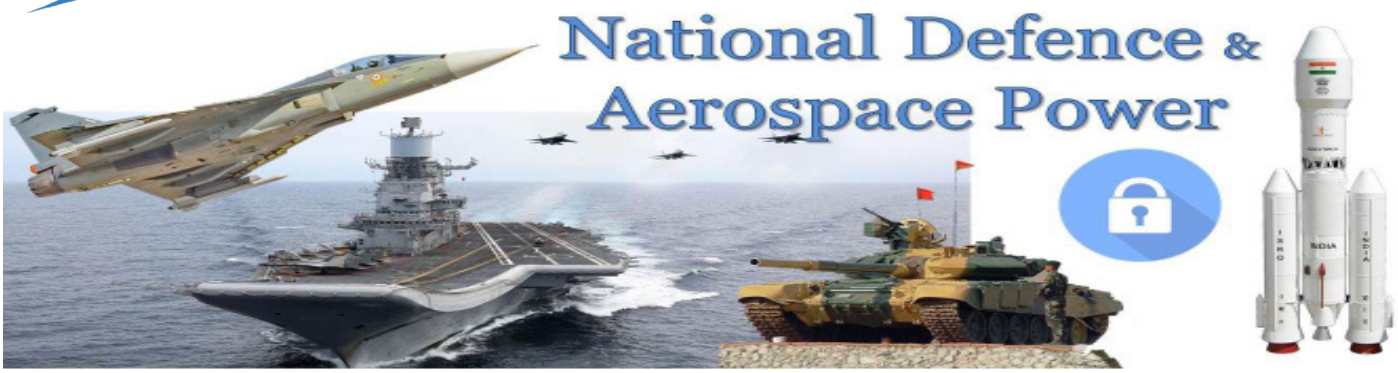
Centre for Aerospace Power and Strategic Studies



Centre for Aerospace Power and Strategic Studies ISSUE BRIEF

10/26

01 October 2026

CLICKS, CRYPTO, AND CALIPHATE: STRENGTHENING INTERNATIONAL COUNTERTERRORISM COOPERATION

Ms Priyadarshini Baruah

Research Associate, Centre for Aerospace Power and Strategic Studies



The threat posed by the Islamic State of Iraq and Syria (ISIS) or Islamic State (IS) and its ideology continues to extend beyond conflict zones, with online radicalisation playing an important role in inspiring individuals to plan attacks. A recent case in the United States (US) highlights this continuing concern. In late August 2026, federal authorities arrested 35-year-old Jessica Bowie, who used the name Aisha Saif, for allegedly plotting an IS-inspired bombing targeting the New York State Capitol.[1] Investigations revealed that Bowie had been communicating with undercover federal agents whom she believed were members of ISIS and had discussed plans to target state officials.[2] This case highlights how IS-inspired narratives can continue to influence/radicalise individuals online, even when they have no direct organisational links to the group. Another example is the December 14, 2025 Bondi Beach attack in Sydney, which targeted a Hanukkah gathering and killed 15 people.[3] It was subsequently celebrated by ISIS' digital weekly *Al-Naba* (issue 526) and used to encourage further violence.[4] While distinct in nature, both cases demonstrate how terrorist networks exploit digital platforms for communication, mobilisation, and propaganda amplification. These developments raise a broader question of how cross-border propaganda, communication, and financing sustain terrorist activity, and where international cooperation can disrupt these connections.

This brief attempts to examine how IS' South and Central Asian offshoot, the Islamic State Khorasan Province (ISKP) and the wider IS network sustain terrorist activity

through digital propaganda, encrypted platforms, and emerging financing methods. Its objectives are to assess existing international responses and identify practical gaps in four areas: platform governance, intelligence sharing, financial disruption, and regional cooperation. Radicalisation, recruitment, and operational financing are connected but distinct processes. The argument advocated forth is that cooperation must address their shared infrastructure without assuming that every propaganda consumer becomes a recruit or every donation finances an attack.

The Evolving Nature of Radical Ideology Online

The online dissemination of radical ideology can be decentralised, transnational and digitally sustained. ISKP, *Al Qaeda* (AQ) and their affiliates no longer require territorial control to disseminate their messages. They exploit social media, encrypted applications, gaming spaces, and cryptocurrency networks to circulate propaganda, recruit sympathisers, and finance their illicit/terror operations across borders.[5]

During IS' territorial expansion and rule between 2014 and 2017, propaganda portrayed the so-called "Caliphate" as stable, prosperous, and religiously fulfilling.[6] Publications such as *Dabiq* and propaganda films like *"Flames of War: The Fighting has Just Begun"* combined sophisticated Hollywood-style production values with apocalyptic rhetoric, particularly targeting diaspora youth seeking identity and purpose.[7] After losing most of its territory by late 2017, IS shifted its strategy towards a networked model that encouraged supporters to act independently (lone wolf attacks) in their home countries rather than travel to Iraq or Syria (core territory of the Caliphate). This increased emphasis on networking drew on secure messaging platforms and encrypted fundraising that helped sustain this virtual ecosystem (virtual caliphate).[8]

ISKP has further developed and refined this model through its propaganda ecosystem, including *Voice of Khorasan* (VOK), combining ideological appeals with cryptocurrency wallet addresses.[9] Supporters are encouraged to make small donations, often framed as "*Sadaqah for Jihad*" (religious duty), through privacy-oriented currencies such as *Monero*, with appeals circulated through *Telegram* channels.[10] Propaganda and terrorist micro-financing can complement one

ISKP has developed and refined this model through its propaganda ecosystem, including *Voice of Khorasan* (VOK), combining ideological appeals with cryptocurrency wallet addresses. Supporters are encouraged to make small donations, often framed as "*Sadaqah for Jihad*" (religious duty), through privacy-oriented currencies such as *Monero*, with appeals circulated through *Telegram* channels.

another: digital media attracts sympathisers, while dispersed micro-donations can help sustain media production and organisational activities. However, wallet addresses demonstrate solicitation, not the amount raised or its eventual use. The proposed feedback loop requires evidence linking appeals, receipts, and expenditure; its plausibility should not be mistaken for proof in every case.

IS and ISKP have moved from centralised territorial propaganda towards decentralised virtual ecosystems that encourage self-radicalisation and IS-inspired lone wolf attacks without direct operational control.

Micro-Financing Across Transnational Terrorist Networks

The transnational character of these terrorist organisations' digital networks makes international cooperation indispensable. Digital platforms operate across jurisdictions, encrypted channels complicate domestic surveillance, and diaspora networks span across continents. IS and ISKP have moved from centralised territorial propaganda towards decentralised virtual ecosystems that encourage self-radicalisation and IS-inspired lone wolf attacks without direct operational control. Investigations in Germany, Poland, Türkiye, and Russia in 2023-24 identified Tajik supporters, including labour migrants and second-generation diaspora members, who made frequent micro-crypto donations of about USD 100 to USD 2,000 to ISKP-linked wallets.[11] Such autonomous mobilisation must be distinguished from attacks involving organisational facilitation or direction. Both can occur within the same ecosystem, but ideological allegiance alone does not establish a command relationship. Financial and communications evidence is needed to distinguish these forms of involvement.

The March 2024 Crocus City Hall attack in Moscow illustrates a different, coordinated form of violence. Four ISKP-affiliated attackers killed at least 145 people and injured more than 500, after which IS claimed responsibility through their *Amaq* Media Agency via *Telegram*.[12] Investigators later reported that approximately USD 2,000 in Virtual Assets (VAs) was received by the attackers shortly before executing the massacre at Crocus City Hall, and this transaction was routed through a high-risk exchange and Central Asian channels.[13] This reported payment illustrates a possible operational financing link. It does not, by itself, establish that numerous micro-donations funded the attack or that reporting thresholds explain the failure to detect it. The cooperation problem is nevertheless clear: relevant information may be divided among the jurisdictions associated with donors, intermediaries, and recipients. Connecting those records is necessary before drawing conclusions about the financing chain.

International frameworks acknowledge this challenge; for instance, the United Nations General Assembly (UNGA) has urged the need to counter terrorist propaganda through information and communication technologies while respecting human rights and international law.[14] The 2019 Global Counterterrorism Forum (GCTF) Zurich-London recommendations emphasise multi-stakeholder cooperation, transparency and digital literacy; the central difficulty, however, is translating broad commitments into timely operational coordination.[15]

Key Dimensions of International Cooperation

International cooperation on counter-radicalisation includes community engagement, ideological counter-narratives, digital literacy, and partnerships with religious organisations, clergy, scholars, youth, and women to challenge radical messaging while addressing grievances such as marginalisation, governance, and underdevelopment.[16] These measures remain important, but the changing digital and financial environment requires stronger cooperation in the following areas.

Digital Platform Governance

Technology companies are essential counterterrorism partners because non-state actors use their platforms to disseminate radical ideologies. The Global Internet Forum to Counter Terrorism (GIFCT), established in 2017 and expanded after the 2019 New Zealand Christchurch attack, brings together more than 35 technology companies, governments, researchers, and civil society groups to strengthen online counterterrorism efforts, share resources, and promote safer digital spaces.[17] Its Incident Response Framework helps to coordinate responses when terrorist groups generate radical content as part of their digital (propaganda) warfare strategy.[18]

However, content moderation remains difficult. For instance, content removed from one platform often reappears elsewhere, while messaging platforms such as *Telegram* complicate surveillance. On the other hand, when governments demand that tech companies conduct surveillance and remove content, concerns about privacy and potential overreach also arise. For example, Germany's Network Enforcement Act (NetzDG) imposed deadlines and penalties on various social media platforms for failing to remove illegal radical/terror content.[19] This approach highlights both the appeal and controversy of content-regulatory enforcement.

Intelligence Sharing and Financial Disruption

To effectively track individuals and networks who are involved in radicalisation or are promoters of radical ideologies requires comprehensive intelligence-sharing mechanisms. Such cooperation often faces obstacles such as mistrust between states, sovereignty concerns, and selective sharing driven by vested interests. Regional platforms such as the Moscow Format Consultations on Afghanistan exist and may facilitate dialogue, but diplomatic dialogue should not be equated with an operational intelligence-sharing mandate.

Financial disruption of radical groups is equally essential. ISKP's use of micro-donations through privacy-enhancing cryptocurrencies like *Monero* and hybrid crypto-*hawala* systems challenges counterterrorism finance efforts to identify financiers and connect dispersed transfers. FATF standards remain central, but states also need tools that can detect dispersed patterns across privacy coins, peer-to-peer exchanges, and informal settlement systems.[20] Small transfers are not inherently suspicious, and analytical systems should not treat donor identity or religious language as sufficient evidence of terrorist financing. The task is to establish credible connections to prohibited activity while avoiding indiscriminate scrutiny of legitimate transfers.

Regional Considerations: South Asia and Beyond

South Asian states confront these threats from uneven institutional positions. Afghanistan remains particularly vulnerable because ISKP operates amid severely constrained governance.[21] Pakistan has improved formal Anti-Money-Laundering (AML) and Counter-Terrorist Financing (CFT) compliance but struggles in informal transfers, charities, and lightly supervised cryptocurrency exchanges.[22] Bangladesh's prohibition-based approach may push activity underground, making it hard to detect. Maldives continues to face gaps in screening and virtual asset (VA) regulation. Terrorist networks do not require every jurisdiction to be permissive; a few exploitable seams can sustain regional activity.

The Sahel region presents a comparable challenge due to the gaps and loopholes in the weak governance system, internal conflicts, and underdevelopment. This allows transnational terrorist organisations to thrive and expand, making Africa indispensable to any global counter-radicalisation strategy. This concerns governance capacity, not evidence that Sahelian groups reproduce ISKP's digital financing practices.

Recommendations for Strengthening International Cooperation

The most urgent gaps lie between traditional financial controls and micro-donation systems, between diplomatic dialogue and operational coordination, and between global frameworks and regional capacity.

International cooperation has evolved into a multi-layered framework involving intelligence sharing, digital governance, financial monitoring, and ideological engagement, but implementation remains uneven. The most urgent gaps lie between traditional financial controls and micro-donation systems, between diplomatic dialogue and operational coordination, and between global frameworks and regional capacity. Bridging these gaps requires stronger regional mechanisms, pattern-based financial analysis, responsible technology partnerships, and sustained investment in community resilience. International cooperation is essential to disrupting cross-border infrastructure, but it cannot substitute for locally grounded prevention. Its value lies in connecting evidence, capabilities, and jurisdictions while preserving the distinction between ideological influence and operational involvement. These challenges require stronger policies and better cooperation.

First, national security agencies should complement transaction-centric detection with pattern-based analysis to identify how small transfers collectively support terrorist activity. FATF should refine typologies for terrorist micro-financing, privacy coins, peer-to-peer exchanges, and hybrid crypto-*hawala* arrangements, while states connect financial data with digital-platform and intelligence reporting.

Second, regional mechanisms, including the Shanghai Cooperation Organisation (SCO) and the Regional Anti-Terrorist Structure (RATS), should establish clearer procedures for exchanging time-sensitive intelligence and coordinating disruption. Since procedures alone cannot overcome political mistrust, cooperation should begin with agreed offences, designated contact points, and safeguards governing onward disclosure. Limited, reciprocal exchanges on specific investigations may be more feasible than unrestricted intelligence pooling.

National security agencies should complement transaction-centric detection with pattern-based analysis to identify how small transfers collectively support terrorist activity. FATF should refine typologies for terrorist micro-financing, privacy coins, peer-to-peer exchanges, and hybrid crypto-*hawala* arrangements, while states connect financial data with digital-platform and intelligence reporting.

Third, international cooperation should strengthen capacities in conflict-prone regions. The Sahel's share of global terrorism deaths and ISKP's operating space around Afghanistan underline the

importance of addressing institutional vulnerabilities. Support should prioritise border security, financial oversight, intelligence capacity, and accountable governance.

Finally, governments should strengthen partnerships with technology companies to coordinate rapid responses, improve detection, and reduce the recirculation of terrorist propaganda. These measures require transparent safeguards for privacy and lawful expression, alongside independent oversight to prevent overreach and ensure accountability.

Digitally enabled terrorist activity is a transnational and adaptive threat. IS/ISKP and similar transnational terror organisations combine virtual networks, propaganda, and emerging financing methods without necessarily abandoning territorial bases or established sources of support. Their ability to radicalise, recruit, and finance operations across borders requires an equally adaptive international response.

Notes:

[1] Department of Justice, United States of America, "Albany, New York Woman Charged with ISIS-Inspired Terror Plot Targeting New York State Capitol," August 20, 2026, https://www.justice.gov/opa/pr/albany-new-york-woman-charged-isis-inspired-terror-plot-targeting-new-york-state-capitol. Accessed on September 11, 2026.

[2] Ibid.

[3] Ely Karmon, "The Chanukah Massacre of Sydney's Jewish Community," International Institute for Counter-Terrorism, December 25, 2025, https://ict.org.il/the-chanukah-massacre-of-sydneys-jewish-community/. Accessed on September 09, 2026.

[4] Kyle W. Orton, "The Islamic State's Global Terrorism Campaign and the Bondi Hanukkah Massacre," *It Can Always Get Worse*, December 29, 2025, https://www.kyleorton.com/p/islamic-state-global-terrorism-hanukkah-massacre-bondi-beach-australia-al-naba-526?has_completed_unsubscribed_unlock=true. Accessed on September 09, 2026.

[5] Colin Neagle, "How ISIS could use Video Games, Messaging Apps to Evade Surveillance," *Network World*, November 16, 2015, https://www.networkworld.com/article/945428/how-isis-uses-video-games-playstation-4-messaging-apps-to-evade-surveillance.html#:~:text=Players%2C%20for%20instance%2C%20can%20use,officer%20reportedly%20told%20Buzzfeed%20News;

Soumya Awasthi, "Gaming Platforms: A New Frontier for Extremist Recruitment and Radicalisation," Observer Research Foundation, December 04, 2024, https://www.orfonline.org/expert-speak/gaming-platforms-a-new-frontier-for-extremist-recruitment-and-radicalisation. Accessed on September 09, 2026.

[6] Rahaf Al Khazraji, "Turning to Terrorism: Why Shamima Begum and Other Women Joined ISIS," *Trends Group*, April 05, 2023, https://trendsresearch.org/insight/turning-to-terrorism-why-shamima-begum-and-other-women-joined-isis/?srsltid=AfmBOoprr-l5TU54Lp0Xr0JQsY9SITwrxQTyanXw3GQww_1Il3HOsp2S. Accessed on September 09, 2026.

[7] Tantan Hermansah and Nofia Natasari, "The Khilafah Discourse in Online Magazine of ISIS: Dabiq," *International Journal of Progressive Sciences and Technologies* vol. 19, no. 1, 2020, p. 134, https://www.repository.uinjkt.ac.id/dspace/bitstream/123456789/61913/3/The%20Khilafah%20Discourse%20in%20Online%20Magazine%20of%20ISIS%20DABIQ.pdf;

Ariel Victoria Lieberman, "Terrorism, the Internet, and Propaganda: A deadly Combination," *Journal of National Security Law & Policy* vol. 9, no. 95, 2017, p. 105 https://nationalsecurity.law.georgetown.edu/wp-content/uploads/2017/04/Terrorism_the_Internet_and_Propaganda_FINAL.pdf. Accessed on September 09, 2026.

[8] Michael Knights and Alex Almeida, "The Islamic State at Low Ebb in Iraq: The Insurgent Tide Recedes Again," *CTC Sentinel* vol. 15, no. 1, 2023, p. 13, https://ctc.westpoint.edu/wp-content/uploads/2022/01/CTC-SENTINEL-012022.pdf. Accessed on September 09, 2026.

[9] Priyadarshini Baruah, "Framing Fear: ISKP's Media Propaganda," Centre for Aerospace Power and Strategic Studies, October 04, 2024, https://capssindia.org/framing-fear-iskps-media-propaganda/;

Animesh Roul, "The Rising of Monero: ISKP's Preferred Cryptocurrency for Terror Financing," Global Network on Extremism & Technology, October 04, 2024, https://gnet-research.org/2024/10/04/the-rise-of-monero-iskps-preferred-cryptocurrency-for-terror-financing/#:~:text=Quest%20for%20Crypto%20Coins&text=However%2C%20Bitcoin's%20initial%20appeal%20faded,methods%20largely%20obsolete%20and%20ineffective. Accessed on September 09, 2026.

[10] Roul, n. 9;Ahmet Yiğitalp Tulga, "Soliciting Terror: ISKP Digital Communications and Financing Tactics through Voice of Khurasan," Global Network on Extremism & Technology, December 12, 2024, https://gnet-research.org/2024/12/12/soliciting-terror-iskp-digital-communications-and-financing-tactics-through-voice-of-khurasan/#:~:text=It%20can%20be%20observed%20that,were%20introduced%20in%20Issue%2033. Accessed on September 09, 2026.

[11] "2025 Crypto Crime Report," *TRM*, February 10, 2025, https://www.trmlabs.com/reports-and-whitepapers/2025-crypto-crime-report. Accessed on September 09, 2026.

[12] "Islamic State Releases Photo of Alleged Attackers in Russia Shooting," *Reuters*, March 23, 2024, https://www.reuters.com/world/europe/islamic-state-releases-photo-alleged-attackers-behind-russia-shooting-2024-03-23/. Accessed on September 09, 2026.

[13] Anna Corsaro, "The New Terror Finance Battlefield: ISKP's Expanding Use of Cryptocurrency," *Homeland Security Today*, December 01, 2025, https://www.hstoday.us/subject-matter-areas/counterterrorism/the-new-terror-finance-battlefield-iskps-expanding-use-of-cryptocurrency/. Accessed on September 09, 2026.

[14] "Counter-Terrorism in Cyberspace," United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), October 2021, pp. 1-6, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/ctc_cted_factsheet_ct_in_cyberspace_oct_2021.pdf. Accessed on September 09, 2026.

[15] "Policy Toolkit: The GCTF Zurich-London Recommendations on Preventing and Countering Violent Extremism and Terrorism Online," Global Counterterrorism Forum (GCTF), 2019, p. 36, https://www.thegctf.org/LinkClick.aspx?amp=&fileticket=joZMSx_b1-g%3D&portalid=1. Accessed on September 09, 2026.

[16] "Letter Dated 26 April 2017 from the Chair of the Security Council Committee Established Pursuant to Resolution 1373 (2001) Concerning Counter-Terrorism Addressed to the President of the Security Council," United Nations Security Council (UNSC), April 28, 2017, https://docs.un.org/en/S/2017/375. Accessed on September 07, 2026.

[17] "About- Terrorist and Violent Extremist Exploitation of the Internet Threatens Open Societies Everywhere," Global Internet Forum to Counter Terrorism (GIFCT), https://gifct.org/about/#:~:text=The%20Global%20Internet%20Forum%20to,extremists%20from%20exploiting%20digital%20platforms. Accessed on September 12, 2026.

[18] "Insight Briefing: Countering the Dissemination of Online Content Relating to Violent Extremist and Terrorist Incidents," United Nations Security Council Counter-Terrorism Committee Executive Director (CTED), August 25, 2022, pp. 1-3, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/concept_note-insight_briefing-18aug2022.pdf. Accessed on September 12, 2026.

[19] "Is online Content that Incites Acts of Terrorism Illegal?" *Tech Against Terrorism*, March 2023, pp. 34-35, https://www.techagainstterrorism.org/hubfs/Germany-Designation-Report-Country-Analysis-Paper-8.pdf. Accessed on September 12, 2026.

[20] "FATF Report – Comprehensive Update on Terrorist Financing Risks," Financial Action Task Force (FATF), July 2025, p. 70, https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/Comprehensive-Update-on-Terrorist-Financing-Risks-2025.pdf.coredownload.inline.pdf;

"Report Teaser: Proportion of Illicit Volume of Crypto Dropped 51% in 2024," *TRM*, January 14, 2025, https://www.trmlabs.com/resources/blog/report-teaser-proportion-of-illicit-volume-of-crypto-dropped-51-in-2024. Accessed on September 12, 2026.

[21] "UNODC Roadmap for Afghanistan and Neighbouring Countries 2025-2027," United Nations Office of Drugs and Crime, 2025, p. 21, https://www.unodc.org/coafg/uploads/documents/UNODC_Roadmap_for_Afghanistan_2025-2027_endorsed.pdf. Accessed on September 12, 2026.

[22] Liaqat Ali, Ghulam Mujtaba Malik, and Tanveer Ahmed Daudani, "Strategic Interventions to Combat Terrorism Financing in Pakistan: Challenges and Pathways," *Annals of Human and Social Sciences* vol. 6, no. 3, 2025, pp. 88-89, https://ojs.ahss.org.pk/journal/article/view/1020/1057. Accessed on September 11, 2026.

Centre for Aerospace Power and Strategic Studies

The Centre for Aerospace Power and Strategic Studies (CAPSS) is an independent, non-profit think tank that undertakes and promotes policy related research, study and discussion on defence and military issues, trends, and development in air power and space for civil and military purposes, as also related issues of national security. The Centre is headed by Air Marshal Nagesh Kapoor, SYSM PVSM, AVSM, VM (Retd).

Centre for Aerospace Power and Strategic Studies
P-284, Arjan Path, Subroto Park, New Delhi 110010
Tel: +91 11 25699130/32, Fax: +91 11 25682533

Editor: Dr Shalini Chawla e-mail: shaluchawla@yahoo.com
Formatting and Assistance: Ms Radhey Tambi, Ms Priyadarshini Baruah and Mr Rohit Singh

The views expressed in this brief are those of the author and not necessarily of the Centre or any other organisation.