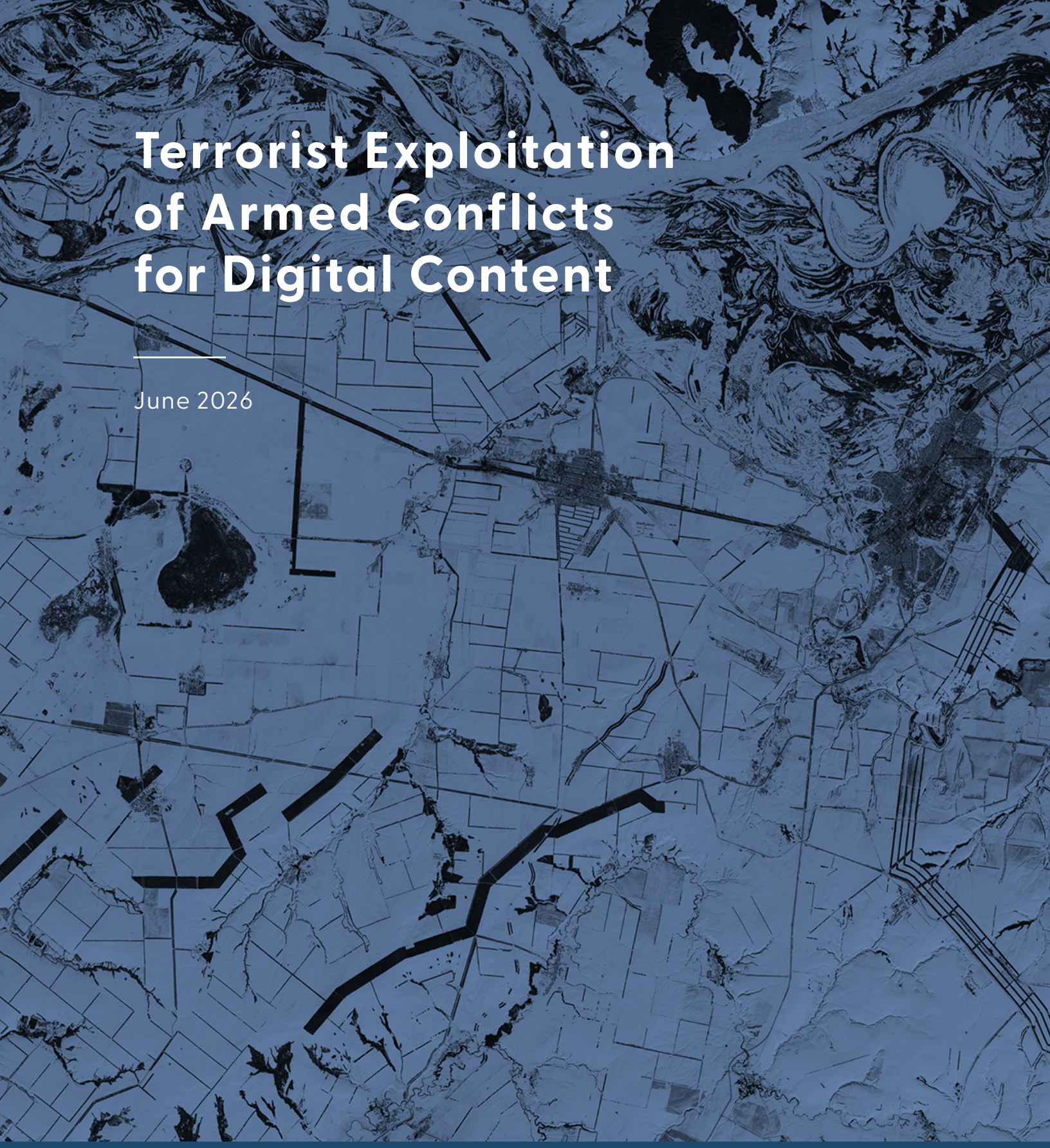


Terrorist Exploitation of Armed Conflicts for Digital Content

June 2026

KONRAD ADENAUER STIFTUNG | UN LIAISON OFFICE NEW YORK

GIFCT
Global Internet Forum to Counter Terrorism

KONRAD ADENAUER STIFTUNG | UN LIAISON OFFICE NEW YORK

GIFCT Global Internet Forum to Counter Terrorism

Table of Contents

The views and opinions expressed in this report are the authors' own and do not necessarily reflect those of GIFCT or KAS.

Introduction

Naureen Chowdhury Fink | Executive Director, GIFCT

The Global Internet Forum to Counter Terrorism (GIFCT) is delighted to partner once again with the Konrad-Adenauer-Stiftung (KAS) on this project examining the implications and impacts of armed conflict on terrorist content online. This collaboration comes at a pivotal moment. Today's global security landscape is shaped by the convergence of protracted conflicts, rapid technological innovation, and social dynamics that increasingly play out online.

New tools and technologies create untold opportunities for progress; they also create unprecedented opportunities for adversarial actors to disseminate propaganda, erode trust, and scale their ambitions. As Blaise Metreweli, head of MI6, recently noted, "Advances in artificial intelligence, biotechnology and quantum computing are not only revolutionising economies but rewriting the reality of conflict, as they converge to create science-fiction-like tools."

Research and practice have long demonstrated that terrorism and armed conflict are deeply linked and mutually reinforcing. Pillar I of the United Nations Global Counter-Terrorism Strategy notes that conditions such as "prolonged unresolved conflicts, dehumanization of victims of terrorism in all its forms and manifestations, lack of rule of law and violations of human rights, ethnic, national and religious discrimination, political exclusion, socioeconomic marginalization and lack of good governance" can create environments conducive to the spread of terrorism. In this context, the digital ecosystem has become a critical arena where conflict dynamics can be amplified, reshaped, and, in some cases, accelerated and adapted to terrorist purposes.

Terrorists and violent non-state actors have consistently exploited such conditions to advance their objectives and legitimize their tactics and goals. They have leveraged conflict settings to generate compelling recruitment narratives, produce and disseminate propaganda, develop instructional materials, mobilize resources, and recruit supporters across borders. Increasingly, conflicts are not only sources of grievance or inspiration but also function as real-time content ecosystems, providing a steady stream of imagery, narratives, and operational signals that can be repurposed and weaponized online.

Terrorist groups like Islamic State and al-Qaeda, and violent extremist networks like The Com, have leveraged technology to develop approaches closely tailored to their target audiences. For example, Islamic State was able to exploit deep-seated grievances about the misrule of Syria by the Assad regime to attract an initial outflow of supporters and portray itself as a state-building enterprise. The conflict in Ukraine prompted early tensions among far right and white supremacist groups as parties each portrayed their tactics as historically shaped entitlements. By adapting their tactics to digital environments – from encrypted messaging applications to mainstream social media and new content formats – they maximize reach, resilience, and impact.

This collaboration between GIFCT and KAS seeks to better understand these evolving dynamics, bringing together global expertise and analysis informed by the private sector, GIFCT initiatives, and regional experts, including contributors to the Global Network on Extremism and Technology (GNET), the research arm of GIFCT.

This report presents a set of analytical briefings, or "snapshots from the field," that examine how terrorist and violent extremist (TVE) actors exploit specific conflict environments to produce and disseminate digital content. Through focused case studies, this project seeks to highlight how violent non-state actors, including terrorists, are exploiting the dynamics of armed conflicts to develop online materials that can be used to incentivize further violence and to raise awareness among policymakers, tech companies, and platforms about the potential content and harms emanating from ongoing armed conflicts.

To facilitate this project, GIFCT hosted a roundtable discussion among experts to inform the key questions and considerations addressed in each chapter, and experts from the KAS network have contributed opening "conflict overviews" to set the scene for explorations of intersections among conflict, terrorism, violent extremism, and technology. Each of the selected cases highlights scenarios with complex multidimensional conflicts involving both inter-state and intra-state violence, and local, regional, and transnational actors.

In the Afghanistan conflict overview, Michael Kugelman highlights that although the security situation has improved, the presence of Islamic State of Khorasan Province (ISKP) and the Tehreek-e-Taliban Pakistan (TTP), along with the tensions at the border with Pakistan, still contribute to continued incidents of violence. This apparent success has come at great cost in human rights, particularly for women and girls, which raises questions about the long-term legitimacy and sustainability of their administration. However, as Abdul Basit outlines in his analysis, groups affiliated with Islamic State and TTP, for example, have exploited the armed conflicts in the country to generate content online aimed at legitimizing their goals, facilitating recruitment and fundraising, and disseminating operational information. The history of conflict among various groups is also reflected in the use of platforms to delegitimize and diminish their opposition, which retain the capacity for violence, especially as seen along the border with Pakistan.

In the Sahel, Ulf Laessing's conflict overview outlines the worsening security crisis that has been exacerbated by transnational terrorist groups expanding their operations into the region and the failures of several international efforts, including those of France and the UN, and the approaches of Russian private contractors who have supported failing governments, often in the hopes of retaining access to critical resources. Against this background, Beverly Ochieng expands on the online components of Islamic State's self-styled Sahel Province (ISGS) operations and those of Jama'a Nusrat ul-Islam wa al-Muslimin (JNIM), including how their online content narratives differ depending on the operational goal, audience, and the global or local context in which

the groups situate themselves. She situates these findings within evolving inter- and intra-group dynamics and regional challenges, noting that in many areas, online content is unlikely to be the primary factor shaping engagement with violent groups.

In Ukraine, Elena Davlikanova and Olya Korbut outline a very different scenario from those in Afghanistan and the Sahel, one of inter-state war, albeit including several sub-state actors. This highlights important questions about the definition and categorization of terrorist groups, often making it difficult to implement clear policies and practices online. As Kacper Rekawek, Uljana Vlagyimirova, and Julian Lanchès point out, in some instances groups have been integrated into formal state structures while maintaining independent online identities, posing particular challenges for tech companies seeking to moderate TVE content. Moreover, the conflict in Ukraine reflects dynamics in the wider far right movement, with external groups exploiting the conflict to promote narratives like the "Great Replacement," they note.

Despite the different sociopolitical contexts, there are similarities across all three conflicts in how TVE actors situate their content within both hyper-local and broader global narratives, seek to raise funds online, build support and legitimacy, and recruit to enhance their offline goals. Each of these cases also highlights a range of international approaches to defining and classifying these groups. Islamic State and al-Qaeda, and several of their affiliated organizations, are on the UN 1267 counterterrorism sanctions list. Other groups may be designated by various national or regional actors, but without a clear global consensus. This raises questions about the opportunities and limitations of existing international policy tools – including sanctions and measures to address terrorism financing – that can be used to counter the activities of these groups, and, by extension, their online presence.

The case studies presented here also raise questions about the extent to which moderation efforts online alone can address the proliferation of TVE content, and highlight the continued importance of investing in efforts to prevent and mitigate conflict. At the same time, these examples show that skilled propagandists can inflame grievances and exploit vulnerabilities to foment violence and foster division. The disappointments of citizens facing prolonged periods of insecurity and instability, corruption in governments unable to address fundamental needs, and experiences of human rights violations, particularly at the hands of states or de facto rulers, have created openings that TVE groups, from the Sahel to Afghanistan to Ukraine, have been quick to exploit.

Industry solutions have come a long way, particularly in the last decade. Tools like hash sharing and incident response have been developed and updated to try to impede the circulation of perpetrator-produced content intended to glorify and amplify their attacks and goals. As individual platforms moved to address terrorist content online, adversarial adaptations and migrations highlighted the critical importance of cross-platform collaboration and dialogue. More research and analysis are available to inform practitioners and policymakers about the dynamics of ter-

rorism, radicalization, mobilization, and their implications online. Nonetheless, as global trends shift and TVEs adapt, it remains critical for industry actors and stakeholders to continuously review and pivot where necessary.

Against the backdrop of numerous armed conflicts worldwide and rising tensions over economic security, climate change, and humanitarian crises, state representatives will convene in 2026 to review the UN Global Counter-Terrorism Strategy, marking its twentieth anniversary. This process provides the international community with a unique opportunity to deliberate on priorities and shape a strategic framework for collaborative counterterrorism efforts. Moreover, these debates often reflect the key priorities and concerns of international actors and global stakeholders, highlighting areas of emphasis and concern for the private sector. The discussions among experts, policymakers, and practitioners around the Strategy highlight ever-evolving threats and contemporary trends, underscoring the importance of the private sector and the need for traditional approaches to armed conflict to reflect the risks and opportunities posed by technology.

Afghanistan

Conflict Overview

Michael Kugelman | Resident Senior Fellow for South Asia, Atlantic Council

Since August 2021, when NATO forces left Afghanistan and the Taliban returned to power, the country has not experienced internal armed conflict, and terrorist attacks have decreased. Nonetheless, Afghanistan still faces significant security challenges, including from violent actors and as a result of border tensions with Pakistan.

This state of affairs is striking for several reasons. First, until 2021, Afghanistan had experienced some form of conflict – whether foreign military interventions, civil war, or anti-state insurgency – for more than four decades. Second, the Taliban are closely allied with most of the terrorist organizations based in Afghanistan; with its return to power, it was expected that the country would again become the hotbed for terrorist activity that it was in the years immediately preceding and following the September 11, 2001, attacks. Indeed, a wide range of regional and international terrorist actors have long operated along the Afghanistan-Pakistan border.

The calmer security situation in Afghanistan can be attributed to several factors. First, the Taliban, despite their brutality, notoriously harsh policies toward women, and lack of legitimacy at home and abroad, have consolidated their power. They control nearly all of Afghanistan (unlike during their rule in the late 1990s, when armed opponents controlled large swaths of territory); they have successfully managed internal divisions within the group; and they have surprised their critics by showing a capacity to implement public policy, from passing budgets to delivering basic services.

While the international community (with the exception of Russia) has not formally recognized the Taliban regime, it has been willing to engage diplomatically. Unlike in the pre-9/11 era, Afghanistan's neighbors have not funneled support to Taliban rivals. This all helps explain why the Taliban face no imminent challenges to their rule. There is no armed resistance, and the Taliban have cracked down hard on Islamic State-Khorasan (ISKP) – one of the few terrorist organizations in Afghanistan not allied with them.

Second, while the Taliban maintain ties to many terrorist groups in Afghanistan, most of them are weak and not very active. These groups include al-Qaeda and several al-Qaeda-allied regional militant groups, such as the Islamic Movement of Uzbekistan (IMU) and the East Turkestan Islamic Movement (ETIM). Other groups in Afghanistan are more active but, for strategic reasons, do not carry out attacks in the country. The most prominent example is Tehreek-e-Taliban Pakistan (TTP). The exception is ISKP, but it has been hit hard by Taliban ground forces in recent years. This may explain in part why ISKP has increasingly turned its attention to targets outside Afghanistan.

However, despite improved security in Afghanistan, there remain three serious security threats that warrant continued monitoring.

First, ISKP remains a dangerous actor, despite being degraded by Taliban ground actions. Since being formally launched in 2015, it has remained resilient, surviving frequent NATO air strikes and Afghan ground offensives, and most recently, Taliban operations. It continues to strike in Afghanistan, even if at a lower rate. Over the last few years, it has claimed major attacks in Iran, Russia, and Turkey. In February 2026, it attacked a Shia mosque in Islamabad, Pakistan, killing more than 30. It has also plotted attacks that were eventually foiled in Europe and the United States.

Second, TTP, using bases in Afghanistan, has ramped up attacks in Pakistan since the Taliban's return. TTP is not as potent now as it was during the 2007–2014 period, when it staged attacks across Pakistan and often targeted civilians. Today, most TTP attacks occur in Pakistan's Khyber Pakhtunkhwa Province and target Pakistani security forces. However, the Taliban's return to power in 2021 had a significant impact on the TTP: it emboldened the group, inspiring it to replicate in Pakistan the Taliban's successful insurgency in Afghanistan. Additionally, the Taliban are a longstanding ally of the TTP and are providing the group with the cross-border sanctuary needed to bolster its campaign against Pakistan. The TTP has been further strengthened by the acquisition of more advanced weaponry and new leadership that has successfully addressed internal fissures.

Third, the Afghanistan-Pakistan border region remains highly volatile. One trigger is the TTP. Since October 2025, the Taliban's refusal to curb the TTP has prompted Pakistan – the Taliban's patron during the U.S.-led war in Afghanistan – to carry out periodic airstrikes in Afghanistan against TTP targets and Taliban military facilities. The Taliban have retaliated with operations against Pakistani military forces. These hostilities constitute the most serious violence between Afghanistan and Pakistan since the Taliban's return to power.

While third-party mediation has produced pledges to de-escalate, tensions are likely to persist, given that the Taliban rarely turn on their militant allies; most famously, they declined to turn on al-Qaeda even when threatened with a U.S. military invasion after the September 11 attacks. Moreover, the TTP is one of the Taliban's closest allies; the two groups previously carried out joint operations in Afghanistan, and some TTP leaders – including its first supreme leader, Baitullah Mehsud – were previously members of the Afghan Taliban.

Another trigger for Afghanistan-Pakistan border tensions is the border itself. The Taliban, like all Afghan governments since Pakistan's independence, do not recognize the border. They reject it as an arbitrary and illegitimate demarcation unfairly imposed on Afghans during the period of British colonial rule in India. This is a longstanding source of mistrust between Afghanistan and Pakistan, and it complicates efforts to address other tension points, such as the TTP issue.

In sum, security conditions in Afghanistan have improved over the last five years. However, it is still home to several dangerous actors, especially ISKP and TTP, which carry out or aim to carry out attacks outside Afghanistan. Additionally, its border with Pakistan continues to be a source of mistrust and a potential trigger for violence. While Afghanistan is not currently experiencing internal conflict, it does constitute a terrorist threat because of the violent actors that use Afghan territory to plot or perpetrate attacks elsewhere. It also continues to be at risk from terrorist attacks inside the country by ISKP, which remains operational despite having been degraded by Taliban ground offensives.

Case Study: Afghan Conflict as a Source for Extremist Content and Material

Abdul Basit | Senior Associate Fellow, International Centre for Political Violence and Terrorism Research, S. Rajaratnam School of International Studies, Nanyang Technological University

Introduction

There is a mutually reinforcing relationship between conflict zones and online violent extremist content. Armed conflicts often serve as primary incubators for online extremist propaganda. The acceleration and amplification of armed conflicts via social media create a conducive environment for violent extremist groups to produce, proliferate, and disseminate online extremist materials, such as videos of beheadings and oaths of allegiance, combat footage, and instructional content on weapons and bomb-making. In turn, the availability of such online content exacerbates conflict by attracting recruits, spreading chaos, funding operations, and influencing on-the-ground perceptions.

In light of this, Afghanistan's conflict zone offers important insights concerning violent extremist actors' exploitation of the country's weak governance and permissive operational environment to advance their ideological objectives, while undermining those of their rival groups. For context, as Michael Kugelman's conflict overview highlights, Afghanistan's conflict zone is a multi-actor threat landscape where various terrorist groups with overlapping and competing agendas coexist in a cutthroat environment.

Paradoxically, both cooperation and competition have compelled Afghanistan-based terrorist groups to develop sophisticated media arms, often through mutual learning, knowledge transfer, or imitation of tactics. Since the Taliban's return to power, violent extremist groups in Afghanistan have substantially improved their propaganda operations. Media arms of various groups have produced slick propaganda to compete and stay relevant in Afghanistan's challenging operational environment. Apart from engaging propagandists with journalism backgrounds, such as TTP's so-called Information Minister Chaudhry Muneeb Jutt, or ISKP's former spokesperson Sultan Aziz Azzam, violent extremist groups in Afghanistan have also leveraged social media platforms and generative artificial intelligence (GAI) to mass produce propaganda in multiple local and regional languages and expand their reach.

Through case studies, this essay examines how terrorist groups in Afghanistan leverage armed conflict to validate their ideological worldviews, focusing on four key areas. First, it provides a snapshot of violent extremist content emerging from the Afghan conflict in the online sphere and its objectives. Second, it analyzes the operational tactics used by violent extremist actors, such as TTP, al-Qaeda in the Indian Subcontinent (AQIS), ISKP, and the Afghan Taliban – both inside and outside Afghanistan – for producing and disseminating online content and variations in these

tactics. Third, it examines the underlying objectives of these violent extremist groups in creating and disseminating such materials, and concludes by considering what the evidence suggests about their success.

Type of Material Terrorist Groups in Afghanistan Produce and Proliferate

The extremist materials emanating from Afghanistan contain three critical themes: ideological treatises, political commentary, and information on violent operations and organizational developments. Across these three categories, terrorist groups advance their organizational agendas and priorities while rejecting those of rival factions.

Ideological Treatises

A recurring theme in online violent extremist content emerging from Afghanistan revolves around ideological rivalries among major terrorist networks, especially the Taliban and ISKP. There are visible displays of ideological outbidding, ranging from dense theological debates on Deobandi and Salafi doctrines to polemical exchanges.[1]

The Taliban and ISKP's theological differences center on the former's Islamic Emirate governance model, which combines Pashtun ethnocentrism and Deobandi orthodoxy, and the latter's espousal of its parent group, Islamic State's self-styled global Sunni Caliphate. ISKP asserts that there is no room for an Emirate when a Caliphate exists. The Taliban, conversely, reject Islamic State's claim to the Caliphate, arguing that it lacks the consensus of Muslim scholars and community leaders and does not fulfill other religious criteria.

The Taliban have established a multilingual online portal, Al Mirsad, which, among other things, offers rebuttals of ISKP's ideological position on global jihadism and frames the group as Khawarij – extremist rebels. Furthermore, it provides religious justifications for the clerical regime's crackdown against the group. It maintains that ISKP and its parent organization have done a disservice to the jihadist movement by creating divisions. Al Mirsad is active on X, Facebook, YouTube, and across multiple channels on WhatsApp and Telegram.

Conversely, ISKP, through its propaganda wing, Al-Azaim Media, which operates through encrypted social media apps like Telegram, Threema, and Rocket Chat, persistently targets the Taliban, depicting the group as apostate, an illiterate tribal militia, and a proxy of the Pakistani intelligence service, among other things. These polemical labels have been used to downplay the Taliban's victory and its significance. ISKP has exerted substantial effort, both through extremist content and terrorist attacks, to undermine the Taliban's claim of having restored peace

1. The Deobandi school of thought is a sub-sect of the Hanafi jurisprudence. It is a literalist Islamist movement that originated in the Indian Subcontinent in 1866 to preserve traditional Islamic teachings, emphasizing Sunni orthodoxy and puritanical interpretations of the Quran and Hadith.

in Afghanistan. The Taliban's foreign relations, especially their ties with China, Russia, and India, are used to criticize them. ISKP alleges that the Taliban's crackdowns against it are intended to secure financial and other material benefits from these states as well as diplomatic recognition. The Taliban's endorsement of territorial nationalism, anathema to ISKP's extremist worldview, is another key theme of the group's anti-Taliban propaganda.

Political Commentary

Violent extremist groups based in Afghanistan also comment on key local and global geopolitical developments by appropriating them within their ideological frameworks. By articulating their respective positions on issues sensitive to the Muslim community, such as the Israel-Palestine conflict, they try to enhance their relevance and ideological legitimacy. Sometimes, certain political events with a strong emotional appeal can trigger an avalanche of online extremist content. It is important to keep in mind that political materials from various groups in Afghanistan also provide a critical reflection of their cooperative and adversarial relationships.

The respective views of the Taliban, TTP, AQIS, and ISKP on Hamas's October 7, 2023, attack on Israel and the latter's disproportionate retaliation in Gaza offer important insights into the political messaging of Afghanistan-based terrorist groups. They illustrate how ideological thinking and local priorities shape political commentary.

For instance, AQIS wasted no time in issuing multiple statements through its Telegram channel and flagship Urdu language magazine, *Nawa-e-Ghazwa-e-Hind*, which later appeared on X as well (albeit for a brief period) to praise Hamas's attack, while comparing it with the 9/11 attacks and the Taliban's victory in Afghanistan. In doing so, it urged attacks and political protests against Israel.

Meanwhile, the Taliban bided their time before commenting on the conflict. Their careful messaging on X and through the Foreign Ministry aimed at bolstering their position as a responsible state actor. They appealed to the International Court of Justice (ICJ) to stop Israel's military aggression in Gaza. The clerical regime also urged Muslim rulers and the Organisation of Islamic Cooperation to play a role. However, while the Taliban criticized the international community's inaction against Israeli human rights violations in Gaza, they simultaneously challenged the validity of international critiques of their policies on girls and women.

TTP, for its part, framed Hamas's attack as a significant victory while trying to garner support for its campaign against the Pakistani military. TTP drew a "David versus Goliath" parallel between Hamas's attack against Israel and its own attacks against Pakistan's military, urging attacks against it. TTP also stressed that its operations were Pakistan-focused and that it posed no global threat. These messages were shared by TTP's propaganda arm, Umar Media, via Telegram, Signal, WhatsApp, and X.

ISKP was the last group in Afghanistan to react to the Hamas-Israel conflict by denouncing the Taliban, Hamas, and Muslim states for failing to establish a Caliphate before confronting Israel. ISKP, through its channels on Telegram, Element, Rocket Chat, and Signal, labeled the Taliban apostates for asking the ICJ to stop the conflict. Separately, ISKP blamed Hamas – calling it a nationalist group – for the suffering of the Palestinian people and urged Muslims to cease their support. It also proposed creating a Caliphate by dismantling the existing Westphalian nation-state system in the Muslim world.

Information Sharing

The third type of online material published by Afghanistan-based terrorist groups relates to information about their violent operations, organizational developments, and leadership changes, among others. For instance, the Taliban-style annual spring offensive has become a hallmark of TTP's violent operations in Pakistan. Each year in April or May, it announces a spring offensive under a new name via encrypted social media channels such as Telegram, Element, Rocket Chat, and Signal, and provides daily updates on its attacks to project operational strength.

Terrorist groups share online information through infographics, reports (daily, weekly, and monthly), and responsibility claims. Additionally, they publish monthly magazines, podcasts, booklets, audio statements, documentaries, and biographies of slain militants. Under this category, terrorist groups in Afghanistan also share instructional materials, including organizational codes of conduct, strategic and operational guidelines, technical information on maintaining privacy and operational security, and tips for avoiding surveillance and communicating securely.

Operational Tactics to Disseminate Content

Despite the interconnected nature of many armed conflicts in the digital age, developments in Afghanistan can best be described as "glocal" – a blend of local and global elements. While Afghanistan-based terrorist groups disseminate content on relevant external issues, they appropriate them to local contexts to fit their ideological and strategic objectives. Rarely do outside actors share Afghan-centric materials, barring al-Qaeda and Islamic State, which occasionally distribute online propaganda materials concerning Afghanistan because they have formal branches, AQIS and ISKP, in the region. Their approach to producing content differs from TTP's, as they exploit local events to bolster their international jihadist reputation.

There is no significant difference in dissemination tactics across the internal and external boundaries of the Afghan conflict, aside from subtle variations. This is because external commentators and on-the-ground actors are part of the same online echo chambers and encrypted channels. As a result, operational guidelines from different terrorist groups to their online propagandists are similar, since geographical distance is less relevant in interconnected virtual communities.

The most common modus operandi used by Afghanistan-based violent extremist groups for online propaganda dissemination involves releases by their respective official media arms, which are then amplified by supporter communities (Mubarizeen) on different platforms. This amounts to simultaneous reliance on top-down (official) and bottom-up (semi-official) tactics to ensure both authenticity and wider circulation.

Violent extremist groups in Afghanistan have also used GAI to produce and disseminate extremist content. ISKP, TTP, and AQIS employ AI to create infographics of their attacks and to translate extremist content into multiple languages to enhance appeal and reach diverse ethnic and linguistic groups.

The most commonly used encrypted platforms by these groups are Telegram, Rocket Chat, Threema, WeChat, and WhatsApp. Their supporters are also present on open platforms such as Facebook, X, YouTube, TikTok, and Instagram, albeit in small numbers. While supporters on open social media platforms indirectly promote their respective groups' ideologies, they cannot share their materials due to platform content moderation practices.

Nonetheless, operational tactics across violent extremist groups vary slightly depending on their nature, agendas, and audiences, providing insights into the inner workings of their propaganda arms. Distinctions in the operational tactics of TTP and ISKP illustrate this point.

TTP pledges its oath of allegiance to the Taliban, and its geographical mandate is limited to Pakistan. As discussed earlier, even when commenting on global conflicts, it reiterates its Pakistan-centric agenda and distances itself from global jihad. By contrast, ISKP frames almost all local developments within its ideological construct of global jihad.

In TTP's propaganda ecosystem, claims of responsibility for attacks come from the group's official spokesperson, while Islamic State claims ISKP's attacks through the Amaq News Agency or Khilafah News. In TTP, the authenticity of shared information is determined by a spokesperson's statement, whereas in ISKP, it is assessed by the signature of established platforms.

ISKP follows a sharply sectarian agenda and an indiscriminate attack strategy, commonly targeting Shia, Deobandi, and Barelvi sects. These attacks target religious scholars from these communities, their places of worship, and seminaries. Likewise, ISKP has also targeted religious minorities, including Sikhs and Christians, in Afghanistan and Pakistan. The propaganda released after these attacks justifies these killings by painting the targets as guilty of apostasy.

In contrast, TTP, despite following a sectarian agenda in the past, has moved away from sectarian militancy, which is consistent with the agenda followed by the Taliban and al-Qaeda. Furthermore, unlike ISKP, TTP does not engage in indiscriminate attacks, barring notable exceptions, and

mostly limits its operations to Pakistani security forces.

Though both TTP and ISKP produce multilingual propaganda materials, they each use very distinct diction. TTP focuses on Pakistan's regional languages, such as Punjabi, Saraiki, Pashto, Balochi, Sindhi, and, on rare occasions, Bengali. ISKP's language choices are regional and transnational, including Persian, Pashto, Uzbek, Tajik, Turkish, Russian, Hindi, Tamil, Malayalam, Arabic, and English.

In terms of propaganda output, TTP's Umar Media produces more content with greater consistency, compared to ISKP's Al-Azaim Foundation, which is going through a slump due to several setbacks it suffered in 2025, including a crackdown on two major communication nodes and the arrests of two key propagandists, Sultan Aziz Azzam and Abu Yasir al-Turki.

Framing Goals

The foremost purpose of producing online violent extremist propaganda is to gain publicity, which serves as oxygen for terrorist groups, as well as to collect funds. Afghanistan-based terrorist groups recognize the importance of propaganda in their tradecraft and have established sophisticated and professional propaganda arms to increase their public appeal.

A large volume of the content that Afghanistan-based violent extremist groups produce revolves around the glorification of violence. It is portrayed as a sacred duty and part of a holy war being waged to defend Islam against apostate Muslim regimes, a label ISKP uses for the Taliban government. TTP, for its part, justifies violence to create a Taliban-like theocracy in Pakistan while framing its current government as a puppet of the United States. Such narratives resonate with peripheral communities that are still suffering the consequences of the war or the ongoing counterterrorism operations, especially in the Afghanistan-Pakistan border region. They have either lost close relatives in the war or experienced displacement. Violent extremist groups like TTP frame their individual grievances within collective religious narratives and offer them an opportunity to seek revenge through a "holy war."

The second purpose is to enhance legitimacy by offering ideological justification for the violent campaigns these groups wage. In Afghanistan's conflict zone, violence is regarded as the ultimate yardstick of a terrorist group's strength. More attacks mean more credibility. Each responsibility claim made by these violent extremist groups explains why they target specific sites. For example, TTP depicts itself as the victim of the Pakistani military's disproportionate use of force in the Afghanistan-Pakistan border region under the guise of counterterrorism. Violence is justified under a careful blend of ethnic and ideological propaganda aimed at preserving Pashtun tribal traditions and Islamic values.

Alongside glorifying violence, terrorist groups in Afghanistan also produce regular content pay-

ing tribute to terrorists killed in counterterrorism operations or suicide bombings. While sharing some basic background information and pictures, the fallen are eulogized as martyrs, holy warriors, and war heroes. The concept of martyrdom holds significant value in Islam, and it serves as a strong recruitment tool for violent extremist groups. Other values promoted in this type of propaganda include chivalry, self-sacrifice, courage, and bravery. Slain militants are presented as symbols of resistance, icons, and role models. For instance, TTP publishes the *Rasm-e-Muhabbat* (tradition of love) series to pay tribute to its so-called martyrs. Similarly, ISKP commemorates its slain militants under the *Memories of Shuhadah* (Martyrs) series in its flagship propaganda magazine, Voice of Khorasan. It publishes biographies containing basic personal information and details of their militant careers.

Furthermore, in their propaganda posts, Afghanistan-based violent extremist groups also share QR codes and wallet addresses to solicit funds in cryptocurrency. ISKP's *Voice of Khorasan* magazine regularly promotes Monero (XMR) and USDT (TRC-20) to raise funds. At the same time, other violent extremist groups like TTP use traditional methods of collecting funds, such as public donations, charity, extortion, and kidnapping for ransom, among others.

Finally, promoting their ideological worldviews is a key purpose of publishing propaganda. A large portion of extremist publications in Afghanistan revolves around discussing the merits of theological systems, such as the Emirate or Caliphate, that these groups aim to establish. Interestingly, terrorist groups in Afghanistan fail to present an alternative policy discourse on how they would manage the economy, education, foreign policy, and other issues if they came to power. However, they expend considerable effort in undermining the Westphalian nation-state system. At the same time, as discussed earlier, ideological outbidding is another central goal, as competing extremist groups frequently engage in caustic denunciations of each other's foundational doctrines.

Conclusion

In Afghanistan, online violent extremist propaganda and terrorist ground operations reinforce each other through the idea-action dialectic: extremist ideas spark terrorist actions, and vice versa. Two examples illustrate this. TTP uses its so-called annual spring offensive against Pakistan for cross-border attacks and online propaganda, announcing launches via encrypted channels and coordinating attacks through instructions to affiliates. In turn, daily attack claims by TTP's Umar Media help the group produce online propaganda to project operational strength. Both attacks and a large volume of online extremist content enable the group to attract recruits and funding. Combined, these interconnected factors increase radicalization among vulnerable youth and proliferate extremist ideologies.

Likewise, ISKP's suicide bombings are accompanied by propaganda, including booklets, videos, and written statements aimed at potential targets. This propaganda vilifies victims, justifies at-

tacks ideologically, and promotes ISKP's extremist worldview, encouraging further violence.

Given the large volume of online violent extremist propaganda and cross-border terrorist attacks, combined with Afghanistan's status as a hub for around 20 violent extremist groups, it is clear that Afghanistan-based terrorist groups are achieving their intended goals. All the major terrorist organizations operating in Afghanistan carry out suicide attacks at will, which means they are well armed, well-financed, and continuously attracting recruits. Moreover, their official propaganda arms produce professional-grade content leveraging encrypted social media platforms and AI tools. Ultimately, the competitive environment within Afghanistan's threat landscape is the strongest indicator of this success – whether the goal is to take control of peripheral border areas where governance structures are weak, to undermine state control, to outcompete rival groups, or to engage in battles for ideological supremacy.

The Sahel

Conflict Overview

Ulf Laessing | Head of Regional Program Sahel, KAS

The Sahel, a semi-arid stretch of land linking northern and sub-Saharan Africa, is home to many impoverished communities that have struggled for more than a decade with a worsening security crisis despite massive foreign intervention. This has included one of the largest UN peace operations, the UN Multidimensional Integrated Stabilization Mission in Mali (MINUSMA); the French counterterrorism mission Operation *Barkhane*; and the deployment of Russian mercenaries and contractors, such as the Wagner Group and its successor, the Africa Corps. What started in 2012 as a local conflict with the arrival of jihadists in northern Mali has turned into a fast-growing crisis threatening much of West Africa. Today, extremist groups linked to al-Qaeda and Islamic State have expanded from Mali to Burkina Faso, Niger, and countries in the Gulf of Guinea such as Benin, linking up increasingly with jihadists operating in Nigeria and the Lake Chad area. They exploit rising poverty, weak and corrupt governments, and competition over shrinking resources like water and land, driven by some of the world's highest population growth rates and climate change. In large rural parts of Mali, Niger, and Burkina Faso, jihadist groups have become the de facto state.

Various foreign interventions have failed to stop the jihadist expansion. In 2013, the French army in Operation *Serval* stopped the advance of jihadists from northern Mali, but only pushed them into the hard-to-penetrate mountains of Mali's northern desert. Since then, however, the Malian state has failed to reclaim those areas or win over its citizens by providing essential public services; as a result, the fighters quickly returned, setting up parallel authorities and undermining MINUSMA and Operation *Barkhane*. The ongoing state vacuum has helped the jihadists turn Mali's north into a retreat base from where they have slowly and steadily expanded, first to the country's center and then to the south, now threatening Bamako.

The most potent jihadist group is the al-Qaeda affiliate JNIM, which dominates parts of Mali, Burkina Faso, and Niger and is currently spreading to the Gulf of Guinea. Its approach is more conciliatory than that of its rival, Islamic State, which is known for its extreme brutality. JNIM has learned the lessons of the 2012 occupation of northern Mali, where the population opposed the rapid application of Islamic sharia and its corporal punishments. With its carrot-and-stick approach of applying force and offering villagers protection from army abuses, JNIM has managed to expand steadily, establishing, most recently, a strong presence in the south. Its fighters are currently threatening the Malian capital of four million, Bamako, by trying to choke off fuel supplies, signaling a newfound confidence to shift the battle from the countryside to the capital. Bringing down the military government would require help from inside Bamako; people's growing frustration over fuel shortages could prompt leaders to negotiate with the jihadists.

In contrast, Islamic State controls less territory than JNIM but is especially active in Niger, where its fighters cooperate with the group's branches in northern Nigeria and around Lake Chad. On January 29, 2026, this cross-border cooperation helped Islamic State stage complex attacks with drones and fighters on motorbikes on two airports in Niger, including in the capital, Niamey. The airport strikes targeted hangars hosting Niger's drones acquired from Turkey, its main weapons against jihadists since the French military's exit. Islamic State has also established a large presence in the Menaka area in northeastern Mali; for the first time, the group controls a foothold large enough to hold kidnapped foreigners hostage until ransom negotiations have concluded.

Thus far, only JNIM has controlled enough territory in northern Mali to hold kidnapped foreigners, turning this into a lucrative business that raises millions of dollars. While JNIM and Islamic State have been fighting each other over control of territory, this has not stopped either from expanding further.

Meanwhile, the overthrow of elected presidents by military juntas in Mali, Niger, and Burkina Faso has exacerbated the crisis. All three governments have contracted Russian mercenaries to help fight jihadists, most notably in Mali, where the Wagner Group and its successor, the Africa Corps, have been blamed for brutality against civilians labeled as "terrorists." Yet survivors of Russian brutality have joined jihadists, who offer protection against the mercenaries and Malian soldiers, who are also regularly accused of abuses against civilians. Violence has therefore spiked since the arrival of Russian forces in Mali in late 2021, allowing especially JNIM to expand and recruit more fighters.

Recently, on April 25, 2026, JNIM teamed up with Tuareg rebels to stage attacks on Bamako and across the country, assassinating the defense minister and seizing three towns in the north, including the strategically important Tuareg stronghold of Kidal. It was the boldest such attack since 2012, when jihadists and Tuareg fighters seized the north until the French army retook it a year later. The military government has survived the attack for now, but JNIM is pressing ahead with a blockade of all goods and traffic to and from Bamako.

In the short term, the jihadist push on Bamako might not succeed, but in the long run, the jihadists hold the advantage. As with the French military withdrawal, Russia may one day depart the Sahel, having predictably failed to improve security while propping up weak Sahelian states, though its regional presence has offered access to key resources which may be difficult to leave behind. Populations in the Sahel are tired of corrupt, failing governments, whether elected or military-run. There remains no military solution to the Sahel conflict, as jihadists are far too entrenched and their parallel authorities far too woven into the social fabric.

For decades, Islamist Salafists – financed by external sources, most notably Gulf donors – have benefited from general dissatisfaction with officials and state corruption, growing their base over

the years. Pressure on Sahelian governments to negotiate with jihadists will mount; that could mean the withdrawal of armed forces from some areas in a de facto split of Mali or a stricter application of Islamic sharia. But the extremists can also bide their time and wait for the Sahelian countries to collapse further, forcing officials to talk to them. An Islamist takeover of parts of the Sahel – or governments such as Mauritania becoming more Islamist – is not an unrealistic scenario. People might find it preferable to an endless cycle of violence, chaos, and state corruption.

Case Study: Terrorist Exploitation of the Sahel for Digital Content

Beverly Ochieng | Senior Analyst, Control Risks

Introduction

Affiliates of al-Qaeda's Sahel branch, Jama'a Nusrat ul-Islam wa al-Muslimin (JNIM), and Islamic State's self-styled Sahel Province (ISGS), have been the dominant threat actors in the central Sahel (Mali, Burkina Faso, and Niger) for more than a decade. Their violent campaign of attrition against Sahelian security forces and occupation has led to an unprecedented expansion of activities from peripheral regions toward key supply routes connecting urban areas.

JNIM emerged in 2017 from the alliance of four Islamist militant groups primarily active in central and northern Mali that had extended violent campaigns toward neighboring Burkina Faso and Niger. These are the Mali-based Ansar Dine, led by Iyad Ag Ghaly; the Macina Liberation Front (FLN), led by Amadou Koufa; Al-Mourabitoun, led by the late Mokhtar Belmokhtar; and the Sahara region of al-Qaeda in the Islamic Maghreb (AQIM). Over the years, JNIM has carried out attacks further afield, targeting security forces in northern Togo, northern Benin, northern Côte d'Ivoire, and northwest Nigeria.

Meanwhile, Islamic State first declared its presence in Mali in 2015, with the majority of its fighters drawn from groups that fell out with AQIM, other affiliates of JNIM, and armed groups in northern Mali led by Western Saharan jihadist Adnan Abu Walid al-Sahrawi. Its main strongholds are Mali's northern Menaka region, Niger's western regions of Tahoua and Tillabéri, and Burkina Faso's northern Sahel Province. ISGS was first acknowledged as the "Sahel Province" by the centralized channels affiliated with Islamic State in 2022; prior to this, ISGS relied on Mauritanian news outlets to disseminate self-produced propaganda videos.

How these rival groups use media is critical to understanding their posture, strategy, and intentions. This paper offers a thematic and contextual analysis of how ISGS and JNIM have used social media. It also examines how content generated by the groups propagates their agenda and is used to recruit and expand operational control. The material also enables the groups to challenge the authority of Sahelian military-led governments that staked their claim to power through a series of military coups between 2020 and 2023 in an effort to end the Islamist militant insurgency.

Centralized Channels, Dispersed Networks

Al-Qaeda and Islamic State each have highly centralized media networks that package and disseminate a variety of messages. These include concise claims of attacks accompanied by brief details and supporting images; highly visual material purportedly depicting militants participating in outreach activities; or lengthy documentary-style audio and video messages that

occasionally feature their respective leaders to reinforce posture, ideology, and the overarching agenda.

This centralization of media output serves to embed the Sahelian branches of al-Qaeda and Islamic State within a broader global movement and project power. By positioning themselves within an international militant network, they gain ideological legitimacy, thereby strengthening their standing both locally and globally. Furthermore, this approach enables the groups to harness localized insurgencies and situate grievances within a broader global context.

Al-Qaeda's propaganda media outfit, Az-Zallaqa Foundation, began documenting JNIM activities as soon as the alliance was established in 2017. Meanwhile, updates on ISGS activities are prepared by Islamic State's Al-Furqan Foundation, which publishes the weekly magazine *al-Naba* every Thursday.

Propagate, Proselytize, Provoke

The main purposes for which Islamic State and al-Qaeda produce content and messages can be divided into three categories: propagating broadcast material to wider audiences, proselytizing to recruit and expand their ranks, and provoking reactions or issuing a call to action in areas where they are active or can extend their activities and presence. Alongside their violent campaign of occupation and destruction against civilians and security forces in the Sahel, content production serves to present their fighters and local leadership as direct stakeholders and interlocutors in political, social, and religious discourse within the Sahel. There are certainly overlaps between propagation, proselytizing, and provocative messaging. For this analysis, these are the characteristics assigned to each theme:

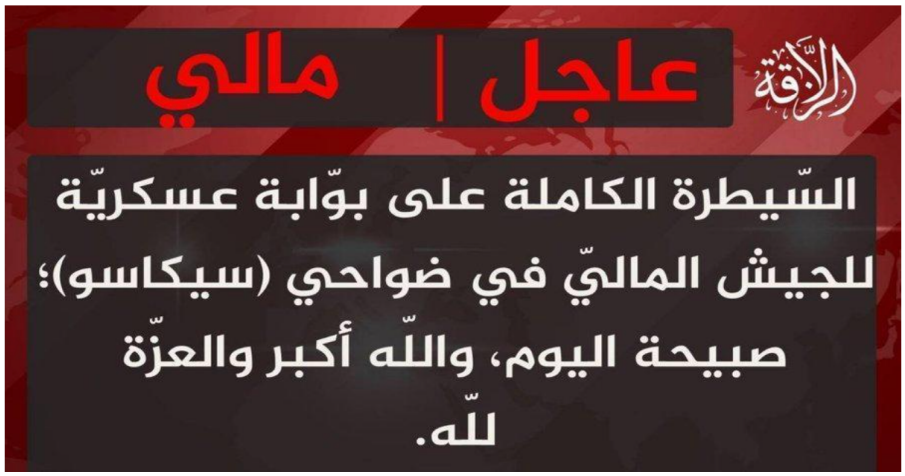
- **Propagation:** Content primarily aimed at broadcasting kinetic activities by militants, including attacks targeting government and pro-government groups.
- **Proselytizing:** Content and messages focused on theology and ideology, outreach activities, and non-violent activities.
- **Provoking:** Messages explicitly calling supporters and sympathizers to action, either to carry out attacks or to refuse to cooperate with authorities.

A review of statements and videos produced by ISGS and JNIM (including those shared outside the centralized platform for al-Qaeda in particular) throughout 2025 provided the following findings:

	Propagation	Proselytizing	Provoking
JNIM	51%	22%	27%
ISGS	65%	17%	18%

Broadly speaking, the primary material shared by JNIM and ISGS consists of statements claiming attacks and activities by their respective fighters, intended to demonstrate territorial reach and capabilities. These range from concise alerts that include information on where an attack occurred, who or what it targeted, and any casualties or levels of destruction. This material is first made available on the official websites and social media handles of Az-Zallaqa and Al-Furqan – specifically ChirpWire and Telegram – before cascading among their respective supporters and sympathizers through more mainstream social media platforms such as X and Facebook, and then being reported by mainstream media.

It is worth noting that censorship and restrictions on security reporting in Mali, Burkina Faso, and Niger have limited mainstream media coverage of militancy from the perspectives of ISGS and JNIM, and that the majority of locally operated outlets rely on official sources. However, statements attributed to Islamic State and al-Qaeda are still shared on Facebook and WhatsApp.



(JNIM statement claim, March 2025)

The sense of cohesion and order within ISGS and JNIM is best conveyed through material intended for proselytizing. Over the years, particularly during auspicious events such as Ramadan and Eid, Islamic State and al-Qaeda have issued elaborate photo sets of their fighters across various branches sharing meals, delivering sermons, or addressing public gatherings. This type of online

content softens the image of their fighters, reinforcing community and inclusion at a time when the majority of Muslims are reflecting on spirituality and focusing on family and communal ties. This year, for instance, Islamic State's Eid photo sets were dominated by its African branches, underscoring the group's ongoing pivot to the continent, seven years since the loss of its so-called territorial Caliphate in the Middle East. ISGS was featured in photos purportedly showing fighters sharing meals, watching leadership messages together, demonstrating unity and cohesion, and offering a community embedded in religious ideology. The slick productions lend themselves well to social media, portraying a utopian environment that sharply contrasts with the conventionally violent tactics and presence associated with Islamic State.

(ISGS, Eid al-Adha, 2024)

Meanwhile, throughout Ramadan, JNIM produced daily videos featuring sermons in various local languages delivered by junior militants, underscoring its efforts to recruit from diverse communities across Mali and Burkina Faso. Sixty percent of the messages were delivered in Pulaar (or Fulani), followed by Arabic and Tamasheq. These sermons, as with other acts of da'wah[2], focus on Quranic messages delivered from physical copies, smartphones, or tablets, highlighting the intersection between technology and ideology.

JNIM's Ramadan showcase, in particular, reinforces its broader outreach activities, which focus on Mali's economic corridors in the south and west, where the group has been establishing a foothold since 2022. As part of this strategy, al-Qaeda has occasionally shared photo sets purportedly showing JNIM fighters' activities, particularly in the southern and western regions of

2. Da'wah: preaching or proselytizing; however, in reference to Islamist militant groups, this involves religious and social outreach with the purpose of recruiting and indoctrinating.

Mali, addressing large gatherings of civilians in open spaces or inside mosques, taking part in da'wah. Such images soften the posture and attitudes of local communities toward JNIM, even as the group's activities undermine the presence, legitimacy, and authority of the government.

(JNIM Eid-al-Adha, 2024)

The broader objective of the propaganda output is to trigger actions and responses that demonstrate the impact and effectiveness of the messages (as explored below). Calls to action have consistently featured in JNIM propaganda, evolving from demands for dialogue and the departure of French counterinsurgency forces to explicit calls for reduced cooperation with the current military-led governments.

The evolution of this messaging also reflects a broader trend specific to JNIM, shifting from posturing within a global theme (anti-Western rhetoric, reliance on al-Qaeda's centralized channels) to more localized messages issued outside Az-Zallaqa and directly addressing constituents in Mali and Burkina Faso.

By contrast, Islamic State calls to action are centralized and then enacted by its affiliates, including ISGS, which reinforces fraternal links and the interpretation of globalized campaigns in a more localized setting. Compared with its nearest affiliate, Islamic State in West Africa Province (ISWAP) – operating in Nigeria, Chad, Cameroon, and southern Niger – ISGS's participation in broader Islamic State campaigns tends to be more subdued. In fact, throughout 2025, ISGS carried out an average of five attacks a month as Islamic State oversaw a campaign dubbed "Inferno of the Camps" aimed at degrading military establishments in all its operational areas globally.

Evading Content Regulation

Islamic State and al-Qaeda media operations have thrived on social media platforms with lenient content moderation, such as Telegram, ChirpWire, and Rocket Chat. The militant groups have also used coded language and dialect to avoid detection by language tools and circumvent or subvert community guidelines on more mainstream social media platforms such as X and Facebook. Encrypted messaging apps such as WhatsApp, which rely on direct interactions in closed groups, lend themselves well to the propagation of propaganda and other content originating from or attributed to ISGS and JNIM. Analysts from Code for Africa (2023) noted that, through such a multiplatform communication paradigm (MCP), extremist groups can "operate in smaller, less detectable networks, making tracking and countering their online activities more difficult."

In an investigative report published in 2023, Nigerian journalist Aliyu Dahuri observed that militant propaganda is often in Arabic dialect rather than standardized Arabic, which, according to him, inhibits automated language tools from effectively censoring or flagging it on mainstream social media platforms. This partly underscores why, despite efforts by Europol to systematically target and remove Telegram accounts sharing terrorist messages or with direct links to Islamic State and al-Qaeda, and temporarily forcing the groups to diversify their media strategy, channels continue to proliferate, and the platform has become the standard venue for militant propaganda.

Dahuri also observed that emojis are used to further encrypt messages and meanings. However, it must be noted that some of the shortcomings in accurately tracking dialects may stem from content moderators' limited expertise with less obvious terrorist messaging and language.

Meanwhile, JNIM propaganda has flourished on WhatsApp, where its fighters, sympathizers, and supporters can coordinate propaganda, financial networks, and logistical operations. For instance, following a yearlong investigation, authorities in Guinea in March 2026 reported that they dismantled a suspected sleeper cell of the group and arrested several nationals from Mali, Niger, Burkina Faso, and Guinea involved in terrorist financing, including through WhatsApp. The suspects were arrested in Guinea's border prefectures with Mali, underscoring the vulnerability of such communities to infiltration and recruitment by JNIM. While no information is publicly available on the content that was shared through these WhatsApp groups, it fits into a wider modus operandi of using end-to-end encrypted channels to infiltrate localities and mobilize logistical resources to complement on-the-ground operations, particularly among communities susceptible to exploitation through such networks due to marginalization and limited literacy on social media use.

The proliferation of JNIM statements on WhatsApp has intensified in the past year as the group has embarked on a campaign to sabotage the Malian military-led government's economic in-

terests. In March 2025, video and audio messages issued by one of the group's spokespersons, identified as Abu Hudheifa al-Bambari (also Huzeifa), began surfacing on WhatsApp, TikTok, Facebook, and X directly addressing Malians and urging them to distance themselves from the junta or face consequences. These messages were notably not shared by Az-Zallaqa, with analysts noting that the explicit threats toward civilians were uncharacteristic of al-Qaeda's overall posture and tactics.

Hudheifa's messages were also delivered in Bambara and sought to exploit prevailing grievances, including tensions surrounding the inconclusive transition to civilian rule in Mali, counterinsurgency failures by the junta as security threats persisted in economic corridors, and alleged abuses by security forces working with Russian paramilitaries. He also ordered public transport operators to segregate women and men, and only allow women covered in the veil to travel.

The directives and threats are not necessarily new. JNIM fighters in parts of central Mali occasionally coerce residents to command authority and control. However, the recent wave of messages demonstrates JNIM's intent to make its authority more mainstream, directly challenging authorities and exploiting long-running grievances. Furthermore, as these messages are not explicitly inciting or violent, and are issued in Bambara, they are less scrutinized. It is more likely that JNIM is being pragmatic about the potential of its message to reach a wider audience, rather than deliberately seeking to circumvent content moderation.

Influencers, Storylines, Language

What makes ISGS and JNIM messaging compelling? The answer is unsurprising: storytelling, characters, and use of language.

Islamic State has harnessed the interplay between identity and emotion by weaving ideology into storylines and characters, thereby humanizing its fighters, cause, and intentions. One clear example of this is Islamic State's long-running series in *al-Naba*, "Story of a Martyr," where militants killed in battle are eulogized. The column lionizes fighters for their "willingness to put behind an ordinary life of worldly pleasures in order to fight alongside Islamic State." The narratives reinforce triumph through adversity, steadfastness despite prevailing challenges, including rival groups, and the physical distances fighters travel to join Islamic State.

While most messages are issued in Arabic, outreach is more effective in local languages. This has been more prevalent with JNIM in the Sahel as it softens its posture in an attempt to gain greater credibility as a political actor. In recent years, figures such as Mahamoud Barry, JNIM's main spokesperson, have emerged to consolidate the various *katibas* (districts) in Burkina Faso and Mali. As highlighted earlier, Hudheifa has been a figurehead of JNIM's economic sabotage campaign in southern and western Mali. Indeed, in one instance in August 2025, following the alleged

arrest of his father by Malian authorities, Hudheifa directly addressed the development, using the opportunity to once again appeal to Malians not to work with the junta and to convey a sense of victimhood under military rule.

It is worth noting that outside the Sahel, Islamic State propaganda has featured fighters addressing followers, supporters, and potential recruits in Swahili, Luganda, Kanuri, and English to serve similar purposes: building proximity with global audiences.

Dualism of Social Media and Smartphone Use

Islamic State has been more explicit in encouraging supporters and sympathizers to use social media. An editorial in issue 130 of *al-Naba* encouraged the group's supporters and sympathizers to use social media to incite others to participate in its cause and to prioritize recruitment. At the same time, Islamic State proactively publicizes the pitfalls of technology and warns against compromising information on its fighters' activities and movements. This can be traced back to 2016 when Islamic State warned its supporters and fighters to abandon mobile devices in Islamic State-held territories to prevent "hostile forces" from tracking and targeting its militants.

In 2018, *al-Naba* issued a lengthy advisory, warning that smartphones can be used to spy on the group. Islamic State warned that smartphones are susceptible to being hacked, which would reveal personal information about its fighters and sympathizers, thereby jeopardizing operations. The advisory entitled "The perfect spy: mobile phones," includes the Quranic verse: "God Almighty said: Oh you who have believed, take precaution" and advises that companies like Google "maintain network IDs to locate nearby Wi-Fi users" and phone companies "record the movements of users."

(Al-Naba, October 25, 2018)

Subsequently, supporters and sympathizers of Islamic State have occasionally shared digital safety tips to evade interception, particularly by authorities, and to avoid compromising information about militant activities. While these do not explicitly address the Sahel branch, they are crucial for understanding the evolution of Islamic State's digital agility and its sympathizers' operational efficiency on social media and with smartphones. For instance, a high-profile Islamic State supporter identified on Facebook as Abu Karish in December 2025 suggested the use of WhatsApp and Telegram through anonymous accounts and to "encrypt the message as much as possible." The user went so far as to state that noncompliance with this directive constituted a "sin." Such messages reinforce longstanding warnings from centralized media channels belonging to Islamic State and constrain authorities from proactively disrupting potentially devastating attacks and activities.

Impact and Effectiveness

Anecdotally, the sustained militancy in the Sahel and the spread of activities from rural areas toward strategic economic corridors implicitly demonstrate that the kinetic and non-kinetic tactics employed by militant groups have been successful. However, this is not limited to social media campaigns. Much of the Sahel has limited internet access, even with the proliferation of smartphones. Furthermore, while limited digital literacy is likely to make communities more susceptible to propaganda from extremist groups present in the region, this factor is unlikely to be the decisive element in the effectiveness of propaganda campaigns linked to ISGS and JNIM. At the same time, it will facilitate the propagation of ideology and posture.

Compared with parts of Europe, where actions by lone attackers have been particularly linked with Islamic State, leading to findings by Qi and He (2023) that messaging by Islamic State "demonstrates a high level of sophistication and effectiveness in causing radicalization without requiring direct physical contact," similar patterns of violence have not been observed in the Sahel. In fact, the dynamics in the Sahel center on building large communities within militant groups to extend territorial control and tactical capacity, effectively challenging government authority and establishing semi-autonomous operational areas.

Technical Recommendations

Addressing weaknesses in the broader information ecosystems in Mali, Burkina Faso, and Niger in particular will remain crucial to protecting communities from infiltration by ISGS and JNIM for recruitment purposes and logistical operations. Censorship by Sahelian military-led governments is a limited measure toward addressing the spread of militant propaganda. Governments will need to invest in establishing trusted networks of information and supporting independent journalism to counter extremist narratives with credible news.

Social media platforms will need to dedicate additional resources toward closely monitoring and understanding the media strategy of Islamist militant groups and their supporters online. This includes human input to detect dialect evolution, translate and convey messages in local languages that would otherwise go undetected by language tools or artificial intelligence, and contextualize narratives within current events. This would also enable platforms to establish early warning systems around trends linked to key developments (military coups, socioeconomic unrest) that Sahel-based militant groups would otherwise exploit to produce targeted, inciting messaging.

Ukraine

Conflict Overview

Elena Davlikanova | Fellow, Center for European Policy Analysis (CEPA)

Olya Korbut | Fellow, CEPA, and Analyst, Black Sea Institute of Strategic Studies

Russia's full-scale invasion of Ukraine in 2022, initially conceived as a "Kyiv in three days" operation, has entered its fourth year as a high-intensity war of attrition. In 2025, Moscow seized roughly one percent of Ukrainian territory at a cost exceeding $100 billion and with monthly casualties surpassing 30,000. Yet despite the clear lack of strategic or military logic in continuing the campaign, as well as genuine, good-faith diplomatic and mediation efforts to end the conflict, Moscow remains unwilling to move toward peace.

It is not only the largest war in Europe since World War II; it is also functioning as a live testbed for a new generation of warfare, evolving from mechanized to digitized and now to AI-enabled "intelligent" combat. New, rapidly evolving tactics, new doctrines, a widening kill zone, strike-to-effect loops measured in minutes, and the massive use of unmanned systems for reconnaissance, strike, logistics, electronic warfare, evacuation, mining, and even coercion have all become routine in top-performing units.

Deep strikes at ranges exceeding 1,000 kilometers have also become routine and increasingly precise, hitting military production facilities, air bases, ports, and several dozen oil and fuel depots, inflicting damage measured in the hundreds of millions of dollars. Ukraine, with its nearly fleetless navy, has destroyed or disabled roughly one-third of Russia's Black Sea Fleet, forcing surviving vessels from Sevastopol to eastern bases and sharply curtailing Russia's ability to use the Black Sea as a launching pad for attacks against Ukraine and NATO's southeastern flank. The historic "Operation Spiderweb" reportedly damaged or disabled more than 10 percent of Russia's long-range aviation assets, underscoring the growing vulnerability of strategic platforms once considered untouchable.

However, two persistent misperceptions risk repeating the miscalculation of 2022. First, that Russia's heavy losses in armor and personnel – more than one million dead and wounded – have left it strategically exhausted and incapable of contesting NATO in the near term; and second, that drone warfare is merely the byproduct of two "poor countries" fighting, while NATO retains unquestioned dominance and would defeat Russia swiftly in a conventional clash. In practice, Ukraine has become a reluctant sparring partner in Russia's re-emergence as a modernized force and a pioneering master of next-generation warfare. Unlike pacifist Europe, Russia – driven by imperial ambitions – shows a great willingness to project aggression beyond Ukraine, disregarding the rules of war.

A related misreading frames drone warfare as the domain of poorer states, assuming that traditional advantages in legacy armored platforms will preserve dominance. The protracted conflict in Ukraine has already set an irreversible trend; once large, manned platforms become too vulnerable and costly to employ alone, militaries will first move toward manned–unmanned teams and then toward forces in which AI-enabled, largely autonomous systems carry most of the fight, with humans retaining strategic direction and legal responsibility rather than physically leading every engagement.

Beyond the battlefield, Russia has set a grim precedent with the systemic use of combined mass strikes against civilian infrastructure across Ukraine. Since February 2022, Russian forces have launched more than 13,000 missiles and over 140,000 attack drones, striking hospitals, kindergartens, markets, schools, and other civilian sites. Recurrent winter campaigns have deliberately targeted power plants, substations, district heating networks, and major urban centers, aiming to deprive millions of electricity and heat. The scale and pattern of these attacks amount to a sustained campaign designed to break civilian resilience and coerce political outcomes.

Despite Ukraine fielding Europe's most advanced integrated air and missile defense, Russia remains relatively successful in terrorizing the country, as ballistic and combined saturation strikes remain a challenge. Countries with thinner, less layered defenses and concentrated critical infrastructure would face far greater disruption under a similar campaign, with rapid depletion of interceptors, prolonged blackouts, and acute political and economic shock.

Since 2022, Russia has leaned on a coercive proxy ecosystem of private military companies, proxy militias, extremist networks, cyber proxies, hacktivist collectives, and criminal syndicates in its war against Ukraine. These include Wagner and successor private military companies (e.g., those linked to Gazprom) used as shock troops, the Russian Imperial Movement and other far right militants supplying fighters and training, and Kremlin-linked cyber units that weaponize ransomware and "hacktivist" groups against Ukrainian and European critical infrastructure – allowing Moscow to project violence while preserving formal deniability. This proxy architecture is further extended through an accelerating effort to recruit mercenary personnel from across the Global South.

Russia is not only absorbing battlefield lessons in Ukraine; it is also transmitting them across its war network. China, Iran, and North Korea have provided personnel engaged through advisory roles, technical observation, and even direct battlefield involvement. The 2026 report by the Independent Anti-Corruption Commission (NAKO), *Russia's War Network: Military-Political Enablers of Aggression Against Ukraine and the West*, maps a sharp deepening of cooperation across technology exchange, co-production, supply chains, and dual-use component smuggling, as well as cyber, intelligence, space, and information warfare coordination.

Belarus, often overlooked in the list of Russia's primary war enablers, has effectively become an integrated component of Russia's war machine, serving as a forward operating base and launchpad for military operations against Ukraine and a potential platform for future aggression against Europe. The result is a rapidly iterating ecosystem and the emergence of a cadre of officers trained in drone swarming, electronic warfare, and precision-strike coordination, accelerating the diffusion of next-generation combat expertise across the anti-Western bloc.

Thus, Russia's full-scale invasion is not just a war over "some" Ukrainian territory. It is the latest phase of a long-running imperial project aimed at restoring Russia as a great power dominating Europe. Claims that the conflict would end if Kyiv ceded the Donbas – a region Moscow has failed to fully conquer for more than a decade – misread both Russia's ambitions and its methods. While NATO enlargement was not the trigger, what motivates the Kremlin is the prospect of a fractured alliance and a weakened, fragmented, and easily dominated Europe. It is precisely this expectation that drives Russia's sustained sub-threshold warfare against the West – mapped in The Everywhere War Tracker – designed to exploit divisions and steadily erode European security.

Case Study: TVE Online Content and the Russo-Ukrainian Conflict

Kacper Rekawek | Senior Research Fellow and Programme Lead, International Centre for Counter-Terrorism (ICCT)

Uljana Vlagyimirova | Research Intern, ICCT

Julian Lanchès | Research Fellow, ICCT

Introduction: Who, When, and How?

Local and external TVE entities have been exploiting the dynamics of the Russo-Ukrainian war to produce digital content since 2014 and have re-energized their efforts since the full-scale war began in 2022. The external TVEs have adopted an "all talk but not a lot of walk" strategy – interest in the conflict, as evidenced by the allocation of resources to comment, mobilize, or fundraise for "their" side, but relatively little offline activism or direct participation by their personnel in the actual fighting. At the same time, the local Russian and Ukrainian TVEs went all in and, especially after 2022, turned the conflict into a central (Ukrainian) or dominant (Russian) theme of both their offline and online strategies.

The Russo-Ukrainian war attracted the attention of almost all TVEs across the globe, but this analysis will focus on established militant far right[3] Russian and Ukrainian TVEs with engagement and interest in the conflict predating 2022, and on larger bodies of online content focused solely on this issue. Their radicalism and often violent far right political activism attracted the attention of both local and foreign organizations that monitor extremism developments in either Russia, Ukraine, or both, such as the SOVA Center and Bellingcat.

In addition to the local TVEs, the later sections of this analysis will also draw attention to two external or semi-external entities (one of which is at least partly Russian) that are most active in terms of calls for political violence and terrorism. The studied sample includes 33 online emanations (19 Russian and 14 Ukrainian) of organizations as diverse as, on the one hand, the Wagner Group, the Russian Imperial Movement, and Rusich, and on the other, the likes of Russian extremists who are currently fighting for Ukraine (e.g., the Russian Centre or White Rex).

Prior to the presentation of the research results, it is important to remember that out of all of the TVE actors operating within the Russo-Ukrainian battlespace, only the Russian TVEs (such as Wagner, Russian Imperial Movement, or the Base, whose leader now resides in Russia) have so

3. According to Cas Mudde's classification, these TVEs would belong to the "extreme right" category of the broader "far right." They are anti-democratic, authoritarian, anti-liberal, anti-equality, nativist, and extremist in nature (i.e., perceiving their political success as intrinsically linked to their opponents' lack of success). Moreover, their members/activists use violence in furtherance of their organization's aims. See Cas Mudde, *The Far Right Today* (London: Polity, 2019).

far been designated as terrorists or proscribed by, e.g., the US, UK, or the EU. No such Ukrainian organization has met a similar fate, and this is at least partly because the Ukrainian TVEs, unlike their Russian counterparts, have not demonstrated any intention of staging violent attacks against foreign targets in Ukraine or abroad.

Before discussing the results of the review and online ethnographic monitoring of the TVEs, it must be noted that both Russian and Ukrainian TVE actors, and, consequently, pro-Russian and pro-Ukraine foreigners external to the conflict, rely on Telegram as their platform of choice for disseminating online content. The platform, originally developed in Russia but seemingly outside the government's purview – although the government has announced plans to ban it on the grounds that it foments terrorism, is the preferred venue for content dissemination or communication for most Russians and Ukrainians.

Moreover, as much as Ukraine is socially and culturally attempting to phase out the Russian language from its media and everyday communication, a sizable chunk of the country's population still uses it as its first or preferred language. This allows both sets of TVE actors to easily reference, tag, or taunt one another in the online content produced by either side, and then share it on Telegram. Russian TVE individuals and groups that decided to fight for Ukraine against "communist" and "Muslim" Russia play a key role in these exchanges and taunts.

The authors scraped the content of 33 Telegram channels from February 2022 to February 2026, covering the duration of the full-scale war. They then developed a thematic analysis of the body of posts to showcase the most recurring themes in the online content produced by the TVEs covered in this analysis. This was done to reflect on two primary questions: 1) What types of content are being produced, and what is their purpose? 2) Are the TVEs successfully deploying this content to meet their goals?

Types of TVE Content and Reasons Behind Their Production

This part of the analysis will focus on the types of content or themes produced by the TVEs and the rationale for their deployment. It focuses on commonalities while also showcasing differences across the 33 monitored channels. From a topical and practical perspective, even though the channels represent TVEs engaged in conflict on opposing sides of the war, there are many commonalities.

TVEs covered by this analysis have had personnel involved in the war since its 2014 "hybrid" phase, while some produced units that today serve in the ranks of the Russian or Ukrainian armies. These units are allowed to maintain separate online identities within their country's armed forces. In a sense, this makes them more dangerous as they have undergone a certain militarization trajectory and no longer function as traditional organizational emanations of extremist movements.

They have made the war central to their existence and, consequently, to the production of their online content.

Moreover, it is not necessarily the old, pre-war TVEs producing such content, but channels affiliated with, associated with, or officially representing the armed emanations or wings, or new factions and splinter groups of these original TVEs. These groups are on the front lines of the war, and their content, which is both the most dramatic and disturbing, is of key importance to the larger or original organization, or even to the whole TVE movement in either Russia or Ukraine.

Russian channels in the sample post more content. Over a week or a weekend, their production can surpass that of Ukrainian channels tenfold. At the same time, the Ukrainian content is more personal – it focuses on individuals whose names, faces, and life stories are showcased. Moreover, Ukrainian channels rely more on interviews with fighters, wounded fighters, or former fighters than Russian channels do. Finally, Ukrainian content is almost entirely war-related, whereas Russian TVEs tend to go beyond Russia in their content or, to some extent, in their coverage of world events. The last point reflects the fact that, from a practical perspective, the Ukrainian TVEs perceive the war in existential terms, both theoretically and practically, as a loss of sovereignty for their country that would effectively force them underground or abroad. This would not be the case for the Russian TVEs, who at times deploy apocalyptic language related to the risk of the failure of the "special military operation." They stress the loss of face or prestige if Moscow were unable to win. However, a lost war would ironically give these TVEs greater visibility and popularity within a destabilized Russia.

The content most featured on the discussed TVE channels can be divided into three main categories:

1. **Battlefield prowess** – presentation of a given unit's successes, heroic and/or successful operations, in memoriam posts related to fallen fighters, interviews with prominent fighters, and their receiving state awards. This allows the given TVE to establish a certain legitimacy with its followers and, potentially, future recruits and donors. In short, TVEs, which in the past would boast about and celebrate instances of political violence against perceived ideological enemies such as LGBTQI+ groups, ethnic minorities, or foreigners (especially from the Global South), are now, thanks to the war, able to construct a completely different narrative and present themselves as heroic warriors seeking approval and endorsement from a wider community than their pre-war TVE supporters.
2. **Recruitment** – once the success or "coolness" of a given entity is established via enticing graphics, videos, and aggressive music, the next category of online content aims to turn passive consumers of that unit's content into active members. Ads and recruitment posters, distributed via TVE online outlets and solely advertising "their" units, offer high salaries, better training standards, and the promise of being looked after or mentored by more professional

and experienced NCOs or officers. These feature prominently and are interspersed with offers of training for war-related professions, with graduates shipped to the given unit (this is especially evident for offers related to future drone operators, engineers, and technicians).

3. **Fundraising** – another avenue for turning a passive consumer of content into an activist, albeit less involved than a recruited fighter, is raising funds for the given entity. The organizations discussed in this article almost continuously fundraise for their fighters and their needs on the front lines – a pattern that aligns with the activities of non-TVE-linked units, especially on the Ukrainian side. This is the most natural and bottom-up way for such military units to address deficiencies in the procurement system. The units sometimes establish dedicated channels for such activities, but also use the main Telegram outlet, which usually has the most followers or subscribers, for these purposes. The TVEs also issue individual fundraisers for specific purposes and targeted purchases of equipment for "their" units, such as drones, Starlinks, transport vehicles (including electric ones), thermal rifle scopes, and other gear. Simultaneously, the discussed entities also sell merchandise to raise funds or sell tickets to events featuring their former members or fighters on leave via local or purpose-built websites. Finally, to offset the high number of fundraising posts, the channels showcase instances in which some of the funds raised go to legitimate charities – often those that tend to the needs of wounded former members or the families of fallen members of a given unit.

Furthermore, the Russian TVE online content offers commentaries on current events, e.g., the Israel-U.S. war with Iran or earlier events in Venezuela. The TVEs do not shy from commenting on news from the so-called "home" front – e.g., Russian groups keenly discuss the alleged Great Replacement, a key white supremacist concept, now allegedly taking place in Russia. Both sides also discuss the difficulties that former or veteran individuals face at home and underscore the shortcomings of social security systems for such individuals. They are also involved in "fan spotting" – posting photos or videos of supporters across the globe who display or create graffiti, tags, or logos on walls or on items such as T-shirts.

Success of the Online Content?

The extent to which deployment of online content by TVEs is successful remains an open question, as the authors are unable to estimate how many people decided to join units fronted by TVE groups because of exposure to their digital content. However, a look at certain indicators allows for a cautious attempt to ascertain how convincing the produced content could have been for the potential audience.

First, and most obviously, the number of subscribers to the TVE channels under discussion serves as an indicator. After August 24, 2022 (six months into the full-scale war), the authors observed a steady, almost uninterrupted rise in median subscriptions across all 33 channels – between 8 to 19 percent increases over subsequent six-month periods throughout 2023–2025. The last six

months, however, have seen a marked drop in median subscriptions of 26 percent. This could be explained by general fatigue with the conflict among both Russian and Ukrainian audiences, by prolonged internet shutdowns in certain Russian regions, and by Moscow's campaign to block Telegram and force its users onto government-controlled platforms.

Second, engagement among users of the Telegram channels would need to stand at between 25 and 30 percent to demonstrate success. The channels covered in this analysis fall short of that threshold, with engagement rates ranging from 2 to 10 percent, most in the 2 to 5 percent bracket. At the same time, most channels see between 10 and 20 percent of their subscribers read the latest post within 24 hours of publication.

Third, the fundraising theme is omnipresent in the digital content, but not always as successful as the TVEs would like. The authors established that the TVEs' fundraising covers a broad spectrum, ranging from autism rehabilitation for a combatant's child to the purchase of drones and the care of wounded former combatants. On many occasions, collections for such items stall. Seventy to eighty percent of the fundraising goal is reached and then expires without reaching the stated goal. To put this seeming lack of success in perspective, however, the sums demanded in these collections often exceed 10,000 euros.

It is evident that more granular research is required to fully measure the success of TVEs in deploying online content, but the indicators outlined above offer an interesting introductory attempt to account for this process.

Violent Outsiders

The two earlier mentioned TVE external or semi-external outsiders to the conflict who are most prodigious users of the online realm to incite violent attacks are the Base, globally designated as a terrorist group, and the network of pro-Russian doxxers who "out" foreigners fighting or assisting Ukraine. These differ from the Russian and Ukrainian TVEs that might focus on the war but refrain from calling for terrorist attacks or assassinations behind enemy lines.

The Base runs a trilingual Telegram operation and sees its posts published in English, Russian, and Ukrainian. On its channels, the group has called for attacks against critical infrastructure in Ukraine as well as government and military sites and personnel. It has also offered financial rewards for documented attacks. Its alleged "portfolio" of attacks includes seemingly innocent spraying of graffiti on the walls of Ukrainian cities, arson attacks (including against military and governmental targets), bombings of police stations, and shootings of Ukrainian security personnel. The attackers are incentivized to stage these activities with promises of payment via cryptocurrency exchanges. Such an approach resembles the Russian tactic of recruiting "disposable agents" for sabotage, diversion, and state terrorism conducted on behalf of Moscow in the West.

The doxxing network, functioning as a loose collective grouped around a string of administrators based in different countries running Telegram channels and websites, functions as an online echo-chamber in which predominantly foreign individuals fighting or assisting Ukraine are framed as "Nazis." Moreover, in the process, they are slurred with anti-Semitic, homophobic, and sexist language. The channels run by, e.g., Germany or Serbia-based administrators, underpinned by a server infrastructure allegedly operating out of EU member states, incite violence against and celebrate the deaths of pro-Ukraine fighters. They also admit to having played a role in the alleged targeted killings of some of these fighters. The doxxers get profiled, quoted, and praised by Russian state media and the so-called Z-bloggers (pro-war über-patriots), which suggests a certain level of "coordination" between the Russian disinformation machine and these doxxing networks.

Conclusion

TVEs local to the Russo-Ukrainian conflict have made the war central to both their offline and online efforts and strategies. They were absorbed into the armed forces of their respective countries and allowed to maintain separate online identities. Their online content bears striking similarities and is predominantly used to mythologize their participation in the war, recruit new fighters, and fundraise. From 2023 to 2025, their efforts were rewarded with a growing number of Telegram subscribers, but this trend has recently ended. The local TVEs struggle with subscriber engagement and are not always successful in their fundraising, as their ambitions often exceed the reach of their fans and followers. At the same time, it is the TVEs external to the conflict that are most active in terms of terrorism incitement against Ukraine.

Conclusion

Erin Saltman | Senior Director of Membership & Programs, GIFCT

Micalie Hunt | Senior Associate of Membership & Programs, GIFCT

Today's global security landscape is shaped by the convergence of protracted conflicts, rapid technological innovation, and social dynamics that increasingly play out online. According to the Armed Conflict Location and Event Data Conflict Index (ACLED), in the last 12 months, over 240,000 people around the world were killed in conflict-related violence, including combatants and civilians. The UN's Global Counter-Terrorism Strategy, adopted by the General Assembly in 2006, has highlighted several conditions conducive to the spread of terrorism, including prolonged and unresolved conflicts. These conditions create an opportunity for terrorists and violent non-state armed groups to take hold within a territory, increasing the likelihood of fractured rule of law, political exclusion, and socioeconomic marginalization.

Working with a wide range of technology companies around the world, GIFCT is aware of the new tools and technologies that create untold opportunities for progress – while also enabling adversarial actors to disseminate propaganda, recruit new members, and scale operations. The case studies discussed in this paper examine three distinct parts of the world that face conflicts at very different points in their lifecycle, in very different sociopolitical contexts.

In Afghanistan, several Islamist extremist terrorist groups remain active, most notably ISKP and TTP. Terrorist attacks against civilians have decreased since the Taliban took power in 2021 after the U.S. withdrawal of military forces; however, repressive measures against civilians have had a wide range of negative consequences. Many global powers are still uncertain how to engage Afghanistan, as six governments[4] continue to designate the ruling governing body of Afghanistan itself as a terrorist organization. In the Sahel, we see a layered transnational network of terrorists and non-state armed groups challenging national authorities, aiming to take control of territory, resources, and infrastructure. In the ongoing Russia-Ukraine conflict, the physical battlefields are tied to two countries, unlike in the Sahel and Afghanistan. Here, we see a range of state and non-state actors looking to influence broader global alliances to sway the conflict and control the narrative for domestic and international audiences. It is also increasingly hard to differentiate between state and non-state actors in the conflict between Russia and Ukraine, with many combatants acting in official and unofficial roles. Each of the three case studies highlights the unique challenges that conflict zones pose for the counterterrorism space and the myriad roles that the online front line plays.

4. The Taliban is designated as a terrorist organization in New Zealand, Canada, Tajikistan, Turkey, the United Arab Emirates, and the United States under Executive Order 13224.

Despite vastly different geographies and sociopolitical contexts, the case studies – informed by an expert discussion hosted by GIFCT and KAS – highlight several similarities in how TVE actors exploit online spaces in conflict zones. Across all three regions, TVE online activities break down into six categories:

1. Broadcasting victories
2. Maintaining a global network
3. Recruiting
4. Financing
5. Disseminating threats
6. Operationalizing attacks

In each of the conflict zones discussed, we continue to see TVE groups broadcast on-the-ground military victories to online audiences to justify continued efforts. These posts seek to promote a group's specific interpretation of real-world events and create a justifying narrative for the violence. TVE groups are even showcasing the hypocrisy or human rights abuses they see as being carried out by the government systems they oppose or groups they are fighting, as discussed in the Russia-Ukraine case study and in propaganda coming out of the Sahel. This can sometimes contradict how mainstream media cover ongoing violence or show gaps in reporting to convey to audiences that the mainstream world order is hiding the "truth."

Increasingly, various terrorist affiliates of Islamic State are leaning into generative AI-enhanced video content to make their "news" reports look like those of professional news outlets, and using large language model support to translate reporting fluently into a range of languages to target specific audiences. TVE entities also continue to use online social networks to maintain connectivity with sympathizers, funders, and potential recruits, reiterating and justifying a specific ideological worldview. Often, experts report a multiplatform user journey, with initial conversations starting on a broader platform and, once vetted, moving the user to smaller, less-regulated, and more private channels for more overt conversations. These tactics aim to evade moderation and build nimble, adversarial online operations.

In conflict zones, this network of communication serves dual purposes: recruiting members domestically and disseminating propaganda locally and abroad. As noted in the snapshots from the field discussed in this paper, these channels are used to proselytize, mentor, recruit new members, and build an operationalized in-group. This external global network is particularly important for many of the groups mentioned, which solicit donations and funds through a myriad of online facilitation methods.

TVE groups also continue to distribute mocking and threatening narratives to undermine a group's perceived enemies. In conflict zones, this type of online content aims to intimidate the opposition,

highlight their failures, and position the organization as the superior force in a region by showcasing its prowess and violence.

Across the three conflict zones, the reports above highlight that terrorists and violent extremists create highly personal content to humanize the individuals within their organizations. In Ukraine, interview-style content centers on the life stories of the fighters, while in the Sahel, Islamic State crafts a narrative arc that blends ideology with the storylines of various fighters to put a human face on them and, by extension, the overall cause. Unlike content that explicitly shows gore, violence, or other material that would be flagged under a tech company's policies, this "softer" content may be more difficult for Trust and Safety teams to identify and act on, as it might not be explicitly policy-violating. If indicators such as group logos or symbols are included and the content belongs to groups that are on a government designation list, content moderation decisions will be simpler. However, this softer content is often intended to evade moderation efforts, so it may be less likely to include explicit signals.

The preceding case studies suggest that terrorists and violent extremists across and within the three regional contexts are hyper-aware of the global and local aspects of their conflict. Local groups that operate within a specific country frame their messaging through on-the-ground contexts, using hyper-local language and narratives, while groups that operate across a broader region often frame local developments within broader global narratives and use regional or transnational languages in their content. Differences in dissemination tactics are less attributable to whether a group exists within or outside a conflict region than to its organizational structure and media approach.

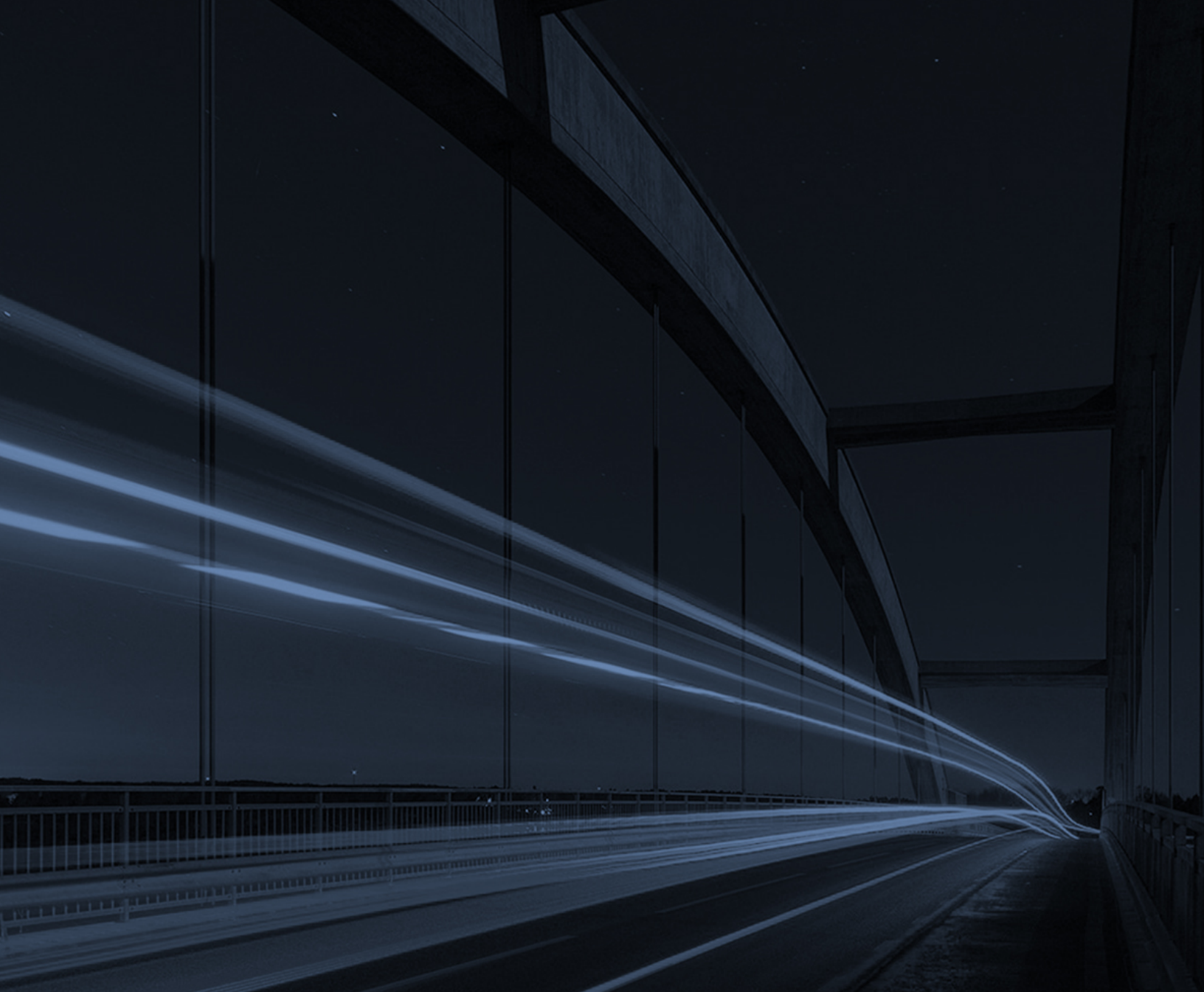
Across the three conflict zones, the authors note that quantifying the success of a particular group is difficult and may depend on the metrics used. In Afghanistan and the Sahel, the reports illustrate a cyclical relationship: offline attacks generate online content that lends credibility to claims of military superiority, prowess, and legitimacy, which in turn exacerbate tensions and lead to further attacks. Territorial expansion, community building, and the continued presence of groups in the region can also be seen as indicators of success, which may not have been possible without online content reinforcing these narratives. By contrast, in Ukraine, while the authors noted increased online followers and subscribers for TVE channels between 2023 and 2025, there has been a decrease in the past six months, which may be due to conflict fatigue or government actions, including blocking online platforms. However, regardless of how success is measured, terrorists and violent extremists continue to exploit conflict zones for digital content.

From these trends and similarities, we can offer broad recommendations for policymakers and tech companies in addressing TVE threats online, which often extend beyond the territory facing prolonged conflict. These recommendations are underpinned by the importance of a cross-sector, multi-stakeholder approach that involves government, industry practitioners, and civil society to address manifestations of the threat across arenas.

- **Keep humans in the loop**. While new technologies like artificial intelligence, 3D printing, and drones can benefit those seeking to counter TVE exploitation of digital platforms, the human element should not be removed. To counter the highly localized messaging used by groups, such as those in the Sahel, researchers and local experts who can trace the evolution of dialects, memetic language, and symbols should be seen as valuable sources of knowledge. These individuals can help translate and contextualize narratives and symbols within both local and global contexts, ensuring that human rights are respected so that symbols or local dialects are not misunderstood or misconstrued.
- **Deepen cross-platform and cross-sector collaboration to understand user journeys**. As the Russia-Ukraine experts mentioned, online forums appear across different platforms, are removed ad hoc by larger platforms, and might persist and broadcast longitudinally from less-regulated online spaces. We can sometimes get an idea of followers and engagement, but it is often hard to fully understand if a terrorist or violent extremist's goals are being met through their online activity. Are posts resulting in increased recruits or funding toward a cause? Is the "enemy" threatened by the propaganda aimed at undermining them? The full picture can only be deciphered when information is shared. The more information available to define key TVE terminology, identify logos, and trace "news outlets" officially affiliated with designated terrorist organizations, the easier it is for platforms to respond with policies and tools to moderate. Crucially, the more practitioners understand the user journey across platforms, the more intervention points they can address. Basic knowledge-sharing among regional experts, law enforcement, and tech platforms can enhance online efforts to curtail the reach of TVE content and activities.
- **Update and refine government designation lists**. Tech companies rely on government designation lists as a key source for identifying the groups and organizations whose content they should be actioning under terrorist or violent extremist-related policies. When dealing with "softer," humanizing propaganda content intended to evade moderation, increase recruitment, appeal to a variety of audiences, and that does not explicitly violate policies, tech companies can fall back on the legal frameworks that underpin designations to act on content based on its author rather than the content itself. Governments and intergovernmental bodies should continually assess and update their lists to enable tech platforms to make moderation decisions rooted in legal frameworks.

Across Afghanistan, Ukraine, and the Sahel, terrorists and violent extremists continue to demonstrate an understanding of the avenues online spaces provide for achieving their operational objectives. Regardless of the unique context of the conflict zone, TVE groups operating there use offline operations to inform and expand their online content strategy. Attacks, community

outreach efforts, and even the fighters themselves become tools in a social media strategy that is self-reinforcing and geared toward the continuation of future violence. In order to break the cycle of offline to online violence, practitioners across government, tech, and civil society must work together to address the threat in both arenas.



GIFCT is a 501(c)(3) non-profit organization and tech-led initiative with over 30 member tech companies offering unique settings for diverse stakeholders to identify and solve the most complex global challenges at the intersection of terrorism and technology. GIFCT's mission is to prevent TVE from exploiting digital platforms through our vision of a world in which the technology sector marshals its collective creativity and capacity to render TVE ineffective online. In every aspect of our work, we aim to be transparent, inclusive, and respectful of the fundamental and universal human rights that TVE seek to undermine.

www.gifct.org **outreach@gifct.org**