the Kabul operation as retaliation for Beijing's policies in Xinjiang, and sought to position the Islamic State as the only jihadi movement willing to translate anti-China rhetoric into action. The involvement of such a wide range of online outlets—spanning official provincial media, translation networks, ideological amplifiers, and supporter-run propaganda channels—illustrates a notable expansion of anti-China narratives across the broader pro-Islamic State media sphere. This has also been observed with the attacks on Pakistani and Russian diplomatic facilities; however, the China attacks have been most frequent in terms of targeting foreign nationals and interests and have evoked the greatest reactions. This suggests that hostility toward China was increasingly becoming a shared theme embraced by a diverse array of Islamic State supporters and affiliated propagandists, rather than remaining solely the focus of Islamic State Central and ISKP.

This trend continued into 2026 with in-house branch media networks and a new pro-Islamic State propaganda outlet explicitly prioritizing anti-China messaging. In late April 2026, ISKP's Voice of Khurasan magazine published an article titled "Who Will Take Revenge for the Uyghur Muslims"—a translation from the Pashto-language original published in February shortly after the attack—using the January attack on a Chinese restaurant in Kabul as both a justification for anti-Chinese violence and a forward-looking declaration of intent. The article framed the operation as religious retribution on behalf of persecuted Uyghur Muslims, constructed China as a structurally defined enemy of Islam, and attacked the Taliban's legitimacy for its engagement with Beijing. Positioning itself as the sole defender of Uyghur Muslims, ISKP signaled that the Kabul attack was not an isolated incident but the opening move in a sustained campaign against Chinese nationals and interests across the region.[76]

Then, on June 1, 2026, the newly established Al-Iman Media Center released an article titled "The Alienation of Muslims in China" in its inaugural magazine issue, which devoted extensive attention to the plight of Uyghur Muslims and portrayed Beijing as a principal enemy of Islam.[77] The outlet's rhetoric and thematic focus closely resembled those of ISKP's Voice of Khorasan magazine, which for years had been among the most prolific Islamic State publications targeting China and highlighting Xinjiang-related grievances. Al-Iman's article framed Xinjiang as an occupied Muslim land, accused Chinese authorities of systematic religious and cultural eradication, and integrated the issue into a broader Islamic State narrative of global conflict between Islam and its perceived enemies. The appearance of a new pro-Islamic State media platform adopting themes long championed by ISKP underscores how anti-China propaganda has continued to diffuse across the wider Islamic State support ecosystem, further broadening the range of unofficial outlets dedicating significant attention to China and the Uyghur issue.

***The Islamic State's Anti-China Campaign Expands to Africa***

Expanding beyond South and Central Asia to include Africa, Islamic State's anti-China campaigning in the mid-2020s began to fuse the same ideological framing developed for Afghanistan and Pakistan with local grievances over resources and governance in conflict zones such as the Democratic Republic of the Congo (DRC) and Mozambique.[78] In Mozambique, this broader pattern had earlier parallels in al-Shabaab's[c] August 2020 attack on and subsequent destruction of a Chinese sawmill called Mr. Forest in Mocímboa da Praia,[79] an attack that underscored how Chinese commercial presence could be folded into insurgent narratives of foreign exploitation.

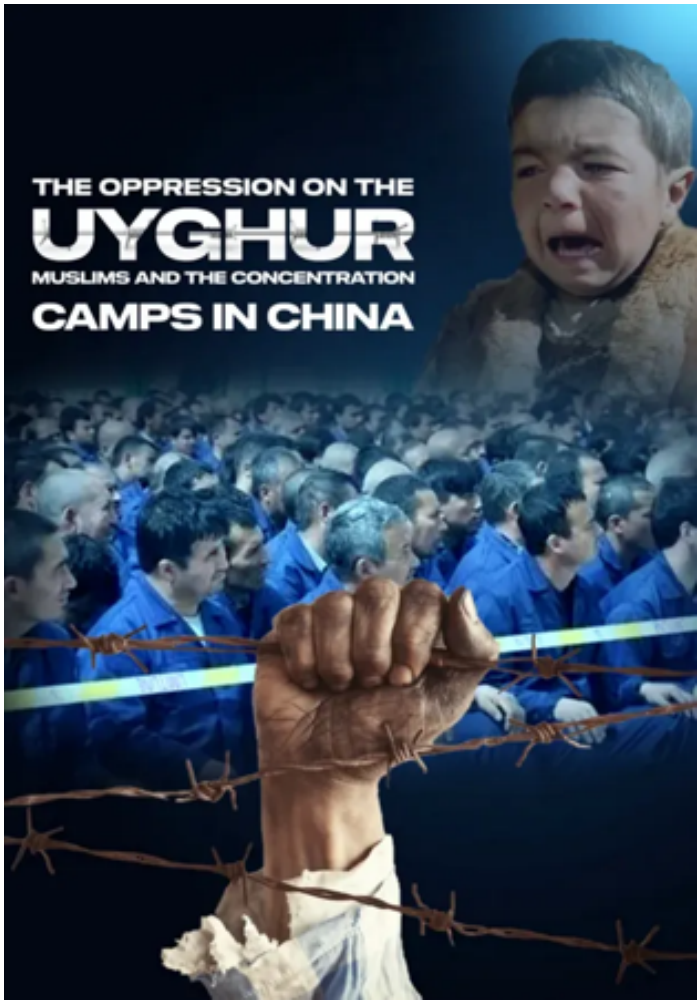


*Figure 6: Voice of Khurasan, Issue 21, p. 37*

The March 2026 ISCAP raid on Chinese-run gold sites in eastern DRC was framed in the same terms used by ISKP: Chinese projects were depicted as instruments of exploitation and foreign domination, and attacks on them were presented as legitimate strikes against an oppressive global order.[80] That framing was echoed explicitly in an earlier Al Naba editorial: The newsletter warned that "Crusader oil companies who have invested billions of dollars" were at risk and argued that foreign powers were using Mozambique's resources for "plunder," claiming that "there is nothing in the country that interests the Crusaders besides its huge reserves of different natural resources and in which American, French and South African companies jointly invest. And Russian

c Note that this al-Shabaab refers to *Ahl al-Sunnah wa al Jamma'ah* (ASWJ), not the al-Shabaab based in Somalia.

and Chinese companies are ambitious to find for themselves a foothold in them as well."[81] Al Naba went further, threatening that South African involvement in the Cabo Delgado conflict "will place it in a great financial, security and military predicament, and may result in prompting the soldiers of the Islamic State to open a fighting front inside its borders," and asserting that if 'Crusader' states intervened to protect investments and "guarantee the continuation of their plunder of the resources of the region," they were "delusional,"[82] because such intervention would only strengthen the insurgents' cause.

Those statements matter because they show how Islamic State central media explicitly links resource extraction to ideological grievance, turning economic actors into symbolic enemies and widening the list of legitimate targets. By casting Western, South African, Russian, and Chinese companies as partners in the "plunder" of Muslim lands, Al Naba supplies local Islamic State affiliates with a directive to attack extractive projects, foreign personnel, and states perceived to defend them. This rhetoric aligns targets with strategic narratives: Operations that might once have been framed as purely criminal or opportunistic can be presented as part of a more coherent global campaign against foreign exploitation. Seen alongside the DRC mine assault, the editorial underscores how anti-China narratives—once cultivated in Afghanistan and Pakistan—are being repurposed to give ideological cover to attacks across Africa, helping to normalize such targeting within the wider Islamic State ecosystem.[83]

As China fills out a more robust presence throughout sub-Saharan Africa, it seems likely that future Islamic State propaganda campaigns will include a more detailed focus on Chinese infrastructure projects, the presence of Chinese nationals, and what the movement views as the exploitation of Muslims' resources in areas where China operates. From the Sahel to the southeastern Swahili coast, the Islamic State remains entrenched, positioning itself as a vanguard against great power meddling and interference in local affairs.[d] Whether through the exploration of critical minerals in the DRC or the development of natural gas deposits in Mozambique, the presence of nation-states and multinational corporations is not going to cease—in fact, as great power competition intensifies, there may very well be a greater and more visible presence of countries such as the United States, China, Russia, France, and others scrambling for access to resources. In turn, the Islamic State will seek to take advantage of more frequent and substantive involvement of great powers on the African continent. As it has with other geopolitical developments, the Islamic State has mastered the art of portraying itself as the perpetual underdog, a David versus Goliath framing that resonates with large swaths of the group's supporters.

## Strategic Implications for China

The evolution of the Islamic State's anti-China campaign carries several important strategic implications that extend beyond propaganda into operational and geopolitical domains.[84] First, China now occupies a structurally embedded position within the Islamic State's global enemy hierarchy. No longer framed solely as a persecutor of Uyghurs, Beijing is increasingly portrayed as a systemic adversary, an ascendant power whose political, economic, and security activities in Muslim-majority regions are interpreted as forms of imperial expansion. This shift reflects a broader recalibration in jihadi discourse, where China is treated alongside the United States, Russia, Iran, and regional governments as part of an interconnected constellation of hostile forces.

**"China now occupies a structurally embedded position within the Islamic State's global enemy hierarchy. No longer framed solely as a persecutor of Uyghurs, Beijing is increasingly portrayed as a systemic adversary, an ascendant power whose political, economic, and security activities in Muslim-majority regions are interpreted as forms of imperial expansion. This shift reflects a broader recalibration in jihadi discourse, where China is treated alongside the United States, Russia, Iran, and regional governments as part of an interconnected constellation of hostile forces."**

Second, the rise of ISKP as the vanguard of anti-China propaganda and operations ensures that Chinese interests across Afghanistan, Pakistan, Central Asia,[85] and beyond will remain exposed to threats.[86] ISKP's ability to integrate local grievances with global ideological narratives allows it to position attacks on Chinese nationals and projects as both strategically meaningful and religiously justified. While other militant actors, such as Baloch separatists or Tehrik-i-Taliban Pakistan, may inflict higher casualties on Chinese nationals and interests in specific contexts, ISKP plays a distinct role in amplifying these incidents through the Islamic State's transnational media ecosystem.[87] This amplification effect magnifies the psychological and strategic impact of attacks, transforming localized violence into components of a broader global campaign.

Third, the normalization of anti-China targeting across official and pro-Islamic State media ecosystems arguably makes more anti-China violence likely. As a result, attacks against Chinese nationals, infrastructure, and commercial interests can now be framed as self-evident acts of jihad. This dynamic increases the likelihood of opportunistic violence by decentralized cells and unaffiliated sympathizers, particularly in fragile environments where Chinese economic engagement is visible, but security provision is uneven.[88]

Fourth, the geographic diffusion of anti-China narratives, most notably into African theaters such as the DRC and Mozambique,[89] signals an important expansion of the threat landscape. In these

d For instance, ISKP Tajik wing published anti-Russian content due to the latter's participation in the Syrian civil war. See "TKD MONITORING: ISKP Magazine (Sadoi Khuroson) Issue 2," Khorasan Diary, June 27, 2024.

contexts, Islamic State affiliates have adopted and adapted the anti-China framing utilized by the Islamic State and popularized by ISKP in multiple languages and consistently throughout time, exploiting them to challenge rival jihadi organizations. Often, they merged it with local grievances over resource extraction, governance failures, and foreign economic presence. By embedding China within a broader narrative of plunder and external domination, Islamic State propagandists provide ideological cover for attacks on extractive industries and foreign personnel with links to China. This convergence of global narrative and local conflict dynamics suggests that Chinese interests are more vulnerable in regions far removed from the original Xinjiang-centric framing.[90]

Finally, China's continued ascent as a global power and its deepening engagement in politically unstable regions will likely sustain, and in some cases intensify, its prominence in Islamic State discourse.[91] Diplomatic outreach, infrastructure investments, and security partnerships are consistently reframed within jihadi narratives as evidence of complicity with apostate regimes and as justification for violent resistance. As this pattern continues, Beijing faces a dual challenge: protecting its overseas personnel and assets while navigating the reputational and perceptual dimensions of its foreign policy in environments where militant groups actively exploit external involvement for recruitment and mobilization. This has implications for Chinese counterterrorism strategy and may affect how China views its security policy, particularly regarding the potential for greater involvement through private security companies, proxies, or local security partners in unstable regions.

Taken together, these dynamics indicate that the Islamic State's anti-China campaign has matured into a durable and adaptable component of its global strategy. Even as the group's operational capabilities fluctuate across regions, the ideological infrastructure underpinning hostility toward China is now firmly established. This makes it very likely that China will remain a recurring target within Islamic State propaganda and operations, with the scale and intensity of the threat shaped by local conditions but sustained by a coherent transnational narrative.[92] CTC

## Citations


1 Lucas Webber, "ISKP Escalates Its War Against Beijing in Latest Attack Targeting Chinese Nationals, Promises More to Come," Militant Wire, January 20, 2026.
2 Lucas Webber, "A History of the Islamic State's Media Warfare Against China," Militant Wire, September 27, 2021.
3 Lucas Webber, "Islamic State in Afghanistan Publishes New Anti-China Book Detailing Beijing's 'Crimes Against Muslims,'" Militant Wire, June 14, 2024.
4 Ibid.
5 Al-Hayat Media Center, 2014, available at Jihadology, July 1, 2014.
6 Bernard Haykel, "The ISIS Primer," Wilson Center, January 21, 2016.
7 Abu Bakr al-Baghdadi, "March Forth Whether Light or Heavy," Al-Furqan Media Foundation, May 14, 2015, transcript published by Inside the Jihad.
8 Abu Muhammad al-Adnani, "Indeed Your Lord Is Ever Watchful," Al-Furqan Media Foundation, September 21, 2014, translated and archived by Aaron Y. Zelin, Jihadology.
9 Haroro J. Ingram, "Psychology, Not Theology: Overcoming ISIS' Secret Appeal," E-International Relations, October 28, 2014.
10 Abdul Basit, "China, Xinjiang and the Uyghurs in Global Jihadist Propaganda," Small Wars Journal, January 17, 2021.
11 Lucas Webber, "Jihadist Perceptions of a Rising Superpower: Troubles Along China's Belt and Road," Small Wars Journal, February 21, 2021.
12 Te-Ping Chen, "Islamic State Video Threatens China With Homegrown Fighters," *Wall Street Journal*, March 1, 2017.
13 Eitan Azani and Francesco Dotti, "The Islamic State's Web Jihadi Magazine Dabiq and Rumiyah: More than Just Propaganda," International Institute for Counter-Terrorism, July 2021.
14 Dabiq, Issue 4, 2014, p. 4.
15 Dabiq, Issue 5, 2014, p. 33; Lucas Webber, "The Islamic State's South Asian Branches are Spearheading an Anti-China Campaign," Global Network on Extremism and Technology (GNET), January 8, 2024.
16 Michael Clarke, "The Islamic State's Chinese Fighters and the Threat to China," *China Brief* 15:17 (2015).
17 Avi Issacharoff, "Bloody Islamic State Video Puts China in Cross Hairs," *Times of Israel*, March 1, 2017.
18 Shannon Tiezzi, "ISIS: Chinese Hostage 'Executed,'" Diplomat, November 19, 2015.
19 Rynn Song Ningyu, "Why Did ISIS Release a Chinese-Language Jihad Song and Who Sings It?" Asia Times, December 22, 2015.
20 Aymenn Jawad al-Tamimi, "New Islamic State Nasheed in Uyghur Language," Jihad Intel, July 7, 2015.
21 David Matthews, "Islamic State Hackers 'Target Top Chinese University,'" Times Higher Education, January 20, 2016.
22 Joseph Hincks, "Uighur Militants Reportedly Threaten China in ISIS Video," *Time*, March 1, 2017.
23 Farangis Najibullah, "Islamic State Claims It Executed Two Chinese Citizens Kidnapped in Pakistan," Radio Free Europe/Radio Liberty, June 9, 2017; "Army releases details of 3-day Mastung operation that targeted 'IS facilitators,'" *Dawn*, June 8, 2017.
24 Colin P. Clarke and Lucas Webber, "ISIS-K Goes Global," *Foreign Affairs*, August 1, 2024.
25 Lucas Webber, "History of ISKP's War Against China: Killing of Mine Worker Marks Latest Act," Militant Wire, March 17, 2025.
26 Chris Zambelis, "Uighur Dissent and Militancy in China's Xinjiang Province," *CTC Sentinel* 3:1 (2010).
27 Lucas Webber, "Islamic State Khurasan Threatens China in New Propaganda Poster Following Killing of Chinese Engineer in Pakistan," Militant Wire, April 2, 2024.
28 Elliot Stewart, "The Islamic State Stopped Talking About China," War on the Rocks, January 19, 2021.
29 Webber, "History of ISKP's War Against China."
30 Lucas Webber, "Uzbek Pro-ISKP Media Threatens China and Celebrates Pakistan Attack on Chinese Nationals," Militant Wire, April 16, 2024.
31 Webber, "A History of the Islamic State's Media Warfare Against China."
32 Lucas Webber, "Baloch Militants Intensify Guerrilla Campaign Against China as Beijing's Footprint Expands in Pakistan," Militant Wire, August 28, 2024.
33 Daniele Garofalo, "The Propaganda of Jihadist Groups in the Era of Covid-19," Jihadica, November 1, 2021.
34 Paul Cruickshank and Don Rassler, "A View from the CT Foxhole: A Virtual Roundtable on COVID-19 and Counterterrorism with Audrey Kurth Cronin, Lieutenant General (Ret) Michael Nagata, Magnus Ranstorp, Ali Soufan, and Juan Zarate," *CTC Sentinel* 13:6 (2020).
35 Ibid.
36 Webber, "History of ISKP's War Against China."
37 Garofalo, "The Propaganda of Jihadist Groups in the Era of Covid-19."
38 Lucas Webber, "Abu Zar al-Burmi: Jihadi Cleric and Anti-China Firebrand," Small Wars Journal, April 6, 2021.
39 Amira Jadoon, Abdul Sayed, Lucas Webber, and Riccardo Valle, "From Tajikistan to Moscow and Iran: Mapping the Local and Transnational Threat of Islamic State Khorasan," *CTC Sentinel* 17:5 (2024).
40 Robin Simcox, "Europe and the Fall of the Caliphate," Counter Extremism Group, September 2020.
41 Voice of Khurasan, Issue 1.
42 Khorasan Ghag, Issue 37, pp. 10-11; Khorasan Ghag, Issue 33, p. 41; Khorasan Ghag, Issue 28, p. 45; Khorasan Ghag, Issue 30, p. 50; Khorasan Ghag, Issue 31, p. 26; "TKD MONITORING: New ISKP Video Describes the History of East Turkestan," Khorasan Diary, December 1, 2023; "TKD MONITORING: New Video from ISKP Criticizes Taliban over Palestine and Xinjiang," Khorasan Diary, November 19, 2023.

43 Khorasan Ghag, Issue 28, p. 45; Khorasan Ghag, Issue 37, pp. 10-11; Yalghar, Issue 6.
44 Lucas Webber, "Perspectives | Islamic State Using China to Vilify Taliban," Eurasianet, November 4, 2021.
45 Ibid.
46 Khorasan Ghag, Issue 34, p. 34; Voice of Khorasan, Issue 37, p. 35; Voice of Khorasan, Issue 38, p. 22.
47 Khorasan Diary, "TKD MONITORING: Islamic State Khorasan (ISKP) mouthpiece al-Azaim published the first issue …," X, January 4, 2023.
48 Sadoy Khorasan, Issue 5, p. 34.
49 Al Naba, 369, December 15, 2022.
50 "ISKP claims attack on Chinese-owned Kabul Longan Hotel - one of the attackers escapes," Afghan Witness, January 2, 2023.
51 Lucas Webber, "ISKP Attack on Chinese Nationals in Kabul Unleashes Wave of Anti-Chinese Jihadist Propaganda," *Terrorism Monitor* 21:1 (2023).
52 Lucas Webber, "Islamic State Khurasan's International Target Strategy: Suicide Bombing Aimed at Taliban Foreign Ministry and Chinese Diplomats," Militant Wire, January 13, 2023.
53 "At least 11 killed in Afghanistan mosque explosion," Al Jazeera, June 8, 2023.
54 Khorasan Ghag, Issue 25, p. 69.
55 Al Naba, Issue 479.
56 Khorasan Ghag, Issue 38, p. 91.
57 Voice of Khurasan, Issue 48, p. 38.
58 "God Grant Victory to the Muslims in East Turkestan," Al-Azaim Foundation, February 19, 2023.
59 "TKD MONITORING: ISKP Book on Diplomatic Ties Between AIG and China," Khorasan Diary, October 2023.
60 "Deadly car bombing in Pakistan targets hotel hosting Chinese ambassador," France24, April 22, 2021; Abid Hussein, "Two get death in Pakistan for attack targeting Chinese engineers," Al Jazeera, November 15, 2022; Ayaz Gul, "Suicide Bombing Kills 5 Chinese Citizens in Pakistan," Voice of America, March 26, 2024.
61 Nida-e-Khorasan, Issue 13, p. 80.
62 Nida-e-Khorasan, Issue 3, p. 25.
63 Lucas Webber and Riccardo Valle, "Islamic State Khurasan's History of Targeting Diplomatic Missions," Militant Wire, September 23, 2022.
64 Lucas Webber, Riccardo Valle, and Colin P. Clarke, "The Islamic State Has a New Target: Russia," *Foreign Policy*, May 9, 2023.
65 Ibid.
66 Lucas Webber, "Voice of Khorasan Magazine and the Internationalization of Islamic State's Anti-Taliban Propaganda," *Terrorism Monitor* 20:9 (2022).
67 Voice of Khurasan, Issue 32, 3.
68 Ibid.
69 Ibid.
70 Lucas Webber, "Islamic State Khorasan: Global Jihad in a Multipolar World," Diplomat, February 1, 2023.
71 Webber, "Islamic State Khurasan Threatens China in New Propaganda Poster Following Killing of Chinese Engineer in Pakistan."
72 Webber, "History of ISKP's War Against China;" "Islamic State says it killed two Chinese teachers kidnapped in Pakistan," Reuters, June 9, 2017.
73 Lucas Webber, "IS-S Seeks to Exploit Geopolitical Tensions in New Anti-China Propaganda Campaign," Militant Wire, February 27, 2024.
74 Webber, "ISKP Attack on Chinese Nationals in Kabul Unleashes Wave of Anti-Chinese Jihadist Propaganda."
75 Lucas Webber, "Deep Analysis: The Islamic State is Using the Bondi Attack to Inspire Violence in the West," Militant Wire, June 9, 2026; Lucas Webber, "The Islamic State vs. Russia in Afghanistan," Diplomat, September 9, 2022.
76 Khorasan Ghag, Issue 38, p. 91; Voice of Khurasan, Issue 48, p. 40; Lucas Webber, "ISKP Boasts January Bombing of Chinese Nationals; Threatens, Alongside Pro-IS Groups, to Increase Attacks Avenging Uyghur Persecution," Militant Wire, June 8, 2026.
77 Lucas Webber, "Al-Iman Media Center: New Pro-Islamic State Outlet Takes Aim at China," Militant Wire, June 2, 2026.
78 Daniele Garofalo, "ISCAP's Insurgency in Eastern DR Congo: Patterns of Violence and Territorial Control," Daniele Garofalo Monitoring, April 29, 2026.
79 Harry Verhoeven and Sérgio Chichava, "Al-Shabaab and Chinese Trade Practices in Mozambique," War on the Rocks, September 23, 2021.
80 Daniele Garofalo, "Islamic State Global Trends: Monthly Analysis | April 2026," Daniele Garofalo Monitoring, May 3, 2026; Lucas Webber, "Islamic State Expands China-Targeted Campaign from Asia Into Africa Following ISCAP Attack on Chinese Gold Mines in DR Congo," Militant Wire, March 19, 2026.
81 "ISIS Threatens South Africa, See Why," Naija News, July 8, 2020.
82 Ibid.
83 Webber, "ISKP Escalates Its War Against Beijing in Latest Attack Targeting Chinese Nationals, Promises More to Come."
84 Bradley Jardine and Edward Lemon, "Terrorist Organisations and Conservative Islamic Influencers are Capitalising on Sinophobia in Central Asia," RUSI, November 4, 2025.
85 Webber, "The Islamic State's South Asian Branches Are Spearheading an Anti-China Campaign."
86 Colin Clarke, "Islamic State-Khorasan Province Is a Growing Threat in Afghanistan and Beyond," Diplomat, April 18, 2023.
87 Lucas Webber, "Islamic State Khurasan Promises to Escalate War Against China," Militant Wire, December 3, 2023.
88 Abdul Basit, "ISKP's Evolving Propaganda Against Chinese Imperialism," *Terrorism Monitor* 20:22 (2022).
89 Garofalo, "ISCAP's Insurgency in Eastern DR Congo."
90 Jason Warner, "Understanding China's New Counterterrorism Ambitions in Africa," *CTC Sentinel* 18:8 (2025).
91 Mollie Saltskog and Colin P. Clarke, "It's China's Turn to Face Transnational Terrorism Threats," Defense One, April 21, 2025.
92 Lucas Webber, Colin Clarke, and Peter Smith, "ISKP's Latest Campaign: Expanded Propaganda and External Operations," Global Network on Extremism and Technology (GNET), June 27, 2024.

# A Domestic Mimetic Chain: Nihilistic Violent Extremism, Youth Radicalization, and School Violence in Italy

By Francesco Marone

**In the spring of 2026, Italy experienced an unusual sequence of school attacks and investigations into alleged plots targeting schools, all involving minors aged 12 to 17. Drawing on official statements, specialist literature, and open-source reporting, this article examines four cases across different regions of the country between March and May 2026, alongside an important precursor case from February 2025. All these different episodes can be situated within the broader landscape of nihilistic violent extremism (NVE), the True Crime Community (TCC), and related subcultures of performative violence. The article argues that these cases should be understood neither simply as conventional ideological terrorism nor as ordinary adolescent deviance. Rather, they constitute Italy's first publicly visible sequence of NVE-linked incidents, with three of the four 2026 episodes suggesting a domestic mimetic chain unfolding over a matter of weeks. The Italian experience also underscores the challenges these phenomena pose for counterterrorism and the need for a comprehensive prevention framework.**

In the spring of 2026, within the space of 65 days, two violent incidents inside Italian schools forced the country to confront a type of threat that it had not yet learned to fully recognize, nihilistic violent extremism (NVE)[a] and adjacent online subcultures of performative violence.

On March 25, 2026, a 13-year-old student in Trescore Balneario (northern Italy) stabbed his French language teacher in a school corridor, livestreaming the attack on Telegram, after publishing a pre-attack text titled "The Final Solution" containing NVE-adjacent references.[1] Then, on May 29, a 12-year-old student in San Vito Lo Capo (southern Italy) attempted to stab his technology teacher in the classroom, wearing a bicycle helmet covered in handwritten references to the True Crime Community (TCC)[2] and recording the act with the intention of livestreaming it.[3]

Furthermore, in the short period between these two incidents at school, Italian authorities conducted two separate police operations concerning minors holding extremist views who were allegedly interested in planning acts of violence at school. On March 30, the Carabinieri (Italy's national gendarmerie) arrested a 17-year-old student in the province of Perugia (central Italy), reportedly fascinated by incel subculture, neo-Nazism, and school-shooting fantasies, who was accused of planning a Columbine[b]-style massacre at his high school and had acquired weapons-manufacturing instructions.[4] On April 4, the Italian State Police (Polizia di Stato) searched a 15-year-old student with white supremacist sympathies in the province of Arezzo (central Italy) who had allegedly expressed admiration online for the perpetrator of the Trescore Balneario school attack and, according to investigators, had shown interest in carrying out a similar act within days.[5]

Each case is alarming in its own right. Taken together, these episodes, all involving minors, also mark the first sustained public recognition in Italy of NVE and NVE-adjacent manifestations that researchers, experts, and security practitioners have been tracking for several years. In turn, on closer inspection, these cases in the spring of 2026 had significant domestic precedents in the years immediately prior, as with the February 2025 arrest of a 15-year-old boy allegedly linked to the 764 network, near Bolzano (northeastern Italy).[6]

This article aims to reconstruct and analyze these 2026 cases and their immediate precedents in Italy, situating them within the broader transnational evolution of nihilistic violent extremism. To do so, it combines various open sources (including official statements and documents, specialist literature, and media reporting in Italian and other languages). Because most of the cases concern ongoing investigations and involve minors, the article distinguishes, where

a The term 'nihilistic violent extremism' has gained traction in recent years among both practitioners and experts but, to date, its exact definition remains contested. A useful contribution was recently made by a *CTC Sentinel* article by Argentino and Lindsay; the two authors identify "six key elements" of this form of violent extremism: active participation in a specific online ecosystem (the "edgesphere"); status and belonging earned through the production and circulation of harm ("clout chasing"); behavioral drivers of anomie, nihilism, and misanthropy; the hybridization of harms, including sadistic online exploitation; a limited or secondary role for ideology; and the absence of a coherent strategic end state. Marc-André Argentino and Angus Lindsay, "Remotely Coerced Violence: 764, The Com Network, and the Hybridization of Threats," *CTC Sentinel* 19:6 (2026).

b The Columbine High School massacre occurred in Columbine, Colorado, on April 20, 1999. Students Eric Harris and Dylan Klebold killed 12 students and one teacher, wounded more than 20 others, and then died by suicide. See, in particular, "Columbine High School," Federal Bureau of Investigation (FBI), n.d. Columbine is widely regarded as one of the most infamous school massacres in the United States and has inspired several copycat attacks in the country and abroad.

*Francesco Marone is an Associate Professor of Political Science at the University of Aosta Valley, Italy. He is also a Senior Associate Research Fellow at the Italian Institute for International Political Studies (ISPI), a Fellow at the Program on Extremism at George Washington University, and an Associate Fellow at the International Centre for Counter-Terrorism – The Hague (ICCT). His research focuses on terrorism and violent extremism.*

possible, between confirmed official information, well-sourced reporting, and still-unverified claims.

## The Bolzano Precedent: Italy's First Case of a 764-Linked Arrest

As noted above, Italy's encounter with the nihilistic violent extremism ecosystem did not begin in the spring of 2026. It can be traced back by at least one year. On February 12, 2025, officers of the DIGOS (the special operations division of the Italian State Police) arrested a 15-year-old boy of Pakistani origin[7] (who cannot be named under Italian law governing minors) near Bolzano, in the predominantly German-speaking region of Alto Adige/South Tyrol, on an array of charges: participation in an association with terrorist aims, the manufacture and use of explosive devices, the unlawful carrying of weapons, aggravated criminal damage, and the possession and dissemination of child sexual abuse material.[8]

At the time, the case drew brief national coverage and then largely faded from public view; in retrospect, it stands as an early warning that the transnational threat later visible at Trescore Balneario, Arezzo, Perugia, and San Vito Lo Capo was already present in Italy.

The 15-year-old boy was allegedly linked to 764.[9] Founded online in 2020 by then-15-year-old Bradley Cadenhead of Texas, this network operates at the intersection of child sexual exploitation and violent extremism and has various offshoots.[10] In December 2025, Canada became the first country to designate 764 as a terrorist entity,[11] together with the adjacent Maniac Murder Cult (Manyaki: kult ubiystva, M.K.Y.).[12]

Italian investigators reportedly traced the activity of the Bolzano boy to a 764 offshoot they identified as "Rage Section 764."[13] Communicating through encrypted platforms, the Italian 15-year-old had allegedly attempted to demonstrate his loyalty in a manner consistent with 764-style initiation practices: He first reproduced the network's insignia on walls and vehicles near a sports facility in the province of Bolzano, the same site he had selected for an intended killing.[14]

According to Italian investigators, the murder plan was tied to a coordinated "Terror Week": 764 adherents were allegedly instructed to select a vulnerable victim (in particular, a homeless or disabled person), murder that victim, record the act, and publish the video on a Russian dark-web site.[15] The killing was therefore meant to function simultaneously as a rite of initiation, proof of commitment, and a bid for status within the online community.[16] The Italian police officially stated that the 15-year-old was "at a very advanced stage of the plan;"[17] he had also already selected a victim (reportedly, a homeless person) and, as mentioned above, chosen the location.

The boy had also assembled and detonated a rudimentary explosive device, filming himself as he tested it; unconfirmed media reports suggested that he had considered detonating an explosive device at his school.[18] Moreover, he had queried AI-powered search tools[19] about the emotional states of terrorists during their attacks and the pain perception of suicide bombers during "martyrdom."[20] Notably, the boy, born into a Muslim family (that appears to have been entirely unconnected to the alleged offenses), despite being active in a neo-Nazi-inspired network, had reportedly developed a growing sympathy for militant Islamism and jihadism and, according to media reports, had searched online for information on how to travel to Palestine.[21]

During the search of his home conducted at the time of his arrest, police seized an axe and improvised explosive devices, along with two computers and a phone containing large quantities of videos of school shootings and killings, child sexual abuse material, neo-Nazi imagery, and Islamic State propaganda.[22] In addition, unconfirmed media reports[23] also mentioned a handwritten "oath of allegiance" to the Order of Nine Angles (ONA or O9A), the transnational occultist and militant accelerationist network that has influenced the 764 milieu.[24] The arrest itself captured the performative character of the case and its connection with a transnational online audience: As DIGOS officers reached his door, the boy reportedly sent a final message to a 764-linked chat: "I have the fed on the door" (in English).[25]

According to available information, the boy had already been subjected to police searches.[26] Following a search in March 2024, Italian authorities established that he was in close contact with a 764 participant based in England, who was arrested by British police a few days later on March 26, 2024, when he was 18 years old.[27] Although the name of that young man is not specified in the official statements of the Italian authorities, it appears clear that, as some Italian media explicitly reported,[28] that person was Cameron "ACID" Finnigan, a prominent 764 propagandist.[29] On January 16, 2025, Finnigan received an extended sentence of nine years (six years in custody followed by a three-year extended license period) for encouraging suicide and possessing both a terrorist manual and indecent images of a child.[30] Finnigan himself had promoted a "Terror Week" and incited others to attack "homeless people."[31] Furthermore, British officers reportedly found online chats in which he encouraged a young woman, believed to be in Italy itself, to livestream her own suicide; they were unable to identify this woman or determine what happened to her.[32]

Clearly, the Bolzano boy was a node in a broader transnational network. This Italian case also appears to exemplify what a recent *CTC Sentinel* article[33] termed "remotely coerced violence," a dynamic in which vulnerable minors are pushed toward self-harm, abuse, or offline violence for circulation within, and status-seeking among, an online network. Viewed through the role typology proposed by Argentino and Lindsay,[34] the Bolzano boy resembles the "directed follower," while Finnigan approximates the roles of "influencer and propagandist," and self-described "high-level extorter." The entirely online and cross-border nature of this alleged relationship makes it especially difficult to address through national instruments alone.

According to later media reporting, by February 2026, the Bolzano boy had been moved to a juvenile facility in southern Italy and was placed in a judicial-probation program (*messa alla prova*); the measure suspended the criminal proceedings[c] while the teenager began an 18-month, court-approved rehabilitative program. The boy enrolled in an agricultural school and reportedly demonstrated commitment to his studies and good conduct. He

c Specifically, under this provision of the Italian juvenile justice system, criminal proceedings are suspended for a period not exceeding three years while the minor (aged 14 or older) follows an educational, rehabilitative, and reparative program under the supervision of juvenile justice services. Successful completion extinguishes the offense; otherwise, proceedings resume. In the event of a trial and conviction, according to Italian media, the Bolzano boy could "face up to 10 years in prison." Chiara Currò Dossi, "Terrorista neonazista a 15 anni, progettava di uccidere un senzatetto: 'Ho sbagliato, grazie per avermi fermato,'" *Corriere della Sera*, December 10, 2025.

also told the court that he was grateful to the magistrates and police who had "stopped him in time."[35]

## The Trescore Balneario Case: An NVE-Adjacent Attack at School

The attack in Trescore Balneario, a small town near Bergamo, operationally inaugurated the sequence of episodes that shocked Italy in the spring of 2026. The March 25 stabbing at a middle school was not spontaneous. The 13-year-old student had spent the prior evening on Telegram, where he posted photographs of weapons and a text he titled "The Final Solution" (written in English, not Italian).[36] The title itself, apparently an unmistakable reference to the Nazi extermination program, is telling: The boy disclaimed any ideological affiliation, and nothing in the text develops an antisemitic argument, but the choice of the most transgressive label available is consistent with the NVE practice of deploying extremist symbols for mere shock value and transgressive effect.

This short manifesto describes intense personal grievances. It begins with a brief, elusive reference to hostility toward the boy's father (who had reportedly separated from his mother about one year earlier): "I didn't find the courage to kill my father." The text then focuses on perceived injustices by his French language teacher; among other alleged wrongs, in his view, this woman did not properly take into account his recently diagnosed attention deficit hyperactivity disorder (ADHD). In the words of this text: "I have come to the conclusion that I can't live a life like this anymore. A life filled with unfairness, disrespect, and mundanes. I'm tired of this so I decided the perfect solution to this is taking the matter into my own hands. I'll kill my rench teacher" [*sic*]. At the same time, the text frames these personal grievances within a language of nihilistic transgression; for example, the 13-year-old wrote that "it's not only an act of revenge, it's something to break a boring routine in the most extreme way possible. I'm tired of being a mundane myself, having to do the same things over and over again. Rules aren't something I should follow, they're something I should break, and there's nothing better to do that than vengeance."[37]

On March 25, shortly before the start of classes, he stabbed his 57-year-old French teacher with a knife at least twice, in the corridor outside her classroom, inflicting serious wounds to her neck and torso. A helicopter evacuation and emergency surgery saved her life. Another 13-year-old student intervened after the first blow, kicking the attacker and forcing him to flee; the attacker was then stopped by another teacher and two school staff members before the Carabinieri arrived.[38]

The boy had a smartphone hanging from his neck, secured with an improvised harness that turned the device into a body-worn camera, to livestream the attack on the Telegram channel he had created the previous day, named "Vendetta" (now closed). Moreover, he wore a white T-shirt bearing the same word. The student also wore military-pattern trousers, and his knife was inscribed with the word "SOLDIER" (in English). In his short manifesto, echoing other school shooters, the boy wrote that "the military uniform isn't a random choice. I chose it because I see myself as a soldier fighting for my rights that got neglected." He immediately associated the uniform with a sense of superiority: "I also feel superior to all my peers. Yes, sometimes they're funny, but I feel like I'm way smarter than them, and wearing a uniform shows how im superior to all these mundanes. I'm no longer one of them, I'm someone better, someone who had the strength to do what many don't, someone who has the intelligence to realise that no one really advocates for us and our needs" [*sic*].

According to available information,[39] the Trescore Balneario boy had previously showcased alternative "outfit" options to the other users of his Telegram channel before settling on his final choice. These included the skull mask he ultimately wore during the attack, while insisting it was selected purely for its aesthetic appeal rather than its far-right symbolic valence:[40] "the skull face masks isn't to express a specific ideology, it's just visually pleasant and I like the aesthetic."

This attention to costume and staging apparently corresponds to the belief, documented in recent NVE research, that an individual's aesthetics and physical appearance can help convert violent fantasy into action.[41 d] The Trescore Balneario attacker's insistence that the skull mask was about appearance rather than its far-right meaning follows the same logic: from this perspective, costume is not merely symbolic decoration, but part of the performance through which violence becomes imaginable and communicable to an online audience.

At the same time, the 13-year-old emphasized that his action was unique. His short manifesto states: "I'm unique and I'm not a copycat of any previous school attack." In the text, he also preemptively dismissed the "natural selection" motif, an unmistakable reference to the slogan worn by one of the April 1999 Columbine perpetrators.[e] Moreover, in the same text, he rejected any clear ideological affiliation: "as for my political ideology I don't fit neatly into any clear ideology because the only thing that matters is me, no one else matters, no life matters beyond mine." This phrase appears to be an almost exact echo of the name and the central counter-slogan of the No Lives Matter (NLM) network, although in this case it was apparently associated mainly with an intensely personal assertion of singularity and self-importance.

According to available information, after the attack, investigators also found material at his home compatible with explosive precursors, pending technical examinations.[42] His Telegram channel was closed after the attack for violating the platform's terms of service, and his account was deleted.

After the arrest, his family's lawyer stated that the Italian boy appeared "detached from reality" during protected questioning and expressed the view that it would have been "very difficult" for him to have acted without external instigation through social networks.[43] To date, however, this remains an allegation rather than an established fact. Because the boy was under age 14, he could not

d For example, as Hart noted, Solomon Henderson, the January 2025 Antioch (Nashville) school shooter, devoted pages of his diary to emulating the look of June 2015 Charleston church shooter Dylann Roof; not because Henderson, who was Black, shared Roof's white supremacism, but because Roof's aesthetic was understood as violence-enabling. Mackenzie B. Hart, "'Less than a speck of dirt': exploring the manifestos of nihilistic violent extremists," *Behavioral Sciences of Terrorism and Political Aggression* (2026).

e During the Columbine High School massacre, Eric Harris wore a white T-shirt with the words "Natural Selection" printed in black. In his personal journals, he had also framed his impending violence as a way to "kick natural selection up a few notches" by eliminating those he deemed inferior. In this context, the phrase was understood in the light of pseudo-scientific social Darwinism and was also influenced in part by Nazi ideas. With this connotation, the expression became a recognizable reference that other school attackers adopted. See, for example, Ralph W. Larkin, "The Columbine legacy: Rampage shootings as political acts," *American Behavioral Scientist* 52:9 (2009): pp. 1,309-1,326.

be prosecuted or punished under Italian criminal law; a juvenile judge instead ordered his placement in a protected community under a provisional security measure.[44]

After the attack, it also emerged that the 13-year-old student had met online a girl of the same age living in Poland who struggled with self-harm and other vulnerabilities. After exchanging several messages, the boy reportedly asked her whether she had a razor, told her to cut herself, and threatened to reveal her secrets to her mother if she refused; the girl then spoke to her mother and left the Telegram group.[45] The Italian boy's reported behavior closely resembles the "remotely coerced violence"[46] pattern typical of NVE.

Thus, different factors made the Trescore Balneario case quickly recognizable to experts and careful observers as NVE-linked or at least NVE-adjacent. The initial "confusion"[47] in much of the Italian media, which struggled to adequately categorize and interpret this shocking event,[f] revealed the country's limited awareness of a phenomenon that had already existed for years.

Finally, it is worth noting that, before the stabbing, the 13-year-old allegedly encouraged members of his Telegram channel to celebrate his act with images and memes, even providing photographs of himself in uniform for "edits."[48] This expectation of post-attack memorialization shows that the intended audience was not only the immediate victim or the school, but also a dispersed online milieu capable of transforming the act into shareable subcultural material. Indeed, the boy was subsequently praised and acclaimed by NVE-inspired "fans" online. Some of them portrayed the Italian boy as a "saint," in line with the broader Saints culture.[g]

## The Arezzo and Perugia Cases: Other School-Attack Plans

In the days immediately following the attack in Trescore Balneario, Italian authorities conducted a series of police operations targeting minors that highlighted links among the threat of school violence, violent right-wing extremism, misogynistic grievance, and NVE-adjacent references.

On April 4, 2026, in the province of Arezzo, not far from Florence, the State Police searched a 15-year-old with white supremacist sympathies, under investigation for hate propaganda and incitement to commit a crime.[49] The youth, who posted violent content online and expressed deep contempt for women, had also voiced admiration online for the Trescore Balneario attacker. Furthermore, according to investigators, he had expressed an intention to carry out a similar act "after Easter" (Easter Sunday fell on April 5).[50] Police also found a video on the teenager's smartphone showing him wielding a large kitchen knife and simulating stabbing motions against a pillow on a sofa in his home.[51] Officers seized his smartphone, a video game console, and paper notes containing references to perpetrators of murders and terrorist attacks.[52]

A few days earlier, on March 30, the ROS (the Carabinieri elite special operations unit) arrested a 17-year-old originally from Pescara who was living in the province of Perugia.[53] He was suspected of hate propaganda and incitement to commit crimes and of possessing material for terrorist purposes. Investigators also documented contacts between this 17-year-old and the leadership of the Telegram group "Werwolf Division"[h] (later renamed "New Dawn Division"),[54] originally created by an Italy-based neo-Nazi group of the same name, that had already been targeted by national counterterrorism authorities in December 2024.[55] The participants in this digital space glorified far-right attackers such as Anders Behring Breivik (Oslo and Utøya, in 2011) and Brenton Tarrant (Christchurch, in 2019) who were elevated as "saints" to encourage emulation.[56]

Investigators alleged that the 17-year-old student had assembled operational instructions for the synthesis of acetone peroxide (TATP, a powerful and notoriously unstable explosive) and the manufacture of firearms, including 3D-printed ones, and had gathered information regarding hazardous chemical and biological substances.[57]

Reportedly, in a 2024 WhatsApp chat, the boy had written: "When I'm in my final year, I'll replicate Columbine." Other messages had expressed similar aspirations: "maybe one day I'll do a shooting and then kill myself;" and "I still have to decide where to do the shooting before checking out."[58] Another message referred to buying a "Natural Selection" T-shirt.[59]

Furthermore, the teenager reportedly described himself as an "incel," and gathered information online about notorious Italian perpetrators of violence against women.[60] Child sexual abuse material was also reportedly found on his smartphone.[61]

As part of the same police operation, the Carabinieri's ROS searched seven other minors, aged 13 to 17, across several Italian provinces. All were allegedly found to be embedded in what investigators described as a transnational virtual ecosystem of neo-Nazi, accelerationist, and white supremacist groups and channels.[62] The investigation, opened in October 2025, grew out of an earlier counterterrorism inquiry concluded in July 2025 by the Carabinieri.[63] That same month, the State Police conducted a separate wave of 22 searches involving youths aged 13 to 17 associated with different forms of violent extremism.[64]

The Perugia case illustrates a familiar dynamic: the "aesthetic adoption" of symbols and figures across ideological categories,[65] including an overlap among neo-Nazi symbols, incel grievance, school-shooting references, and NVE-linked aesthetics. From this perspective, far-right attackers such as Breivik and Tarrant and school shooters such as the Columbine perpetrators may function together as figures of rupture in a shared mythology of violence. NVE-inspired actors venerate attackers from across the ideological spectrum "for their action, not their ideological convictions;"[66] the in-group is defined primarily by violence circulated, glorified, and at times performed, rather than by beliefs held.

It is worth adding that the Arezzo and Perugia cases have at least one important Italian precedent. In January 2021, the DIGOS arrested a 22-year-old from Savona (northwestern Italy)

f It is also worth highlighting that premeditated school attacks have historically been extremely rare in Italy. Cf. Nils Böckler, Thorsten Seeger, Peter Sitzer, and Wilhelm Heitmeyer eds., *School Shootings: International Research, Case Studies, and Concepts for Prevention* (New York: Springer, 2013).

g Adherents to militant accelerationism and adjacent extremist milieus often glorify perpetrators of terrorist attacks and massacres as exemplary figures to be emulated, and venerate them as "saints," mimicking Christian iconography. This practice has also extended to the incel subculture and NVE itself. Among others, see Jonathan Lewis, Joshua Molloy, and Graham Macklin, "The Lineage of Violence: Saints Culture and Militant Accelerationist Terrorism," GNET Research, April 27, 2023; Graham Macklin, "Evaluating 'Transnationalism' as an Analytical Lens for Understanding REMVE Terrorism," *CTC Sentinel* 17:11 (2024).

h The German name "Werwolf" (werewolf) apparently evokes the 1944 Nazi plan to create a resistance force that could operate behind enemy lines.

for terrorist association, hate propaganda, and racially motivated incitement aggravated by Holocaust denial.[67] This neo-Nazi sympathizer, radicalized largely online, had founded an online group, Nuovo Ordine Sociale (New Social Order), explicitly modeled on Atomwaffen Division, ran a neo-Nazi Telegram channel (Sole Nero, "Black Sun"), and venerated far-right attackers from Breivik to Tarrant.

What makes it an interesting forerunner of the Perugia case is its early fusion of different strands: neo-Nazism and militant accelerationism, a fascination with school shootings (in the reported words of the then 22-year-old from Savona, "better to die with honor in a school shooting than to live a life of filth alone"), and, additionally, explicit incel self-identification ("we will be the first Italian incels to take action").[68] Originating from the case of a radicalized 17-year-old in Turin and later widened to additional suspects, that investigation reportedly ended in 2022 with a reduced sentence against the Savona man on grounds of partial mental infirmity.[69]

## The San Vito Lo Capo Case: A TCC-Inspired Attack at School

On the morning of May 29, 2026, at a middle school in the small town of San Vito Lo Capo, Sicily, a 12-year-old[i] attempted to stab his technology teacher in class with two small knives. The boy wore a helmet and a face mask and had fixed a smartphone to the helmet to record the action and transmit it to a Telegram audience. Reportedly, the attack may have been recorded but not successfully transmitted live.[70] The student was disarmed by the teacher, who sustained only minor abrasions.

According to currently available information, the teacher had given the student poor grades in the past, but the 12-year-old had since improved his performance and did not appear to harbor clear hostility toward that teacher or other colleagues.[71]

What distinguishes this case is the density and specificity of the TCC and NVE-adjacent symbolism on display. Before the attempted attack, the boy had reportedly posted on TikTok a photograph of the helmet he intended to wear, using the hashtags "#truecrimetok" and "#stream" before the attack.[72] The first hashtag was a legible signal within the TCC fandom ecosystem, while the second clearly pointed to the intended communicative dimension of the attempted attack.

As documented in a February 2026 *CTC Sentinel* article, the TCC functions as a layered fandom ecosystem organized around mass-casualty perpetrators, including school shooters, whom adherents research, aestheticize, incorporate into a shared mythology, and sometimes even attempt to emulate.[73] Central to TCC dynamics, too, is the tendency to replace ideology with aesthetics: TCC adherents often disregard the motivations of the criminals they revere, focusing instead on deeply researching and replicating their attire, mannerisms, weapons, and other reproducible markers.[74] In other words, the signs matter first of all because they are legible to insiders; they are not just public spectacle, but also a request for recognition by the fandom itself.

The helmet bore the word "INCEL" prominently on the front and "MIZANTHROPY" [*sic*] on the back, along with several references to school shootings, mass-casualty attacks, and their perpetrators. In chronological order, these included: "TEXAS SNIPER -18" (possibly referring to Charles Whitman's 1966 University of Texas tower shooting, linked to a total of 18 deaths); "COLUMBINE" (the 1999 school massacre); "ATTIAS" (likely David Attias, the perpetrator of the 2001 attacks in Isla Vista, California, near a university attack); "VIRGINIA TECH -32" (the 2007 campus shooting in Virginia, in which 32 victims were killed); "2012 SANDY HOOK" and "LANZA" (the 2012 school shooting in Connecticut and its perpetrator, Adam Lanza); "ELLIOT" (likely Elliot Rodger, the perpetrator of the 2014 misogynistic attacks in Isla Vista); "ISLA VISTA -6 -5" (apparently pairing Rodger's 2014 attack, in which six people were killed, with Attias' 2001 attack, that resulted in the deaths of five people in total); "CRUZ -17" (likely Nikolas Cruz, the perpetrator of the 2018 Parkland high school shooting in Florida, who killed 17 people); "KERCH -20" (the 2018 Kerch Polytechnic College massacre in Crimea, with 20 deaths) "PERM -6" (likely the 2021 Perm State University shooting, in Russia, in which six people were killed); "AUDREY HALE" (the perpetrator of the 2023 Covenant School shooting in Nashville, Tennessee); "TIMOFEY" (likely Timofey Kulyamov, the suspected perpetrator of the 2025 Odintsovo school attack in Russia); and "SAN DIEGO -3" (possibly the May 2026 San Diego shooting, in California, a suspected anti-Islamic attack in which three people were killed).[75] Some of these references, including Columbine and Elliot Rodger, have also firmly established themselves in the TCC pantheon.[76] Importantly, the surname of the Trescore Balneario attacker was also on the helmet. The full name of an Italian man who had murdered members of his family and a neighbor before taking his own life in Sardinia in 2024 was also written on it. Moreover, the helmet bore an acronym that plausibly refers to a gore-related website.[77]

The 12-year-old student also repeatedly used the scorekeeping idiom familiar from NVE/TCC circles and other spaces of atrocity glorification, in which attacks and body counts are tallied as victories. Before the attack, the Italian boy wrote in English on TikTok: "my biggest fear is not even getting -1" (meaning, not killing even one person). As noted above, similar numerical notations also appeared on the helmet and reportedly on the knives (specifically, one knife bore "-51" and "-10," possibly referring to the far-right attacks in Christchurch in 2019 and in Buffalo in 2022, respectively).[78] These notations can be interpreted as a sign of "gamification" of violence operating in real time;[79] NVE/TCC texts and posts frequently assign point values to the tactics, weapons, and targets of earlier attacks, converting violence into a "game" in which users are encouraged to commit and to document their own attacks in pursuit of new "high scores."[80]

On the other hand, that morning, the student wore a black T-shirt bearing the Italian phrase "*Me ne frego*" ("I don't give a damn"), one of the most recognizable rallying cries of Italian fascism. The slogan may have appealed to him as a marker of nihilistic indifference to consequence, but its political resonance should not be dismissed: Before the attack, the boy had reportedly told an online interlocutor that he was taking action "for political reasons" and had previously expressed sympathy for symbols and figures associated with Italian fascism and with contemporary violent right-wing extremism.[81]

The 12-year-old had also published an announcement in English on TikTok the night before the attack: "Don't blame me for what I will do in 4 hrs."[82] Once again, the choice of the English language is consistent with a community whose *lingua franca* is not Italian. Under that TikTok post, dozens of users wrote comments

i Early press reports stated that the student was as old as 11; the age was later corrected.

**"Italy's recent NVE-linked and NVE-adjacent cases are not anomalous or accidental. They represent the national expression of a transnational phenomenon that has been developing for years."**

suggesting at least partial awareness of what was coming: Some asked for a streaming link, others referred to a possible "manifesto," and others used the notation "+1" and "-1."[83]

Following the attempted attack, it emerged that the 12-year-old had reportedly expressed a desire online to target specific schoolmates, all of foreign origin. In his reported words: "my main targets are three clueless Muslim classmates of mine, another Muslim immigrant in a different class, and a Black girl, though I don't know which class she's in." As investigators highlighted, this information raises the possibility that he had at least discussed with other users or fantasized about carrying out a racially motivated massacre.[84]

According to available information, the 12-year-old showed no clear signs of remorse during protected questioning. Because the boy was under 14, he could not be held criminally responsible. The Palermo juvenile prosecutor's office opened an investigation into possible encouragement or instigation by unidentified third parties.[85] The school imposed a 16-day disciplinary removal from the school community and, at the end of the school year in June 2026, did not admit him to the next grade.[86]

## The Connections Between the Trescore Balneario and San Vito Lo Capo Cases

Italian investigators are actively examining whether the two students in Trescore Balneario and San Vito Lo Capo were connected, beyond their partially shared online subculture. Investigators are also examining whether an online intermediary linked the two cases. According to current reporting, a user presenting as a foreign-national girl was in contact with both minors.[87] The Trescore Balneario attacker referred to her at the end of his short pre-attack text, saying he was "in love with her." In the San Vito Lo Capo case, this supposed girl allegedly appeared in the boy's Telegram environment, was tagged in TikTok posts showing preparatory material, and claimed to possess the video of the attempted attack;[88] furthermore, according to media reports, when other users asked the Sicilian boy how they could watch the stream of the imminent attack, he told them to ask "her."[89] However, direct contact between the two Italian minors has not been confirmed as of this writing.

What is confirmed is that the Sicilian boy reshared content celebrating the Trescore Balneario attack and, as noted above, wrote the boy's surname on his helmet. In brief, within weeks, the Trescore Balneario attacker had entered his pantheon.[90] In the community's own logic, the Sicilian boy was apparently attempting to "add to the lineage."

This "lineage" dynamic has been documented by several scholars and experts: An NVE-linked attack can trigger fan content, which enters the community's "mythology" and provides a model for the next participant to act, creating a self-reinforcing logic of attention, imitation, and competitive outbidding.[91] The dynamic is not entirely new; an analogous "cumulative momentum" has been documented in far-right terrorism,[92] with each attacker positioning himself within a chain of predecessors. What is distinctive in the NVE/TCC context is the organization of this process around aesthetics, fandom, and competitive imitation, rather than around a relatively coherent political project.[93]

In this context, Italy now appears to have the first publicly visible links of a domestic mimetic chain, unfolding over a matter of weeks, while available evidence does not prove coordination.

## The Challenges Posed by NVE

NVE poses several complex challenges. First, the phenomenon itself still requires clear and precise focus. The initial confusion of a large part of the Italian media about the nature of these acts or alleged plans and their real motivations reflects a broader conceptual gap, which has practical consequences. Indeed, the terminological instability around NVE is not merely an academic concern; it can complicate legal responses and interagency coordination.

Moreover, it is clear that this type of threat reflects transnational dynamics. The pattern of behavior observed in the 2026 cases is consistent with international NVE documentation, including celebratory references to earlier perpetrators, pre-attack staging, English-language posts, texts or manifestos aimed at a transnational audience, the channeling of proximate personal grievances into a nihilistic performance, the livestream as constitutive element of the act, and/or a limited or unstable role for coherent ideology. The online platforms involved, including Telegram and TikTok, also operate on a global scale.

These Italian cases also involved warning signs (texts, posts, photographs, hashtags, etc.) visible before the violence or alleged planned violence. This is consistent with the research on "leakage:" Lone actors are significantly more likely than group-based violent extremists to communicate their intent before acting.[94] The policy challenge is to connect platform moderation, law enforcement, school-based threat assessment, families, and mental-health services quickly enough to matter, without treating every potential adolescent provocation as a terrorist signal.

One notable institutional response was the application of the Christchurch Call Protocol (originally developed in response to the 2019 mosque shootings in New Zealand) to the Trescore Balneario livestream, which was removed from Telegram and flagged through the Global Internet Forum to Counter Terrorism (GIFCT) content hash-sharing system.[95] This is significant because it represents the first confirmed Italian application of that mechanism to an NVE-linked violent incident, and reflects an understanding that what happened in Trescore Balneario, however different from jihadi or far-right livestreamed violence in ideology and scale, shares key aspects of its communicative logic: The act's damage is not only physical but also informational and has a potential mimetic character.

Another source of serious concern is that numerous NVE manifestations are structurally based on processes of imitation and of competitive outbidding. These dynamics demand a rapid response. The 65 days between Trescore Balneario and San Vito Lo Capo are consistent with a pattern in which the cycle from act to attempted replication can unfold in weeks. Mobilization "in service

of solely an aesthetic" may proceed on shorter timelines compared with mobilization within violent extremist groups requiring deeper ideological indoctrination.[96]

Additionally, it is well documented that individuals in NVE milieus are often very young. Italy's recent cases push the age frontier in ways that concern investigators, in addition to families and schools. In particular, the San Vito Lo Capo student, at 12 years old, appears to be among the youngest TCC-linked actors publicly documented. The Italian boy was born the same year as the 2014 Isla Vista attacks and a full 15 years after the Columbine massacre; he arguably absorbed their mythology mostly, if not entirely, through the online TCC ecosystem.

Such a young age poses serious practical challenges. From a criminal standpoint, in Italy the threshold for criminal liability is 14 years of age.[97] This means that both the Trescore Balneario and San Vito Lo Capo attackers cannot face criminal proceedings, although juvenile courts can impose protective or security measures where the legal requirements are met. As in other national jurisdictions,[98] this condition tends to create an asymmetry between the seriousness of the acts and the legal instruments available in response.

Some minors may even understand and exploit this legal vulnerability. In his short manifesto, the Trescore Balneario attacker explicitly wrote: "since apparently 'kids' can't understand what's good and what's not, I'll use this in my favor, I can't be imprisoned, since in Italy the minimum age for criminal liability is 14, I can't be trialed at all, so I'll do what I always wanted to do, kill her [the French language teacher] and everyone that tries to stop me from doing that." The San Vito Lo Capo student reportedly showed a similar awareness online.[99]

This is not an Italian idiosyncrasy but a pattern documented across different NVE milieus: For example, in the Swedish "Slain764" case, the senior figure who coerced and blackmailed a 14-year-old into carrying out a stabbing near Stockholm in September 2024 explicitly reassured him that, as a minor below the age of criminal responsibility, he had effectively no serious consequences to fear and should simply go ahead.[100]

NVE cannot, however, be understood solely as a law-enforcement problem, particularly when very young people are involved. A 12-year-old who has apparently internalized elements of the NVE/TCC repertoire of meanings, symbols, and incentives is also a child in acute crisis, one who has found in those online ecosystems a structure of meaning, identity, and belonging that that he did not find and recognize in his immediate social environment.[101]

This aspect highlights a significant vulnerability unique to Italy. Unlike most Western countries, Italy still lacks a comprehensive national strategy for preventing and countering violent extremism (P/CVE). It could be argued that in this field, Italy has to a certain extent been a victim of its own success: The limited number of extremist attacks, with very few casualties—due in part to an expert, well-coordinated, and proactive counterterrorism apparatus[102]—has meant that such a comprehensive prevention framework has appeared less urgent in the country. However, recent cases such as those discussed in this article highlight the need to develop a P/CVE national strategy promptly, drawing on international best practices and lessons learned. This effort should also include referral mechanisms and programs tailored to schools.

Encouragingly, the Bolzano case suggests that timely intervention may work: As noted above, according to available information, the same boy who was "at a very advanced stage" of a murder plan in February 2025 was, a year later, a dedicated student expressing gratitude to those who had stopped him.

## Conclusions

Italy's recent NVE-linked and NVE-adjacent cases are not anomalous or accidental. They represent the national expression of a transnational phenomenon that has been developing for years. In NVE milieus, ideological orientations may be absent or, at the very least, may function mainly as aesthetic, status, and identity markers. This does not make NVE less dangerous or less consequential; it makes it harder to classify and interpret. The phenomenon typically sits at the intersection of terrorism, targeted violence, child exploitation, self-harm, and youth mental-health crises. Overexpanding the "terrorism" label risks obscuring peculiar dynamics (such as aesthetic fascination, status-seeking, coercion, and juvenile vulnerability) and may produce blunt responses; however, treating these cases as ordinary "adolescent deviance" risks understating their seriousness and ignores their networked structure, imitative dynamic, and performative logic.

The Italian sequence makes these patterns visible in different forms. In particular, the Bolzano case points to the transnational 764/Com ecosystem and to "remotely coerced violence;" Trescore Balneario shows how personal resentment can be recast as livestreamed, NVE-adjacent performance at school; Arezzo and Perugia illustrate the fusion of far-right references with school-attack fantasies and misogynistic grievances; and San Vito Lo Capo offers the clearest Italian example to date of a TCC-coded attack attempt, only weeks after the earlier school attack in the country.

This examination also makes manifest that a 12- or 13-year-old can be at the same time a vulnerable child and a potential source of serious public violence. Ultimately, while effective counterterrorism is essential, an even deeper challenge concerns prevention. For Italy, as for other countries facing this threat, the task is to develop and enhance a comprehensive system capable of identifying and 'stopping' such individuals, including children, in time, and offering them something to return to afterward. CTC

## Citations

1 For example, "Il 'manifesto' choc del 13enne di Trescore: 'Ucciderò la mia insegnante di francese. Le piace prendermi di mira,'" Giorno, March 26, 2026.
2 In particular, Peter Smith, Cat Cadenhead, and Clara Broekaert, "True Crime Community: Understanding the Depths of Digital Fandom and Performative Violence," *CTC Sentinel* 19:2 (2026).
3 For example, Salvo Palazzolo, "Dodicenne assale prof in diretta social. L'annuncio su TikTok, sul casco scritte sulle stragi Usa," *Repubblica*, May 30, 2026.
4 "Progettava una strage a scuola in stile 'Columbine', arrestato un 17enne e indagati altri sette giovani," Ansa, March 30, 2026.
5 Simone Innocenti, "Arezzo, la minaccia di un 15enne: 'Accoltellerò anche io una prof, lo farò dopo Pasqua,'" *Corriere della Sera*, April 8, 2026.
6 "Quindicenne arrestato a Bolzano per terrorismo suprematista," Ansa, February 12, 2025.
7 Maria Cristina Palai, "La presenza dei minori nei circuiti di propaganda, reclutamento e adescamento delle organizzazioni terroristiche. Analisi del fenomeno e attività investigative," Scuola Superiore della Magistratura, June 16, 2025, p. 14.
8 "Bolzano: minorenne arrestato per terrorismo," Polizia di Stato, February 12, 2025.
9 In particular, Leonardo Bianchi, "Cos'è '764', la rete terroristica neonazista a cui aderiva il 15enne arrestato a Bolzano," Facta, February 14, 2025.
10 In particular, Marc-André Argentino and Angus Lindsay, "Remotely Coerced Violence: 764, The Com Network, and the Hybridization of Threats," *CTC Sentinel* 19:6 (2026).
11 "Government of Canada Lists Four New Terrorist Entities," Public Safety Canada, December 10, 2025.
12 See Marc-André Argentino, Barrett Gay, and Matt Bastin, "Nihilism and Terror: How M.K.Y. Is Redefining Terrorism, Recruitment, and Mass Violence," *CTC Sentinel* 17:8 (2024).
13 Martina Capovin, "'Grazie a magistrati e polizia che mi hanno fermato in tempo': a 15 anni pianificava l'omicidio di un senzatetto con una setta neonazista," *Il Dolomiti*, February 18, 2026.
14 "Preparava un omicidio a 15 anni," *Il Dolomiti*, February 13, 2025.
15 "Bolzano: minorenne arrestato per terrorismo."
16 Ibid.
17 Ibid.
18 "Bolzano, arrestato 15enne in un gruppo satanista: pianificava una strage," Rai News, February 13, 2025.
19 Cf. Andrew Glazzard, David Mcilhatton, and Paul Martin, "Will Generative AI Fundamentally Change Terrorist Threats?" *CTC Sentinel* 19:5 (2026).
20 "Preparava un omicidio a 15 anni."
21 Chiara Currò Dossi, "Quindicenne arrestato per terrorismo a Bolzano: la molotov, l'ascia nell'armadio e il dark web: 'Voleva andare in Palestina,'" *Corriere della Sera*, February 23, 2025.
22 "Bolzano: minorenne arrestato per terrorismo."
23 Chiara Currò Dossi, "Terrorista neonazista a 15 anni, progettava di uccidere un senzatetto: 'Ho sbagliato, grazie per avermi fermato,'" *Corriere della Sera*, December 10, 2025.
24 Among others, see Marc-André Argentino, Barrett G and M.B. Tyler, "764: The Intersection of Terrorism, Violent Extremism, and Child Sexual Exploitation," GNET Research, January 19, 2024.
25 "Quindicenne arrestato a Bolzano per terrorismo suprematista."
26 Palai, p. 14.
27 See "Sentencing Remarks of Mr Justice Jay: R v Cameron Finnigan," Judiciary of England and Wales, January 16, 2025, p. 2.
28 Marco Angelucci and Chiara Currò Dossi, "Quindicenne arrestato per terrorismo, FdI porta il caso in Parlamento: 'Era pronto al martirio per l'Islam,'" *Corriere della Sera*, February 18, 2025.
29 See also Argentino and Lindsay, p. 43.
30 "Sentencing Remarks of Mr Justice Jay: R v Cameron Finnigan."
31 Ibid., p. 6.
32 Angus Crawford and Tony Smith, "Abuse terror warning as 'Satanist' teenager jailed," BBC, January 16, 2025.
33 Argentino and Lindsay.
34 Ibid.
35 Ibid.; Capovin.
36 For example, "L'accoltellamento di Trescore: la diretta e il messaggio del tredicenne sui social," L'Eco di Bergamo, March 29, 2026. Cf. Mackenzie B. Hart, "'Less than a speck of dirt': exploring the manifestos of nihilistic violent extremists," *Behavioral Sciences of Terrorism and Political Aggression* (2026).
37 Cf. Jacob Ware, "A Terrorism of Vengeance," Lawfare, December 16, 2025.
38 For example, "Dimessa la professoressa accoltellata, 'salvata da uno studente coraggioso,'" Ansa, March 30, 2026.
39 See, in particular, Manfredi Pozzoli, "A Growing Global Threat: A Streamed Nihilistic Attack in Italy," GNET Research, May 7, 2026.
40 Cf. H. E. Upchurch, "The Iron March Forum and the Evolution of the 'Skull Mask' Neo-Fascist Network," *CTC Sentinel* 14:10 (2021).
41 In particular, Hart, pp. 12-13.
42 "Mimetica ed esplosivo, il tredicenne in diretta su Telegram," Ansa, March 25, 2026.
43 "Prof accoltellata da studente 13enne a Trescore Balneario, il legale: Difficile che abbia fatto tutto da solo," Giorno, March 28, 2026.
44 "Trescore, il giudice: lo studente di 13 anni che ha accoltellato la prof Mocchi andrà in comunità," *Repubblica*, April 9, 2026.
45 Giusi Fasano, "L'amica ricattata in chat dal 13enne che ha cercato di uccidere la prof: 'Mi disse: tagliati o rivelo i tuoi segreti,'" *Corriere della Sera*, March 26, 2006.
46 Argentino and Lindsay.
47 Antonio Pellegrino, "Scuola del terrore | Trescore Balneario e la Columbine italiana, prenderne atto eviterà errori," Linkiesta, March 28, 2026.
48 Pozzoli.
49 "Digos: perquisito un minore, indagato per propaganda d'odio," Polizia di Stato, April 7, 2026.
50 Innocenti.
51 "Digos: perquisito un minore, indagato per propaganda d'odio."
52 Ibid.
53 "Antiterrorismo: arrestato un minore per propaganda e istigazione a delinquere," Arma dei Carabinieri, March 30, 2026.
54 "Antiterrorismo." See also Giuseppe Baldessarro, "Arresto ragazzo neonazista: cos'è il gruppo 'Werwolf Division' finito sotto inchiesta a Bologna," *Corriere della Sera*, March 30, 2026.
55 "Arrestate 12 persone appartenenti al gruppo suprematista 'Werwolf division,'" Polizia di Stato, December 4, 2024.
56 "Antiterrorismo."
57 Ibid.
58 For example, "Progettava una strage a scuola, 17enne arrestato a Perugia. Indagati altri 7 minorenni," Rai News, March 31, 2026.
59 Ilaria Sacchettoni, "Il piano del 17enne che voleva fare una strage a scuola: 'Replicherò Columbine'. I manuali sui colpi di Stato, gli incel, Turetta e Izzo nel cellulare," *Corriere della Sera*, March 31, 2026.
60 Ibid.
61 "Progettava una strage a scuola, 17enne arrestato a Perugia. Indagati altri 7 minorenni."
62 "Antiterrorismo." See also "Progettava una strage a scuola," Ansa, March 30, 2026.
63 For example, Pierluigi Ferrari, "Brescia, propaganda fascista online: arrestato un operaio 21enne, perquisizioni in tutta Italia," Rai News, July 17, 2025.
64 "La Polizia di Stato esegue 22 perquisizioni nei confronti di giovani evidenziatisi in contesti estremisti di matrice suprematista, accelerazionista, antagonista e jihadista," Polizia di Stato, July 31, 2025.
65 For example, "Terror Without Ideology?" Institute for Strategic Dialogue, May 8, 2025.
66 Hart, pp. 15-16.
67 "Terrorismo: arrestato 22enne suprematista e negazionista," Polizia di Stato, January 11, 2022. See also Francesco Marone, "Black Sun: A Case of Radicalization Between Neo-Nazism and Incel Ideology," ISPI Commentary, January 27, 2021.
68 Ibid.
69 "Vizio di mente, pena ridotta al suprematista di Savona," *Il Secolo* XIX, January 26, 2022.
70 Leonardo Bianchi, "'Nessuna vita conta': la minaccia dell'estremismo nichilista violento in Italia," Facta, June 9, 2026.
71 "Porta a porta: Parla il prof accoltellato da un 12enne a San Vito Lo Capo," Rai News, June 4, 2026.
72 "Prof aggredito da 11enne, sul casco del ragazzo le scritte sulle stragi Usa," *Adnkronos*, May 30, 2026.
73 Cadenhead, Smith, and Broekaert.
74 For example, Beyond Extremism: Platform Responses to Online Subcultures of Nihilistic Violence, ISD – GIFCT – GNET Research, February 2026.

75 Bianchi.
76 Smith, Cadenhead, and Broekaert.
77 Cf. Ali Fisher and Arthur Bradley, *Gore and Violent Extremism: An Explorative Analysis of the Use of Gore Websites for Hosting and Sharing Extremist and Terrorist Content* (Dublin: VOX-Pol, 2025).
78 For example, Velia Alvich, "Le dirette video e i serial killer come idoli: cos'è la 'true crime community' a cui aderiva lo studente che ha attaccato un docente," *Corriere della Sera*, May 31, 2026.
79 Among many others, cf. Linda Schlegel and Rachel Kowert eds., *Gaming and extremism: The radicalization of digital playgrounds* (Abingdon: Routledge, 2024) and Francesco Marone, "Giochi pericolosi? Potenzialità e limiti dei videogiochi nella 'gamification' dell'estremismo politico violento," *Quaderni di scienza politica* 32:1 (2025).
80 Among others, Hart.
81 Luca Mariani, "San Vito Lo Capo: l'aggressore 12enne cita Tarrant, Gendron e Timofey," AGI, June 2, 2026.
82 For example, Giorgio Ruta, "Tentato accoltellamento al prof, l'undicenne aveva scritto 'non incolpatemi per ciò che farò,'" Rai News, May 30, 2026.
83 Laura Pace, "Aggressioni ai professori, i ragazzi nella stessa chat: da Trapani a Bergamo, i casi (e i punti di contatto)," *Messaggero*, May 31, 2026.
84 Salvo Palazzolo, "Il piano del dodicenne: 'Uccido 3 compagni di scuola musulmani. Prima di 14 anni non fanno processo,'" *Repubblica*, June 2, 2026.
85 Salvo Palazzolo, "'Il ragazzo con il coltello istigato da qualcuno sui social'. La procuratrice: 'Voleva una strage,'" *Repubblica*, May 31, 2026.
86 Francesca Capizzi, "Aggredì il prof a San Vito, arriva la bocciatura a scuola," *Giornale di Sicilia*, June 18, 2026.
87 For example, Salvo Palazzolo, "Un gruppo Telegram dietro il dodicenne. Il Ros a caccia di 'Euno': 'Ho il video dell'attacco,'" *Repubblica*, June 3, 2026.
88 Ibid.
89 Pace.
90 Cf. Allizandra Herberhold, "The 'True Crime Community Stoplight Model': Understanding Digital Pathways and Tumbler Ridge," GNET Research, May 1, 2026.
91 Among others, Smith, Cadenhead, and Broekaert.
92 See Amarnath Amarasingam, Marc-André Argentino, and Graham Macklin, "The Buffalo Attack: The Cumulative Momentum of Far-Right Terror," *CTC Sentinel* 15:7 (2022).
93 Hart, p. 7.
94 For example, Anne-Lynn Dudenhoefer, Charlotte Niesse, Thomas Görgen, Laura Tampe, Marcella Megler, Christina Gröpler, and Rebecca Bondü, "Leaking in terrorist attacks: A review," *Aggression and Violent Behavior* 58 (2021).
95 "Incident Response: Perpetrator Content Incident Activated in Response to Violent Extremist Event in Trescore Balneario, Italy," GIFCT, March 27, 2026.
96 Beyond Extremism, p. 22.
97 Italian Criminal Code, Article 97 ("Minore degli anni quattordici".)
98 Tanya Mehra and Menso Hartgers, "Fury and Void: Legal Pathways to Counter 764," ICCT, October 2025.
99 Mariani.
100 Argentino and Lindsay, pp. 43-44.
101 Cf. Cécile Rousseau, Cindy Ngov, and Sébastien Brouillette-Alarie, "Referral Pathways and Clinical Profiles among Individuals Involved in Violent Extremism and Violent Nihilism," *Perspectives on Terrorism* 20:2 (2026).
102 For example, Francesco Marone, "The Italian Way of Counterterrorism: From a Consolidated Experience to an Integrated Approach," in S.N. Romaniuk et al. eds., *The Palgrave Handbook of Global Counterterrorism Policy* (London: Palgrave Macmillan, 2017), pp. 479-494.