About the Authors:

Kyrylo Bohdanets

Kyrylo is a Security Studies student at Leiden University, pursuing a BSc focused on global security challenges, governance, and risk management. His main interests include security policy, defence, intelligence, and the MENA region. He aims to contribute to developing effective strategies and institutions that enhance stability and resilience in complex security environments.

Nicole Siembieda

Nicole is a first-year graduate student pursuing Dual Master's Degrees in

International Security and Conflict, Security, and Development at Sciences Po Paris and King's College London. She also holds a Bachelor of Arts in International Studies from the University of Michigan. Her research experience includes an Undergraduate Research Fellowship with the Nam Center for Korean Studies. Nicole hopes to work in security studies or international relations when she graduates.

About the publication:

3 Main Points:

This brief addresses which counter-terrorism adaptations are necessary for European Union policymakers to address threats from ISIS 2.0, which has transitioned to a digital front, revealing gaps in the EU's existing response. Recommendations include enhanced collaboration among Member States, improved protection against terrorism financing, and the implementation of cognitive defence strategies.

Highlight Sentence:

"EU policymakers must adapt their current counter-terrorism strategy by expanding interstate collaboration and implementing cognitive defence to account for ISIS 2.0's new fronts."

Definition:

Cognitive defence is practised by protecting the minds of influential people and the general populace from propaganda that aims to change one's viewpoint on language, symbols, and ideas.

ISIS 2.0: Assessing the Evolving Threat and Policy Response in the European Union

Introduction

The defeat of the Islamic State of Iraq and Levant's (ISIS) territorial caliphate did not mark the end of the organisation itself. Since 2019, ISIS has become a decentralised network of regional affiliates operating across the Middle East and Africa, continuing to pose security challenges despite reduced political and international attention. Recent assessments by international and European security bodies indicate that this transformation has significant implications for contemporary counter-terrorism policy, with research highlighting the continued relevance of Jihadist networks to European security through foreign fighters, returnees, and transnational facilitation structures (Van Ginkel and Entenmann, 2016).

Despite these developments, much of Western policy continues to be shaped by the logic of territorial defeat. The collapse of the Islamic state project in Syria and Iraq during the battle of Baghuz Fawqani in 2019 has been widely interpreted as a strategic victory. This interpretation has been reinforced by policy narratives that have framed ISIS primarily as a defeated territorial actor. Early warnings emphasised that disengagement from Syria, as proposed by Trump in his first term, risked enabling "ISIS 2.0", defined less by territorial control and more by decentralised operational coordination across regions in the Middle East and Northern Africa (Crocker et al., 2018). Nevertheless, political discourse surrounding the group's apparent defeat contributed to the reduction of counter-terrorism engagement even as officials acknowledged the persistence of ISIS structures in the region (Katkov, 2017).

This brief, therefore, asks what counter-terrorism and intelligence adaptations are required from European Union (thereafter referred to as EU) actors to address ISIS's post-2019 trajectory across Europe, including all territories under EU jurisdiction. This paper argues that current EU counter-terrorism strategies do not adequately address ISIS's ideologically resilient threats and contemporary decentralised organisation, and thus it is highly advisable to implement heightened interagency

collaboration, protections against terrorist funding through cryptocurrency, and cognitive defence.

Organisational Evolution

Since the Global Coalition to Defeat ISIS's territorial win and the subsequent United States' major withdrawal of troops from Syria in 2019, the organisation has continued to pose a threat to EU states due to its capacity to recruit online, conduct disinformation campaigns, and carry out attacks, as seen increasingly in Sahel Africa (McCary, 2024). ISIS has also gained new territorial strongholds due to the security vacuum created by the fall of Asad's regime in Syria (Brennan, 2024). Despite this, the organisation largely now exists as a network, spreading its ideology and recruiting new members from non-conspicuous physical spaces in regional hotspots or through social media and online chatrooms, including Telegram and WhatsApp (Aksu et al., 2025). However, the EU counter-terrorism strategy fails to take into account ISIS's new network structure, focusing on border security and stabilisation of neighbouring states.

This disconnect reflects a broader conceptual problem in European counter-terrorism thinking, which continues to treat ISIS as a territorially bounded terrorist or insurgency organisation, despite its transformation into a decentralised network. Being able to differentiate between these terms is important because it influences the choice of tools, legal frameworks, and intelligence priorities for a given threat. Terrorism is often defined narrowly as "the intentional use of, or threat to use, violence against civilians or against civilian targets in order to attain political aims" (Ganor, 2002, p. 288). In contrast, Kilcullen (2009) conceptualises insurgency as a broader political struggle in which terrorism functions as one tactic among others, including territorial control and population mobilisation. Between 2014 and 2019, ISIS fit this insurgent model through sustained territorial governance in Iraq and Syria. Following the collapse of its caliphate, the group largely lost its territorial capacity, reverting to decentralised terrorism-based networked cells and ideological propagation. This shift from insurgency to decentralised terrorism is reflected in the

geographic pattern of ISIS's post-2019 activity, with the organisation concentrating its efforts within specific locations rather than pursuing territorial control.

Since 2019, ISIS has shifted from territorial control to a decentralised, network-based model, where it relies on autonomous cells and digital coordination rather than overt governance or sustained military presence (Ingram et al., 2020). For the EU, this model creates security risks, not only because Europe's digital infrastructure can be exploited for recruitment, financing, and remote communication, but also because decentralisation can create blind spots and exploit the legal fragmentation resulting from a lack of a universal term for 'terrorism' among EU member states. Thus, these security and legal gaps limit effective cross-border collaboration and create a need for an updated and coordinated EU counter-terrorism strategy.

Two Emerging Fronts

The contemporary jihadist terrorism threatening the EU is best understood as operating across two emerging and interconnected fronts. First, there is the digital front, where recruitment, radicalisation coordination, and financing increasingly occur online within EU territory. The second is the border and mobility front, where the exploitation of the EU's shared border system allows transnational movement, facilitation, and ISIS's operational resilience.

ISIS's digital front presents an evolving threat to the EU in several novel ways. For example, Europol reports that early-stage radicalisation, online exposure, and youth vulnerability are recurring features of recent jihadist cases in the EU, showing that enforcement approaches alone are insufficient (Europol, 2025). Social media allows recruitment to reach anyone in any place. Teenagers and young adults are targeted by online propaganda used by ISIS recruiters (Shtuni, 2025). Artificial intelligence, employed through algorithmic and automated digital propaganda, facilitates the indoctrination of people from within EU countries. The danger of this new form of recruitment can be exemplified through ISIS's "kill them wherever you find them" campaign, which encourages members to commit acts of jihadist violence at home

rather than in a territorial hotspot (Rubin, 2025). This type of rhetoric has inspired plots on the Paris Summer Olympic Games and the European Cup in Germany in 2024 (Mohamed, 2024). In addition to online propaganda and recruitment, the digital front has galvanised a new method of terrorism through cyberattacks, which cause ramifications for cybersecurity and cyber infrastructure from afar.

On the digital front, ISIS 2.0 utilises the internet to spread new forms of propaganda. This manifests itself as automated extremist content, intended for a specific audience that is determined by an algorithm (Corsaro, 2025). Jihadist extremist content can also emerge on the internet as deepfakes and chatbots, which create an illusion that the ideology is common in their community or nation (Corsaro, 2025). ISIS can be categorised as an adhocracy, which is an organisation that tends to emerge in environments that are ever-changing and require temporary teams to confront a specific issue (Ingram et al., 2020). Thus, ISIS's digital front constitutes a form of cognitive warfare, which targets the minds and behaviours of military targets, as the organisation can reach anyone who has access to the internet (*Cognitive Warfare - NATO's ACT,* 2023). To counter the adhocratic nature of ISIS 2.0, EU leaders must introduce cognitive security and cognitive defence, which is protecting the minds of policymakers, political elites, and the general populace (Hoffman, 2025).

Furthermore, ISIS 2.0's digital front presents new opportunities for terrorist funding. Post-9/11 financial regulatory laws blocked traditional paths for financing terrorism through anonymous Swiss bank accounts (Chandrasekhar, 2021). However, cryptocurrency, public fundraising, and financial fraud, particularly in dark web markets, have expanded the opportunities for funding terrorism (Elliptic, 2023). For example, ISIS 2.0 is able to crowdsource funds using cryptocurrency exchanges (Elliptic, 2023).

While the digital front enables ISIS 2.0 to radicalise, mobilise, and finance actors remotely, presenting novel challenges for EU counter-terrorism policy, it does not operate in isolation. Digital mobilisation is increasingly complemented by physical

movement across jurisdictions, logistical facilitation, and the leveraging of shared borders within the Schengen area. In particular, according to Europol (2025) reporting, there are documented cases of terrorists leveraging migration routes used by migrants and asylum seekers to enter or move within the EU. The EU's shared borders cause gaps in governance and jurisdiction for preventing terrorists from entering and existing within the EU, further demonstrating the need for a collective counter-terrorism policy at the EU level.

Policy Recommendations

ISIS 2.0 represents a dilemma for policymakers in the European Union: how can terrorism be prevented when counter-terrorism policy must go beyond traditional territorial defence? Policymakers in the EU need to understand this new manifestation of terrorism, as well as pinpoint responsibility for an issue that transcends the traditional understanding of borders. Although the EU has already taken action in this regard, current policies aimed at preventing the dissemination of content online do not fully capture the evolving nature of terrorism. Thus, the EU is advised to continue utilising the European Commission, Europol, and shared databases like Eurodac to implement a common policy framework to boost efficiency and effectiveness in countering terrorism within its borders but also adopt new policies to prevent and combat the emergence of new forms of terrorism in Europe.

First, border security should be reconceptualised to reflect the realities of the European Union's shared border system, the Schengen Zone. In a Schengen environment, counter-terrorism effectiveness depends on the ability to manage movement through better intelligence sharing and coordination between various law enforcement bodies. The EU TE-SAT 2025 shows that contemporary terrorists are transnational, shaped and facilitated by developments beyond the EU borders. Europol documents cases in which individuals involved in terrorist activities travelled across multiple EU jurisdictions, as well as exploited immigration pathways meant for asylum seekers and migrants before being arrested (Europol, 2025). Rather than reintroducing systematic internal border checks, the European counter-terrorism

stance should prioritise the consistent use and interoperability of existing EU information systems, real-time information sharing across member states, and ensuring that alerts related to suspected extremist activity are shared across jurisdictions. The European Commission could increase collaboration by using existing interagency sharing tools like Eurodac to coordinate counter-terrorism initiatives. These policies would be highly feasible, as similar policies have passed before and have a high impact (Bakowski, 2025). This also supports greater investment in early-stage intervention and prevention-oriented measures that address online radicalisation and social vulnerabilities before they develop into security threats. Practical models already exist, such as EXIT Germany and Denmark's Aarhus model, which combine early identification counselling and community-based disengagement. These approaches could be scaled at the EU level through cooperation between member states.

As for financial regulation, this paper recommends several anti-money laundering and combating the financing of terrorism (AML/CFT) best practices for the EU. The EU should continue to partner with private sector AML/CFT efforts within financial institutions, which have strict regulations on anonymous account holders (FATF Report, 2023). In the context of crowdsourcing, this could be implemented through cooperation with platforms such as GoFundMe or PayPal, whose teams know the vulnerabilities of their respective platforms (FATF Report, 2023). Furthermore, the current EU regulations on crowdsourcing permit member states to have divergent national regulations and do not specify AML/CFT actions that companies must practice (EUR-Lex, 2020). This paper recommends enacting policy at the EU level, which specifies AML/CFT guidelines that crowdsourcing websites must implement for flagging tactics for suspicious transactions (FATF Report, 2023).

Furthermore, this paper recommends that European Union leaders implement counter-terrorism practices that go beyond operational measures. Currently, the EU's cognitive defence relies on task forces and planning, resulting in a defence strategy that is reactive rather than strategic (Catena et al., 2025). While cognitive deterrence

is highly impactful since it stops terrorists at their origins, it has relatively low feasibility due to the complexity of opportunities and motivations for terrorists. Implementation could manifest itself as civilian programmes that provide media literacy education, implementing cognitive security assessments as part of threat evaluations, and adding more resilient data privacy laws to the EU data governance infrastructure (Catena et al., 2025). For example, if there is a hybrid threat to EU infrastructure, NATO or EU Intelligence and Situation Centre should be required to conduct an assessment of if and how cognitive warfare was used amid the threat. Additionally, the EU could implement cognitive deterrence and defence by expanding intelligence capabilities to analyse biases and thought patterns in terrorist behaviour (Wasson and Bluesteen, 2017). In practice, the EU could use the conclusions gathered from an analysis of biases and behavioural patterns to manipulate the perception of the value or accessibility of a target. For example, the EU could use social media communication or physical deterrents like cameras and armed guards to convey the cost and perceived difficulty of attacking a given target (Watson et al., 2017). Success for these policy recommendations are difficult to measure but could be quantified by the number of civilians educated on cognitive biases or attacks directly foiled due to a lack of accessible information.

References

Aksu, S. O., & Cubukcu, G. S. (2025, September 23). *ISIS's transition and the interplay of online and face-to-face recruitment.* Small Wars Journal by Arizona State University. https://smallwarsjournal.com/2025/09/23/isis-transition-online-and-face-to-face-recruitment/

Brennan D. (2024.). *Syria post-Assad power vacuum poses unexpected problems for Middle East, US.* ABC News. Retrieved January 17, 2026, from

https://abcnews.go.com/International/syria-post-assad-power-vacuum-poses-unexpected-problems/story?id=116592032

Catena B., Ditrych O., & Kovalcikova N. (2025, October 7). *Smoke and mirrors: Building EU resilience against manipulation through cognitive security | European Union Institute for Security Studies*. https://www.iss.europa.eu/publications/briefs/smoke-and-mirrors-building-eu-resilience-against-manipulation-through-cognitive

Chandrasekhar, A. (2021, September 8). *How the "War on Terror" exposed compliance gaps in Swiss companies.* SWI Swissinfo.ch. https://www.swissinfo.ch/eng/business/how-the-war-on-terror-exposed-compliance-gaps-in-swiss-companies/46915746

Cognitive Warfare - NATO's ACT. (2023, December 12). NATO's ACT. https://www.act.nato.int/activities/cognitive-warfare/

Corsaro, A. (2025, August 11). *ISIS 2025: The Silent Resurgence - HSToday*. HSToday. https://www.hstoday.us/featured/isis-2025-the-silent-resurgence/

Council of Europe. (2023, February 9). Council of Europe adopts new counter-terrorism strategy for 2023-2027. *Counter-terrorism*. https://www.coe.int/en/web/counter-terrorism/-/council-of-europe-adopts-new-counter-terrorism-strategy-for-2023-2027

Crocker, A. R., O'Hanlon, M. E., & Baev, P. K. (2018, April 7). *How do we prevent ISIS 2.0? Withdrawing from Syria is not the answer.* Brookings. https://www.brookings.edu/articles/how-do-we-prevent-isis-2-0-withdrawing-from-syria-is-not-the-answer/

Elliptic. (2023). *How terrorist groups are exploiting crypto to raise funds and evade detection.* Retrieved January 17, 2026, from

https://www.elliptic.co/blog/how-terrorist-organizations-are-exploiting-crypto-to-raise-funds-and-evade-detection

Europol. (2025). European Union Terrorism Situation and Trend Report 2025. Europol. https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2025-eu-te-sat

FATF Report: Crowdfunding for Terrorism Funding. (2023). https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf

Ganor, B. (2002). *Defining terrorism: Is one man's terrorist another man's freedom fighter?* Police Practice and Research, 3(4), 287–304. https://doi.org/10.1080/1561426022000032060

Hoffman F. (2025). Assessing "Cognitive Warfare." (n.d.). *HSToday.* Retrieved January 18, 2026, from https://www.hstoday.us/subject-matter-areas/counterterrorism/assessing-cognitive-warfare/

Ingram, H., Whiteside, C., & Winter, C. (2020). *Global war.* In Oxford University Press eBooks (pp. 177–198). https://doi.org/10.1093/oso/9780197501436.003.0009

Katkov, M. (2017, November 17). *Pentagon says it's staying in Syria, even though ISIS appears defeated.* NPR. https://www.npr.org/sections/parallels/2017/11/17/564620907/pentagon-says-its-staying-in-syria-even-though-isis-appears-defeated

Legal framework of EU data protection—European Commission. (n.d.). Retrieved January 18, 2026, from https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en

McCary, I. (2024, March 21). *The Islamic State Five Years Later: Persistent Threats, U.S. Options | The Washington Institute*. Www.washingtoninstitute.org. https://www.washingtoninstitute.org/policy-analysis/islamic-state-five-years-later-persistent-threats-us-options

Mohamed. (2024, April 26). IntelBrief: Islamic State Threat to the West and New Campaign Targeting Sporting Events. *The Soufan Center*. https://thesoufancenter.org/intelbrief-2024-april-26/

Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European Crowdfunding Service Providers for Business, and Amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937 (Text with EEA Relevance), 347 OJ L (2020). http://data.europa.eu/eli/reg/2020/1503/oj

Rubin, A. J. (2025, January 4). *How the Islamic State radicalizes people today.* The New York Times. https://www.nytimes.com/2025/01/04/world/middleeast/isis-propaganda-new-orleans-attack.html

Shtuni, A. (2025). *The Islamic State in 2025: an Evolving Threat Facing a Waning Global Response*. International Centre for Counter-Terrorism - ICCT. https://icct.nl/publication/islamic-state-2025-evolving-threat-facing-waning-global-response

Wasson, J., & Bluesteen, C. (2017, March 30). *Cognitive defense: Influencing the target choices of less sophisticated threat actors.* Homeland Security Affairs. https://www.hsaj.org/articles/13770

Van Ginkel, B., & Entenmann, E. (Eds.). (2016). *The foreign fighters phenomenon in the European Union: Profiles, threats & policies* (ICCT Research Paper). The International Centre for Counter-Terrorism – The Hague.