



COMBATING TERRORISM CENTER AT WEST POINT

CTCSENTINEL

OBJECTIVE · RELEVANT · RIGOROUS | JUNE 2026 · VOLUME 19, ISSUE 6



FEATURE ARTICLE

Standing With Iran

Examining the integrated combat performance of
Iran-backed Iraqi militias during Operation Epic Fury

MICHAEL KNIGHTS, ALEX ALMEIDA, AND CRISPIN SMITH

A VIEW FROM THE CT FOXHOLE

Brigadier General Matthew Ross

DIRECTOR, JOINT INTERAGENCY
TASK FORCE 401

Contents

FEATURE ARTICLE

1 Standing With Iran: The Integrated Combat Performance of Iraqi Militias During Operation Epic Fury

MICHAEL KNIGHTS, ALEX ALMEIDA, AND CRISPIN SMITH

INTERVIEW

30 A View from CT Foxhole: Brigadier General Matthew Ross, Director, JIATF-401

SEAN MORROW AND DON RASSLER

ANALYSIS

36 Remotely Coerced Violence: 764, The Com Network, and the Hybridization of Threats

MARC-ANDRÉ ARGENTINO AND ANGUS LINDSAY

FROM THE EDITORS

In our cover article this month, Michael Knights, Alex Almeida, and Crispin Smith examine the “unprecedented” involvement of Iran-backed militias in Iraq (*muqawama*) in the current conflict between the United States and Iran. “The current Iran/U.S.-Israel war has exposed a far broader and deeper pattern of PMF [Popular Mobilization Forces] complicity in terrorist actions against Iraqis, U.S. persons, and nations in the Arab world and Europe,” they find. While the Iranian proxy Lebanese Hezbollah recovers from significant losses and the Iran-backed Houthis stay largely out of the current fight, “the 2026 conflict has shown a different side of the Iraqi *muqawama*,” the authors write, “a tougher, more risk-acceptant side that has seen the Iraqi groups claim to have undertaken their most intensive ever series of attacks against the United States, Kurdistan, and the Gulf States.”

Our interview is with Brigadier General Matthew Ross, the director of Joint Interagency Task Force 401, which is tasked with consolidating and enhancing the U.S. military’s response to the drone threat at home and abroad. “I do think that drones are changing the character of modern combat, but they’re not changing the nature of combat,” BG Ross remarks. “Victory still belongs to those who adapt fastest, those who strike the hardest and endure the longest, and so countering drones is key to force protection, mission success, and survival on the modern battlefield.”

Finally, Marc-André Argentino and Angus Lindsay situate 764 and The Com Network within the broader nihilistic violent extremist landscape. Drawing on case studies and an arrest dataset of 295 Com Network-linked offenders across 33 countries, they explore how “764 and adjacent groups combine sadistic online exploitation, cybercrime, self-directed violence, animal abuse, school-violence threats, and terrorist or violent-extremist conduct.” They find that “what unifies these cases is not a shared ideology but a shared ecosystem, a shared status economy in which standing is earned by producing and circulating harm, a shared behavioral orientation in anomie, nihilism, and misanthropy, and a shared reliance on sadistic online exploitation and coercive control as the means through which that harm is enacted.”

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

CTCSENTINEL

Editors-in-Chief

Don Ressler

Kristina Hummel

EDITORIAL BOARD

Colonel Heidi Demarest, Ph.D.

Department Head

Dept. of Social Sciences (West Point)

Colonel Sean Morrow, Ph.D.

Director, CTC

Brian Dodwell

Executive Director, CTC

CONTACT

Combating Terrorism Center

U.S. Military Academy

752 Thayer Road, Mahan Hall

West Point, NY 10996

Phone: (845) 938-8495

Email: ctc@westpoint.edu

Web: www.ctc.westpoint.edu/ctc-sentinel/

SUBMISSIONS

The *CTC Sentinel* welcomes submissions.

Contact us at ctc@westpoint.edu.

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

Cover: A member of the Iraqi Hashd Shaabi (Popular Mobilization Forces - PMF) waves an Iranian national flag during a pro-government rally in downtown Tehran, Iran, on April 6, 2026. (Morteza Nikoubazl/NurPhoto via Getty Images)

Standing With Iran: The Integrated Combat Performance of Iraqi Militias During Operation Epic Fury

By Michael Knights, Alex Almeida, and Crispin Smith

On June 2, 2026, two U.S.-designated foreign terrorist organizations in Iraq—Asaib Ahl al-Haq and Kataib Al-Imam Ali—announced their intention to begin the handover of their heavy weapons to the Iraqi state. Their statements came hot on the heels of the most intense military campaign fought by the Iran-backed militias (the ‘*muqawama*’) since the withdrawal of U.S. combat forces from the country in 2011. This campaign witnessed unprecedented military integration between Iran’s Islamic Revolution Guard Corps and hundreds of Iraqi collaborators spread across at least 36 major units in Iraq’s state-run Popular Mobilization Forces (PMF). Iraqi militia groups targeted U.S. bases, Jordan and the Gulf States, and Iraqi energy sites, sustaining an operational tempo that was an order of magnitude higher than in any previous conflict. The unprecedented military integration of the *muqawama*, including the capture of large swathes of Iraq’s state-funded security forces by militias and Iran’s Islamic Revolutionary Guard Corps, poses serious risks for Iraq’s stability, for U.S.-Iraq relations, and complicates the deterrence, sanctioning, and potential disarmament of Iraqi *muqawama*.

This study is the ninth in a series of *CTC Sentinel* articles since 2019 that have detailed the ongoing rise of the self-styled, Tehran-backed resistance (*muqawama*) factions in Iraq, and of Iran’s growing dominance within the Iraqi state. While more recent pieces since 2023 have focused on militia ‘capture’ of non-military institutions of the Iraqi state (political,¹ oil,² telecommunications³), this study will revisit the original focus on accelerating militia capture of the security sector and the acute security threat posed by Iran-backed militias in Iraq to Iraqi citizens, the Iraqi government, the United States and other international presence in Iraq, and to the broader region, notably the Gulf States.⁴

To recap this body of work briefly, the first was the August 2019 *CTC Sentinel* report⁵ on the growing geographic control and government funding of the Popular Mobilization Forces (PMF), Iraq’s equivalent of the Iranian Islamic Revolutionary Guard Corps (IRGC).⁶ This study, “Iran’s Expanding Militia Army in Iraq,” showed how a new parallel military had been created in Iraq during the opening days of the counter-Islamic State war in 2014 by Iran’s closest militia partners in the country, increasing the size of those Iran-backed militia forces 15-fold.⁷ The piece built on Knights’ 2017 identification of a pan-Shi’a PMF “colonization zone,” where the predominately Shiite PMF had established long-term garrison presence and economic value extraction systems in majority-Sunni

areas.⁸ “Iran’s Expanding Militia Army in Iraq” was the first study^a to fully map out PMF areas of control across Iraq. A book-length study of the PMF then followed⁹ (co-authored with Hamdi Malik and Aymenn al-Tamimi) that examined the dominant roles of the IRGC-founded Badr and Kataib Hezbollah in the leadership and organization of the PMF.

Four more *CTC Sentinel* studies followed, digging deeper into the military organization and activities of the Iraqi *muqawama*. In February 2020’s “Soleimani is Dead,” the key research question was why the Iraqi *muqawama* chose to restart kinetic operations against the U.S. diplomatic and military advisor presence in Iraq for the first time since the end of the post-2003 U.S. military mission in 2011.¹⁰ Later in November 2020, “Back Into the Shadows,” discussed how Kataib Hezbollah emerged from its “incubator,” the Badr movement, and became the premier IRGC partner force in Iraq, and how KH was positioning to be the coordinator of a strata of Iran-backed militias within the PMF that was increasingly focused on projecting power via missile bases in Iraq and Syria.¹¹

In the 2021 *CTC Sentinel* article “Discordance in the Iran Threat Network in Iraq,” an enlarged author team (including Crispin Smith and Hamdi Malik) described in detail how the IRGC Quds Force (IRGC-QF) under its new commander, Brigadier General

a Credit must always be given to the Institute for the Study of War’s (ISW’s) Order of Battle study for the Iraqi security forces and the Hashd, published in December 2017. This was the first study in open source to delve deeply into the Hashd institutional directorates and the PMF groups with assigned brigade numbers. The first detailed description of these offices came in the Institute for the Study of War report in 2017. See Jesse Rose Dury-Agri, Omer Kassim, and Patrick Martin, “Iraqi Security Forces and Popular Mobilization Forces – Order of Battle,” Institute for the Study of War, December 2017.

Dr. Michael Knights is the Chief Product Officer at strategic advisory Horizon Engage. He is also an Adjunct Fellow with the Washington Institute for Near East Policy, where he co-founded the Militia Spotlight platform. X: @mikeknightsiraq

Alex Almeida is the Research Director for Security Services at Horizon Engage. He is the co-author of Back to Basics: U.S.-Iraq Security Cooperation in the Post-Combat Era, Washington Institute for Near East Policy, 2020. X: @AlexAlmeida2020

Crispin Smith is an attorney based in Washington, D.C. His research focuses on international law and the law of armed conflict, as well as operational issues related to irregular warfare, information operations, and lawfare. Previously, he co-founded the Militia Spotlight platform.

Esmail Qaani, had developed a military coordination forum (the *tansiqiyah*)^b by the end of 2020 that could deconflict proprietary single-group *muqawama* military efforts and also employ new IRGC-QF-directed “teaming” efforts that drew upon the most dedicated anti-U.S. militants from across the PMF personnel base.¹² While December 2023’s article “Iraq’s New Regime Change” was more focused on militia state capture of non-military organs,¹³ it included a section on IRGC-QF’s ongoing efforts to coordinate Iraqi militia attacks against the United States and Israel after the October 7 massacres.¹⁴

Structure of the Study

This study will take forward the chronology of the military evolution of the Tehran-backed *muqawama* factions in Iraq by looking in depth at Iraqi militia military performance in the 2026 war between Iran and the U.S.-Israel coalition. The article draws upon the same kind of detailed interview process with U.S. and Iraqi subjects that underpinned the prior *CTC Sentinel* studies referenced above, including detailed attack data provided by Knights’ on-the-ground contacts in Iraq.

Such interviews are undertaken within the context of a broader investigative effort that draws upon deep, existing datasets and an author team with 40 years of consecutive, overlapping experience monitoring the Iraqi militia scene, including all of the post-2014 period in which the PMF has existed. The geolocated incident database maintained by two of the authors (Knights and Almeida) is a key source of information, including two decades of geospatial place-marking of militia attacks, militia bases, security force locations, and other contextual information. Extensive, judicious use was made of *muqawama* propaganda materials gathered on platforms including Telegram,¹⁵ including close analysis of *muqawama* attack claims through posted statements, purported launch footage, and propaganda videos.^c The article also builds upon the numerous relevant entries and group profiles in the Militia Spotlight blog, which two of the authors (Knights and

“The overarching theme of this article and its component parts is that the current Iran/U.S.-Israel war has exposed a far broader and deeper pattern of PMF complicity in terrorist actions against Iraqis, U.S. persons, and nations in the Arab world and Europe.”

Smith) founded and ran.^d This, plus open source image collection and verification, allowed for the creation of a dataset of weapons intelligence images related to *muqawama* attacks in the current war. All these layers have combined to create this article, which is a synthesized research product based on feeds from human intelligence, social media intelligence, weapons intelligence, and open-source intelligence.^e

To begin with, the study provides key context and recaps the historic playbook of *muqawama* involvement in military conflicts involving Iran. This shows an underwhelming record of Iraqi contribution until this current war. The article then proceeds and is organized in three parts. In Part I, the article timelines five observed phases of Iraqi militia involvement in the 2026 war, a conflict that witnessed unprecedented militia mobilization of the Iraqi state’s PMF personnel, bases, and military materiel in support of Iranian regime objectives. In Part II, the article explores the four fronts in the Iraqi *muqawama* war effort—and the vital fifth front of information warfare (deception and psyops) and lawfare. Part III builds off of the article’s prior two parts and more thoroughly examines the support and assistance that Iraqi Popular Mobilization Forces provided to Iran’s war effort. It identifies PMF units and locations that are demonstrably linked to the Iran threat network, with a special focus on the Badr Organization, which functioned, in effect, as a part of the IRGC order of battle (from which it was born in the 1980s).¹⁶ The concluding section highlights emerging issues and outstanding questions for policymakers and intelligence analysts to pay attention to.

The overarching theme of this article and its component parts is that the current Iran/U.S.-Israel war has exposed a far broader and deeper pattern of PMF complicity in terrorist actions against Iraqis, U.S. persons, and nations in the Arab world and Europe. Thirty-six PMF units, about half the formations of the PMF, have demonstrably provided material support to U.S.-designated foreign terrorist organizations such as the IRGC, IRGC-QF, KH, Kataib

b As of January 2026, the *tansiqiyah*’s Telegram channel claimed that it comprised KSS, Kata’ib Karbala, HAAA, HaN, AAH, and KH. This roughly corresponds, in the view of the authors, with the core of the *muqawama* groups that participated in attacks against the United States during the 2026 conflict. Similarly, on June 4, 2026, an influential KH spokesman released a statement noting that “[t]he five factions of the Islamic Resistance (*muqawama al-islamiyya*), in addition to the Karbala Brigades, will remain cohesive and will carry out their tasks as long as there is occupation [of Iraq], violation of its airspace, and usurpation of political decision-making.” The authors assess that the “five factions” refer to KSS, HAAA, HaN, AAH, and KH.

c Based on the author team’s decade-spanning work in this space, the authors assess that claimed attacks and Telegram commentary from select media outlets are worth close analysis as markers of intergroup dynamics, overall strategy, and trends in military activity. It is almost certain that some Telegram material is deliberately misleading, designed to obfuscate attribution, attack origin, and group strengths and size. Nevertheless, militias have been historically reluctant to be caught in a lie: Rival groups have openly mocked those seen not pulling their weight or faking attacks. Meanwhile, there has been a historic correlation between militia attacks claimed on Telegram and proven attacks, albeit during periods where attacks were less frequent and of lower volume. The authors have documented these trends previously in Michael Knights, Crispin Smith, and Hamdi Malik, “Discordance in the Iran Threat Network in Iraq: Militia Competition and Rivalry,” *CTC Sentinel* 14:8 (2021). More recently, a militia spokesman framed the importance of accurate claims: “The Security Media Cell must not rush to issue statements; it should ascertain the facts before making any declaration that might aim to level accusations against the Resistance and demonize it, in line with the objectives of the enemy.” Telegram post by Abu Mahdi al-Jaafari, March 21, 2026.

d Militia Spotlight’s online blog and group profiles were established to track this process in detail and produce evidentiary building blocks, using legal standards of proof and certainty. The project collects militia statements in Arabic and other languages, archives evidence that risks being taken offline at a later point, and uses a data fusion process to synthesize information and analyze trends. The Militia Spotlight blog is at <https://www.washingtoninstitute.org/policy-analysis/series/militia-spotlight> and the Militia Spotlight profiles page is at <https://www.washingtoninstitute.org/policy-analysis/series/militia-spotlight-profiles>

e Each type of feed often makes the others more useful. For instance, ground-sourced human intelligence on a launch from a specific area at a specific time can be combined with claim video data and with target impact data to produce findings that would have been impossible to glean from any one source type alone.

Sayyid al-Shuhada (KSS), Harakat al-Nujaba, Harakat Ansar Allah al-Awfiya (HAAA), Asaib Ahl al-Haq (AAH), Kataib al-Imam Ali (KIA),^f as well as the Badr Organization and many smaller undesignated groups. Major PMF forces also deployed inside Iran during the war (see Phases and Badr sections below),^g without formal Iraqi government approval, effectively setting their own foreign and security policy independently of the Iraqi state—the country that financially supports the PMF and in direct violation of Iraq’s constitution and laws.^h

In the view of the author team, this suggests that counter-militia reforms in Iraq sought by the United States need to reflect this broader and deeper Iranian and Iraqi *muqawama* penetration and instrumentalization of the PMF. Large swathes of the PMF have turned into a parallel military that undertook to fight its own war with the United States—a war that other parts of Iraq’s government did not declare and is not a formal party to (but may nevertheless

bear some legal responsibility for).ⁱ This should be of strong interest to any U.S. agency charged with monitoring the implementation of security sector reform in Iraq or executing the maximum pressure effort on Iran’s regime, most recently re-energized in February 2025 by the United States via National Security Presidential Memorandum 2 (NSPM-2).^{17j}

Context: Recapping the Historic Playbook of Iraqi Militias in Recent Wars Involving Iran

Until the present war, the Iraqi *muqawama* arguably had a poor record as a military force. The start had been promising in the 1980s: The Badr Corps had been formed from Iraqi Shiite exiles and prisoners of war and had fought in the Iran-Iraq War as a light infantry division within the IRGC order of battle.¹⁸ In the 1990s, Badr had supported a low-level, cross-border insurgency against Saddam Hussein’s military from bases in western Iran.^k In 2003, Badr entered Iraq as a military division via the Iranian border at the same time that U.S. forces were racing toward Baghdad.¹⁹ After Saddam’s fall, Badr saw many of its fighters folded within the U.S.-backed new Iraqi military, where they *mostly* fought alongside, instead of against, U.S. soldiers.²⁰

Other Badr militants (self-styled *muqawama*) instead fought an insurgency against American and British forces in Iraq prior to 2011,²¹ but they represented such a small proportion that they were termed ‘special groups’ and were dealt with as a terrorist threat operating with the connivance of some parts of the Iraqi government and Shiite body politic, but not all or even most.²² Prior to 2011, Iraqi Shiite militants had not deployed to fight in Iran’s conflicts outside Iraq, and were not regularly attacking the Gulf States, the United States, or Israel in support of Iran’s regional

f Broadly, the United States Treasury or State Department can designate entities as “Specially Designated Global Terrorists” (SDGTs) under the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. § 1701 et seq., and Executive Order 13224 (as subsequently amended). This causes designated entities to be added to the Office of Foreign Assets Control’s list of Specially Designated Nationals and Blocked Persons (SDN List) and subject to certain economic sanctions. Entities may also be designated a “Foreign Terrorist Organization” (FTO) by the Secretary of State under the Immigration and Nationality Act (INA), also adding the entity to the SDN List while criminalizing those providing material support or resources to it (18 U.S.C. § 2339B). The core members of the *muqawama* are all subject to U.S. designation: KH, AAH, HaN, KSS, KIA, and HAAA are each designated as both FTOs and SDGTs. The IRGC (along with various sub-components) is also designated both as an FTO and SDGT, in addition to being subject to economic sanctions under various other programs. See generally, “Office of Foreign Assets Control’s Specially Designated Nationals and Blocked Persons List,” U.S. Department of the Treasury.

g The claim that significant numbers of PMF forces controlled by *muqawama* factions entered Iran is discussed at various points in the study and draws upon both open-source evidence (social media imagery during the war of PMF forces in traffic jams at the border crossing points between Iran and Iraq) and interview data (gathered by Knights) from a range of Iraqi contacts in a position to identify forces crossing from Iraq into Iran. The phenomenon of PMF fighters taking part in foreign wars without government approval is well-evidenced in the case of Syria already. For the earliest substantive work on this issue, see Phillip Smyth, “The Shiite Jihad in Syria and Its Regional Effects,” Washington Institute for Near East Policy, February 2, 2015. Then read the ISW report to gain detailed insight into the unauthorized transnational operations of numerous PMF units in 2014-2017: Dury-Agri, Kassim, and Martin, “Iraqi Security Forces and Popular Mobilization Forces – Order of Battle.” The phenomenon of PMF fighters entering Iran with the rationale of providing humanitarian support, while not demonstrating any prime ministerial authorization of such actions, is also documented. For instance, see references to the PMF deployment in Iran in 2019 in Golnaz Esfandiari, “Iraqis To The Rescue? Iranians Wary Of Paramilitary Forces Sent For ‘Flood Relief’ Efforts,” RFE/RL, April 16, 2019. Thus, while the deployment of large numbers of PMF forces into Iran is significant and may surprise some readers, it is not a controversial claim, and more of an underdiscussed ‘open secret’ regarding how the PMF operates as a transnational actor.

h Under Iraq’s constitution and laws, the prime minister is the commander in chief of the armed forces. No armed group may legally exist outside of the framework of the armed forces, and the laws governing the PMF explicitly place the formation under the prime minister’s authority – though in practice, PMF elements have frequently ignored this chain of command. See, for example, Crispin Smith, “Servants of Two Masters: the Risks Inherent in Iraq’s Hashd al-Shaabi Legislation,” *NYU Journal of International Law and Politics* 52:1 (2019).

i Iraq likely bears legal responsibility for some of the actions of the *muqawama* through the international law of state responsibility, either because factions have been formally adopted as official government entities integrated into the Iraqi state through PMF legislation, or due to Iraq’s failure to exercise due diligence in preventing attacks from its territory. For a discussion of Iraqi responsibility for elements of the *muqawama*, see Smith, “Servants of Two Masters.” See also Crispin Smith, “Iraq’s Legal Responsibility for Militia Attacks on U.S. Forces: Paths Forward,” *Just Security*, March 10, 2021.

j NSPM-2 directs U.S. officials to impose “maximum pressure” on Iran to compel it to abandon its nuclear program and support for terrorist groups while directing the imposition and enforcement of more stringent sanctions, the pursuit of Iran’s diplomatic isolation, and taking legal steps against Iranian activities inside the United States.

k Badr operated a network comprised of three ‘axes’ that smuggled firearms, 107mm and 122mm rockets, and other weapons, including advanced Explosively Formed Penetrator (EFP) roadside bombs into Iraq in the late 1990s and early 2000s. Many of the same border crossings, smuggling routes, and in some cases even the same cast of veteran Badr operators were reactivated ahead of the recent conflict, reprising their 1990s role as logisticians for the IRGC-QF. For a comprehensive review synthesizing material from the declassified Saddam-era Harmony documents, see Joseph Felter and Brian Fishman, *Iranian Strategy in Iraq: Politics and “Other Means”* (West Point, NY: Combating Terrorism Center, 2008).

policy of ‘resisting’ these states.^l

The Iraqi *muqawama* began to take on broader regional military tasks from 2011 onward, driven by opportunities created by the Arab Spring, the start of the Syrian civil war, and the withdrawal of U.S. combat forces from Iraq.²³ Iraqi *muqawama* bases became sanctuaries and training grounds for Gulf Shiite militants from Bahrain and Saudi Arabia in the low-level terrorist campaigns that Iran supported after the Arab Spring protests in those countries.²⁴ The *muqawama* quickly refocused its most restless and aggressive IRGC-supported commanders and forces on providing a foreign legion of Iraqi Shiites to support the Assad regime and Iranian policy in Syria.²⁵ (Iraq’s prime minister and parliament, the sole constitutional authorities allowed to command forces and declare war, did not authorize this decades-spanning military mission.²⁶) Within Iraq, the 2014 formation of the PMF (under the leadership of U.S.-designated terrorists)²⁷ in theory folded most of the *muqawama* under an Iraqi state umbrella, but this did not restrict the ability of Iraqi fighters to take part in foreign wars en masse.²⁸

By 2017, with the Islamic State territorially defeated, the Iraqi *muqawama* began to turn back toward anti-U.S. militancy.^m This coincided with—and perhaps was hastened by—the post-2017 U.S. policy of applying “maximum pressure” to Iran.²⁹ In 2017-2019, shadowy, ill-defined groups of Iraqi *muqawama* were threatening anti-U.S. and anti-Gulf actions³⁰ and by May 2019 were undertaking counter-pressure actions on Iran’s behalf against U.S. partners in the Gulf, demonstrating that U.S. pressure on Iran’s oil industry would be met with Iraqi explosive drone attacks on Saudi Arabia oil export infrastructure.ⁿ When major protests against Iran and its partners took place in Lebanon, Iraq, and then Iran itself in 2019, the Iraqi *muqawama* may have interpreted this as a deliberate U.S. and Israeli effort to overthrow the Iranian government, Lebanese

Hezbollah, and the militia-backed government in Iraq.^o The January 3, 2020, U.S. killing of IRGC-QF commander Qassem Soleimani and Iraq’s senior *muqawama* leader Abu Mahdi al-Muhandis energized years of *muqawama* revenge attacks, compounding the pre-existing militant effort to compel the removal of all U.S. forces from Iraq.³¹

Iraqi Underperformance in Iran Threat Network Conflicts

Yet, in the assessment of the author team, for all the bluster, the Iraqi *muqawama*’s military bark proved to be way worse than its bite in 2020-2025. In 2020-2023, as *CTC Sentinel* has chronicled in detail, the Iraqi *muqawama* were rebuilding themselves after the loss of Soleimani and al-Muhandis, but they never notably avenged their deaths³² and only tentatively attacked U.S. forces in Iraq and Syria. Even these attacks were usually undertaken from behind the cover of “façade” online brands (which the authors have previously termed “façade groups”³³) used to claim attacks—an effort to derive some intra- and inter-group credit, while veiling the exact identity of the attacking group to external parties. Prior to 2023, the Iraqi *muqawama* did not contribute to the ‘Axis of Resistance’ struggle against Israel, even during the major military crisis in Gaza in March 2021.^p They were quite easily deterred from continuing their short-lived attacks on Turkish bases in Iraq in 2022 after Turkish retaliation struck *muqawama* sites in northern Iraq.³⁴

It was only after the October 7, 2023, massacres in Israel that the Iraqi *muqawama* sought to mount a high-tempo, sustained military campaign against the U.S. presence in Iraq and against Israel. First, the Iraqi militias focused on their near enemy: the U.S. bases in Iraq and Syria. The tempo of Iraq-launched attacks against U.S. bases in Iraq and Syria achieved a metronomic-like cadence of regularity that had never been seen before,³⁵ but the Iraqi groups nonetheless proved fragile when threatened by painful reprisals.³⁶ From October 2023 until February 2024, the Iraqi *muqawama* mounted 197 strikes (an average of 1.75 strikes per day) on U.S. bases in Iraq, Syria, and Jordan³⁷—a very high tempo compared to the 0.2 attacks per day reported in 2020-2022.³⁸ But this new level of effort came to a halt and the more tentative approach returned as soon as the U.S. mounted a trio of painful leadership strikes on *muqawama* commanders between December 2023 and February 2024.³⁹

The Iraqi *muqawama* then switched its main target to Israel, launching 157 long-ranged attacks (at a rate of 0.67 per day) on

l One small deviant case study was the Arab League Summit in Baghdad in March 2012. In 2011-2012, one of the authors (Knights) was leading threat analytic teams in Iraq and watching closely for signs that the *muqawama* would turn against other types of targets once the U.S. military had drawn down completely. Coming after the Arab Spring Shi`a uprisings were put down in Bahrain, the Arab League Summit, which was held in Baghdad on March 29, 2012, was opposed by some *muqawama* cells, resulting in the ‘not welcome’ mat being rolled out in the form of three rocket attacks on government sites in Baghdad during the summit. “Rocket explodes as Baghdad Arab summit begins: Source,” Reuters, March 29, 2012.

m In October 2017, the *muqawama* killed their first U.S. soldier since U.S. military withdrawal in 2011. One of the authors (Knights) had always assessed the October 1, 2017, roadside-bombing murder of U.S. Army Private First Class Alexander Missildine as a *muqawama* operation. This was confirmed by Ashab al-Kahf on May 18, 2023. See Michael Knights and Hamdi Malik, “Ashab al-Kahf Claims Six-Year-Old Unsolved Murder of U.S. Soldier,” Militia Spotlight, Washington Institute for Near East Policy, May 18, 2023.

n In May 2019, a video emerged claiming the establishment of the so-called Free Revolutionaries Front, which featured several individuals with blurred faces but set against the flags of the Hashd and multiple PMF factions: specifically, Liwa al-Tauf, Asaib Ahl al-Haq, Saraya Ashura, Saraya Talia al-Khurasani, Kataib Sayyid al-Shuhada, Kataib Jund al-Imam, the Badr Organization, Kataib Hezbollah, Kataib al-Imam Ali, and Saraya al-Salam. In the video, the speaker declared the factions’ unity to confront the U.S. presence and called on Iraqis to join the front.

o It is an open question to what extent the *muqawama* and the Iranian regime truly believed that the 2019 protests were foreign-induced or purely domestic or some combination. What can be said with certainty is that the protests in Iran and Iraq in 2019 were portrayed as foreign-backed. In November 2019, a range of regime figures – from Supreme Leader Ali Khamenei to Iran’s Ministry of Intelligence of Security to President Hassan Rouhani – accused protestors of acting with the training, assistance, and direction of foreign intelligence services. For an example, see “Iran Supreme Leader calls recent mass protests a ‘conspiracy,’” Associated Press, November 27, 2019. What the Militia Spotlight team detected from close monitoring of social media inside Iraq was a visceral *muqawama* campaign of blaming the protests on foreign-backed ‘jokers’ (Jawkara, Ganga al-Jawkara) (the *muqawama* phrase) that sparked a wave of killings lasting two years. For a good description of this campaign, see Ela Khaled and Inna Rudolf, “The Iraqi Politics of Memory and Victimhood,” International Centre for the Study of Radicalisation (ICSR) and XCEPT Research, February 15, 2022.

p Nujaba and Kata’ib Al-Imam Ali were the main Iraqi *muqawama* groups trying to signal solidarity against Israel in the pre-2023 period. For their Golan Heights stunts, see “Profile: Hezbollah Harakat al-Nujaba,” Militia Spotlight, Washington Institute for Near East Policy, April 17, 2021.

Israel from February 2024 until Lebanese Hezbollah leader Hassan Nasrallah's assassination by Israel on September 27, 2024.⁴⁰ After Nasrallah's funeral, which was attended by numerous Iraqi *muqawama* representatives,⁴¹ Iraqi group's attack numbers rose to 2.69 per day against Israel for about six weeks.⁴² But again, the Iraqi groups curtailed their attacks almost entirely (to 0.5 attacks per day) after Israel made rhetorical threats of retaliation against the Iraqi *muqawama* at the United Nations in November 2024.⁴³

Things went from bad to worse for the transnational military record of the Iraqi *muqawama*. In December 2024, the Iraqi groups did not cross the Syrian border to aid the Assad regime⁴⁴ and only acted as a shelter for retreating Iraqi, Syrian, Afghan, and Pakistani militias supported by Iran.⁴⁵ The *muqawama* laid very low for the whole first year of the U.S. President Donald Trump's second term in 2025, with Iraqi groups participating only in a limited way in the Iranian military response during the Twelve Day War between Iran and the U.S.-Israel coalition in June 2025.⁴⁶ Finally, in August 2025, facing U.S. sanctions threats, the *muqawama* were unable to pressure the Iraqi body politic into passing a law that would have permanently enshrined the PMF as a government ministry.⁴⁶ The United States has breezed right past every deadline for U.S. military withdrawal ever set by the Iraqi *muqawama*.⁴⁷

By the lead-up to the current war, the Iraqi 'resistance' had arguably thus not been effectively resisting the United States or Israel for years.^r The Iraqi *muqawama* demonstrated little ability or even willingness to powerfully back Iran or Lebanese Hezbollah,

or to avenge the killings of Iranian, Hezbollah,^s and even Iraqi militant leaders.^t The Iraqi groups seemed to collectively have a 'glass jaw'—the term for a boxer who was easy to knock-out with the right punch—in this case referring to the *muqawama*'s sensitivity to U.S. and Israeli threats to their leaderships. When the kinetic cells of the *muqawama* did strike in 2025, they seemed content to burnish their militant *raison d'être* purely with niche strikes on soft targets such as the Iraqi Kurds, oil investors in Iraqi Kurdistan, and defenseless Iraqi civil society—what the authors would characterize as the twisted militia equivalent of empty 'virtue signaling'.^u

By the start of 2026, this left the Iraqi *muqawama* firmly in the shadow of the Houthi movement, Ansar Allah.⁴⁸ Despite attempting to hit Israel far less frequently than the Iraqis, the Houthis emerged from 2025 with a far better claim than Iraqi groups to be Iran's strongest remaining military partner, with a proven track record of never bending in the face of the Saudi-led Gulf Coalition, a U.S.-U.K. joint effort, and the Israelis.⁴⁹ But there was always reason to believe that many Iraqi fighters and their leaders felt embarrassment due to their growing second-class status as militants, and that they might play a more significant role in a future war.^v

Part I: Phases of Iraqi Militia Involvement in the Current War

With Lebanese Hezbollah still recovering and fighting for survival,⁵⁰

q The militias undertook only five attacks on U.S. military and diplomatic points of presence in Iraqi Kurdistan throughout the Twelve Day War, concentrating the bulk of their attacks (around 35 in total) on Kurdish intelligence and security sites, local and internationally operated energy assets, and Iranian Kurdish opposition bases. Attack data is drawn from the authors' geolocated SIGACT dataset, which spans the 2017-2026 period of *muqawama* kinetic operations in Iraq.

r Elements of the *muqawama* even took to internal dissent, calling out the ineffectiveness of the resistance strategy. In 2021, for example, AAH and KH engaged in a public war of words over *muqawama* strategy (which Militia Spotlight termed the "Tuna and Noodles saga"). This episode saw KH media channels criticize AAH's rocket attacks for only damaging parked cars and AAH media channels lampoon the KH convoy strategy for "targeting convoys of tuna and noodles." In essence, both sides criticized the seriousness of the other's resistance effort. See, for example, Hamdi Malik, "The Tuna and Noodles Saga: Findings from a War of Words Between Militias," Militia Spotlight, Washington Institute for Near East Policy, March 3, 2021. Later that year, Badr leader Hadi al-Ameri was publicly berated by young *muqawama* members during a funeral for militiamen who were killed in a U.S. airstrike on June 28, 2021. The crowd demanded serious action against U.S. troops, yelling at the leaders, "We don't want condemnation ... either take revenge or don't come [to these funerals] anymore." See Knights, Smith, and Malik, "Discordance in the Iran Threat Network in Iraq." Incidents like these created a risk that militia leaders seemed to be sensitive toward: that Iraqi militias increasingly appeared to be undertaking what might be called 'fake resistance,' while actually getting rich off of asset-stripping the state.

s Claimed attack frequency against Israeli and U.S. targets did rise following Nasrallah's killing in September 2024. See Lina Khatib, "The Degradation of Iran's Proxy Model," Belfer Center for Science and International Affairs, April 2026. And many militia leaders attended his funeral. See Amir al-Kaabi, Hamdi Malik, and Michael Knights, "Hassan Nasrallah's Funeral: Iraqi Militia Response and Attendance," Militia Spotlight, Washington Institute for Near East Policy, February 27, 2025. But overall, under pressure from U.S. retaliation, Iraqi government constraints, and the risk of wider escalation, the pace of claimed *muqawama* attacks declined over time, and by mid-2024, the campaign had largely faded into sporadic, low-intensity activity rather than a sustained front. By 2025, meanwhile, the combination of external pressures by the United States and Israel, the fall of the Assad regime, and the loss of capacity by Hezbollah and the Houthis drove most *muqawama* factions to shift their focus to domestic survival. Despite rhetorical escalation, *muqawama* factions diverged sharply over participation in direct conflict with Israel. During the Iran-Israel war in June 2025, the *muqawama* refrained from direct involvement. IRI groups did so because Iran wanted to preserve them after the military defeat of Hamas and Hezbollah. This is not only because of their political and military importance to Iran but also because they provided it with an economic lifeline to circumvent sanctions. But for most of the other factions, non-intervention reflected fear of losing political capital, manpower, and military infrastructure as well as economic clout. See Khatib, "The Degradation of Iran's Proxy Model."

t Underlining the *muqawama*'s sensitivity over leadership targeting, the immediate trigger for their joining in the war appears to have been the killing of Kataib Sayyid al-Shuhada (KSS) security chief Haider al-Mousawi in a U.S.-Israeli airstrike at the al-Sheeb border crossing with Iran on June 21, 2025. Data drawn from the authors' geolocated SIGACT dataset covering the 2026 conflict. See also Tamer Badawi, "Analysis: First Iraqi Paramilitary Casualty in Israel-Iran War Marks Escalation Risk," Iraq Nexus, Substack, June 22, 2025.

u This is the turn of phrase selected by the author team to reflect the fact that militias want to be active and seemingly living up to their ideals, while often risking little and achieving little.

v The Militia Spotlight team has consistently felt the tension within the *muqawama*, often shown in the statements of junior militia members on social media and their interactions with their leaders at moments when the rank-and-file (and some commanders) seemed to want to contribute more to the transnational struggle. For one example of the discussion of these issues, see Amir al-Kaabi, Hamdi Malik, and Michael Knights, "Iraqi PMF Chief of Staff Commits to Fulfill Iranian Supreme Leader's Plans," Militia Spotlight, Washington Institute for Near East Policy, April 8, 2024.

and with Yemen's Houthis also either rearming or mostly showing restraint in the 2026 conflict,⁵¹ the Iraqi armed factions have had a rare opportunity to break the above pattern and function as the IRGC's main military partner. In the author team's assessment, the Iraqi *muqawama* have arguably risen to this challenge, to the best of their ability. The 2026 conflict has shown a different side of the Iraqi *muqawama*: a tougher, more risk-acceptant side that has seen the Iraqi groups claim to have undertaken their most intensive ever series of attacks against the United States, Kurdistan, Jordan, and the Gulf States. (As detailed by two of the authors (Smith and Knights) in a recent issue of *CTC Sentinel*, the Iraqi *muqawama* also mounted its first known attempted 'external operations'—the series of terrorist attacks attempted by the "Harakat Ashab al-Yamin al-Islamiya" (the Islamic Movement of the Companions of the Right Hand (HAYI or IMCR)) terrorist effort in Europe and North America.^{52 w)}

In the view of the author team, the evident expansion of Iraqi *muqawama* operational tempo has required both a much broader utilization of PMF armed forces inside Iraq, and unprecedented Iranian logistical and 'advise and assist' support to the Iraqi factions. If studied carefully, the 2026 war is probably uniquely rich as a source of insight about the changing nature of the Iraqi Shiite armed groups, their instrumentalization of the state-funded PMF, and their military relationship with Iran. The following is a preliminary effort to break the Iraqi war effort since early 2026 down into its key phases (with the nomenclature of the phases being the author teams' characterization, not that of the militias themselves, unless explicitly stated).

Phase Zero: Preparation (January-February 2026)

Phase Zero was characterized by pre-conflict preparation and signaling. In the assessment of the author team, the Iraqi *muqawama* had worked in the first months of 2026 to prepare themselves for a larger role in a conflict that was widely expected to be an existential struggle for the Islamic Republic of Iran, with potentially far-reaching consequences for the Iran-backed Iraqi groups as well.⁵³ With war looming, weapons systems were shown off by the Saraya Awliya al-Dam (SAD) façade brand (which the authors assess to be operated by Kataib Sayyid al-Shuhada or KSS).⁵⁴ A large cave was the setting for the January 31, 2026, video^{55 x} and many later SAD propaganda videos.^y In the cave, SAD displayed a double-rail truck launcher carrying two 'al-Qari'

w Notably, the Department of Justice claims that al-Saadi "planned, coordinated, and claimed responsibility for at least 18 terrorist attacks in Europe," including eight high-profile attacks in the United Kingdom, in addition to "two additional attacks in Canada," all conducted in the name of "Harakat Ashab al-Yamin al-Islamiya" (the Islamic Movement of the Companions of the Right Hand (HAYI or IMCR)). See "Iraqi National Arrested and Charged with Providing Material Support to Iranian-Backed Terrorist Organizations and Directing Attacks Targeting U.S. Citizens and Interests," U.S. Department of Justice, May 15, 2026.

x The video shows SAD members trucking al-Qari' CRBMs (Close-Range Ballistic Missile) into a man-made underground facility comprising large tunnels. The Arabic caption reads: "Our steps are as firm as an unshakeable mountain, and our resolve is like our swords, drawn in their sheaths; not to impress, but to be summoned at the decisive moment, a moment that knows no mercy. #Al-AwliyaFacility #Saraya_Awliya Al-Dam."

y These included a February 19 video showing off SAD's varied arsenal of drone systems and a May video showing SAD members operating forklifts and walking around inside a large underground bunker facility stacked with dozens to hundreds of Shahed-101/107 and CRBM boxes.

Close-Range Ballistic Missiles (CRBMs),^z plus an assortment of Iran-produced drone systems, including Shahed-101s and heavier Shahed-107s and Ababil (Qasaf-2K) drones.^{aa}

Probably in anticipation of being targeted intensively, as interviews undertaken by one author (Knights) suggest, the *muqawama* dispersed missile and drone systems to new hide sites by February 21, 2026, a week before the war started.⁵⁶ This 'shuffling' was reported to be occurring at scale in Nineveh (facing targets in the Kurdistan Region of Iraq (KRI) and in western Anbar (facing Jordan and Israel), and may have happened elsewhere as well.⁵⁷ Counting new arrivals and pre-existing stocks, the *muqawama* was then in possession of what the authors will call their "first load" of munitions.⁵⁸ Other long-range weapons—possibly existing stocks of cruise missiles—were dispersed to industrial areas adjacent to Kataib Hezbollah's Jurf as-Sakr redoubt.⁵⁹

According to interview material gathered by one author (Knights),⁶⁰ there was also an inflow of Iran-provided advanced conventional weapons (i.e., drones and missiles) around February 15-20. This included complete weapons systems^{ab} but also stocks of drone components needed to facilitate local assembly.^{ac} Other interview material also suggests a parallel effort in February and March to accelerate a pre-existing effort to 'salvage' Iran-provided advanced conventional weapons that had been left in Syria—unintentionally or intentionally—after the fall of the Assad regime in December 2024.⁶¹ Iranian Medium-Range Ballistic Missiles (MRBMs) with the range to strike Israel also appear to have been brought (from Iran) and located just inside Iraq's eastern border in Wasit and Maysan provinces.^{62 ad} Alongside drones already inside Iraq at the start of 2026, the Iraqi *muqawama* now possessed its

z A weapons system previously unattested in the Iraqi *muqawama* arsenal, the al-Qari CRBM appears to be a version of the Iranian Ababil or Arman missile, a tactical guided artillery rocket with a range of 85 km roughly comparable to the United States' GMRLS system. For background, see Fabian Hinz, "Iranian missile deliveries to Russia: escalating military cooperation in Ukraine," IISS, September 18, 2024.

aa Based on the authors' comprehensive review of launch footage, the latter drone seems not to have featured at all in the 2026 conflict despite being displayed by SAD, and appears to have been largely phased out in favor of the ubiquitous Shahed-101/107 family of drone systems.

ab The primary resupplied weapons system appears, based on one author's (Knights) interviews, to be Shahed-101/107 type fixed wing drones, which were provided in distinctive dual-use carrying and launching crates that look different from delta-wing carrying crates. Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.

ac Additional engines and warheads for Shahed-101 and Shahed-107 X-tail drones were brought into Iraq in large consignments just prior to the commencement of fighting on February 28, 2026, seemingly to ensure supply for a sustained launch campaign from Iraqi soil. Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees. The idea of creating local assembly lines for drone fabrication seems to be an Iranian template, used in Lebanon and Yemen as well. A worthy line of inquiry is how IRGC and the *muqawama* may have cultivated drone industry technical skills and capacity using their control of Iraq's university system via the Asaib Ahl al-Haq Minister of Higher Education and Scientific Research in 2023-2026. See Jawad Mahdi, "Injecting New Blood into Militias: The Gradual Takeover of Iraqi Higher Education by the Popular Mobilization Forces," Fikra Forum, Washington Institute for Near East Policy, July 12, 2024.

ad To be able to strike Israeli targets with ballistic missiles from this area, the type of missile would need to have the range (at least) of an Iranian MRBM system such as Kheibar Sheikhan. Such mobile solid-fuel systems would seem to be the most likely to be deployed in Iraq, away from Iranian liquid fuel storage facilities in the assessment of the authors.

'first load' of munitions.⁶³

A final aspect of pre-war preparation is likely to have been target selection and allocation. Drones and cruise missiles require mission planning software packages (with target coordinates, flight route, and altitude pattern programming), and other guided missiles require aimpoint coordinates. This 'mission profile' is often loaded to the weapon shortly before launch, as GPS calibration is undertaken (see the image at Figure 1 as an example).^{ae} By February 2026, the *muqawama* likely had a library of targeting solutions on-hand that might be thought of (in the authors' suggested nomenclature) as the 'starting target deck.'

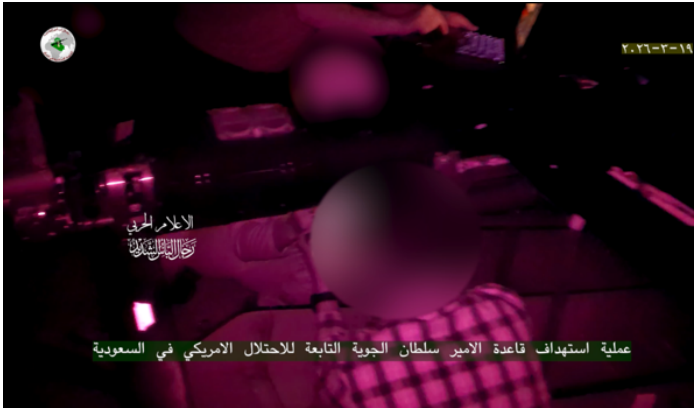


Figure 1: *Rijal al-Bas al-Shadid (RBS) drone crew prepares a Shahed-107 for launch in an April 19, 2026, post-facto claim video regarding an attack allegedly carried out before the April 8, 2026, ceasefire. Note the militia operator using a laptop to upload the mission profile to the drone's autopilot system. At least three other members of the drone crew are visible in the video attaching the tail fins and underslung rocket booster. Note also the tan-colored GNSS guidance pucks in 'stovetop' configuration on the upper fuselage. During the war, Shahed-107s with these new pucks increasingly displaced drones with black plastic pucks in militia claim videos, a likely indicator (in the assessment of the author team) of the arrival of a fresh 'reload' from Iran.⁶⁴*

Phase One: Spasm (February 28 – March 5, 2026)

A strong surge of attacks from Iraqi groups was unsurprising, being that the war began with the United States' killing of Iran's Supreme Leader Ali Khamenei, the pivotal political-religious reference for

Iraq's *wal'ai* militant groups.^{af} (Of interest, the Iraqi *muqawama* also surged attacks on Israel following Nasrallah's death in September 2024 and might have done so after the January 3, 2020, assassination of al-Muhandis, except for Iran's instruction that Tehran would lead the retaliation for Soleimani and al-Muhandis with a ballistic missile strike on Al-Asad.⁶⁵) In the same manner that Iran 'went big' from the opening moments of its response to Epic Fury,^{ag} Phase One (assessed by the authors to span February 28 to about March 4-5) was a 'spasm' of strikes that saw the Iraqi *muqawama* operate orders of magnitude more intensely than in any previous military campaign.⁶⁶ To give a metric, the most intense prior bombardment campaign mounted by the *muqawama* was the aforementioned May-November 2024 'Al Aqsa Flood' operations room campaign against Israel, which averaged 1.57 claimed strikes per day. In the first five days of the 2026 war, Iraqi *muqawama* claims averaged 28.2 strikes per day.⁶⁷ (Each of these claimed 'attacks' tended to involve one to four fixed-wing drone attacks or one to two missile launches.⁶⁸)

af The militias that make up the *muqawama* in Iraq are overwhelmingly adherents to the Shi'a doctrine of *velayat-e faqih* (guardianship of the jurists), in practice requiring absolute loyalty to the Supreme Leader of the Islamic Republic of Iran. Badr and its offshoots (including KH, KSS, and HAAA) is a *wal'ai* movement, meaning that if called upon, it will recognize Iran's Supreme Leader as a higher authority than Iraq's prime minister. As a young commander fighting on Iran's side, Hadi al-Ameri is on record as stating, "We are with the Imam [Khomeini] ... If our Imam says war then we say its war, if Imam says peace, then its peace ... Now we know the Imam represents Islam." See, for example, Michael Knights and Crispin Smith, "Badr Organization: Iran's Oldest Proxy in Iraq," Hudson Institute, June 3, 2025. See also al-Kaabi, Malik, and Knights, "Iraqi PMF Chief of Staff Commits to Fulfill Iranian Supreme Leader's Plans," noting that Abu Fadak, de facto operational head of the PMF and a senior KH leader, publicly and bluntly admitted to taking orders from then Supreme Leader Ali Khamenei: "We are waiting for the [Supreme] Leader to express his view on the next step ... What will the response be to the aggression on the Iranian consulate and the killing of some of the [Islamic Revolutionary Guard Corps, or IRGC] commanders? ... After the criminal [attack] on the consulate in Damascus, we came to the Islamic Republic to first express our solidarity with the vision and the plan of the Leader and the Imam ... and second is to renew our covenant [i.e., loyalty to the Supreme Leader] and wait for the Leader's decision." Even as other groups and militia leaders attempt to present themselves as mainstream Iraqi nationalists, they remain deeply anchored to this ideology. For instance, Asaib Ahl al-Haq (AAH) leader Qais al-Khazali frequently uses strategic dissimulation to appear pragmatic in public, while internally reaffirming his strict belief in *velayat-e faqih* and his unwavering adherence to Ayatollah Khamenei's leadership to his militant base. See, for example, Hamdi Malik, "The Dual Face of Qais al-Khazali: Extremist at Heart, Politician by Necessity," Washington Institute for Near East Policy, March 17, 2025.

ag Within hours of the opening of Operation Epic Fury (in which joint U.S. and Israeli strikes killed Iran's supreme leader, Ayatollah Ali Khamenei, along with senior commanders of the Islamic Revolutionary Guard Corps and key intelligence officials), Iran struck back by launching hundreds of ballistic missiles and drones not only at Israel but also across the Gulf. The strikes hit U.S. bases, but also killed civilians, shuttered airports, threatened shipping and oil exports, and tarnished the region's image of stability and safety, and have been characterized as a strategy of horizontal escalation. Robert Pape, "Why Escalation Favors Iran," *Foreign Affairs*, March 9, 2026. This initial burst of activity ultimately gave way to a more measured strategy based around creating economic and diplomatic pressure on the United States and allies and characterized by a reduction in rate of fire (possibly necessitated by loss of missile launchers) and a partial narrowing of target sets. Hamidreza Azizi notes that over time, "the character of [Iran's] campaign shifted. As the war entered its second and third weeks, Iranian actions and messaging converged around a different organizing principle: attrition." Hamidreza Azizi, "How Iran Rewrote Its War Strategy," *Iran Analytica*, March 25, 2026.

ae Launch videos frequently show drone operators uploading the mission profile to the drone's flight control module from a laptop immediately before launch. A drone used in an attack on an energy facility in the KRI in 2023 featured a commercial, off-the-shelf Pixhawk 4 autopilot controller, but the newer Shahed-101 and 107 models use an as-yet unidentified flight controller unit, likely of Iranian make. The exact mission planning software is also unknown, but the use of regular laptops to upload the packages suggests one of several open-source mission planning and flight software. Data drawn from the authors geolocated SIGACT dataset and attack claims database. On the Shahed-101/107 flight control unit, see <https://war-sanctions.gur.gov.ua/en/components/part/5009>

Attack Claim Groups

The Islamic Resistance in Iraq (IRI)⁶⁹ was, from the beginning, the main claim mechanism, accounting for 89 percent of attack claims in Phase One. IRI is the Iraqi *muqawama* collective claim mechanism intended to ensure the ‘unity of fronts’ in the post-October 7, 2023, war against Israel.⁷⁰ The Militia Spotlight profile of IRI notes that “the balance of available evidence suggests that the IRGC-QF plays a role in coordinating the IRI brand.”^{ah} Of note, in contrast to the hundreds of IRI claims from 2023-2024, IRI did not provide any breakdown of the geographic focus of its attacks, instead using the catchall phrase ‘Iraq and the region,’ referring to the broader Middle East region.⁷¹

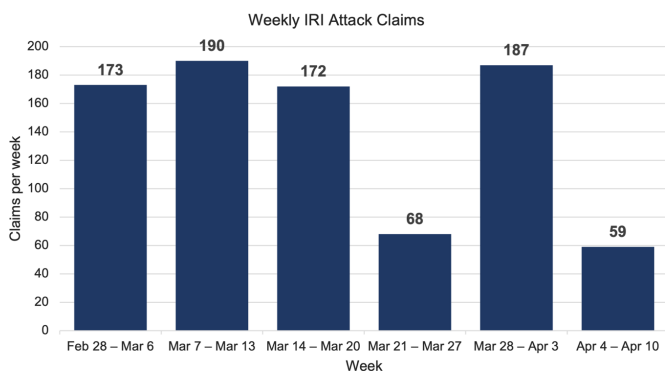


Figure 2: Weekly attack claims by IRI. (Metrics charting by Alex Almeida). Of note, IRI attacks did not specify the location struck in each claim but instead were delivered as a near-daily digest of the tally of attacks by IRI that day, referring only to attacks ‘in Iraq and the region.’

Three other Iraqi claim brands were active from the first day: One was SAD, which was the only other claimant of Iraqi *muqawama* strikes in the 2023-2024 campaign, aside from IRI.^{ai} The other was an enigmatic new brand called Rijal al-Bas al-Shadeed (“RBS,” Men of Great Valor) that activated its online presence on March 4, 2026,^{aj} retrospectively claiming its first seven attacks starting on February 28, 2026.⁷² Ashab al-Kahf (AK), a brand associated strongly with Harakat al-Nujaba (HAN),⁷³ made its first claim of the war on February 28. These and other claim brands mostly did provide a geographic location for all claimed strikes in the opening

weeks of the war, if not throughout.^{ak}

Targeting During the Spasm

In Phase One, around half of all claims related to a specific location related to attacks on the KRI (i.e., 14 of 30 location-specific claims).⁷⁴ SAD was the initial claimant against Iraqi Kurdistan,⁷⁵ including a documented use of an Al-Qari CRBM on the U.S. military annex at Erbil International Airport (EIA) on March 1.⁷⁶ News and social media reporting aggregated and geolocated during the war by the author team suggest a much larger stream of attacks on the KRI than are represented solely by the non-IRI claims.^{al} Even after filtering out direct Iranian strikes on Iranian Kurdish oppositionist camps,^{am} the remaining ‘unclaimed’ impacts observed in Erbil probably represent non-located IRI claims on U.S. and KRI government targets in the Kurdistan Region.^{an} There are many reasons why KRI aimpoints may have been prevalent in the ‘first target deck’ used in the war. Logically, EIA was the main U.S. military site in Iraq as the war began, following the reported closure of bases such as Al-Asad and Harir. The *muqawama* also viewed Iraqi Kurdistan as a historic dumping ground for attacks, a den of spies and Iranian oppositionists, and a soft target within range of even short-range *muqawama* weapons that has historically lacked the military power to effectively deter such militias or Iran.^{ao} (In Phase One, U.S. forces struck locations facing the Kurdistan Region linked to PMF brigades 14 (KSS), 30 and 50, based on launch areas west of Erbil.⁷⁷)

ak Both SAD and Jaysh al-Ghadab (JG), a new online brand activated shortly before the conflict, began shifting to claiming attacks on unspecified regional targets in the latter phase of the war, echoing IRI’s pattern of not identifying specific targets. Authors’ database of *muqawama* attack claims.

al The Community Peacemaker Teams – Iraqi Kurdistan (CPT-IK) non-governmental organization is a good source for ground-level reporting of strikes. They calculated that 153 strikes were suffered in the February 28 to March 9 period, a 10-day timeframe that encompassed the Phase One period and extended into the transition to Phase Two. Only 25 located claims relate to Kurdistan in the same period, with some claims pointing toward being multi-weapon or even multi-target. Even if one presumes each located claim represents three attacks, this still suggests claimed attacks represented around half of observed strikes on the KRI. (More likely, under half of all attacks were claimed by non-IRI groups.) “Escalating Attacks on the Kurdistan Region of Iraq: 196 Strikes by Iran and Affiliated Groups Kill Four and Injure 19,” CPT-IK, March 9, 2026.

am The authors feel fairly confident in assessing that the bulk of the strikes on Iranian Kurdish opposition sites were launched directly out of Iran. This is based on claim statements from the semi-official, IRGC-linked Tasnim news agency, attribution of those strikes directly to Iran by KRG authorities and Iranian Kurdish opposition groups, and the fact that of the strikes appear to have featured weapons systems – Shahed-136 type drones and Short-Range Ballistic Missiles (SRMBs) – that are not common in the militia weapons arsenal.

an Among these attacks, 43 targeted the headquarters of Iranian Kurdish opposition parties in the Kurdistan Region, and 58 were against the U.S. Consulate General in Erbil and military bases and headquarters related to the U.S. government. The other 95 attacks targeted hotels, residential areas, headquarters of the Peshmerga forces, oil fields, companies, and civilian-populated areas. CPT-IK will continue to monitor the impact of these attacks on civilians and to document potential war crimes in the Kurdistan Region of Iraq.

ao The *muqawama* have long had a fixation on the foreign intelligence (U.S., U.K., and allegedly Mossad) presence in the greater Erbil area, which they have typically associated with hotels like the Khanzad (formerly the site of the British consulate in Erbil) and Divan and various residential villas and security compounds in Erbil’s northeastern outskirts associated with the KDP political and business elite. Several of these sites, including the Khanzad and Divan hotels, were struck during the 2026 war. Data drawn from the authors’ geolocated SIGACT dataset.

ah Iraqi armed groups tend to jealously guard their individual identities and the credit they derive (directly or via façade groups linked to them) from attacks, so their willingness to submerge these identities and even recant an individual group attack claim suggests that a higher power is coordinating them. Hamdi Malik and Michael Knights, “Profile: The Islamic Resistance in Iraq,” Washington Institute for Near East Policy, October 21, 2023.

ai In 2023-2024, IRI claimed 569 (94 percent) and SAD claimed 31 (six percent). See Michael Knights, Amir al-Kaabi, and Hamdi Malik, “Tracking Anti-U.S. Strikes in Iraq and Syria During the Gaza Crisis,” Militia Spotlight, Washington Institute for Near East Policy, October 24, 2023, updated until December 3, 2024.

aj A Telegram post by Rijal al-Bas al-Shadeed on March 4, 2026, showed the group’s logo with the caption “in the name of the smasher of the oppressor; the Islamic Resistance in Iraq Rijal al-Bas al-Shadeed.” Note, the Telegram channel itself was created in 2025, and prior to March 4, 2026, had posted occasional generic news content relevant to Shi’a youth and Basra (possibly to build up a followership). On March 4, 2026, the channel deleted all prior posts and converted to its new façade group persona.

The most enigmatic portion of the *muqawama* war effort would be attacks on targets outside Iraq. Some Iranian Short-Range Ballistic Missiles (SRBMs) systems^{ap} may have been fired at the Gulf from Iraq in the first week of the war, with the Iraqi PMF providing logistical support and security for launches.^{aq} U.S. strikes on a range of KH-linked southern Iraq locations in the first phase of the war might suggest *muqawama* activity against the Gulf States.^{ar} But actual claims of attacks on the Gulf were non-existent in the first phase. The IRI might have struck targets outside Iraq during this phase, albeit without leaving any trail in the claim record, but interview material gathered by one author (Knights) suggests no major early sequence of IRI strikes on the Gulf in Phase One,⁷⁸ with two known exceptions. One was an unclaimed March 3 drone strike on the U.S. Embassy in Riyadh;⁷⁹ the other was the March 4 disruption in Basra of an CRBM launch against Kuwait using four Sarem or Al-Aqsa 1 CRBMs.^{as}

From February 28, new claim brand RBS demonstrated a special focus on claiming attacks on Jordan, most frequently at Muwaffaq al-Salti Air Base (MSAB), the main regional U.S. combat aircraft basing location in the war.⁸⁰ In its announcements, RBS claimed to be launching Shahed-101/107 drones during its attacks at MSAB, which suggests—based on conservative range estimates of 600-800km for these drone types—that RBS was utilizing Anbar province launch locations.⁸¹

Phase Two: Quality Operations (March 6-17, 2026)

In the author group's opinion, from as early as March 4-5 and unfolding in the second week of the war (March 7-13) and some of the third week (March 14-17), the Iraqi *muqawama* started shifting toward a deliberate approach that aligned more closely with Iran's own evolving war strategy of raising costs to the global economy and broadening the war.⁸² Instead of generating as many

strikes as possible but causing little impact outside Iraq, the focus would shift to qualitative impact. On March 13, KSS leader Abu Alaa al-Walal (real name: Hashim Bunyan al-Siraji) publicly referenced a new phase of the war that had begun and which marked a shift to 'qualitative objectives.'⁸³ at (Abu Alaa has a track record of retrospectively announcing phase changes in *muqawama* campaigns, for instance the early 2024 targeting shifts toward Israel.^{au})

The new phase did not happen all at once, but instead became visible at a number of points. First, a much more intense Baghdad sub-campaign began (see the section below on this sub-campaign), part of the effort against remaining U.S. military and diplomatic points of presence. Second, claims of Iraqi attacks on the Gulf States surged by over 80 percent,⁸⁴ and unclaimed attacks are also reported in Knights' interviews to have intensified.⁸⁵ Third, a sequence of unclaimed attacks began to target oil sector locations in Iraq and the Kurdistan Region with a strong known or suspected connection to the U.S. energy industry.^{av}

And lastly, a new 'second load' of Iranian munitions began to enter Iraq to enable a sustained Iraqi effort.⁸⁶ This reloading mechanism is worth a whole article of its own, but in broad terms, it was undertaken mainly via the Iran-Iraq border crossings at Badra (Wasit province), Al-Sheeb (Maysan), and Mandali and Muntheriyah (Diyala).⁸⁷ This reload included (for the first time)

ap To reach the Gulf from eastern Iraq, one could use a number of Iranian Short-Range Ballistic Missile types. If one assumes that solid-fuel systems might be easier to deploy outside Iran (as opposed to liquid fuel systems that require more storage and fuel cycling arrangements), then this narrows the options. If interview material (Knights) concerning the physical appearance, portability, and length of the systems appearing in Iraq is factored in, then a low-confidence assessment can be made that these systems were Zolfaqr or Fateh-110/313 SRBMs.

aq According to interview material gathered by one author (Knights), an unprecedented 40-missile launch came out of the Iskandariyah-Latifayah-Yusufiya triangle immediately east of KH's Jurf as-Sakr on March 1, 2026. Other major launches involving tens of Iran-operated missiles, secured by Badr personnel from PMF 27th brigade (PMF 27) are also reported to have originated from Wasit and Maysan during Phase One. Strikes on Israel out of the Jurf and Iran-Iraq border launch baskets would imply the forward-deployment onto Iraqi soil of large numbers of true Iranian Medium Range Ballistic Missiles (MRBMs), likely Shahab-3 (range 1,300km) class or above.

ar During this opening phase, U.S. counterstrikes targeted major KH and KH-partner base locations such as Jurf as-Sakr and Muthanna, both of which have been used to launch drones southwards into the Gulf before. For a description of these prior Gulf attacks, see "Profile: Awliyat Al-Waad al-Haq," Militia Spotlight, Washington Institute for Near East Policy, April 1, 2021. On the Jurf and Muthanna strikes, this insight is derived from the authors' database of U.S. strike reports from the 2026 war.

as Two container truck trailers, each housing a pair of elevating launch tubes, were found in the desert near the Kuwaiti border on March 4. The distinctive tail fin configuration identifies the missiles as either Sarem or Al-Aqsa-1 CRBMs, believed to be export variants of Iranian missiles known as the BM-45 and BM-120 (Fath-360 in Iranian service), respectively. The Sarem and Al-Aqsa 1 CRBMs were revealed by *muqawama* in November 2023 in an IRI-claimed strike on Al-Asad Air Base in Anbar province.

at The Telegram post reads: "Hardly any time had passed since the ill-conceived American venture in the Middle East when some 70,000 Americans, including military personnel, staff, and civilians, departed. It was a chaotic withdrawal akin to a rout – or what military parlance terms a 'repositioning toward the nearest airfield.' They left bearing heavy memories that will haunt them for a long time, much like those that plagued occupation troops after the 2003 invasion of Iraq, when many returned home to psychiatric care. While entering West Asia was once easy, exiting it today has become costly, particularly as Islamic resistance operations enter a second phase characterized by high-impact, strategic objectives. This phase marks a shift in the confrontation to a new level of pressure and deterrence, rendering the occupation's continued presence in the region increasingly costly with each passing day." [emphasis added by authors].

au Abu Alaa announced the second phase of Iraqi *muqawama* operations in solidarity with the Gaza war in February 2024: "[This phase] will include enforcing the blockade on Zionist maritime navigation in the Mediterranean Sea and render the [Israeli] entity's ports out of service ... This will continue until the unjust siege on Gaza is lifted and the horrific Zionist massacres against its people are stopped." See Michael Knights, "Saraya Awliya al-Dam Finds New Mission in Israel Attacks," Militia Spotlight, Washington Institute for Near East Policy, June 27, 2024.

av These included strikes on Iraqi oilfields that were being considered for U.S. inward investment (Majnoon, West Qurnah 1); U.S. oilfield services equipment warehouses in oil hubs like Basra and Erbil; a U.S.-operated oilfield in Iraqi Kurdistan (hit twice, with debilitating strikes on key infrastructure); Iraq's largest U.K.-operated oilfield (Rumailah); and various small refineries in Iraqi Kurdistan owned by major Kurdish political families and supplied by U.S.-operated oilfields and supply chains. These attacks were very rarely claimed (i.e., just once by SAD, in the first attack on the U.S.-operated oilfield in Kurdistan). The almost negligible damage to Iraqi oilfields in Basra suggested the strikes were intended to add to the general 'spooking' of oil markets by the Iran threat network without actually damaging Iraq's future revenues. Data drawn from the authors' geolocated SIGACT dataset covering the 2026 conflict.

jet-powered Hadid-110 (Dalahu) delta-wing drones,^{aw} which were detected in use for the first time on March 10.⁸⁸ Greater effort was made to distribute weapons caches to new locations through ‘partnering’ or ‘teaming’ arrangements between attack cells and collaborators within a range of ground-holding PMF units.^{ax} In the view of the author team, mid-March—and particularly the Baghdad sub-campaign—marked the point when Iraqi militias went ‘all-in’ on the war and an unprecedented number of factions began to take part in attack operations.⁸⁹ According to interview material gathered by one author (Knights), from this period until the end of the war, Badr and Asaib Ahl al-Haq (AAH) operated ‘one-way attack’ drone attack cells focused on U.S. targets in Baghdad and the KRI.⁹⁰ Activating an expanded set of previously unused drone cells would make sense in order to maintain the high daily tally of claimed strikes in March 5-13, an average of 33.7 per day, with each strike typically including multiple drones.⁹¹

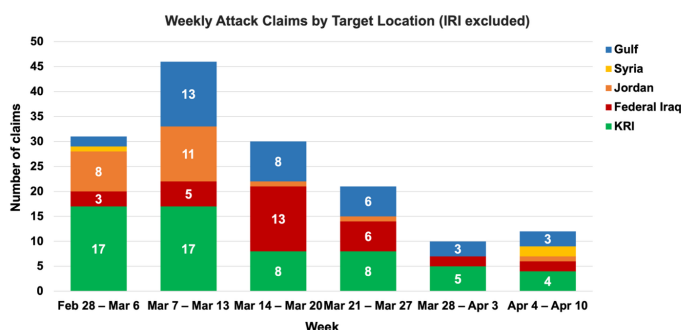


Figure 3: Claimed attacks on target location categories by week. Note that these only refer to located claims, which mean they represent a subset of about 12 percent of claimed attacks. IRI-claimed (but not located) attacks may be striking a different proportion of each target location by week. (Metrics charting by Alex Almeida)

Though each of these trends will be explored in greater depth in the sections below, the author team’s assessment of the broad pattern in Phase Two is that the IRGC-QF probably ‘gripped’ the Iraqi *muqawama* and broadened its ambitions to include better-resourced attacks on U.S. sites in Baghdad and on the Gulf States.⁹²

aw Unveiled by Iran in February 2025 and first attested in Iraq during the current conflict, the stealthy Hadid-110 has an estimated speed of 510 km/h and carries a 30kg warhead. With a range of 350 km, it is primarily a high-speed, short-range strike weapon, and appears to have been used exclusively against Kuwait, Erbil in the KRI, and possibly Jordan. The drone was used most heavily by IRI, though RBS also claimed an early Hadid-110 launch. Distinctive delta-shaped Hadid-110 launch boxes also turn up in a SAD ‘cave video’ after the ceasefire. TRADOC G-2, “Cyber,” Operational Environment Data Integration Network (ODIN) – Hadid 110 (Dalahu) Iranian Unmanned Aerial Vehicle (UAV), accessed June 19, 2026. See also Telegram post by Saraya Awliya al-Dam on May 21, 2026. The caption reads “A poem: We are Awliya al-Dam.” The accompanying video is essentially a music video for a SAD song (“We are Awliya al-Dam”) depicting a range of SAD activities, weapon systems, and militiamen wearing SAD uniforms. The Hadid-110 boxes can be seen at minute 1’08.”

ax In the geographic focus section, these trends are laid out region by region, and these relationships are shown in this article’s map and in the table of complicit PMF units on page 21. To give a quick preview of such ‘teaming’ here, drone launches in the Nineveh Plains in Mosul were undertaken by KSS and related local ground-holding PMF units (brigades 30 and 50); some of the caching of munitions for this effort was undertaken by PMF brigades 40 and 53, and the distributing link between them was the logistics support given by PMF brigade 29, among others. This is the authors’ collective conclusion, based on their synthesis of the known facts, and explored further through this text.

The greater the Iranian technical input into the targeting and ‘weaponizing’ process, the more control Iranian agencies might have had over the design and execution of the *muqawama* drone and missile campaign.^{ay} More granular understanding of who produced *muqawama* ‘mission profile’ programming packages is a line of inquiry that would probably yield very valuable insights about the design of the *muqawama* campaign. Clearly, some of the Iraqi teams that performed final loading of mission profiles into drone guidance systems and who filmed the launches for propaganda purposes knew which target areas they were broadly striking, as evidenced by the placards (showing the date and target) held up in front of drones and missiles before many non-IRI launches.^{az}

Phase Three: Reset and Reload (March 18-27, 2026)

From around March 18, as the Baghdad sub-campaign seemed to culminate (see the below section), the Iraqi *muqawama* effort powered down but never stopped. In the nine days between March 19 and March 27, the numbers of claimed attacks dropped off precipitously.⁹³ (IRI claims were not posted for four of the nine days, and were uncommonly low on a fifth.⁹⁴) SAD attacks also declined sharply in this period.^{ba} While observed launches at greater Erbil appear to have undergone a limited decline,^{bb} and strikes on the U.S. Embassy in Baghdad were paused, the *muqawama* still kept up a string of “quality” attacks on the Baghdad Diplomatic Support Center (BDSC), the U.S. diplomatic annex adjacent to Baghdad

ay The author team assesses the design of mission profiles to be significant because whichever entity has the technical capability to create such profiles can influence what target is attacked and by how many projectiles, and in what sequence. Longer-ranged and more complex mission profiles, which certainly seem to the author team to be in evidence in this war, might require greater intelligence support capabilities than the *muqawama* possesses organically, especially when operating at unprecedented operational tempo. (For instance, every profile needs to set altitude levels for ingress to target, factoring in numerous potential obstacles like power lines, towers, tall buildings, and hills.) If the IRGC provided many or even all the mission profiles, in addition to providing the Iran-origin weapons in nearly all cases, they could, if they wished, be the main driver of targeting and the operational tempo of the *muqawama* campaign.

az In the view of the author team, having obsessively reviewed each claim video multiple times for small details, the placards (showing claim group, time and day, and target) were used by all the non-IRI claim brands – SAD, RBS, Jaish al-Ghadab, and AK. One wonders if these are being used simply to keep different videos properly ‘tagged’ (like a movie crew’s ‘clapper-board’ or ‘slate’) or if they relate to a political motive, for instance, protecting the claim brand against allegations of exaggerating attack numbers through reuse of imagery.

ba SAD claims had averaged average 14 per week in the first three weeks of war, but dropped to an average of just five per week on March 21-27. This insight is derived from the authors’ detailed attack claims database from the 2026 war. A spokesman for SAD posted on Telegram on March 27, 2026, noting that “we assure the Iraqi people that the decrease in the pace of Islamic Resistance operations, in all their forms, is due to the adverse weather conditions on the one hand, and the withdrawal of the occupying American forces from some of their bases in Iraq and the region on the other.”

bb The authors’ geolocated SIGACT dataset suggests a decline in the volume of incoming drones at Erbil during the March 19-27 window, but hard, quantified data on daily drone intercepts over Erbil is hard to come by. The authors’ data shows Erbil continued to receive daily attacks for every day during this period, except March 21. Data drawn from the authors’ geolocated SIGACT dataset covering the 2026 conflict.

International Airport, and other targets in the Baghdad area.^{bc}

On March 18, KH had announced a conditional five-day pause on its operations against U.S. forces, which marked the beginning of a nine-day period in which IRI claims appeared at best every two days, instead of daily. This followed an apparent success for the militias—their claims to have forced partial U.S. evacuations from Baghdad by March 20.^{bd} But the hard-pounding of BDSC and the Embassy came at an apparent cost in terms of strikes on mid-level KH leadership. First, KH reported the death of its security official Abu Ali al-Askari by a U.S. airstrike on March 16).^{be} Then, the most senior IRGC-QF official working exclusively on the Iraq file, Hajji Hamid, was reported as killed or seriously wounded in a March

16 U.S. airstrike on a leadership meeting house in Jadriyah).^{bf} In the author team’s assessment, by the end of Phase Two, the *muqawama* showed signs of feeling the strain, probably caused by some combination of exhaustion, attrition, and thinning weapon inventories.

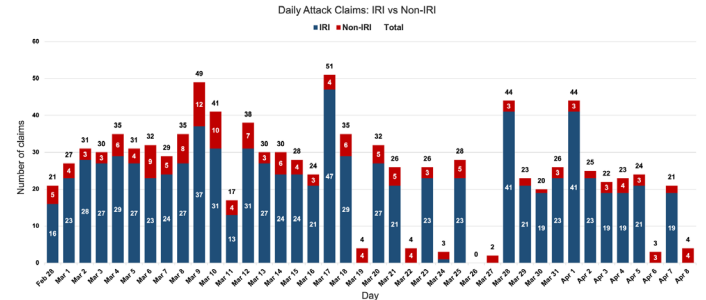


Figure 4: Daily attack claims by Iranian-aligned Iraqi militias. Dark blue are claims by the IRI umbrella. Red shows non-IRI (SAD, RBS, JG, and AK) claims. The data label atop each column is the daily total claim number (IRI and non-IRI combined). (Metrics charting by Alex Almeida).

Phase Four: Going the Distance (March 18 – April 8, 2026)

In the fourth and final phase of the war (prior to the April 8 ceasefire), the *muqawama* military campaign regained some of the vigor it had shown throughout the first half of March.⁹⁵ On March 28, the militias started to churn out higher numbers of attacks once more.⁹⁶ Based on the interviews conducted by one author (Knights), this happened at the same time as the arrival of a new ‘third load’ of Iranian munitions.⁹⁷ According to interviews conducted by one of the authors (Knights), this inflow had begun to enter Iraq during Phase Three,⁹⁸ being stockpiled at major storage facilities like Camp Ashraf⁹⁹ during the relatively quiet fourth week of the war (March 21-27).⁹⁵ This resupply included greater numbers of cruise missiles^{9b} and stealthy Hadid-110 jet drones, plus longer-range drone systems

bc These included a 107mm rocket shot from a launcher concealed inside the trunk of a civilian sedan at the ISOF’s Area IV compound adjacent to the BDSC, as well as effective quadcopter strikes on a radar site and U.S. medevac helicopter at the BDSC (the first of the war), plus another lethal quadcopter attack on the INIS headquarters in Baghdad’s Mansour district (an Iraqi Kurdish INIS officer was killed in the attack). In the KRI, a drone attack was undertaken against a Peshmerga outpost in the Makhmour area – the only such attack on a Peshmerga frontline outpost position during the war. Attack data is drawn from the authors’ geolocated SIGACT dataset covering the 2017-2026 period of *muqawama* kinetic operations.

bd Militia channels celebrated an apparent drawdown of U.S. positions around this time. In the early hours of March 22, 2026, Ashab al-Kahf posted on Telegram to note that “the cowardly enemy, under the protection of the counter-terrorism apparatus, is fleeing from some of its bases towards Jordan. We have sufficient and detailed information about their current location and which base they will use as a hideout.” The following day, a spokesman for AK posted a lengthy statement on Telegram, noting that “we are following with interest and caution the humiliating withdrawal of the occupation forces from beloved Baghdad as a result of the resistance’s strikes – a victory granted to us by God. We are also monitoring the small number remaining, ostensibly for guard duty, in addition to the withdrawal of NATO forces. We promise you that we will follow you wherever you go until you leave the entire region.” Also on March 22, 2026, a spokesman for SAD posted a statement on Telegram noting “the Americans and NATO requested from the Iraqi government a 24-hour truce with the Iraqi *muqawama* factions to facilitate the withdrawal of their forces from Victoria Air Base in Baghdad to Turkey . . . NATO’s aircraft failed to land at Victoria Air Base yesterday due to the heavy fire from *muqawama* factions targeting the base . . . The Americans are now only present in the Kurdistan Region after the *muqawama* factions, in all their blessed forms, expelled them from all their positions.”

be KH official media channel Kaf announced Abu Ali al-Askari’s death in a March 16, 2026, statement, signed by KH Secretary General Abu Hussein al-Hamidawi and posted on Telegram. No mention of the cause of death was made, though his death was referred to as a “martyrdom.” Abu Ali al-Askari’s last public statement was posted on March 6, 2026. The Kaf statement noted that Abu Ali’s role would be taken up by a new official, Haj Abu Mujahid al-Assaf. On March 17, 2026, a new Telegram channel was created under that name, which then picked up posting statements on behalf of KH’s military wing in the same manner and style as Abu Ali al-Askari.

bf On March 16, 2026, at least four persons were reported killed in a U.S. airstrike on a villa in Jadriyah, Baghdad. The strike followed drone attacks on the U.S. embassy. See “Four killed in Iraq’s Baghdad as US forces, Iran-backed groups trade fire,” Al Jazeera, March 16, 2026. Some local reports claimed that the strike targeted two officials linked to Iran’s activities in Iraq, with the primary target a figure known as “Nasiri,” who manages Iran’s economic file in Iraq, along with another official responsible for the Islamic Revolutionary Guard Corps (IRGC) file inside the country. See “Source: Baghdad strike aimed at Iran-linked operatives,” Shafaq News-Baghdad, March 17, 2026. “Nasiri” likely refers to Hajji Hamid Nasser, a known IRGC official. (Brigadier General Hajji Hamid Nasser is the IRGC-QF Jihad Assistant for Iraq.) Author (Knights) interviews, multiple Iraqi contacts, multiple sessions with significant detail, 2021, exact dates, name, and places withheld at request of the interviewees.) Two of the authors (Knights, Smith) have encountered lively anecdotal discussion within their Iraqi contact networks regarding theories of who was present from the *muqawama* and the IRGC at the Jadriya villa at the time of the explosion.

bg In a March 24 video showing the launch of several drones from a hidden bunker complex, SAD announced the activation of a second underground storage facility, likely hinting at the arrival of a fresh ‘reload’ from Iran. SAD Telegram post, March 24, 2026.

bh Cruise missile attack claims generally referenced Arqab cruise missiles, the Iraqi *muqawama* designation for the Iranian Paveh/358 series of land attack cruise missiles, first attested in the militia arsenal in January 2024. An early-war IRI claim showing the launch of a ‘Jamal-10’ cruise missile suggests the *muqawama* may have additional Paveh-variant cruise missiles during the conflict. See Alex Almeida and Michael Knights, “Iranian Made Quds-2 Missile Photographed in Iraq,” Washington Institute for Near East Policy, January 5, 2024, and IRI Telegram post, March 8, 2026.

such as the Shahed-136, KAS-04, a new and rarely seen ‘puller-propeller’ drones patterned on the Shahed-101 series.¹⁰⁰ From March 27-29, this ‘third load’ was distributed mainly to southern launch areas such as Jurf as-Sakr, Wasit, Diwaniyah, Maysan, and Basra.¹⁰¹

These longer-ranged systems were able to strike not only the northern Gulf (as had been the case throughout the conflict with Shahed-101/107 systems launched from border areas in Basra and Muthanna) but also the UAE and new Saudi Arabian targets (such as Shaybah oilfield in the Empty Quarter, the East-West pipeline, and the Red Sea oil loading terminus at Yanbu).¹⁰² In late March and early April, various militia façades and spokesmen openly threatened escalation against the Gulf States.¹⁰³ In Phase Four of the war, smaller claim brands (like Jaysh al-Ghadab) for the first time claimed anti-Gulf strikes using cruise missiles.¹⁰⁴ Within the strong IRI claim numbers for this late-war period (March 29 to April 4),¹⁰⁴ the author team assesses there are also likely to have been a number of strikes on the Gulf.¹⁰⁵

Inside Iraq, Phase Four appears to have been the period when

bi On March 30, 2026, Abu Alaa al-Walaji posted a Telegram statement noting the role of the Axis of Resistance in targeting locations in the Gulf. On April 2, 2026, KH official Telegram channel “Kaf” posted direct threats against regional countries, stating that “The bias of the rulers of Jordan, Saudi Arabia, and the UAE towards the crimes of the Zionist-American enemy against the Islamic Republic, and their treachery against the honorable free people of Iraq; This represents the height of depravity and treachery, necessitating a firm response from the Iraqi government. This response should begin with punishing Jordan specifically, as it is one of the launching points for enemy aircraft targeting the Popular Mobilization Forces and Iraqi security forces. This punishment should include the complete closure of the land border crossing and the cessation of Iraqi oil shipments, which they rely on for sustenance. This should serve as a lesson and a warning to all who betray the causes of their nation. While we affirm that the Iraqi resistance targeted American forces in Kuwait in the early days, it avoided harming their economic interests and infrastructure. While we urge that the interests of the State of Qatar – excluding American bases – be spared, in appreciation of its responsible stances on the Palestinian cause and the axis of resistance, we warn countries allied with the enemy of the repercussions of allowing their territories to be used to attack the Islamic Republic.” On April 4, 2026, AK posted on Telegram: “The targeting of border crossings between Iraq and the Islamic Republic of Iran – which disrupts people’s lives and leads to a rising cost of living in Iraq regarding food and household necessities, effectively imposing an economic blockade through Zionist-American raids aided by Gulf states – compels us to respond in kind. Our targets will be the interests of the peoples of the Gulf, a consequence of the reckless, Zionist-aligned policies of their monarchs. While we strive – by all religiously sanctioned means – to spare these peoples from this war, their rulers refuse to allow it. The peoples of the Gulf must know and fully grasp what their rulers are doing to them; because of these rulers, upcoming strikes will target their very economic and vital existence. We also affirm that the targeting of oil fields in Iraq is being carried out from the normalizing statelet of Kuwait and from the governorates of northern Iraq. Therefore, we say to them: If forced to do so, we will strike your oil fields as well.” Meanwhile, the façade group AWH made its second and final statement of the conflict on Telegram on April 1, 2026, noting that “our mujahideen from the sons of the Arabian Peninsula continue their jihad by targeting the Barakah [UAE] nuclear reactor until its destruction, making its facilities a testament to the downfall of the rule and subservience of the sheikhs of the Emirates. Our eyes will not close, nor will the fires of our anger be extinguished, until these people cease providing services to the Zionist-American enemy by using the Emirates as a launching pad for aggression against the Islamic Republic of Iran.”

bj Gulf governments began to call in Iraqi ambassadors to receive their protests about the increased attacks from Iraq in April 2026, with these occurring on April 9 (Kuwait), April 12 (Bahrain, Saudi Arabia), and April 14 (UAE). See “Iraqi Diplomats Face Wave of Summons as Regional Neighbors Protest Militia Attacks,” Kurdistan 24, April 14, 2026. The Kuwaiti demarche also referred to the overrun and burning of Kuwait’s consulate in Basra on April 7, 2026. David Cloud, “Pro-Iranian Protesters Attack Kuwait Consulate in Southern Iraq,” *Wall Street Journal*, April 7, 2026.

special effort was focused on the exhaustion of air defense systems in Erbil,¹⁰⁶ both using small salvos of three or four Shahed-101/107 drones, and using the jet-powered delta-wing drones (Hadid-110 and Shahed-238 or jet Shahed-136) now available in greater numbers.¹⁰⁵ The former (Shaheds) soaked up anti-drone guided weapons, and the latter (jets) could only be intercepted using Counter-Rocket, Artillery, and Mortar (C-RAM) systems.¹⁰⁷ In Baghdad, remaining suspected U.S. points of presence around Baghdad airport were struck increasingly with un-jammable fiber-optic guidance First-Person View (FPV) quadcopter drones¹⁰⁸ and with guided 122mm rocket systems.¹⁰⁶ A persistent trickle of unclaimed drone attacks struck Iraqi oil sites that were viewed as linked to U.S. energy industry interests, using jet drones in at least one case.¹⁰⁷

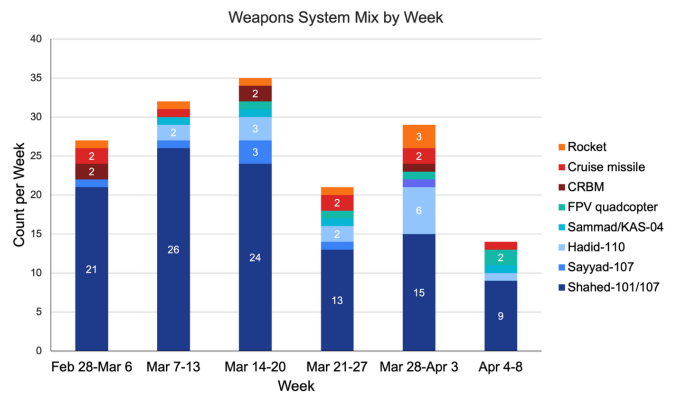


Figure 5: Weekly attack claims by muqawama groups by weapon type. Note that these only refer to claims with specific attribution of a weapon type in a defined attack, which means they represent a subset of under 15 percent of claimed attacks. Weapon type is often unclear in multi-attack claims such as IRI’s claims and some SAD claims. (Metrics charting by Alex Almeida)

Deploying PMF Units into Iran

The period leading up to the April 8 U.S.-Iran ceasefire witnessed one more important trend: an apparent commitment of PMF units inside Iran itself at a time when the crisis might still have veered toward sharp escalation—including even the widely rumored prospect of U.S. ground operations inside southern Iran.¹⁰⁸ Iraqi PMF personnel had frequently been reported inside Iran during prior protest cycles in 2019 and 2022, seemingly used to add additional capacity to Iranian regime security forces in the Arab and Kurdish areas of Iraq.¹⁰⁹ (These were disguised as humanitarian relief missions for instance to provide flood relief in 2019.¹¹⁰) According to interview material gathered by one author

bk In the view of the authors, the effort may have served a number of purposes: First, cost-imposition by using cheaper attack systems than the defending expendable munition; and second, capability development and operational lessons learned about penetration of air defenses.

bl The authors’ day-to-day monitoring of attacks on the greater Erbil area showed marked increase in close-in C-RAM intercepts during this period.

bm FPV quadcopters proved to be one of the more effective weapons used by the muqawama during the war, scoring direct hits on two C-RAM radar sites, a U.S. medevac Black Hawk, as well as fuel tanks, a hangar, and communications mast and at the Baghdad airport. The three-drone ambush of a U.S. diplomatic convoy at the BDSC on April 8 may also have employed quadcopter drones. Authors’ geolocated SIGACT dataset and claims database. See also David S. Cloud, Robbie Gramer, and Stephen Kalin, “An Iraqi Drone Attack Barely Missed a Security Convoy for a Freed U.S. Hostage,” *Wall Street Journal*, April 12, 2026.

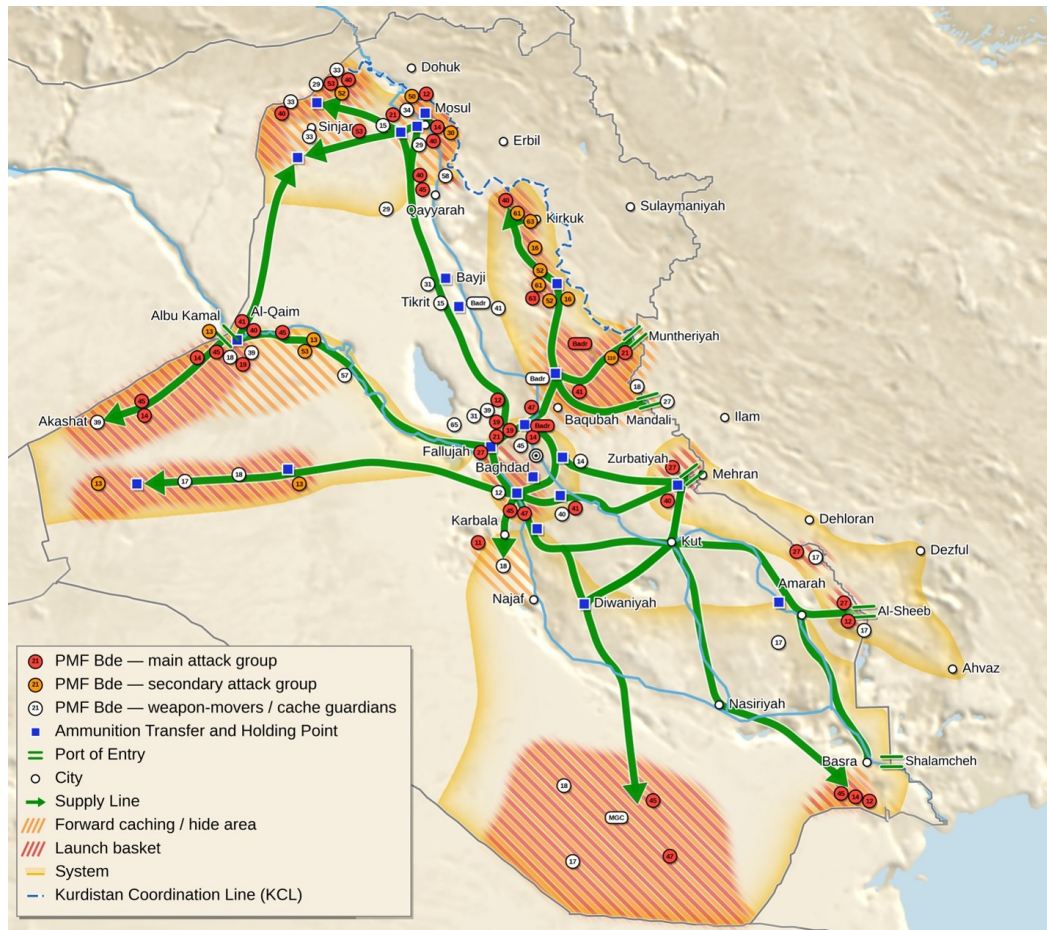


Figure 6: Network map of Iraqi *muqawama* and PMF involvement in 2026 kinetic attacks on U.S. targets, Iraq and the Kurdistan Region of Iraq, Jordan, the Gulf, and Syria. (Data created by the author team; design by Alex Almeida.)

(Knights),¹¹¹ this occurred again during Phase Four of the Iran war in 2026, again sometimes disguised as humanitarian aid convoys.^{bn} Badr 'special forces,' IRGC's Iraq-based Afghan and Pakistani proxy forces,¹¹² some Iraq-based Houthi volunteers,^{bo} and some smaller *muqawama* groups (such as Saraya Khursani, PMF 18)¹¹³ reportedly crossed into Iran in at least four convoys via the unofficial Mandali crossing (between Diyala and Sumar in Iran), the Zurbatiyah crossing (between Badra and Mehran in Iran), and the Shalamcheh crossing (between Basra and Ahvaz in Iran).¹¹⁴ Most of these crossings happened between March 28 and April 3, when long queues of PMF vehicles became bottlenecked at Iraq-Iran border crossings and were videoed.¹¹⁵

According to interview material gathered by one author (Knights),¹¹⁶ between 18,000 and 26,000 PMF personnel crossed

into Iran during this period, transported using large numbers of PMF vehicles and accompanied by large numbers of engineering vehicles belonging to the PMF and the PMF-operated (U.S.-sanctioned) Muhandis General Company.¹¹⁷ Other interview material gathered by the same author suggests that Iran-provided drone systems were shifted en masse from the Muthanna launch complex toward Basra in the same period on PMF trucks.^{bp} On April 4, the United States conducted heavy strikes on one such column in Shalamcheh,¹¹⁸ resulting in an apparent tit-for-tat cycle of retaliation between U.S. forces and AK (i.e., Nujaba) until after the ceasefire took effect on April 8.¹¹⁹ Though Iraqi groups (most

bn In early April 2026, numerous videos and still pictures began to appear on Iraqi social media of large traffic jams of PMF vehicles at the border ports of entry to Iran, headed into Iran. Phillip Smyth paid close attention to these convoys and reposted a number of images of them. He noted they were often emblazoned with Red Crescent markings, although no Iraqi Red Crescent missions were formally announced at the time and no new humanitarian crises were identified in Iran either. For an example of Smyth's work, see Phillip Smyth, "The 'Hashd (Iraqi PMFs) aid convoy' for Iran. Note a few issues . . .," X, April 3, 2026.

bo For instance, on April 1, 2026, 200 Houthi personnel were reported to have crossed via Mandali into Iran. Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.

bp It is interesting to note that the Basra area is probably not optimal (due to range restrictions) for the launching of Shahed-107 drones into the Hormuz and southern Gulf area, which was the apparent emerging locus of the war in late March. In contrast, Ahvaz province, just inside Iran, provides launch areas that allow the *muqawama's* most main drone systems to reach the southern Gulf.

clearly KSS) signaled their willingness to keep striking the Gulf,^{bq} the KRI and U.S. targets, the *muqawama*'s war effectively shut down on April 8, the last day that IRI issued a daily claim, and when it announced a ceasefire of two weeks 'in Iraq and the region.'¹²⁰

Part II: The Four Wars Within the War for *Muqawama* Networks

In the 2026 war, there were four sub-campaigns undertaken by the *muqawama* that overlapped and unfolded in parallel. They are tackled below in the order in which they emerged, but it should always be borne in mind that they occurred in an overlapping manner, not sequentially. In Part I, the authors have described the temporal phases of the war, but a geographic level of analysis is also needed. The following sections run through each of the main *muqawama* operating zones in the 2026 war—the north versus Kurdistan and Syria, the west versus Jordan, the Baghdad sub-campaign, and the launch campaign against Gulf targets.

The Northern War

For many years, the KRI has been the 'punching bag' of the Iraqi militias.^{br} The key targets in Erbil were U.S. sites: the U.S. and coalition annex at Erbil International Airport (EIA); the U.S. consulate; KRI military and government sites, and private venues, where U.S. or other intelligence services might be operating in the Iranian axis' view; and U.S. oil companies. Setting aside the Iranian Kurdish bases—which appear to have been almost^{bs} entirely struck directly by Iran^{121 bt}—this was the 'target deck,' and it did not change a great deal during the war. The KRI was attacked from two sides:

bq On April 8, 2026, Abu Alaa Al-Walaid posted a statement on his official Telegram channel noting that "we emphasize the necessity of keeping the battle open with the rapacious entity [Israel], which does not respect international law, and against normalizing with states that harbor the interests of the Zionist entity, such as the UAE, Bahrain, and other countries in the region." On April 20, 2026, SAD posted on its Telegram channel that "we in the Islamic Resistance in Iraq – Saraya Awliya al-Dam – are fully prepared to resume our military operations, which have exceeded 200, against the occupying presence in Iraq and the region, with greater intensity and impact, in a manner that will gladden the hearts of the believers and enrage the infidel aggressors."

br When Iraqi *muqawama* have felt the need to flex their muscles but have needed to be cautious around major powers such as the United States and Israel, they have often attacked Iraqi Kurdistan. They are partly following their own prejudices, as many Arab, Turkmen, and micro-minority militiamen have their own communal and territorial grudges against Iraq's Kurds. Anti-KRI attacks rarely draw Iraqi public backlash onto the militias, due to the troubled relationship the Kurdistan Region has with federal Iraq's body politics and media, and Iraqi Kurdistan has no real retaliatory capability to factor. Iran seems to have no reservations about striking the KRI either: The IRGC regularly strikes Iranian Kurdish oppositionists in Iraqi Kurdistan and shares the view of the *muqawama* that the KRI is too close to the Americans, the Turks, and maybe even the Israelis. In the 2026 war, IRGC paranoia about an Iranian Kurdish uprising supplied via the KRI reached its zenith. Little surprise then that the KRI was the single most heavily targeted location in the *muqawama*'s war effort. This is the authors' collective conclusion, based on their synthesis of the known facts, having monitored *muqawama* anti-Kurdistan attacks across the 2017-2026 period.

bs As the authors describe in footnote DX, a number of anti-Iranian Kurdish strikes may have been launched from Iraq by Iraqi militias, including Badr and SAD.

bt There were some notable exceptions to this pattern, including a twin-drone attack on Kurdish opposition bases in Sulaymaniyah claimed by SAD on March 24 (SAD's only such claim during the war) and an April 3 drone attack on a Komala villa in an urban Sulaymaniyah residential neighborhood, which authors assess was also launched out of Iraq. SAD Telegram post, March 24, 2026, and authors' geolocated SIGACT dataset.

a Nineveh launch area to the west and an 'eastern Tigris'^{bu} launch area to the south. Militiamen in both these areas had extensive, fresh experience in bombarding the KRI, albeit not at the high rate of fire seen in the 2026 war.¹²²

The Nineveh Launch Area

The Nineveh Plains has long been the key launch area for attacks on Erbil from the west,¹²³ and it is located so close to the KRI capital that even 122-mm rocket systems can threaten the city's outskirts.^{bv} The Nineveh Plains are controlled by Liwa al-Shabak/Quwwat Sahl Nineveh (PMF brigade 30),¹²⁴ formed by Waad Qado,¹²⁵ and the other is Babiliyun (PMF 50),¹²⁶ formed the Rayan Kildani.¹²⁷ Both leaders were sanctioned by the United States for human rights abuses under the Global Magnitsky Human Rights Accountability Act.¹²⁸ The key 'trigger-pulling' militia operating from the Nineveh Plains is assessed by the author team to be KSS (claiming attacks as SAD),^{bw} using the sites controlled by PMF 30 and 50.¹²⁹

In the 2026 war, militias seem to have realized even before the war began that operating solely from the Nineveh Plains might be much more difficult than in the past, and they prepared to bombard the KRI at a greater remove than before (i.e., launching from beyond visual distance of Kurdistan's border, even from scores of kilometers inside federal Iraq).^{130bx} Prior to the war (in Phase Zero), discussions were held between 'the usual suspects' (KSS (PMF 14), PMF 30 and PMF 50) and a range of PMF brigades and other *muqawama* players active in Mosul and the expanses of Nineveh between the Tigris and the Syrian border.¹³¹ Advanced conventional weapons began to be cached in a wider variety of locations, from the Rashidiyah area, north of the Tigris on the east Mosul side, all the way west to Syrian border locations such as Rabia, Khanasor,

bu This is the author team's formulation, but it does echo many uses of the geographic divider (east of the Tigris) by Iraqi security forces over the years, including the current PMF East Tigris Operations Command. Michael Knights and Alex Almeida, "Militia Schisms: The Dissolution of the PMF Northern Axis," Militia Spotlight, Washington Institute for Near East Policy, August 5, 2024.

bv Most notably, in September 2020, a 122mm rocket was launched at Erbil from a concealed truck launcher in eastern Nineveh Plains. The rockets were launched at an extreme range of 40km, from a site in the 'no man's land' between the Kurdish and Iraqi internal border checkpoints. On March 5, 2026, a similar truck-launched 122mm shoot at Erbil out of the same launch basket was successfully foiled by U.S. or Kurdish Peshmerga forces. Data drawn from the authors' geolocated SIGACT dataset covering the 2017-2026 period of *muqawama* kinetic operations.

bw In February 2021, a botched 107mm shot from a truck infiltrated into the KRI, spraying rockets across Erbil airport and the city's northwestern quadrant, where most of the major international hotels and business towers in the city are concentrated. The attack was subsequently linked to a KSS cell that had recruited a local Turkmen with a Kurdistan residency permit to assist in the purchase and emplacement of the truck launcher inside the KRI. Data drawn from the authors' geolocated SIGACT dataset covering the 2017-2026 period of *muqawama* kinetic operations. See also Michael Knights, "The Erbil Rocket Cell: Insights from Haidar Hamza al-Bayati's Confession," Washington Institute for Near East Policy, March 7, 2021.

bx A launch point closer to the target is usually preferred because it minimizes the distance the drone's inertial navigation system will accumulate drift error and cuts down on flight plan complexity, including the number of programmed waypoints required to maneuver around major terrain obstacles. Launch baskets during drone campaigns against Kurdistan, including the brief June-July 2025 attack series and the long-running micro-campaign against the Khor Mor gas plant were generally located within 20-25km of the Kurdish internal border. Data drawn from the authors' geolocated SIGACT dataset. Data drawn from the authors' geolocated SIGACT dataset covering the 2017-2026 period of *muqawama* kinetic operations.

Sinjar, Baaj, and to the south in Hatra.¹³² The author team assesses that the main connective tissue between attack cells and storage sites—fulfilling the role played by the Distribution Company of a U.S. Army Brigade Support Battalion—were two PMF units: Kataib Ansar al-Hujja (PMF 29) and Kataib Al-Imam Ali (PMF 40).¹³³ The latter seems to play a senior coordinating role in *muqawama* drone and missile logistics in Nineveh.^{by}

The *muqawama* equivalent of the U.S. Army's Ammunition Transfer and Holding Point¹³⁴ were the PMF bases operated at the edges of Mosul city and in western Nineveh.¹³⁵ The caches were run by Kataib Al-Imam Ali (PMF 40); Quwwat Waad Allah (PMF 33); Liwa al-Hussein (PMF brigade 53); Quwwat al-Shaheed al-Sadr (PMF 15); plus Kataib Ansar al-Hujja (PMF 29); KH (PMF 45, 47); and KSS (PMF 14).^{136bz} From the first days of March 2026, with PMF 30 and 50 locations in the Nineveh Plains being repeatedly struck by U.S. aircraft,¹³⁷ most *muqawama* weapons seem to have been stored outside the plains until they were ready for immediate use, whereupon they would be driven from Rashidiyah or across the Tigris and used as soon as was practicable. Some of the 'first load' used in the war may have been recovered from Syria-located caches.¹³⁸ Interviews (Knights) suggest a 'second load' of drones and missiles seems to have been fed into this network of ammunition transfer and holding points in western Nineveh directly from central ammunition supply points (Camp Ashraf, Diyala; Jurf as-Sakr, Babil) and areas close to the Iranian border).¹³⁹

The East Tigris Area

The 'East Tigris' area (author team's nomenclature) is a more spread-out set of launch areas. As noted above, even before the current war, the militias in the Kirkuk, Salah al-Din, and Diyala provinces were

among the most practiced in bombarding the KRI.^{ca} Farthest north, cells in Dibis had regularly launched drones and rockets at Erbil and U.S. or French bases in the adjacent Makhmour and Kirkuk city areas since 2018.^{cb} In this war, Kataib Al-Imam Ali (PMF 40) sites in locations such as Qayyarah and Dibis were bombed by the United States multiple times,¹⁴⁰ but (in the assessment of the author team) these sites were probably also basing launch cells from KH, KSS, and particularly Nujaba (PMF 12).¹⁴¹ (There is a publicized precedent for this kind of 'landlord' role for Kataib Al-Imam Ali. On December 2, 2023, five Nujaba drone operators were killed by a U.S. strike on a Kataib Al-Imam Ali base at Dibis.^{cc})

Farther south, a second set of experienced kinetic drone and rocket cells have long been active between Kirkuk and Tuz Khurmatu: the Badr-linked Quwwat al-Turkmen (PMF 16), Fawj Amerli (PMF 52), and new micro-units like PMF 61 and 63.¹⁴² All were struck regularly by the United States throughout the 2026 war.¹⁴³ These predominantly Turkmen units are coordinated by the head of the PMF North and East Tigris Operations Command,¹⁴⁴ Abu Hussam al-Sahlan (Hamid Ibrahim Abdal-Ridha), a veteran operator whose service under the IRGC as a senior Badr officer goes

by PMF units in Nineveh are nominally supposed to answer to the PMF Nineveh Operations Command, which is dominated by al-Muhandis appointee Ali Kadhimi al-Musawi and his powerful deputy, Kataib Al-Imam Ali operative Hajj Ali Kerwei. Michael Knights, "Iran's Expanding Militia Army in Iraq: The New Special Groups," *CTC Sentinel* 12:7 (2019). See also Michael Knights, Hamdi Malik, and Aymenn Al-Tamimi, "Honored, Not Contained: The Future of Iraq's Popular Mobilization Forces," *Policy Focus* 163, Washington Institute for Near East Policy, 2020.

bz To preview the method used, these linkages and role divisions were identified using different overlapping sources and types of data. For instance, two human sources suggest that PMF 29 is supporting KSS attacks in the Nineveh Plains by transporting drones to and from arms caches extending west into the Rabia area, and another source suggests PMF 53 is caching weapons in three parts of the Rabia area. The authors' historic datasets include numerous references to PMF 29 and PMF 53 activities in these areas, aiding assessment of their sourcing and sometimes resulting in exact matches of geolocated arms storage points from different sources, whose reporting is separated by months or years. Old datasets of geolocated property use (i.e., a water and sanitation motor pool) allows enrichment of and validation of certain details from reports. The authors' incident database makes sure that reported deliveries of weapons match up with launch reports, and they may match with prior launches from previous years. The authors' dataset of U.S. strikes might then also note a U.S. strike nearby to the locations mentioned, suggesting the United States also view the hamlet as an active enemy point of presence. These 'man-draulic' non-AI calculations, report by report, combine to become a mesmerizing synthesis effort spanning multiple maps and whiteboards that may include some mistakes, but which also undoubtedly contain some interesting intelligence findings.

ca Some of the most experienced 'trigger-puller' units in this area were PMF brigades 16 and 63, two local Turkmen militia units stationed along the Turkmen corridor from Tuz Khurmatu in Salah ad-Din to Dibis, northwest of Kirkuk. Both units have been intimately involved in the long-running micro-campaign against the Khor Mor gas plan since 2023, and were big providers of launch crews during last year's June-July attack series. The authors suspected that during the current campaign, these units likely graduated from providing the grunt labor, security 'wrappers,' and last-mile logistics to operating their own drone cells. Data drawn from the authors' geolocated SIGACT dataset covering the 2017-2026 period of *muqawama* kinetic operations.

cb PMF brigades 61 and 62 – two brigades developed from bodyguard units loyal to Abdul-Ridha Yilmaz al-Najjar, al-Sahlan's predecessor as commander of the Northern Axis – are among the suspected 'trigger puller' units in this area alongside Brigade 40. Since the Twelve Day War last year, the link between these local ground-holding units and the specialized drone operators appears to be Bassim Ghazi al-Amerli, the Altun Kupri-based head of KSS' political wing (and failed parliamentary candidate), and former head of intelligence in the PMF Northern Axis. Data drawn from the authors' geolocated SIGACT dataset covering the 2017-2026 period of *muqawama* kinetic operations.

cc The apparent Nujaba cell leader killed at Dibis, Hussein Hadi al-Aqabi, apparently had close ties to Abu Taqwa, the high-level Nujaba leader killed on January 4. See Michael Knights, "Who Are Nujaba and Why Did the U.S. Just Strike Them?" Washington Institute for Near East Policy, January 4, 2024. On December 3, a U.S. airstrike in Kirkuk killed five members of the Iran-backed militia Harakat Hezbollah al-Nujaba (HaN) as they were preparing to launch a one-way attack drone. See Michael Knights, Hamdi Malik, Ameer al-Kaabi, and Crispin Smith, "Profile: Harakat Hezbollah al-Nujaba," Washington Institute for Near East Policy, April 27, 2021. Social media affiliated with HaN immediately mourned the dead fighters. Shortly after the U.S. strike, Sabereen News and other platforms close to HaN identified the slain operators as part of the Islamic Resistance in Iraq (IRI) brand and claimed that they were killed while conducting their duty. See Hamdi Malik, Crispin Smith, and Michael Knights, "Profile: Sabereen News," Washington Institute for Near East Policy, April 9, 2021, and Malik and Knights, "Profile: The Islamic Resistance in Iraq." On December 4, the five fighters were buried in Najaf after a funeral service in Baghdad. Their coffins were covered with HaN's flag, not the Iraqi or PMF flag. Ameer al-Kaabi, "Overlap Between the Islamic Resistance in Iraq and the Popular Mobilization Forces," Washington Institute for Near East Policy, December 12, 2023.

back to the 1980s, according to the CTC's Harmony files.^{cd}

The final set of kinetic threat actors facing the northern front is the collection of Diyala-based Badr units (PMF 20, 21, 22, 23, 24, and 27) and the Badr-formed Shia Kurdish unit Fawj Fayli (PMF 110).¹⁴⁵ These units appear to have provided a support architecture for at least two Badr low-profile kinetic action cells undertaking drone strikes on the KRI, and perhaps striking U.S. locations in Baghdad from the eastern fringes of the city.¹⁴⁶ These cells were operating under the control of the head of the PMF Diyala Operations Command, Badr veteran Sayyed Talib al-Musawi (Taleb Mohammed Hussein)^{ce} and his Badr comrade Abu Jassim al-Askari.¹⁴⁷ In this war, the author team suggests, Badr went further than just importing, moving, and hiding weapons for terrorist groups such as KH and KSS.¹⁴⁸ Badr also undertook at least 20 drone attacks on U.S. and Iraqi targets,¹⁴⁹ just over half of which were launched into the KRI from northern Diyala.¹⁵⁰ In the assessment of the author team, Badr undertook its attacks within the IRI claim mechanism.^{cf} On the last full day of the war, April 7, the United States mounted multiple strikes on Badr's main ammunition supply point at Camp Ashraf.¹⁵¹

The Mini-War on Jordan

In the 2026 war, Jordan played an even more important role than it had in the prior 2023-2025 conflicts involving the Iraqi *muqawama*. In the post-October 7 (2023) period, Jordan acted as additional strategic depth for Israel as it defended against drone

attacks from Iran and Iraqi militias.^{cg} In 2026, Jordan's air bases were also one of the most vital launch points for U.S. combat aircraft since most U.S. aircraft were withdrawn from the Gulf prior to hostilities.^{ch} Only 22 attacks on Jordan were claimed by the Iraqi *muqawama* in the 2026 war,¹⁵² though this low figure may mask a much larger number of additional attacks obscured within the non-located IRI claims. In an intriguing conundrum, 12 of the 22 Jordan attack claims were made by the aforementioned new claim brand Rijal al-Bas al-Shadeed (RBS, Men of Great Valor).¹⁵³

Effectively striking locations such as Muwafiq al-Salti Air Base (MSAB) with the workhorse *muqawama* weapon, the Shahed-101/107,^{ci} required launch sites along Iraq's western border with Syria, from as far north as Rabia (Nineveh), but more practically from western Anbar.^{cj} This area had been a prolific drone and rocket launch area in the near past due to the U.S. bases in western Anbar and eastern Syria,¹⁵⁴ but by February 2026, the U.S. base at Al-Asad (in Anbar) had closed, and the United States had collapsed its ongoing presence at the string of outposts they had previously maintained in eastern Syria.¹⁵⁵ Anbar provides an excellent launch pad for attacks on Israel, but in 2026, the Iraqi *muqawama* mirrored Iran's own apparent strategy^{ck} by eschewing a long-range war against Israel, and instead focusing on nearer enemies (the United States, Iraqi Kurds, and the Gulf). This left Jordan as practically the only game in town for drone cells in western Anbar. In this war, at least, every other remaining target in the region could

cd During the 1980s, al-Sahlani lived in a Badr compound in Khorramshar with now-deceased PMF chief Abu Mahdi al-Muhandis, emerging as one of al-Muhandis' top proteges. In the 1990s and early 2000s, he headed Badr's Southern Axis in Maysan, Dhi Qar and Muthanna, smuggling EFPs and other Iranian munitions into Iraq. In addition to heading the ETOC, he currently also serves as Badr chief Hadi al-Ameri's executive deputy and 'jihad assistant.' Harmony Document ISGQ-2005-00038283, <https://alghadeertv.iq/archives/375633>. The former is an interview from Khamenei's official Arabic-language website featuring an interview with al-Sahlani where he describes his relationship with Muhandis and Soleimani. The latter is from the official Badr news agency's recent report on their Shura meetings with al-Sahlani and Abu Jassim al-Askari seated on either side of Hadi al-Ameri.

ce Abu Jassim headed Badr's Investigation and Inspection Directorate in the late 1990s and early 2000s and currently serves as Hadi al-Ameri's political deputy, the 'civilian' counterpart to al-Sahlani's role as jihad assistant. Harmony Document ISGQ-2005-00038283, "Iraqi Intelligence Study about the Badr Corps," <https://alghadeertv.iq/archives/375633>

cf An earlier footnote discussed the labyrinthine synthesis effort involving historic and new geolocated attack data: A very similar effort was undertaken using all available claim data, videos, imagery, prior patterns set by the claim brands, location targeting trends linked to the brand, and human intelligence gathered by Knights. This allowed multi-source synthesis involving how detailed interview data regarding the targeting and point of origin of Badr drone attacks in the 2026 war interacted with claim data from the appropriate days. Interview-identified Badr strikes (for instance against BDSC in Baghdad, or an Iranian Kurdish opposition base, or an oil company location) frequently coincided with no RBS, JG or KSS/SAD or Nujaba/AK located claims that day or shortly thereafter. Though there could be factors unknown to the authors, and it is conceivable that Badr attacks might be claimed by no one in some or all cases, it seems more likely to the authors that Badr kinetic actions were enfolded within the non-detailed, non-located IRI attack claim totals. This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.

cg On October 1, 2024, Iran attacked Israel with ballistic missiles, and Jordan's air defense intercepted some of the incoming projectiles. See "Jordan: Background and U.S. Relations," Congressional Research Service. In June 2025, during the Twelve Day War, Israel and Iran launched barrages of missiles and drones against each other. Many of these crossed Jordanian airspace, and with U.S. assistance, Jordanian forces shot down Iranian missiles crossing over Jordan, leading to widespread domestic anger and charges that Jordan was, in effect, helping to protect a State of Israel that was at that same moment killing large numbers of Palestinian civilians. Curtis R. Ryan, "With Friends Like These: Jordanian Security Amidst the US-Israel War on Iran," Project on Middle East Political Science, June 2026.

ch Riley Mellen, Christoph Koettl, and Eric Schmitt in "Dozens of U.S. Planes Are at Jordan Base, Satellite Images and Flight Data Show," *New York Times*, February 20, 2026, indicated a tripling over usual levels in the number of American warplanes stationed at Muwaffaq al-Salti Air Base in central Jordan. According to Ghaith al-Omari and David Schenker, because U.S. bases in the Gulf states are closer to Iran and more vulnerable to missile and drone attacks, the kingdom has emerged as a critical node in the "Western Basing Strategy," enabling the safer positioning of American assets. See Ghaith al-Omari and David Schenker, "Jordan's Wartime Balancing Act," Washington Institute for Near East Policy, April 15, 2026.

ci The authors estimate the Shahed-101/107 accounted for some 75 percent of all identifiable projectile launches during the war. It was the only weapons system in continuous use from the opening burst of attacks to the April 8 ceasefire. Data drawn from the authors' attack claims database and geolocated SIGACT dataset. Always an apparent easy job to assemble, the Shahed-101/107 has been made even more simple to transport, set up, and launch by being supplied inside a reusable carrying case that doubles as a pop-up launcher stand.

cj Assuming a range of around 800km. For a brief discussion of the difficulties of estimating the range of the Shahed-107 drone system, see footnote CX.

ck Israel accounted for only a tiny fraction of the claimed targets in the authors' detailed attack claims database from the 2026 war (two claims by RBS), though a larger number of attacks on Israel may have been rolled into the IRI's daily digests.

be hit more easily from somewhere else.^{cl}

As was the case farther north, the Anbar militias appear to have begun preparing for the war since mid-February 2026.¹⁵⁶ One aspect of this was the acceleration of what appears to have been a salvage effort on advanced conventional weapon caches in the Syrian Euphrates Valley areas such as Al Bu Kamal and Baghuz.¹⁵⁷ In the view of the author team, it makes sense that not all weapons could be evacuated during the rapid collapse of the Assad regime in December 2024, or immediately after while U.S. forces were present for part of 2025.¹⁵⁸ Local smuggler networks are very strong in these areas and would probably not hesitate to squirrel away any potentially valuable materiel to later sell to the highest bidder.^{cm} In Anbar, this recovery effort seems to center on Al-Qaim, involving Kataib Al-Imam Ali (PMF 40), KH (PMF 45), and KSS (PMF 14) as the receiving parties on the Iraq side.¹⁵⁹

The network of *muqawama* ammunition transfer and holding points handrail Anbar's loop of highway corridors clockwise from Al-Qaim to Hit, Ramadi, Rutba, the H-3 airbase, Akashat, Akkas, and back to Al-Qaim.¹⁶⁰ Key cache guardian groups and kinetic launch operators include KH, Harakat Allah al-Awfiyah (PMF 19), Saraya al-Jihad (PMF 17), and Liwa al-Tafuf (brigade 13).¹⁶¹ The United States attacked these units from the start to the end of the war in recurring strikes on Al-Qaim, Akashat, the H-3 airbase, Rutba, Kilo 160, and other *muqawama* sites.¹⁶² The distribution company role in Anbar appears to be played by Harakat al-Abdal (PMF brigade 39), with Saraya Talia al-Khorasani (PMF 18) handling cross-province movements to the south (Jurf al-Sakr, Muthanna) and Liwa Hussein (PMF 53) running weaponry from Al-Qaim up the border to Nineveh.¹⁶³

The 'Ring of Fire' Around Baghdad

As discussed in Part 1, Phase Two of the *muqawama* campaign was characterized in large part by a determined effort to drive U.S. forces out of various remaining points of presence in Baghdad. This effort had not been part of Phase One, which had hardly touched

Baghdad.^{cn} In the view of the authors, the *muqawama* have drawn a distinction between Baghdad diplomatic targets since at least 2021—vice military targets outside the capital.¹⁶⁴ This meant Baghdad sites were not attacked from day one of the war. Instead, ramping up a multi-group Baghdad attack surge appeared to take nearly two weeks to hit its stride, spanning almost the whole length of Phase Two.¹⁶⁵

The IRI's contribution to the campaign is hard to gauge due to the non-located nature of most of its claims, though IRI did break its own pattern (in almost the only such instance^{cp}) to openly claim the successful March 24 FPV quadcopter drone attacks on a U.S. medevac helicopter and radar at BDSC.¹⁶⁶ According to interview material gathered by one author (Knights),¹⁶⁷ the IRI effort encompassed attacks on BDSC and the U.S. military advisor group at Area IV of the Baghdad airport by the Badr movement (nine attacks) and by Asaib Ahl al-Haq (five attacks).¹⁶⁸ These included a 'stonk' of five heavy 240mm Falagh-1 rockets on March 15 that wounded five airport employees and security guards,¹⁶⁹ and possibly also the March 22 107mm shot at the ISOF's Area IV compound, which wounded five Iraqi commandos.¹⁶⁹

Of the individual claim brands, SAD (the KSS façade group) arguably made the longest and most sustained effort of the war to evict U.S. presence out of Baghdad.¹⁷⁰ SAD's 15 attack claims included three FPV drone attacks¹⁷¹ (plus an initial quadcopter

cl Western Anbar's value as a launch area is likely to increase in future conflicts however, since it can range targets such as Onda airbase in the Israeli Negev, where the United States based F-22 fighters during the current conflict, the British Sovereign Base Areas on Cyprus, and, using long-range drone systems, Chania airbase in Crete, as well as U.S. operating locations in the Western Basing Network such as Camp Yanbu and the Saudi airbases at Tabuk and Taif, not to mention NEOM and other civilian Vision 2030 development projects at the head of the Red Sea. Authors' range calculations. See also John Gambrell, "US exploring new bases in Saudi Arabia amid Iran tensions," *Military Times*, January 26, 2021, and Michael R. Gordon and Lara Seligman, "In a First, U.S. Deploys Combat Jets to Israel for Potential Wartime Mission in Iran," *Wall Street Journal*, February 26, 2026.

cm This stretch of the Syrian border was always a major problem for modern states. In the authors' collective 40 years of covering Anbar and Nineveh, no government (Baathist Syria or Iraq, the successor regimes, or the military forces of the U.S.-led coalition and the Syrian Defense Forces) have ever really outmatched cross-border smuggling networks along this border. Likewise, whenever chaos has struck, locals in Iraq (and Syria and Yemen) have (in the lived experience of one author, Knights) typically been very quick to identify abandoned or unguarded military materiel, relocate it, and sell it later.

cn The BDSC at Baghdad airport appears to have suffered only three or four drone attacks prior to March 5, one of which was claimed by SAD. An unfired bank of 107mm rocket tubes was also found in Abu Ghraib, west of the airport, on March 3 (possibly left to be found, as a signal). On March 6, SAD claimed a 122mm rocket shoot at the BDSC; an elevating dump truck-type launcher was near the airport on the previous night. The immediate trigger for the shift to a more kinetic in the Baghdad area on March 5 may have been a raid by ISOF commandos (based at Area IV, adjacent to the BDSC) on a suspected PMF ammunition storage site on East Baghdad's Palestine Street (central Baghdad urban turf with a strong level of KH ground presence and control) on the previous day. Authors' geolocated SIGACT database from the 2026 war and *muqawama* attack claim database.

co Militia leaders in statements will often draw a distinction between military targets outside of Baghdad, targets viewed as 'military' (such as the Baghdad Diplomatic Support Center) on the outskirts of Baghdad, and diplomatic sites in central Baghdad. Targeting of these categories represents progressive steps up a kind of escalatory ladder. This is the authors' collective conclusion, based on their synthesis of the known facts, and based on monitoring of all *muqawama* operations against Baghdad diplomatic targets since 2019.

cp The former U.S. special operations at Harir Airfield near Erbil is the other exception, with two location-specific claimed attacks by IRI. The only other exception was a FPV drone attack on BDSC claimed by IRI. These insights derived from the authors' detailed attack claims database from the 2026 war.

cq A truck with three banks of two 240mm rocket tubes was found near Radwanayah outside the airport perimeter on the night of March 15. Analysis by the authors shows the same launch truck featured in IRI video claiming an attack on an undisclosed 'occupation base.' 240mm rockets are only rarely employed by the *muqawama* in Iraq. The last recorded 240mm attack was another, two-rocket shoot at the BDSC in January 2022. That attack was claimed by Saraya Ababil, assessed by the authors to be an AAH-run brand. Authors' geolocated SIGACT database, IRI Telegram post, March 16, 2026, and Crispin Smith and Hamdi Malik, "Saraya Ababeel Claims Baghdad Drone and Rocket Attacks," *Militia Spotlight*, Washington Institute for Near East Policy, January 7, 2022.

recon flight over the BEC on March 16).^{cr} (It is interesting to note that on September 10, 2024, SAD claimed a quadcopter attack on BDSC.^{cs}) Early in the war, the enigmatic RBS undertook a specialized mini-campaign using the rarely spotted Sayyed-107 V-tail drones to try to destroy the C-RAM system protecting BDSC.¹⁷² The assessed Nujaba claim brands—Ashab al-Kahf and Jaysh al-Ghadab—claimed eight attacks on BDSC and Area IV.¹⁷³ These included Jaysh al-Ghadab's claimed use of 'Shaib-12' guided 122-mm rockets on March 29,¹⁷⁴ which appear to have been targeted on Iraqi military transport aircraft present at Baghdad airport for an unknown reason.^{ct}

The Logistics Ring Around Baghdad

The militia support system in Baghdad has long been characterized as a ring of advanced conventional weapon storage sites, each under the control of one of the main armed groups.^{cu} The Kataib Hezbollah effort is often viewed as being centered on Jurf as-Sakr,¹⁷⁵ but this war showed a more dispersed system that may have tried to operate away from known sites, many of which were struck during the war: notably Jurf as-Sakr, KH locations near Palestine Street, Baghdad, and the PMF Anbar Operations Command complexes in Habbaniyah and Taqqudum.¹⁷⁶ According to interview material gathered by one author (Knights),¹⁷⁷ KH (PMF 47, in this case)

shared Baghdad facilities in the war with KSS,^{cv} such as the Camp Saqr (Falcon) base in western Baghdad and various water treatment plants in Nahrawan, on the southeast edge of the city. KH's 'arc' of the city is southern-focused but not limited to Jurf.¹⁷⁸

In the same manner that KH is not apparently limited to the southern arc of Baghdad, Harakat al-Nujaba may not be limited to the northern edge of Baghdad, where its better-known Tarmiyah and Taji strongholds are located.^{cw} Nujaba also operated a large advanced conventional weapons distribution hub south of the city, near where highways 1 and 8 meet.¹⁷⁹ Badr played a major role in securing two parts of the 'Baghdad belts'—the western roads linking northern Baghdad and Fallujah (under Badr's PMF 27),¹⁸⁰ and the Jisr Diyala area to the southeast.¹⁸¹ Both Kataib Al-Imam Ali (PMF 40) and AAH's PMF 41 suffered heavy U.S. strikes during the war on their logistics hubs near Suwayrah, Wasit, south of Baghdad.¹⁸²

The Southern Campaign Against the Gulf

The effort by Iraqi militias to strike the Gulf States is the least understood *muqawama* sub-campaign of the 2026 war. Only 35 location-specific attack claims pertain to Gulf targets,¹⁸³ and even the ACLED database only contains 65 attacks assessed to have struck the Gulf in the 2026 war after being launched from Iraq.¹⁸⁴ An unknown number of anti-Gulf strikes may be concealed within the IRI's non-located claims.

Sixteen claims concerned Kuwait,¹⁸⁵ a major U.S. basing location that can be struck from deep within Iraq with Shahed-101/107 drones or from the border with any militia weapon, even tactical rockets, quadcopter drones and CRBMs.¹⁸⁶ On March 4, two concealed double-CRBM systems were found unfired in Basra on the border with Kuwait,¹⁸⁷ and from the second week of the war onward, Iraq-based attacks on Kuwait were claimed multiple times a week.¹⁸⁸

Fifteen attacks were claimed against Bahrain,¹⁸⁹ a much more distant target that lay at the outer range of Shahed-101/107 drones launched from the border or longer-range systems (KAS-04, Shahed-136 and cruise missiles) launched from the Iraqi interior. (Of note, in April 2024, a KAS-04 long-range drone strike on Israel was jointly claimed by IRI and Bahraini group Saraya al-Ashtar.¹⁹⁰)

Only three claims involved Saudi Arabia,¹⁹¹ involving two Riyadh locations (Prince Sultan Air Base and Iskan Village) positioned in a similar 'range band' to Bahrain. No Iraqi militia claimed attacks

cr No targets were struck in the SAD video of the March 16 overflight, but the overflight was likely post-operation reconnaissance for an (unclaimed) attack that took out Saab 1X Giraffe C-RAM tracking radar at the BEC on March 14. SAD's coyness about openly claiming the March 14 attack hints at the *muqawama*'s demarcation between sensitive diplomatic targets in the Baghdad IZ and the outlying military sites. Authors' geolocated SIGACT database from the 2026 war, SAD Telegram post, March 17, 2026.

cs Kataib Hezbollah denied involvement. Kataib Sayyid al-Shuhada (KSS) reported faster than any other Shi'a platform. See Michael Knights, Amir al-Kaabi, and Hamdi Malik, "Tracking Anti-U.S. and Anti-Israel Strikes From Iraq and Syria During the Gaza Crisis," Militia Spotlight, entry dated September 10, 2024.

ct Possibly misidentified as an U.S. military transport, though the targeted aircraft — an An-32 turboprop — is also used by the Iraqi military to fly ISOF commandos around the country. Use of the Arash guided long-range 122mm rockets is rare in Iraq. The last such attack, in July 2025, also targeted an Iraqi special operations location, the ISOF's Kirkuk commando battalion base at Kirkuk airport. Beyond their vendetta against Iraq's U.S.-partnered special operations forces, the *muqawama* also seem to have developed a fixation on Iraq air defense radar sites, with least two successful and four near-misses or intercepted drone attacks on Imam Ali (Tallil) airbase, al-Asad, Balad, Taji, Basra, and Umm Qasr during the current conflict. Air defense radars at Kirkuk, Taji, al-Asad, and Tallil (the headquarters of Iraq's southern, central, western, and northern air defense regions) as well as Balad, were also targeted during the Twelve Day War last year. This insight is derived from the authors' detailed attack claims database from the 2026 war.

cu In the authors' collective experience, it has long been discussed by human sources and contacts that the main 'issue points' for Iran-provided drones are a ring of drone caches in the Baghdad outskirts.

cv One intriguing recurring feature of interview data gathered by Knights is the repeated mention in multiple provinces (Baghdad, Diyala, Nineveh) of drone and missile caching and distribution using Ministry of Water Resources and municipality locations and vehicles over which *muqawama* forces have attained access. This fits with some historical observed trends: the caching of weapons at so-called 'no-strike locations' protected from air attack by international humanitarian law and longstanding anecdotal evidence (from Iraq and Yemen) and some video (from Houthi Yemen) received by one author (Knights) showing water tanker 'disguises' applied to transporter-erector launchers being used to transport missiles. Author (Knights) interviews, multiple Iraqi contacts, 2023-2026; exact dates, names, and places withheld at request of the interviewees. See also author (Knights) interviews, multiple Yemeni, UAE and Saudi contacts, 2018-2026; exact dates, names, and places withheld at request of the interviewees.

cw It is worth recalling that the senior Nujaba commander Mushtaq Talib Al-Saeedi (Abu Taqwa) was identified as the deputy head of the PMF Baghdad Belt Operations. Militia Spotlight noted at the time of his death that he "was known to distribute advanced Iranian conventional weapons (drones and missiles) warehoused in the Baghdad Belts area." Knights, "Who Are Nujaba and Why Did the U.S. Just Strike Them?"

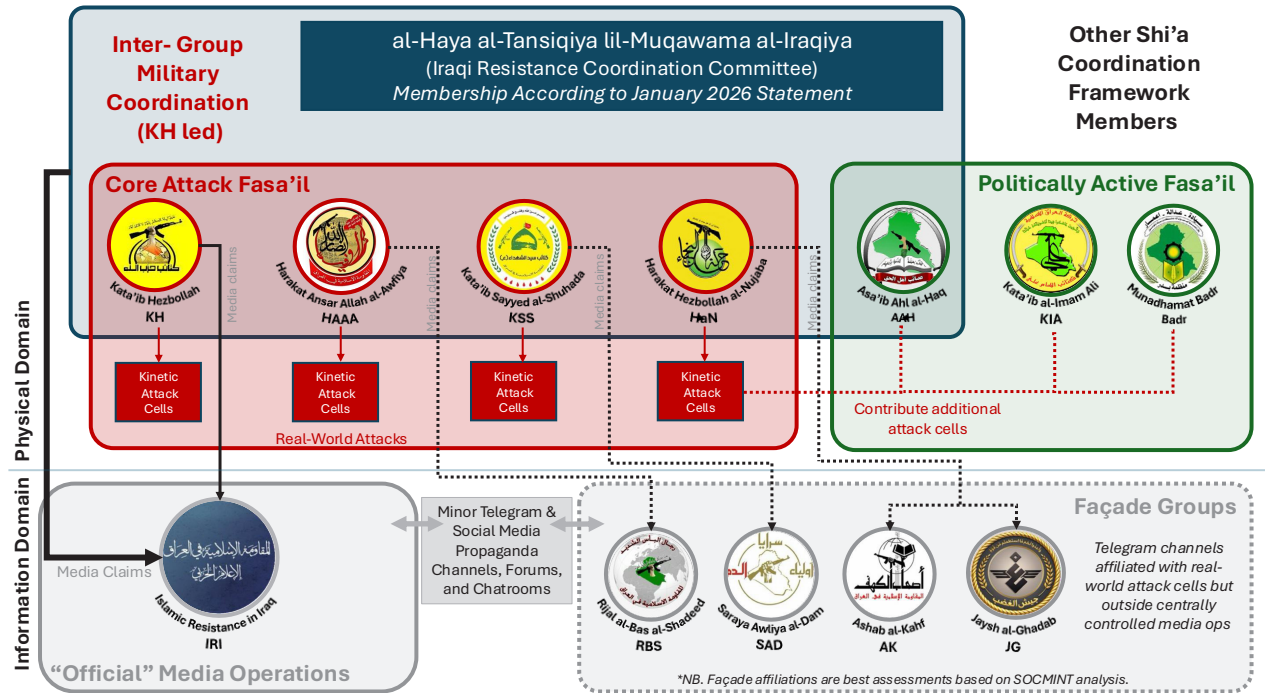


Figure 7: Proposed schema for the relationship between real-world armed groups and online 'façade' claim brands. The graphic reflects the insights gleaned in this report, with dotted lines suggesting rebuttal propositions (theories) presently supported by the balance of available data, which would benefit from ongoing testing. (Graphic produced by Crispin Smith)

on any Saudi infrastructure,¹⁹² nor the March 3 drone strike in the U.S. Embassy in Riyadh (which news interviews with an unnamed Saudi official suggested was a strike launched from Iraq by Iraqi militias).¹⁹³ RBS (who claimed the two Riyadh strikes¹⁹⁴) also claimed a very long-range strike on Al-Dhafra air base in the UAE using a Shahed-107 drone,¹⁹⁵ which either suggests the authors' 800km estimate for the Shahed-107 is too conservative, the drone was launched from a point outside Iraq (such as a boat), or the claim is inaccurate in some way (including the possibility a Shahed-107 was not used).^{cx} (Whichever of these is true, including the possibility of RBS fabricating a claimed attack on the UAE, there is probably something interesting to learn from this outlying, somewhat unique claim.)

Many small indicators suggest there may be more to the story of anti-Gulf attacks than is presently known, probably including larger numbers of attacks that are unclaimed or hidden within the IRI non-located claims. First, according to interview material gathered by one author (Knights)¹⁹⁶ and also by news reporting from Al-Monitor and Reuters,^{cy} significant numbers of attacks were

detected by Saudi Arabia to have originated in Iraq. Second, also according to interview material gathered by the same author¹⁹⁷ and also by news reporting from the same two news outlets,¹⁹⁸ Saudi Arabia and the UAE are reported to have mounted retaliatory air strikes in Iraq during the war, a very serious and unusual step for these Gulf States. These attacks targeted areas run by the PMF economic conglomerate, the Muhandis General Company, and seem to have been concentrated in the second and third weeks of the war (approximately March 10-20).¹⁹⁹ Third, diplomatic tension between Iraq and the Gulf States became more intense toward the end of the war,²⁰⁰ a Saudi strike was reported in southern Iraq on the war's last day, and anti-Gulf strikes extended briefly into the post-ceasefire period.^{cz}

The Other War: Information Operations, Claims, and Façades
The *muqawama* continues to place great store in the importance of media war and psychological warfare.²⁰¹ ^{da} Ashab al-Kahf's

cx Iran claims a range of 1,500 kilometers for the Shahed-107. Based on Ukrainian analysis of recovered Shahed-107 drones exported to Russia by Iran, the authors opt for a more conservative 800 km. Gun-cam footage and kill markings on Al-Dhafra-based French Tiger helicopters show some Shahed-101/107 drones were intercepted over the UAE, but it remains unclear if those drones came out of Iraq or southern Iran. See Harold Altman and Taylor Rogoway, "Russia Now Using Iranian Shahed-107 Drones To Strike Beyond The Front Lines," War Zone, November 18, 2026, and Armée de Terre, "Embarquez avec nos experts aéromobilité, engagés au Proche et au Moyen-Orient avec . . .," X, May 30, 2026.

cy Mid-April news reporting from Al-Monitor and Reuters has suggested that Saudi officials view the number of probable attacks originating from Iraq as a significant portion of all attacks. "Saudi Warplanes Struck Militias in Iraq, Sources Say," Reuters, May 13, 2026; Amberin Zaman, "Majority of attacks on Saudi Arabia carried out by pro-Iran militias in Iraq," Al-Monitor, May 18, 2026.

cz AK, for example, claimed one last attack on April 8, 2026, via a statement on its Telegram channel reading: "We adopt responsibility for targeting the interests of the Zionist-American enemy in the region (oil facilities, industrial areas, infrastructure) on April 8, 2026, using appropriate weapons." See footnote BQ.

da While kinetic rocket, drone, and IED attacks against U.S. forces receive the most Western attention, the use and misuse of law and the courts is a core militia strategy, decisive in state capture efforts over the last half-decade, with soft war often more successful than kinetic efforts.

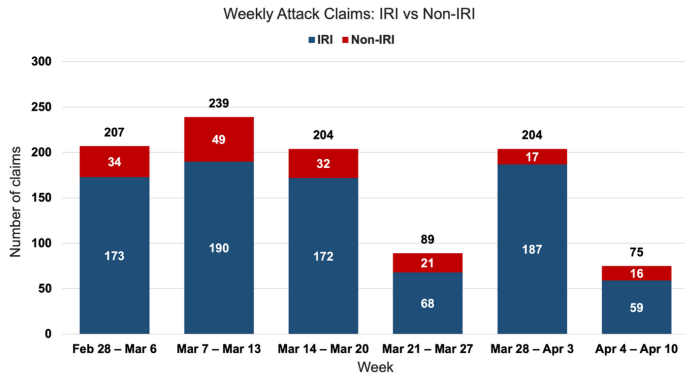


Figure 8: Weekly attack claims by brand. Dark blue are claims by the IRI umbrella; all non-IRI claims are shown in red. (Metrics charting by Alex Almeida)

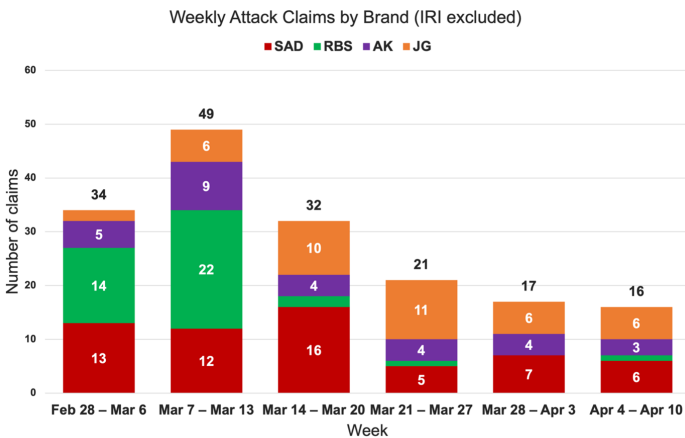


Figure 9: Weekly attack claims by non-IRI claim brands. Saraya Awliyah al-Dam (SAD) is in red, Jaysh al-Ghadab (JG) in orange, Rijal al-Bas al-Shadid (RBS) in green, and Ashab al-Kahf (AK) in purple (Metrics charting by Alex Almeida)

March 8 public insistence of the importance of media war^{db} is telling, underlining a wider Iranian Axis of Resistance focus on winning strategic messaging battles (and thereby securing political and diplomatic victories).²⁰² The U.S. FBI’s arrest and ongoing prosecution of IRGC-QF and *muqawama* operator Mohammad Baqer al-Saadi²⁰³ has also begun to shed some light on *muqawama* media strategy. As part of his role in the *muqawama*, al-Saadi stated to U.S. law enforcement that he was “in charge of media and psychological warfare” with his activities part of the “psychological warfare” that the *muqawama* is waging against the United States.²⁰⁴ Al-Saadi previously impressed on KH members the “need to engage in ‘psychological warfare’” while stressing in the context of attacks he orchestrated on the European homeland

that “anything that distracts the enemy is useful.”²⁰⁵ Al-Saadi was an experienced media operator, was connected with operators of major *muqawama* accounts, and almost certainly had prior experience of the façade group strategy.²⁰⁶ His attitude toward media operations is, therefore, very likely to be representative of wider QF and *muqawama* media strategy.

The *muqawama*’s love affair with the media is a double-edged sword, offering one of the best ways to look inside their minds and their organizations. As documented throughout this article, *muqawama*-affiliated Telegram channels posted hundreds of attack claims, using written ‘press releases,’ launch footage, high-production-value videos, and supposedly comprehensive round-up lists of alleged attacks (often broken down by the general location of target). In the authors’ view, the façade group strategy remained firmly in place.²⁰⁷ Over 800 launches were claimed by a range of media fronts, some pre-dating the 2026 conflict, others apparently created specifically for the war.²⁰⁸ These front channels are explicitly designed to obfuscate real-world groups’ involvement: consequently determining precise affiliation requires analysis of (inter alia) engagement patterns (observing trends in wider engagement with a given channel, including reposts and—equally telling—silences); analysis of language and the use of specific phrases; brand imagery and logo details; analysis of the locations of launch sites and claimed targets; imagery of weapon systems; and so on.²⁰⁹ This allows a rudimentary, if imperfect, assessment of likely affiliations.

Evolution of the Façade Strategy

That the *muqawama* continued to claim attacks through a range of façade groups was in itself a curious feature of their recent campaign,^{dc} with five major brands, principally operating via Telegram, used to disseminate threats, propaganda, and claims of attacks on U.S. and allied targets.²¹⁰ As noted above, the use of ‘façade’ brands to claim attacks reflects the balancing act facing militias: They want to derive some intra- and inter-group credit by claiming attacks, but there are many potential downsides to doing so. Their imperfect solution is to *lightly* conceal the exact identity of the attacking group from external parties, at least to less determined investigators for a while. In the view of the author team, the façade group strategy has enduring value for the *muqawama* as a form of legal warfare²¹¹ (complicating retaliation by obfuscating attribution); as an aid to recruitment and retention (by showing militia support bases that the *muqawama* continued to “resist” the United States and Israel); and as a form of inter- and intra-group competition, allowing groups to engage in one-upmanship.²¹² Even in the context of large-scale war, the façade strategy seems to have continued to perform many of these functions.

The *muqawama*’s use of façade groups is thus not new, but the latest round of conflict reveals some developments in the information environment. First, as noted above, centrally

db Ashab al-Kahf posted a statement on March 8, 2026, indicating the importance to the *muqawama* of media warfare noting: “We call upon all resistance and jihadist media outlets, at this critical juncture in our nation’s history, to unite and stand shoulder to shoulder within the axis of resistance alongside the Islamic Republic of Iran in confronting American and Zionist tyranny. It is incumbent upon all resistance media platforms to join forces and cooperate in conveying news and facts to the entire world. The battle today is not merely military; it is also a media war that demands a conscious presence and a unified voice to reveal the truth and expose the aggression of the arrogant powers. Telegram post on March 8, 2026, by Ashab al-Kahf.

dc In 2021, two of the authors (Smith and Knights) examined the rise of fake media brands (which they called “façade groups”) used by real-world *fasail* to propagandize their attacks and activities while obfuscating the true identities of any given perpetrator – delaying or confounding retaliation (whether kinetic or legal). Over years and through the Militia Spotlight project, a team of experts observed and documented the rise and fall of different media accounts, continuously assessing the likely affiliations of specific media channels to better attribute (very real) attacks to specific militias and cells. See Militia Spotlight at <https://www.washingtoninstitute.org/policy-analysis/series/militia-spotlight> and Knights, Smith, and Malik, “Discordance in the Iran Threat Network in Iraq.”

orchestrated media operations—a 2022-2023 development^{dd}—have continued under IRI.²¹³ In 2023-2024, IRI made 94 percent of *muqawama* claims—with an impressively boring and disciplined visual style that took all group personality out of claim postings.^{de} In 2026, IRI was again a disciplined machine: It started its claims on the war’s first day, February 28, and ended them on the last day of the war, April 8.²¹⁴ This is still an impressive level of centralized control.

SAD (which is strongly assessed as claiming for KSS)^{df} is the one claim brand that operated separately from IRI in both 2023-2024 and 2026. In the 2026 war, it made 59 claims (about six percent of the total, a similar proportion to its share of claims in 2023-2024).²¹⁵

New claim groups also wanted to show off their flair outside of IRI in 2026, marking a partial return to proprietary brands and separate claims. The IRI quotient dropped in the 2026 war to 83 percent (849 out of 1,015 claims).²¹⁶ Who was behind these groups? The below findings are provisional, and should be treated as rebuttable propositions that are worthy of further study.

On the basis of available evidence, Jaysh al-Ghadab is a new Nujaba-linked façade.²¹⁷ If so, then it is Nujaba’s second such brand, in addition to Ashab al-Kahf (which returned to its original name late in the 2026 war, shedding its moniker since August 2024, Kataib Sarkhat al-Quds).^{de} Collectively, they represent 67 claims or about six percent, on par with SAD. If Jaysh al-Ghadab is a Nujaba front, this raises a lot of questions. What makes a group develop a second façade brand, one that does not claim attacks that differ greatly from each other? And what makes a group like Nujaba

choose to stay outside IRI in the present war? These questions are fertile ground for future in-depth investigations of the *muqawama* information environment.

RBS is also deserving of closer investigation. There are weak indicators that RBS might have splintered internally around March 10, with its main kinetic cells folding into the IRI claim structure thereafter.^{dh} One theory worth testing is whether RBS is an AAH or Harakat Ansar al-Awfiya façade that largely joined IRI partway through the war.^{di} A new channel, created in October 2025 but with its first post on March 4, 2026, digital engagement patterns with RBS indicate lesser affiliation with mainstream *muqawama* media channels but notable levels of AAH-affiliated engagement.^{dj}

Part III: Iraqi Popular Mobilization Forces Join Iran’s War Effort

In the 2019 *CTC Sentinel* article “Iran’s Expanding Militia Army in Iraq,”²¹⁸ one of the authors (Knights) profiled the 60 or so PMF brigades as they ended their first five years of mobilization as government-paid Iraqi security forces.²¹⁹ At that stage, the author assessed 25 PMF brigades to qualify as ‘Iran-backed’ based on their relationships with U.S.-designated terrorist groups or the IRGC.²²⁰ In the 2026 war, this author team finds (and has laid out in detail in this piece) that 36 PMF brigades either launched weapons at U.S. forces, Iraqi civilians and infrastructure, or neighboring states, or provided material support to the groups undertaking such attacks²²¹ (i.e., U.S.-designated terrorist groups such as KH, KSS, and Nujaba).²²² With around 65-70 PMF brigades in existence,²²³ this means that for the first time, half or more than half of the PMF units demonstrably have members providing support for terrorist groups.

dd A critical moment in enforcing this centralized media discipline occurred when Sabereen News was subjected to a forced suspension between March 28 and April 8, 2022. The shutdown was likely ordered by higher *muqawama* leadership or Iranian sponsors. See Hamdi Malik, Crispin Smith, and Michael Knights, “Sabereen’s Suspension (Part 1): Signs of Dissent and Noncompliance,” *Militia Spotlight*, April 11, 2022. The ultimate centralization of the *muqawama* media strategy then came following the outbreak of the Gaza conflict in October 2023. Rather than competing for credit under their individual militia names or various façade groups, the militias consolidated their kinetic attack claims under a single, generic umbrella brand: the Islamic Resistance in Iraq (IRI). See Amir al-Kaabi, Michael Knights, and Hamdi Malik, “Facade Group Linked to Iran Claims Five Attacks on Americans in Iraq and Syria,” *Militia Spotlight*, October 20, 2023.

de The IRI primarily posts dry text-based statements in a laconic format: The statement will state the time period it covers (often “the last 24 hours”), a statement as to the number of IRI operations launched in the timeframe, a general indication of the general type and quantity of weapons used (e.g., “dozens of drones and rockets”), and a very general indication of the target location (often simply “enemy bases in Iraq and the region”).

df First profiled by *Militia Spotlight* in 2021, SAD has maintained its own online identity independent from (for example) IRI for most of its documented history, and claimed to have launched attacks on Israel from Syria and Lebanon between 2023 and 2024. From 2021 onward, the group appeared to be a front for KSS (claiming attacks against U.S. locations in Erbil from as early as February 2021). The brand’s current online channel was created in 2023 and its second post congratulated KSS commander Abu Alaa al-Walal for his inclusion on a U.S. sanction list.

dg First profiled by *Militia Spotlight* in 2021 (and dating to at least 2019), AK is one of the oldest façade groups and has gone through multiple iterations. In August 19, 2024, the group changed its name from Ashab al-Kahf to Kataib Sarkhat al-Quds (KSQ) (Cry of Quds Brigade) as part of ongoing operations against Israel, indicating an effort to expand beyond Iraq (AK was also one of the only Iraqi groups to have claimed to have attacked Israel prior to 2023). In March 2026, the group appears to have retired the KSQ name, and reverted to AK, likely in order to show a return to an Iraq focus. The group AK is likely affiliated with Harakat al-Nujaba.

dh As noted earlier when discussing how the fusion of claims data and human intelligence can give low-confidence insights into how real-world groups interact with new façade brands, this kind of synthesis and claim-watching can help to notice potential organizational changes in the *muqawama*. One is the near-cessation of claims by RBS after March 10, 2026, as the second phase of the *muqawama*’s war began to take effect. A tiny fraction of RBS claim activity continued, while RBS’ main unique feature (exclusive use of the obscure Sayyed-107 drone) ended, and from March 10 all Sayyed-107 use now exclusively occurred under the IRI claim brand (where there had been no Sayyed-107 use before by IRI or any other group). This is the authors’ collective conclusion, based on their synthesis of the known facts, and explored further through this text.

di Again, this might be thought of as an interesting low-confidence theory derived from claim-spotting using some advanced techniques that should not be discussed in case exposure prejudices future use of the techniques. RBS’ online existence has a notably stronger connection to AAH-related online entities than any other online community. Alternately, RBS could be a HAAA façade, based upon its early-war focus on Jordanian targets attacked from HAAA’s Anbar operating areas and the group’s sudden downward change of activity immediately after receiving heavy U.S. strikes on March 10-12, 2026. (Based on the authors’ database of U.S. strikes in the 2026 war.) Either are interesting theories to dig into. This is the authors’ collective conclusion, based on their synthesis of the known facts, and explored further through this text.

dj RBS is a new channel, created in October 2025, with its first post on March 4, 2026. Of all the channels that posted significant numbers of attack claims in the 2026 war, engagement patterns with RBS indicate lesser affiliation with mainstream *muqawama* media channels – although the channel had notable levels of AAH-affiliated engagement. In the past, apparent AAH alignment has been recognized later as broader Sadrist heritage (which can point to present or former members of Nujaba, Kataib al-Imam Ali, Fadhila, or even Saraya al-Salam).

Main Attack Groups	Secondary Attack Groups	Weapon-movers and Cache Guardians
- Kataib Hezbollah PMF 45, 46, 47	- Liwa al-Tafuf PMF 13	- Badr Quwat al-Shaheed al-Qaid Abu Muntadher al-Muhammadawi PMF 27
- Kataib Sayyed al-Shuhada PMF 14	- Liwa Shabak PMF 30	- Kataib al-Imam Ali PMF 40
- Harakat Hezbollah al-Nujaba PMF 12	- Harakah Babilioun PMF 50	- Kataib Ansar al-Hujja PMF 29
- Harakat Ansar Allah al-Awfiya PMF 19	- Fawj Fayly PMF 110	- Harakat al-Abdal PMF 39
- Kataib al-Imam Ali PMF 40	- Fawj Amerli PMF 52	- Saraya Talia al-Khurasani PMF 18
- Liwa Hussein PMF 53	- Quwwat al-Turkmen PMF 16	- Saraya al-Jihad PMF 17
- Asaib Ahl al-Haq PMF 41	- Asaib Ahl al-Haq PMF 42, 43	- Kataib al-Tayyar al-Risali PMF 31
- Badr Organization PMF 21	- Liwa Ali al-Akbar PMF 11	- Lalish Brigade PMF 36
	- PMF Brigades 61 and 63 PMF 61, 63	- Quwat Waad Allah PMF 33
		- Quwat al-Shaheed al-Sadr PMF 15
		- Quwat al-Shahid al-Sadr al-Awwal PMF 25
		- Kataib Jund al-Imam PMF 6
		- PMF Brigades 51, 57, 58 PMF 51, 57, 58

Note: Entities indicated in red are U.S.-designated foreign terrorist organizations (FTOs)

In the author team’s informed view, the evidence laid out in Part II of this study is worthy of deeper investigation by government intelligence agencies because it suggests that PMF support for foreign terrorist organizations (FTOs) has been substantial in the 2026 war.²²⁴ The information relayed in Part I of this study (especially pre-war dispersal of weapons and intra-war reloading from Iran) and Part II (geographic munitions flows to the sub-campaigns) suggests extensive *muqawama* use of the PMF’s vast physical laydown of cantonments, camps, and compounds across

north, western, central, and southern Iraq in the war.^{dk}

The *muqawama*’s 2026 drone campaign arguably also required the mobilization of significant militia manpower, including many members of the state-funded PMF. If the *muqawama* is assumed to have adopted significant operational security precautions (i.e., regular rotation and resting of attack cells),^{dl} then a high-end estimate by the author team suggests the existence of as many as 135 drone cells operating during the war.^{dm} Each drone is likely made up of around three to five militia operators,^{dn} yielding a total of around 400-650 drone crew members if there were the high-end estimate of 135 crews working in rotation. Of these, only a very small fraction are likely to have been trained, specialized drone operators.^{do} Instead, most of the 400-650 cell members would serve as drivers, unloaders, and security.^{dp} A broader community of cache guardians, long-distance truckers, and security ‘wrappers’ for the drone teams (mostly drawn from the local ground-holding PMF brigades)²²⁵ might number in the very low thousands, assuming the high-end estimate of 135 cells is correct and if a normal ‘tooth-to-tail’ ratio between combat and non-combat forces is assumed.^{dq} Even if one assumed a far leaner manpower base, the 2026 war unarguably relied upon a greater pool of *muqawama* operators and

dk The number of sites struck by the United States during war – over 60 identified target locations belonging to a range of PMF brigades – likely represents only a fraction of the extensive PMF physical infrastructure that was commandeered by the *muqawama* war effort, ranging from large cantonments and logistics bases with hardened ammunition storage bunkers to small compounds and rural farm properties.

dl This cautious operational security model would require that any given drone crew will disperse and go to ground for a period of three to four days after conducting a launch to evade overhead ISR tracking, dispose of any electronic ‘emitters’ (i.e., mobile phones), and break any “pattern of life” signatures.

dm To generate this estimate, the authors used the median number of daily claimed attacks (34) as the baseline operational tempo. The authors then applied the cautious operational security assumption. Multiplying the median daily tempo by the estimated length of the drone cell operational cycle (one attack day, plus two to three ‘off’ days) yields a pool of around 135 drone teams operating in continuous rotation across federal Iraq.

dn This figure is based on a review of attack claim videos showing militia crews assembling and launching the drones. Authors’ database of attack claims and associated video archive of the 2026 war. Also, the authors are drawing on their broader analysis of 2023-2026 *muqawama* drone operations, which have included scores of videos showing the same kinds of launch procedures. The heavier Shahed-107 type drone will typically require at least two men to manhandle the fuselage tube into position, plus another operator to load the drone’s mission plan.

do The Shahed-101/107 and Hadid-110 type drones are preloaded in special ‘ready to launch’ boxes that include pop-up erector stands. Setting up the launch stand and attaching the wings, tail fins, and rocket booster is likely not a technically demanding process, though a specialized drone operator is probably still needed to upload the flight plan to the drone’s autopilot module.

dp Trained or relatively unskilled, the high-end estimate of 400-650 drone crew personnel are likely to have been drawn from a vetted sub-set of KH, KSS, and other core ‘tier one’ *muqawama* groups.

dq Beyond the attack cells, the ‘outer layer’ of logistics and support personnel provide cache guardians and security ‘wrappers’ for the drone teams (mostly drawn from the local ground-holding PMF brigades). Thus, those handling the transportation and distribution of drone systems in total must necessarily number in the very low thousands, if a normal tooth-to-tail ratio is assumed – usually around one to three in modern military ground force operations. See John J. McGrath, *The Other End of the Spear: The Tooth-to-Tail Ratio (T3R) in Modern Military Operations* (Fort Leavenworth, KS: Combat Studies Institute Press, 2007).

“In a new post-2023 age of existential wars fought by the Islamic Republic of Iran, the author team assesses that the Badr military machine seems to be more openly playing its original intended role as an auxiliary of the IRGC when the Islamic Republic of Iran’s existence is threatened. Since October 2023, Badr’s leaders have become more vocal in their opposition to Israeli and U.S. actions against Hezbollah and Iran.”

support services that in any previous conflict.^{dr}

The PMF as an institution has arguably been shifting toward an Iran-allied position for many years.²²⁶ As noted in one of the authors’ book-length studies, *Honored Not Contained: The Future of Iraq’s Popular Mobilization Forces* (co-authored with Hamid Malik and Aymenn Al-Tamimi),²²⁷ by 2020 the civilian and military leadership of the PMF and its most powerful directorates became dominated by KH and Badr leadership figures with a tight, decades-spanning connection to the IRGC.²²⁸ In the wars since October 7, 2023, KH leaders such as the PMF’s military commander Abdal-Aziz al-Mohammadawi (aka Abu Fadak) have undermined the expectation that the PMF, as a formal Iraqi security force, answers only the constitutional commands of Iraq’s prime minister.²²⁹ For instance, the PMF leadership represented Iraq at Axis of Resistance command conferences (for instance, see the April 5, 2024, wartime conference in Tehran on counter-Israeli and counter-U.S. strategy).²³⁰ At that event, Abu Fadak stated, “The PMF is a fundamental part of the battle in Gaza and Palestine.” He admitted to taking orders primarily from a foreign official, Iran’s [then] Supreme Leader Ali Khamenei, stating: “We are waiting for the [Supreme] Leader to express his view on the next step ... We came to the Islamic Republic first to express our solidarity with the vision and plan of the Leader and the Imam ... and second to renew our covenant [i.e., loyalty to the Supreme Leader] and wait for the Leader’s decision.”²³¹

In 2026, following Khamenei’s death, the Iraqi *muqawama* leadership atop the PMF structure took their covenant to its natural conclusion by entering the war on Iran’s side. The unauthorized steps taken by the PMF-*muqawama* leadership included the importation of major military arsenals from a foreign power (Iran);²³² the prosecution of an unprecedented military campaign against Iraq’s international partners (the United States and European powers in the coalition military advisory group, and Arab states) from Iraqi soil involving both Iraqi and Iranian forces;²³³

the deployment of major Iraqi PMF units outside the country (into Iran),²³⁴ and the killing and wounding of Iraqi citizens and the destruction of Iraqi civilian infrastructure.²³⁵ The possibility of the *muqawama* pulling Iraq into a regional war that the country had not joined caused a degree of alarm within Iraq’s body politic. In an unprecedented statement by the Iraqi judiciary, Iraq’s Supreme Judicial Council issued a public statement on March 27 clarifying the necessary constitutional and parliamentary steps required to lawfully issue a declaration of a state of war in Iraq.^{236 ds}

Badr: Reintegrating into Iran’s Order of Battle?

One of the most important analytical findings of this article is the new light it sheds on the kinetic and logistical roles played by Iraq’s thus-far unsanctioned Badr Organization. In the 2019 *CTC Sentinel* article “Iran’s Expanding Militia Army in Iraq,”²³⁷ one of the authors (Knights) dwelt on the critical role that Badr would have in shaping the PMF due to its multi-decade experience at developing conventional armed forces. Badr was the main provider of expertise and manpower in the PMF “enabler” units, such as the armor, artillery, and missiles directorates.²³⁸ Badr members—and KH and KSS members who originated in Badr—still occupy the positions of the PMF’s military commander, chief of operations, and head of the intelligence, internal security, training, and religious instruction directorates.²³⁹ In 2019, the author (Knights) wrote in *CTC Sentinel*: “Disentangling Badr networks from [KH] and IRGC-QF networks is thus not a simple proposition ... Badr was a unit of the Islamic Revolutionary Guard Corps in the Iran-Iraq War, so its ties with Iran run very deep.”²⁴⁰

In those Iran-Iraq War days, Badr was literally a military division of the IRGC, and it remained so, at the very least, during its 2003 invasion of Iraq (which occurred in parallel to Operation Iraqi Freedom).²⁴¹ Now, in a new post-2023 age of existential wars fought by the Islamic Republic of Iran, the author team assesses that the Badr military machine seems to be more openly playing its original intended role as an auxiliary of the IRGC when the Islamic Republic of Iran’s existence is threatened.²⁴² Since October 2023, Badr’s leaders have become more vocal in their opposition to Israeli and U.S. actions against Hezbollah and Iran.²⁴³ In the years since apparent Israeli strikes on Badr’s Camp Ashraf,^{dt} many anecdotal reports have reached the author team from Iraqis

ds It notes that “unilateral declaration of a state of war by [*muqawama*] factions in practice – through engaging in activities of a military nature – constitutes a clear violation of the [Iraqi] Constitution. [The authority to declare war] is exclusively reserved for legitimate constitutional institutions that represent the will of the people and operate within an organized legal framework. When some [*muqawama*] factions [unilaterally declare war], they undermine the authority of the state and erode the principle of the rule of law.” Though the court’s statement addressed the issue of who has authority to formally declare war on behalf of the Iraqi state, it failed to address legal issues arising from the international law of state responsibility; in many cases, Iraq likely bears legal responsibility for the actions of the *muqawama*, either because the factions have been formally adopted as official government entities integrated into the Iraqi state through legislation, or due to Iraq’s failure to exercise due diligence in preventing attacks from its territory. For a discussion of Iraqi responsibility for elements of the *muqawama*, see Smith, “Servants of Two Masters.” See also Smith, “Iraq’s Legal Responsibility for Militia Attacks on U.S. Forces: Paths Forward.”

dt Israel struck Camp Ashraf in July 2019 as it tried to interdict the flow of precision weaponry and advanced conventional munitions to Syria and Lebanon via the “land bridge of Iraq.” See Michael Knights and Alex Almeida, “Militias Are Threatening Public Safety in Iraq,” Washington Institute for Near East Policy, August 14, 2019.

dr A number larger than the manpower roster of KH during the group’s early covert phase in 2010 (around 400 personnel). See Michael Knights, “The Evolution of Iran’s Special Groups in Iraq,” *CTC Sentinel* 3:11 (2010).

concerning greater logistical involvement between Badr and the IRGC regarding transshipment of Iranian advanced conventional weapons through Iraq (to Syria and Lebanon), and lately (in 2023–2024) of stronger Badr preparations to undertake kinetic attacks on Iran’s enemies.^{du} Statements made by Badr leaders also speak to that intent. For example, on October 10, 2023, following Hamas’ attacks on Israel, Badr leader Hadi al-Ameri uncharacteristically threatened: “If the Americans intervene in the battle with Hamas, we will attack all U.S. targets.”²⁴⁴

In 2026, this author team concludes, Badr did cross the line from a non-kinetic supporting role to actually launching kinetic drone attacks on U.S. forces in Iraq.²⁴⁵ According to detailed attack data gathered by the author team,²⁴⁶ Badr directly undertook eight drone attacks on the U.S. BDSC site, six on the U.S. complex at Erbil airport,²⁴⁷ and at least one known drone strike on a Basra oilfield in which a U.S. investor was negotiating entry into.^{dv} Badr also fired drones at Iranian Kurdish sites in the KRI,^{dw} a throwback to Badr’s longstanding role in the 1980s–2000s as the IRGC’s main tool for attacking Saddam-backed Iranian opposition militants based in Iraq.²⁴⁸ Other interviews undertaken by one of the authors (Knights) identified various cross-border escorting of, and securing of, Iranian missile launchers, including Badr fighters protecting sites inside Iran or sites just inside Iraq.²⁴⁹ The locations mentioned are old Badr operating locations during and since the Iran–Iraq War, notably Badr’s 1990s–2000s base locations in Defful, Dehloran, Mehran, and Ahwaz.^{dx} Badr seems to still have great ability to operate fluidly across the Iran–Iraq border, whether to bring materiel and personnel into or out of Iraq.²⁵⁰ (Many Badr operators have Iranian as well as Iraqi citizenship and have families and property in western Iranian areas.^{dy}) As noted in the Phase 4 section of Part I above, Badr also appears to have moved significant PMF forces to Iran to support Iranian regime security and internal defense missions in the last week of the war.

du This has been a recurring theme in human reporting gathered by Knights and Smith. Since at least 2019, more and more scattered human reporting has discussed a growing Badr logistical role, and (since 2023) also a low-profile kinetic role for Badr. This is two authors’ (Knights and Smith) collective conclusion, based on their synthesis of the known facts, and explored further through this text.

dv A jet Shahed-136 drone crashed in Majnoon oilfield in Iraq on September 28, 2025. The incident coincided with the lead-up to the October 8, 2025, signing of a contract for a U.S. oil company to operate the field. Data drawn from the authors’ geolocated SIGACT dataset covering 2025.

dw On March 16, a Badr kinetic cell in northern Diyala led by Fayli (Shiite) Kurd commander Baqir al-Kinani struck one Iranian oppositionist camp in Qara Dagh, Sulaymaniyah, and another was struck in Qaladize, Sulaymaniyah, on May 29 by a Badr cell by another Fayli commander Jah Sadiq al-Fayli. Badr is the dominant militia among the Fayli community, which extends all the way down the Iran–Iraq border from Khanaqin to Badra. Data drawn from the authors’ geolocated SIGACT dataset covering the 2026 conflict.

dx It makes sense that Badr personnel who lived in these areas of Iran for parts of three decades would maintain ties and familiarity there, and from time to time, the authors have heard indications of this from Badr members and informed persons. This is the authors’ collective conclusion, based on their synthesis of the known history of Badr. Knights and Smith, “Badr Organization.”

dy This has been a consistent theme in Knights’ interview materials and discussions with Badr members spanning back to 2003. Many senior Badr members do not dispute (in private) that they hold Iranian citizenship and have property and dual-national family members there. This is Knights’ conclusion, based on his synthesis of the known data across 23 years of Iraqi interviews.

Badr’s Role in IRGC Logistics in Iraq

Yet above and beyond all these combat roles, in the considered view of the authors, logistics was an even more important Badr contribution to the Iranian war effort in 2026.²⁵¹ As noted, Badr appears to have moved weapons through Iraq for the IRGC for many years,²⁵² but Badr’s recent role was as the logistical backbone for *muqawama* efforts inside Iraq.²⁵³ Throughout the conflict, Badr essentially functioned as the rear ‘third line’ logistics element for large parts of the Iraqi *muqawama*,²⁵⁴ most likely in support of groups other than KH that lack their own large-scale logistics organizations.²⁵⁵ In interview data, a recurring observation is the splitting of Iranian weapons cargos just inside Iraq into two main batches—one carried onward by a KH system and one by another system in which Badr was the main land transportation provider through its control of PMF trucking fleets.²⁵⁶ The key Badr logistics unit running this effort is Quwwat al-Shaheed al-Qaid Abu Muntadher al-Muhammadawi (PMF 27),²⁵⁷ named after the deceased Badr leader to whom Camp Ashraf has also been dedicated by Badr.^{dz}

In the 2026 war, Badr appears to have served as the clearinghouse for non-KH combat logistics, supported by distribution units from Kataib al-Imam Ali (PMF 40), Saraya al-Jihad (PMF 17), Saraya al-Khurasani (PMF 18), Kataib Ansar al-Hujja (PMF 29), Harakat al-Abdal (PMF 39), and Kataib al-Tayyar al-Risali (PMF 31).²⁵⁸ Camp Ashraf was, and likely will be in the future, a key national stockpile and ammunition supply point for the Iraqi *muqawama*.²⁵⁹ Yet, until Badr is designated as an FTO, its units and sites may be more difficult to target than the FTOs it delivers to and those it partners with, most notably KH.

Final Questions for Analysts

This analysis has highlighted many unanswered questions in the course of its exploration of the prior history of the Iraqi *muqawama* at war, the phasing of their involvement in the 2026 conflict, the sub-theaters of the Iraqi war, and the role of information operations and logistics. At a higher level, there are strong indicators that the coming years will involve increased demand from policymakers in the United States and elsewhere for assessments and supporting materials on the Iraqi *muqawama*.

The first area of raised demand may be for assessments that identify lessons in deterrence success and failure during the war. The Iraqi *muqawama* were successfully ‘backed-down’ from escalating attacks by the United States in December 2023 to February 2024 and by Israel in November 2024.²⁶⁰ In the 2026 war, detailed analysis based on classified data will probably be necessary to uncover what worked and what did not in the U.S. (and the Gulf States’) effort to restrict Iraqi *muqawama* attacks. The Iraqi *muqawama* leadership appears from a thorough open-source review to have escaped the war with remarkably few leadership

dz The official Iraqi government name for Camp Ashraf is Abu Muntadher al-Muhammadawi.

casualties,^{ea} though the March 16 U.S. airstrike on a reported IRGC-QF and *muqawama* leadership meeting did seem to trigger an attempt led by KH to (unsuccessfully) arrange a rolling truce with the United States.²⁶¹ Understanding whether Iraqi *muqawama* avoided targeting—and if so, how—is an interesting topic. A related inquiry is whether the Iraqi *muqawama* would have displayed its observed ‘glass jaw’ if their fielded forces had received less focus and its leaders had been threatened more effectively. Or did the context of the 2026 war—a long record of *muqawama* military disappointment, Khamenei’s death, and a potentially existential war for the IRGC—make Iraq’s factions much harder to deter? Is this an enduring change in their mindset?

A second demand driver for intelligence analysis may be related to sanctions and export controls. Despite a multi-decade track record of corruption, state capture, human rights abuses, and terrorist activities, Badr has consistently escaped serious regulatory or law enforcement sanction by the U.S. government and its allies.²⁶² This could change.^{eb} Intelligence analysts may be asked to support sanctions activities involving Badr, PMF departments and a raft of other currently unsanctioned Iraqi entities whose instrumentalization by the IRGC has been exposed by the war.

A third future focus area for analysts regarding the Iraqi *muqawama* may be provision of intelligence support to security sector reform (SSR) and demobilization, disarmament, and reintegration (DDR)²⁶³ initiatives involving *muqawama* groups and the PMF more generally. As noted in the introduction to this article, three Iraqi armed groups (including two FTOs, Asaib Ahl al-Haq (PMF brigades 41-43) and Kataib Al-Imam Ali (PMF 40))

announced their intention to enter a disarmament process,²⁶⁴ with the latter two FTOs clearly hoping to be granted some benefits (such as taking up cabinet roles or being given a pathway to sanctions delisting). Other FTOs and those seeking to avoid being sanctioned may follow suit. Policymakers will request assessment as to whether these are genuine initiatives or merely efforts to blunt U.S. ‘lawfare’ and undermine the U.S. maximum pressure strategy.

On this issue, unprecedented Iraqi *muqawama* involvement in the 2026 war—including major external operations undertaken by these groups—underlines the important role of intelligence in placing the focus on the proven behavior of individuals and groups, not on the labels they have chosen for themselves or been given by Western governments. This article suggests that many Iraqi factions not currently designated as terrorist groups (such as Badr) nonetheless provided material support to FTOs during the war. Likewise, many groups that are formally members of Iraq’s government security forces (through the PMF) aligned themselves with a foreign power (Iran); materially supported Iranian FTOs such as IRGC and IRGC-QF; gave Iran access to Iraqi territory to launch attacks; and deployed forces outside Iraq or attacked targets outside Iraq without Iraq having declared war on the United States. Groups previously described by Western think-tanks as “parochial” armed factions^{265 ec} due to their ascribed main focus on domestic political and economic status were actually full combatants in this war. The military actions of supposedly parochial factions were often indistinguishable from those of the so-called transnational terrorist “vanguard,”^{266 ed} strongly suggesting that individual and group behavior (not labels) may become the key level of assessment regarding the *muqawama* in the future. **CTC**

ea No top-level *muqawama* leaders – such as KH head Abu Hussein, KSS head Abu Alaa, or Nujaba head Akram Kaabi – were killed. The most high-profile militia fatalities included Jaafar al-Husseini, the face behind KH’s Abu Ali al-Askari social media spokesman, and KH’s security chief for its Jurf al-Sakhr cantonment (and key drone operator), Ali Hussein al-Furaiji, plus a bevy of mid-level missile and rocket specialists killed in Baghdad. Data drawn from the authors’ geolocated SIGACT dataset.

eb Two of the authors (Knights and Smith) have noted in a previous report Badr’s activities and affiliations could make it eligible for sanctioning under at least three extant sanctions programs. Knights and Smith, “Badr Organization.”

ec This study loosely broke PMF militias into two broad categories, which the study terms “vanguard networks” (with tight-knit leaderships but weak ties to society and closer ties to Iran) and “parochial networks” (which the study characterizes as having less coherent leadership but strong social bases in Iraq). The study classes Saraya al-Salam, AAH, and Badr as parochial networks.

ed The study principally categorizes KH as a “vanguard” group, claiming that “KH has weak vertical ties to its base and the communities where it operates” and arguing that with fewer domestic stakes, KH and other vanguard groups are more willing to push the transnational confrontation forward.

Citations

- 1 Unpacking this chronology in detail is the focus of Michael Knights, Hamdi Malik, and Crispin Smith, “Iraq’s New Regime Change: How Tehran-Backed Terrorist Organizations and Militias Captured the Iraqi State,” *CTC Sentinel* 16:11 (2023).
- 2 Michael Knights, “Iraqi Oil and the Iran Threat Network,” *CTC Sentinel* 18:4 (2025).
- 3 Michael Knights, “Rise of the E-Militias: Designated Terrorist Groups Infest Iraq’s Digital Economy,” *CTC Sentinel* 18:11 (2025).

- 4 Michael Knights, “Iran’s Expanding Militia Army in Iraq: The New Special Groups,” *CTC Sentinel* 12:7 (2019); Michael Knights, “Soleimani Is Dead: The Road Ahead for Iranian-Backed Militias in Iraq,” *CTC Sentinel* 13:1 (2020); Michael Knights, “Back into the Shadows? The Future of Kataib Hezbollah and Iran’s Other Proxies in Iraq,” *CTC Sentinel* 13:10 (2020); Michael Knights, Crispin Smith, and Hamdi Malik, “Discordance in the Iran Threat Network in Iraq: Militia Competition and Rivalry,” *CTC Sentinel* 14:8 (2021); and Knights, Malik, and Smith, “Iraq’s New Regime Change.”

- 5 Knights, "Iran's Expanding Militia Army in Iraq."
6 Ibid.
7 Ibid.
8 Michael Knights, "Predicting the Shape of Iraq's Next Sunni Insurgencies," *CTC Sentinel* 10:07 (2017).
9 The best deep-dive on the PMF is Michael Knights, Hamdi Malik, and Aymenn Jawad Al-Tamimi, "Honored, Not Contained: The Future of Iraq's Popular Mobilization Forces," Washington Institute for Near East Policy, March 23, 2020.
10 Knights, "Soleimani Is Dead."
11 Knights, "Back into the Shadows?"
12 Knights, Smith, and Malik, "Discordance in the Iran Threat Network in Iraq."
13 Knights, Malik, and Smith, "Iraq's New Regime Change." This study was augmented by a further study in 2025, which argued that the militias' most decisive successes in the 2020s stemmed from lawfare and institutional capture, specifically by co-opting the judiciary and legislative branches to overturn democratic outcomes. Crispin Smith and Michael Knights, "How Iran aligned militias seized Iraq: irregular warfare, lawfare and regime change," *Small Wars & Insurgencies Journal*, 2025.
14 Knights, Malik, and Smith, "Iraq's New Regime Change."
15 The authors maintain a detailed attack claims database from the 2026 war, which includes tabulated date, claim group, narrative details, branding, achieved offline Telegram posts, and related videos and imagery.
16 Michael Knights and Crispin Smith, "Badr Organization: Iran's Oldest Proxy in Iraq," Hudson Institute, June 3, 2025.
17 National Security Presidential Memorandum-2/NSPM-2, The White House, February 4, 2025.
18 Knights and Smith, "Badr Organization." See also Michael Knights, Crispin Smith, and Hamdi Malik, "Profile: Badr Organization," *Militia Spotlight*, Washington Institute for Near East Policy, September 2, 2021.
19 Knights and Smith, "Badr Organization."
20 This process – known as *demaj* (amalgamation) – is described in depth in Knights, Malik, and Al-Tamimi, "Honored, Not Contained."
21 See the in-depth discussion of Badr-KH ties in the Badr sections of Knights, "Back into the Shadows?"
22 See Michael Knights, "The Evolution of Iran's Special Groups in Iraq," *CTC Sentinel* 3:11 (2010).
23 This is a broad historical observation by the author team, and probably not a very controversial one.
24 The role of Iraqi *muqawama* training and support to Gulf militants is explored in depth in Michael Knights and Matthew Levitt, "The Evolution of Shi'a Insurgency in Bahrain," *CTC Sentinel* 11:1 (2018). See also the section on the training of Gulf militants in Knights, "Back into the Shadows?"
25 Phillip Smyth, "The Shiite Jihad in Syria and Its Regional Effects," Washington Institute for Near East Policy, February 2, 2015.
26 See an examination of this command-and-control issue and the Syrian case in Knights, Malik, and Al-Tamimi, "Honored, Not Contained."
27 See Ibid.
28 Smyth, "The Shiite Jihad in Syria and Its Regional Effects."
29 Michael Eisenstadt, "Deterring Iran in the Gray Zone: Insights from Four Decades of Conflict," SMA/STRATCOM Academic Alliance Speaker Series, September 30, 2021; Michael Knights, "Iran's Counter-Pressure Campaign: Strategy, Tactics, and the Quest for Regional Dominance," Washington Institute for Near East Policy, June 11, 2026.
30 Knights, "Back into the Shadows?"
31 This is essentially the history that was captured as it unfolded by the Militia Spotlight blog from 2022-2025, and within the parallel series of *CTC Sentinel* articles from the same years that functioned as the long-form synthesis outputs from the blog.
32 Knights, "Soleimani Is Dead."
33 Knights, Smith, and Malik, "Discordance in the Iran Threat Network in Iraq."
34 See the profile of this group at Militia Spotlight: Michael Knights, "Profile: Liwa Ahrar al-Iraq," *Militia Spotlight*, Washington Institute for Near East Policy, July 19, 2022. See also Alex Almeida and Michael Knights, "The Muqawama's Duel with Turkey," Washington Institute for Near East Policy, May 17, 2022.
35 See Michael Knights, Amir al-Kaabi, and Hamdi Malik, "Tracking Anti-U.S. Strikes in Iraq and Syria During the Gaza Crisis," *Militia Spotlight*, Washington Institute for Near East Policy, October 24, 2023, updated until December 3, 2024.
36 See Knights, al-Kaabi, and Malik, "Tracking Anti-U.S. Strikes in Iraq and Syria During the Gaza Crisis."
37 Ibid.
38 Ibid.
39 A good listing of the deceased commanders can be found here: Michael Knights and Ameer al-Kaabi, "Militia List of U.S. 'Greatest Hits' Gives Insight Into Attack Cell Structure," *Militia Spotlight*, Washington Institute for Near East Policy, November 26, 2024.
40 See Knights, al-Kaabi, and Malik, "Tracking Anti-U.S. Strikes in Iraq and Syria During the Gaza Crisis."
41 Ameer al-Kaabi, Hamdi Malik, and Michael Knights, "Hassan Nasrallah's Funeral: Iraqi Militia Response and Attendance," *Militia Spotlight*, Washington Institute for Near East Policy, February 27, 2025.
42 See Knights, al-Kaabi, and Malik, "Tracking Anti-U.S. Strikes in Iraq and Syria During the Gaza Crisis."
43 Ameer al-Kaabi, Michael Knights, and Hamdi Malik, "Iraqi Militias Downscaling Their Anti-Israel Actions," *Militia Spotlight*, Washington Institute for Near East Policy, November 26, 2024.
44 Hamdi Malik, "PMF Non-Deployment to Save Assad: Sudan's View Contradicted by Iran," *Militia Spotlight*, Washington Institute for Near East Policy, January 21, 2025.
45 Hassan al-Araji, Michael Knights, Hamdi Malik, and Sary Mumayyiz, "The Fatemiyoun/Zainabiyoun Influx: Iraq's Intensified Hosting of Two U.S.-Designated Terrorist Groups," *Militia Spotlight*, Washington Institute for Near East Policy, February 11, 2025.
46 Michael Knights, "The Danger of Letting Iraq's PMF Authority Law Pass," *Militia Spotlight*, Washington Institute for Near East Policy, April 8, 2025.
47 This history has been covered in detail as it unfolded, through the Militia Spotlight blog (until 2025) and the *CTC Sentinel* article series by the authors since 2020.
48 For military analysis of the Houthis, see Michael Knights, "An Heir and a Spare? How Yemen's 'Southern Hezbollah' Could Change Iran's Deterrent Calculus," Washington Institute for Near East Policy, December 2023.
49 See the two *CTC Sentinel* studies published in 2024 and 2025: Michael Knights, "Assessing the Houthi War Effort Since October 2023," *CTC Sentinel* 17:4 (2024) and Michael Knights, "A Draw Is a Win: The Houthis After One Year of War," *CTC Sentinel* 17:10 (2024). For a detailed analysis of Iran-Houthi relations, see Michael Knights, Adnan al-Gabarni, and Casey Coombs, "The Houthi Jihad Council: Command and Control in 'the Other Hezbollah,'" *CTC Sentinel* 15:10 (2022).
50 Orna Mizrahi, "'The Roaring Lion' – Hezbollah's War for Survival," *INSS Insight* No. 2118, March 24, 2026.
51 "Houthi Escalation Calculus Following Cautious Entry into the Iran War," Institute for the Study of War, April 3, 2026.
52 Crispin Smith and Michael Knights, "Mohammad Baqer al-Saadi: Profiling an IRGC and Iraqi Militia Operative," *CTC Sentinel* 19:5 (2026).
53 To give one example of the kind of analysis that foresaw an existential war for the Iranian regime, see Bilal Saab, "What Trump wants from Iran talks – and what Tehran is prepared to give," Chatham House, February 6, 2026.
54 Michael Knights, "Profile: Kataib Sayyid al-Shuhada," *Militia Spotlight*, May 3, 2021 (updated November 17, 2023).
55 Saraya Awliya al-Dam post on Telegram, January 31, 2026.
56 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
57 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
58 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
59 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
60 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
61 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
62 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
63 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
64 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
65 Knights, "Soleimani Is Dead;" Knights, al-Kaabi, and Malik, "Tracking Anti-U.S. Strikes in Iraq and Syria During the Gaza Crisis."
66 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
67 Authors' database of *muqawama* attack claims.
68 Authors' database of *muqawama* attack claims.
69 Hamdi Malik and Michael Knights, "Profile: The Islamic Resistance in Iraq," Washington Institute for Near East Policy, October 21, 2023.
70 Ibid.

- 71 Authors' database of *muqawama* attack claims.
- 72 Authors' database of *muqawama* attack claims.
- 73 Crispin Smith, Hamdi Malik, Michael Knights, and Sary Mumayiz, "Profile: Kataib Sarkhat al-Quds (formerly known as Ashab al-Kahf)," *Militia Spotlight*, Washington Institute for Near East Policy, April 1, 2021, updated October 18, 2024.
- 74 Authors' database of *muqawama* attack claims.
- 75 Authors' database of *muqawama* attack claims.
- 76 Six of 14 but it was also joined in targeting by RBS and AK on March 4-5.
- 77 This insight is derived from the authors' database of U.S. strike reports from the 2026 war.
- 78 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 79 "Saudi Warplanes Struck Militias in Iraq, Sources Say," Reuters, May 13, 2026; Amberin Zaman, "Majority of attacks on Saudi Arabia carried out by pro-Iran militias in Iraq," *Al-Monitor*, May 18, 2026.
- 80 Riley Mellen, Christoph Koettl, and Eric Schmitt, "Dozens of U.S. Planes Are at Jordan Base, Satellite Images and Flight Data Show," *New York Times*, February 20, 2026.
- 81 This insight is derived from the authors' detailed attack claims database from the 2026 war, which includes tabulated date, claim group, narrative details, branding, achieved offline Telegram posts, and related videos and imagery.
- 82 This is the author group's assessment based on all available information gathered during the course of this research project.
- 83 Telegram post from "Abu Alaa al-Walai – Official Channel," March 13, 2026.
- 84 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 85 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 86 Knights gathered over a dozen individual detailed reports of inbound drone and missile shipments in this period. Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 87 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 88 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 89 This is the author group's assessment based on all available information gathered during the course of this research project.
- 90 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 91 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 92 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 93 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 94 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 95 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 96 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 97 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 98 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 99 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 100 Interview data is corroborated by the authors' detailed attack claims database and geolocated SIGACT dataset, which shows a marked increase in the use of these new 'exotic' drone models beginning in the war's third week (see Figure 5).
- 101 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 102 Stephen Kalin, "Saudi Arabia and Iraq Are Caught in a Hidden War Within the War," *Wall Street Journal*, April 20, 2026.
- 103 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 104 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 105 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 106 Authors' database of *muqawama* attack claims.
- 107 April 1 Shahed 238. This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 108 For an example of this kind of expectation, see Priyanka Shankar, "Is the US ready to invade Iran? What Trump's moves tell us so far," *Al Jazeera*, March 30, 2026.
- 109 Knights and Smith, "Badr Organization."
- 110 Ibid.
- 111 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 112 Al-Araji, Knights, Malik, and Mumayiz, "The Fatemiyoun/Zainabiyoun Influx."
- 113 Michael Knights, "Punishing Iran's Triggermen in Iraq: Opening Moves in a Long Campaign," Washington Institute for Near East Policy, December 6, 2019.
- 114 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 115 See Phillip Smyth, "The 'Hashd (Iraqi PMFs) aid convoy' for Iran. Note a few issues . . .," X, April 3, 2026.
- 116 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 117 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 118 Fadhel al-Nashmi, "Air Strike Cuts Southern Iraq Off from Iran," *Asharq Al Awsat*, April 5, 2026.
- 119 This insight is derived from the authors' database of U.S. strike reports from the 2026 war.
- 120 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 121 See footnote AM.
- 122 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 123 Data drawn from the authors' geolocated SIGACT dataset covering the 2017-2026 period of *muqawama* kinetic operations.
- 124 Hamdi Malik, Michael Knights, and Yaqoub Beth-Addai, "Profile: Hashd al-Shabak (30th PMF Brigade)," *Militia Spotlight*, Washington Institute for Near East Policy, June 22, 2022, updated June 3, 2024.
- 125 Ibid.
- 126 Michael Knights and Yaqoub Beth-Addai, "Profile: Kataib Babiliyoun (50th PMF Brigade)," *Militia Spotlight*, Washington Institute for Near East Policy, March 16, 2023, updated November 27, 2023.
- 127 Ibid.
- 128 "Treasury Sanctions Persons Associated with Serious Human Rights Abuse and Corrupt Actors in Iraq," U.S. Department of the Treasury, July 18, 2019.
- 129 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 130 This is the authors' collective conclusion based on a synthesis of geolocated interview material and the authors' geolocated SIGACT dataset.
- 131 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 132 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 133 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 134 See "ATP 4-35: Munitions Operations and Distribution Techniques," U.S. Army, September 2014.
- 135 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 136 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 137 This insight is derived from the authors' database of U.S. strike reports from the 2026 war.
- 138 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 139 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 140 This insight is derived from the authors' database of U.S. strike reports from the 2026 war.
- 141 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 142 Data drawn from the authors' geolocated SIGACT dataset covering the 2017-2026 period of *muqawama* kinetic operations.
- 143 This insight is derived from the authors' database of U.S. strike reports from the 2026 war.
- 144 Michael Knights and Alex Almeida, "Militia Schisms: The Dissolution of the PMF Northern Axis," *Militia Spotlight*, Washington Institute for Near East Policy, August 5, 2024.

- 145 See Knights, Malik, and Al-Tamimi, "Honored, Not Contained."
- 146 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 147 Both Sayyed Talib al-Musawi (Taleb Mohammed Hussein) and his Badr comrade Abu Jassim al-Askari are mentioned repeatedly in interview material. Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 148 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 149 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 150 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 151 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 152 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 153 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 154 Insight gathered from the authors' geolocated SIGACT dataset covering the 2017-2026 period of *muqawama* kinetic operations.
- 155 The contraction of the coalition footprint in federal Iraq can be traced in successive OIG quarterly reports on Operation Inherent Resolve, available at <https://www.dodig.mil/Reports/Lead-Inspector-General-Reports/Tag/47804/operation-inherent-resolve/>
- 156 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 157 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 158 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 159 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 160 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 161 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 162 This insight is derived from the authors' database of U.S. strike reports from the 2026 war.
- 163 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 164 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 165 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 166 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 167 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 168 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 169 Data drawn from the authors' geolocated SIGACT dataset covering the 2026 war.
- 170 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 171 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 172 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 173 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 174 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 175 See the in-depth section on Jurf as-Sakr in Knights, "Back into the Shadows?"
- 176 This insight is derived from the authors' database of U.S. strike reports from the 2026 war.
- 177 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 178 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 179 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 180 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 181 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 182 This insight is derived from the authors' database of U.S. strike reports from the 2026 war.
- 183 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 184 Sherwan Hindreen Ali, "Are Iran-backed Iraqi militias escalating attacks against the Gulf?" ACLED, May 21, 2026.
- 185 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 186 This is the authors' understanding based on years of research on range limitations of *muqawama* weapons.
- 187 Data drawn from the authors' geolocated SIGACT dataset covering the 2026 war.
- 188 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 189 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 190 Michael Knights, Amir al-Kaabi, and Hamdi Malik, "Is Kataib Hezbollah Behind Saraya al-Ashtar's Claimed Attack on Israel?" Militia Spotlight, Washington Institute for Near East Policy, May 4, 2024.
- 191 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 192 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 193 "Saudi Warplanes Struck Militias in Iraq, Sources Say," Zaman, "Majority of attacks on Saudi Arabia carried out by pro-Iran militias in Iraq."
- 194 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 195 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 196 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 197 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 198 See footnote CY.
- 199 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 200 See the demarches mentioned earlier in footnote BJ. See also "Iran's Revolutionary Guards set up covert Iraqi cells to attack Gulf neighbors, sources say," Reuters, June 19, 2026.
- 201 See, for example, Crispin Smith and Michael Knights, "Remaking Iraq: How Iranian-Backed Militias Captured the Country," Just Security, March 20, 2023, noting the militias' obsession with *al-harb an-nā'ima* (soft war) and *al-harb al-qānūniyya* (legal warfare).
- 202 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 203 Smith and Knights, "Mohammad Baqer al-Saadi."
- 204 "Dual Iranian-Iraqi National Indicted for Providing Material Support to Terrorist Organizations," U.S. Department of Justice, May 29, 2026.
- 205 Ibid.
- 206 Smith and Knights, "Mohammad Baqer al-Saadi."
- 207 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 208 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 209 Developing and exercising these skills has been the primary focus of the Militia Spotlight team since 2021.
- 210 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 211 For a discussion of *muqawama* use of lawfare, see Smith and Knights, "Remaking Iraq." See also Crispin Smith, Hamdi Malik, and Michael Knights, "Team of Legal Gladiators? Iraqi Militias' Tortured Relationship with Law," Just Security, April 12, 2021.
- 212 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 213 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 214 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 215 This insight is derived from the authors' detailed attack claims database from the 2026 war.
- 216 This insight is derived from the authors' detailed attack claims database from the 2026 war.

- 217 Jaish al-Ghabab was created on February 23, 2026, days before the start of the conflict in February 2026, and it posted its first post on February 25, 2026. Given its limited history, assessing the group's affiliation is difficult. Preliminary analysis suggests it is likely an HaN affiliate, based on patterns of reposting and amplification.
- 218 Knights, "Iran's Expanding Militia Army in Iraq."
- 219 See Knights, Malik, and Al-Tamimi, "Honored, Not Contained."
- 220 Knights, "Iran's Expanding Militia Army in Iraq."
- 221 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 222 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 223 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text. The authors maintain a roster of all known active brigades. At any time, a smattering of PMF units display a very low level of activity or are partway through amalgamation, and new small units pop up regularly, so the range of 65-70 is defensible and appropriately inexact.
- 224 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 225 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 226 See Knights, Malik, and Al-Tamimi, "Honored, Not Contained." Also peruse the Militia Spotlight profiles page to see over 30 PMF brigades characterized in terms of their close relationships with the *muqawama*.
- 227 Knights, Malik, and Al-Tamimi, "Honored, Not Contained."
- 228 Ibid.
- 229 Amir al-Kaabi, Hamdi Malik, and Michael Knights, "Iraqi PMF Chief of Staff Commits to Fulfill Iranian Supreme Leader's Plans," Militia Spotlight, Washington Institute for Near East Policy, April 8, 2024.
- 230 Hamdi Malik and Michael Knights, "The PMF Represents Iraq at the Axis of Resistance Conference in Tehran," Militia Spotlight, Washington Institute for Near East Policy, May 24, 2024.
- 231 Al-Kaabi, Malik, and Knights, "Iraqi PMF Chief of Staff Commits to Fulfill Iranian Supreme Leader's Plans."
- 232 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 233 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 234 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 235 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 236 See "Constitutional Declaration of a State of War," Republic of Iraq Supreme Juridical Council, March 27, 2026, available at <https://www.sjc.iq/view-en.79344/>.
- 237 Knights, "Iran's Expanding Militia Army in Iraq."
- 238 Knights, Malik, and Al-Tamimi, "Honored, Not Contained."
- 239 Ibid.
- 240 Knights, "Iran's Expanding Militia Army in Iraq."
- 241 Knights and Smith, "Badr Organization."
- 242 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 243 Knights, Malik, and Smith, "Iraq's New Regime Change."
- 244 Amir al-Kaabi and Michael Knights, "Iran-Backed Militias Applaud Hamas, Threaten Americans by Amir al-Kaabi," Militia Spotlight, Washington Institute for Near East Policy, October 13, 2023.
- 245 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 246 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 247 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 248 This has been a consistent theme in Knights' interview materials and discussions with Badr members spanning back to 2003.
- 249 Note the earlier footnote regarding Zolfaqer and Fateh-110/313 SRBMs inside Iraq.
- 250 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 251 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 252 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 253 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 254 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 255 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 256 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 257 Knights, Malik, and Al-Tamimi, "Honored, Not Contained."
- 258 Author (Knights) interviews, multiple Iraqi contacts, 2026; exact dates, names, and places withheld at request of the interviewees.
- 259 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 260 This is the authors' collective conclusion, based on their synthesis of the known facts, and explored further through this text.
- 261 See footnote BD.
- 262 Knights and Smith, "Badr Organization."
- 263 Knights, Malik, and Al-Tamimi, "Honored, Not Contained."
- 264 Seth Frantzman, "Several Iranian-backed militias in Iraq say they accept state control of weapons," FDD's Long War Journal, June 3, 2026.
- 265 Renad Mansour, "Networks of power: The Popular Mobilization Forces and the state in Iraq," Chatham House, February 2021.
- 266 Ibid.

A View from CT Foxhole: Brigadier General Matthew Ross, Director, JIATF-401

By Sean Morrow and Don Rassler

Brigadier General Matthew Ross is the Director of Joint Interagency Task Force 401. As Director, he supervises the Department of War's consolidated effort to rapidly develop and provide counter drone capabilities at scale to enable the department to protect U.S. and allied forces, defend critical infrastructure, and assist federal agencies in securing population centers from unmanned aerial system threats.

Throughout his career, Brigadier General Ross has deployed multiple times for combat and contingency operations. He has a bachelor's degree from West Point, a master's degree from Central Michigan University, and served as a fellow at Duke University's Sanford School of Public Policy.

CTC: You serve as the Director of the Joint Interagency Task Force 401, and you've previously spoken about how you've dealt with drone threats and counter unmanned systems in the field and on operations, and how you've also utilized drones for offensive operational purposes. How has your experience shaped your approach to the director role and the work that you're doing at JIATF-401?

Ross: Because of my previous roles, I think about every military situation as the aggressor, or from a proactive approach, and I try to share that with the JIATF team. I really see our counter-UAS [unmanned aerial systems] equipment as the last resort or last line of defense. It's easy to think, from a counter-UAS perspective, that the equipment will save us. But I'm convinced that there's no silver bullet and the equipment won't save you. It is going to be the responsibility of the individuals who are trying to accomplish a mission to ensure that the threat of small drones or unmanned systems does not prevent them from being able to accomplish their mission. And so that's the very proactive approach.

A lot of the things we've done here recently at JIATF focus on removing the archer instead of the arrow. So, you focus on attacking the drone pilot first. Even just in the last 24 hours, we had one case of a successful interdiction on a military installation, and that's how it ended up playing out. We identified the ground control station, and we were able to get a team out there to apprehend the individual.

CTC: Do you remember a moment in your career when you realized just how transformative small drones would be and that it wasn't just a tool you were fighting, but a revolution in tactics?

Ross: I think I will give an answer that's unlike others. I think a lot of people would reference Operation Spiderweb or other conflicts in the Middle East. They might reference day-to-day fighting in

Ukraine and the proliferation of mass in terms of drones. For me, what was most concerning is the way adversaries fought with the use of proxies. We use proxies because we want to manage attribution and escalation, and so what you have to do to use proxies effectively is you have to be able to share or proliferate advanced conventional weapons to give them some type of state-like military capability. That's what drones do. Drones provide capability to small groups and individuals that were previously reserved for state adversaries. So, whether it's exquisite ISR [intelligence, surveillance, and reconnaissance], the ability to collect on signals of interest, the ability to weaponize an unmanned system that you could use from great distance, that is what has been most concerning for me.

I actually think that the larger transformation will be the inclusion of much larger systems. The advancements in autonomy are going to allow us to scale that even more. For example, when I was in a previous role, we were looking at autonomous breaching. This wasn't just limited to the use of small drones; it was an entire ecosystem of autonomous technologies that would allow you to accomplish a military task without putting service members at risk. I knew immediately that this was going to change the way we fight into the future.

CTC: JIATF-401 was established by the Department of War in August of 2025. Why was JIATF-401 created? What problems is it trying to solve? What unique features or authorities does it have, and what are its primary lines of effort?

Ross: First, I would say counter-UAS is a domain that's advancing so quickly that we wanted to ensure that we weren't just trying to keep pace with the threat within pockets of excellence. Instead, we wanted to *synchronize* efforts across the Department. We wanted to make sure that we shared everything that we have been learning with our interagency partners because counter-UAS is both a warfighting and a homeland defense imperative. We, as the Department, put a bunch of resources into RDT&E [Research, Development, Test, and Evaluation] and development of new technology. And so how do we take those investments and transfer them to federal authorities, to state, local, tribal, and territorial partners as they get responsibility to protect against the threat of drones? How do we make sure that they're well equipped to accomplish that task? That's what the team at JIATF-401 has been taking on.

I do think that drones are changing the character of modern combat, but they're not changing the nature of combat. Victory still belongs to those who adapt fastest, those who strike the hardest and endure the longest, and so countering drones is key to force protection, mission success, and survival on the modern battlefield. So, I believe that incorporating unmanned systems into the fight is critical, and I would say that's true both from an offensive standpoint and from a defensive standpoint. We tend to bifurcate the two. But we have to continue to do that both with aerial systems, including

“I do think that drones are changing the character of modern combat, but they’re not changing the nature of combat. Victory still belongs to those who adapt fastest, those who strike the hardest and endure the longest, and so countering drones is key to force protection, mission success, and survival on the modern battlefield.”

unmanned aerial drones and counter-UAS, and unmanned systems more broadly, especially as we start incorporating larger ground vehicles, surface vessels, or underwater vehicles.

Over the past five years, two of the things that has changed the most when it comes to drones is their increased resiliency—their ability to operate in contested environments—and mass. What we’ve seen is that when the cost goes down, you’re able to expand production and you’re able to introduce mass to a battlefield. When I look at what we’ve seen in the most contested environments, like the current fight between Ukraine and Russia, what catches my attention most is the innovation cycle and the iteration. When we talk about innovation, people tend to think about the platforms themselves. I actually think it’s the TTPs [tactics, techniques, and procedures]. It’s how we use the tools that were provided, and so when people would say there’s an iteration cycle of 72 hours or seven days in Ukraine, they’re not saying that they’re rolling out new technology every seven days. But the way they use that technology, the frequencies that they’re using, the TTPs, that is what is evolving quickly. And that’s what we need to replicate.

We have three lines of effort inside JIATF. The first is defense of the homeland. The second is support to warfighter lethality, and the third is joint force training. I think all three are critical, so defending the homeland is where we spend a lot of our effort in support of the Secretary [of War] through things like Domestic Shield and the provision of counter-UAS technology to help defend critical infrastructure. But support to warfighter lethality is also critically important. Operation Epic Fury has given us the opportunity to sprint towards that objective by introducing new technology, TTPs, and solutions into a contested environment. That enables us to see what works and what doesn’t.

CTC: JIATF-401 has been a test case for new acquisition processes and authorities. Can you help our readers understand what’s changed? How it’s enabled your organization and if it’s scalable outside of JIATF to the Army and DoW?

Ross: I think we were the first program acquisition executive as part of the changes to the acquisition process across the Department. One thing that is unique to us is our structure. I work directly for DEPSECWAR and serve as the senior advisor on counter-UAS to the Chairman [of the Joint Chiefs of Staff], which allows us to connect directly from the corporal on the frontline to the senior levels of the Department to understand the greatest challenges.

When people think about acquisition authority, they typically think about traditional acquisition process: how we go through the testing and evaluation of new technology to make sure that it’s safe to use, it meets the requirement, and that we can get it out to the formations with full DOTMLPF [Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities] considerations. That’s only a piece of it, as once we deliver those solutions, we’ve got to make sure the guidance, the ROE [rules of engagement], the permissions and authorities for those service members allow them to use the equipment effectively.

We say we have one measure of effectiveness inside JIATF and that’s delivering state-of-the-art counter-UAS capability to our warfighters both at home and abroad. But I think that’s so much more than delivering a new piece of equipment. As an example, if I go to talk to a patrol leader on the southern border as part of JTF [Joint Task Force] Southern Border today and I ask them what their greatest challenges with UAS are, they won’t tell me that they need a new interceptor. They’ll tell me that they need to be able to see everything they can see in the JOC [Joint Operations Center] on a mobile device when they’re out on patrol. That is their greatest limiting factor, and so we should address that problem first before we start progressing into the next piece of advanced technology.

What I love about JIATF’s mission is that we are responsible for all of that. The guidance, the policy, law, where it applies, the authority to operate, the authority to connect to a specific system, spectrum approvals, target engagement authority, and the training through the Joint Counter-UAS University (JCU). By looking at that whole ecosystem, we have the ability to affect meaningful change.

One of the things I’m most proud of that we did within our first 90 to 120 days is clarifying the guidance from SECWAR to our installation commanders on how they should be approaching the problem and their authorities to counter UAS because it wasn’t clear at the time. While that seems like a really small thing, it makes a huge difference for that person who’s sitting in the operations center, who has to identify an incursion and make a determination about what they should or should not do. Having clear guidance from the top is helpful in that process.

CTC: You’ve talked about JIATF’s one clear measure of effectiveness (MOE)—to rapidly put state-of-the-art c-UAS capabilities into the hands of warfighters at home and abroad. What type of progress do you feel JIATF has made toward that goal thus far?

Ross: The first thing we did was to clarify the authorities and approvals for counter-UAS, and then we started addressing the network. We identified the fact that we need a common tactical user interface for counter-UAS. We should be able to share information between agencies that are working side by side, especially if it’s inside the continental United States. We should also be able to share data with partners and allies if we’re working OCONUS in places like the Middle East. And so first, we addressed the policies and authorities. Second, we addressed the network, and now we’re at the point where we’re starting to integrate additional sensors and effectors across the force.

For context, when I say sensors, I’m talking about a number of different sensors, including active and passive sensors. Passive sensors would be things like acoustic sensors and passive radars.

We're actually running a pilot program with passive coherent radar right now that uses available signals in the environment to identify a disruption, so you know that there's a device there. It gives you a less precise location, but it gives operators enough to know that there is an incursion that needs attention. Another layer of sensing would be day and night cameras, EO/IR [electro-optical/infrared] cameras. By layering all these sensors together, we can build depth in our ability to understand when a threat's coming at us. In the past, we would approach counter-UAS like integrated air and missile defense, and there's a concept in integrated air and missile defense called Castle Defense that is guided by the view that we're going to sit here within our walls and we're going to defend from inside of our perimeter. I don't think that's how we should approach counter-UAS. We need to get outside of that perimeter to be able to sense in depth so that we can increase our decision space.

When I talk about effectors, there's both kinetic and non-kinetic effectors. Non-kinetic effectors would include jammers, something that would deny a specific link that's targeted. It may be a barrage jammer that jams the entire spectrum so it's hard for adversaries to operate. It may be a cyber takeover system, and so with some systems, you can actually take over the flight and be able to land a drone into a safe area. And then there's kinetic effectors, which include interceptor drones, which is a place that we're investing in right now—think drone-on-drone warfare with small interceptor drones. We've had these for Group 3 [UAS] and above, and we've thought of it as ground-based air defense. We're building the exact same capabilities for Group 1 and Group 2 [UAS]. Then, there are also effectors that utilize directed energy. We're running a directed energy pilot for the Department, specifically looking at lasers and high-powered microwave and trying to determine where they are most applicable in our layered defense for counter-UAS.

For a long time, especially in the homeland, we have limited ourselves to non-kinetic options, meaning I would have a system that would detect a radio frequency for a ground control link and then I would try to attack that link to defeat the drone, which works really well for commercial systems. It's less effective for a system that has been modified. So, what we do now is attack the physics of flight. Every single drone has some type of physical mass, which means it's observable through passive and active sensing. It has some type of rotors that allow it to stay aloft and stable. It's got some type of camera or sensor that will allow it to see where it's going so it can get to its final objective. If we attack those first principles in terms of how we try to counter UAS, then our solutions will be more resilient as the modality of control changes for these drones.

For example, here's one other thing we've done over the past 12 months, which I think is a step in the right direction. We're working in support of NORTHCOM and JTF Southern Border and with the other federal agencies along the southern border, all 1,954 miles. We've surveyed the entire border to first ensure that we have shared air domain awareness. We've looked at where we need to place sensors along the entire border so that we have full domain awareness across the southern border and when that is integrated into a common C2 [command and control], we can start layering in effectors that allow us to protect the homeland. That is an effort that we've been moving against pretty quickly. We made a ton of progress over the past several months, and in just the last four months, we've allocated more than \$20 million in counter-UAS technology to support this goal.

CTC: A cornerstone of JIATF-401's effort has been the creation of a counter-UAS marketplace, "a centralized mechanism that allows interagency and law enforcement partners to access DoW test data, operational user feedback, and validated procurement options."¹ The marketplace went live in February and reportedly features at least a dozen counter-UAS systems and a "continuously expanding inventory ... [of] a wide array of sensors, effectors, and system components."² Tell us a bit about the marketplace, the process of building it, some of the capabilities or systems you're excited about, and how you plan to evolve it.

Ross: I would say that there are two problems we need to solve with the marketplace. The first problem is where we typically start inside of the War Department and that is making drones and counter-UAS capability available to our formations. That's a very real challenge. In the past, when we thought about unmanned systems, we centrally managed those systems because they were expensive, complex, and we had limited quantities, like MQ-9 reaper drones. Over time, we saw that those systems got smaller and less expensive and that we required them at echelon.

So, we changed our approach and said, 'Hey, we actually need these at every level of our formations.' And so, we need to make sure that they're accessible to the companies, the battalions, and the brigades. And that's what SECWAR laid out with his drone dominance memo last year.³

I would argue that counter-UAS is the same thing, and so in the past, these systems have been large and complex, limited in quantity, and centrally managed. What that means is that in an Army formation, if you go to a division, the only thing they have for counter-UAS may be a counter-UAS battery. That is completely insufficient. We need a variety of counter-UAS tools at echelon based off their most likely threats.

So, problem one is ensuring that we have accessibility across the Department to those capabilities for counter-UAS. Problem two, and this is the part that I'm more interested in from a JIATF-401 perspective, is making sure the counter-UAS technology is available to all members of the JIATF *and* our partners and allies. What that means is that the other interagency parts that use different systems for their procurement need to be able to have access to our market, understand the testing and validation that we've done on these systems, and then have access to the industry partners that provide those capabilities.

Counter-UAS is a problem not just inside of the Department. It's a problem for the FBI and DHS like we've talked about on the southern border. The Department of Corrections, anybody who runs a prison today has problems with drones delivering contraband inside of their walls. So, they also have a requirement for counter-UAS. But they don't know where to go to fill that requirement. Similarly, industry can't see the aggregated demand for counter-UAS systems. So, what we have done with the counter-UAS marketplace is we've made it fully open—a two-way marketplace. If somebody wants to deliver a counter-UAS solution into our ecosystem, they can go to the counter-UAS marketplace and upload their product and say, 'Here's what it does.' Then we as JIATF-401 will test the product, and if it does exactly what they've described, we'll put a JIATF-401 badge on it, so people know that it's been validated. If it does not perform as advertised, they need to make improvements before we will endorse the product.



Brigadier General Matthew Ross

I think this is really important for counter-UAS, especially as you talk about investment over time because 80 percent of what we buy or field, especially in the small drone space, is commercial equipment. So, by pulling this marketplace together, we have the ability to aggregate demand so that U.S. industry can build breadth and depth in our industrial base, so that we have the capacity for that next conflict where we know our requirements are going to be higher than they are today.

CTC: What is the role of private capital in the c-UAS fight? How can we incentivize companies to invest in your needs, particularly from non-primers, who maybe haven't historically had access to DoW development?

Ross: I've actually spent quite a bit of time with private capital investors trying to help them see what I believe the market is. I think the biggest thing we can do to help them is aggregate that demand, and so part of the counter-UAS marketplace [is] it will provide analytics and be able to tell us things like the purchases for a 12-month period. We'll be able to tell you that two and a half billion dollars went to small-form radars with a range of 20 kilometers and below. When industry sees that, they'll be able to make a better assessment of where they should put their capital. We'll be able to tell you how much money went into specific interceptors, acoustic sensors, or software that enables an operator. Today, we struggle to see that because we have treated counter-UAS as a military-specific problem; that is just not the case anymore.

If you look at what's happening in Colombia with the FARC, the Colombians have a very high demand for counter-UAS technology, and they're trying to figure out where to put those resources. If you go to the Middle East today, all of our partners and allies are trying to buy counter-UAS technology, and they want to buy from the U.S. industrial base. So, we've got to make it accessible to them.

CTC: A lot of what we have learned about c-UAS is rolling off the battlefield of the Ukraine war. Given the speed of innovation

that we have seen, how do you make sure that we're learning the right lessons at the right speed while also considering future threats so that our responses do not quickly become obsolete?

Ross: I've been studying the Ukraine conflict closely, partially because I am a member of the profession of arms, and I think anytime somebody's in conflict, you must watch really closely, especially as we see these changing characteristics of warfare. When I look at what works really well in Ukraine, I think of it similar to our first-principles approach. How could that apply to our warfighting concept? It doesn't mean we can pick up what they're doing in Ukraine and directly transplant it to another environment because our ecosystem is going to be different. The Ukrainians fight very well with limited resources. We fight very well and have access to more resources, and what that means is as we take their lessons learned, we need to apply it to the U.S. Department of War's Joint Warfighting concept to get the full benefit from those lessons.

What's most impressive to me as I watch the Ukrainians is their ability to innovate and evolve rapidly. That's what I want to build for us. I don't think it's about any specific platform. It's about building an ecosystem that allows us to identify an emerging or adapting threat and then evolve with it fast enough to keep our warfighters safe.

CTC: Can you share a bit about some of the testing and experimentation that you've done regarding platforms and systems? For example, we've been able to read about your testing of the Bumblebee V1 C-UAS drone round ammunition, which "breaks apart mid-flight and effectively becomes buckshot"⁴ and multipurpose, high-energy lasers.

Ross: When it comes to testing and experimentation, the first thing we have to do is make sure that when we test or evaluate something, we share it across the Department and our interagency. So, probably the most impactful thing we have done in this area is that we established a common characterization for counter-UAS evaluation. We developed test standards and put them out across the entire department and across all the labs. We've got 77 labs across the U.S. Department of War that are actively working on this problem. We publish our list of problems so that people are working on the challenges that we see in the counter-UAS fight. Then, when somebody develops a countermeasure and they evaluate it, they evaluate it to the standard. That allows us to make a relative comparison between two different systems that were tested on different days in different locations. As an example, EUCOM and USAREUR-AF just ran Flytrap 5.0, which is a counter-UAS exercise executed at scale and echelon. They did it with 7th ATC [Army Training Command] in Lithuania. Simultaneously, we had testing going on in Nevada for counter-UAS. We should be able to compare how something performed in Nevada to how something performed in Lithuania, and we can't do that without establishing a common standard, and that's what we've done.

Second is we've started looking at the inclusion of kinetics because I believe that kinetics will be imperative as we attack the first principles of flight for a drone that could present a threat. If we want to be able to take that drone out of the sky, then we have to be able to test those kinetics. That's what we've done with the Bumblebee V1 and V2, which are small drone interceptors enabled with automatic target recognition and pilot enhancing

software that allows it to go on a terminal attack. The automation is software enabled instead of hardware enabled, which means it can be updated immediately. If you buy one of those today, and we continue to iterate on the algorithm, then 12 months from now, the system is more capable because all you have to do is load the update.

The other thing that we've done with testing and evaluation is ensure that we can use all available tools in the national airspace, and we're doing that with the FAA [Federal Aviation Administration], who's been a great partner for us. As we talk about directed energy or the testing that we've done with high-energy lasers, which are now being approved for use inside the national airspace, we're ensuring—if you go back to those authorities and approvals, which are our greatest challenge, it's not necessarily the technology itself—that we have an ability to use it effectively. We're making sure that as part of our testing: one, it's common across the department and then two, everything that we introduce into the counter-UAS ecosystem is actually usable by our service members that are out on the field.

CTC: What can you tell us about the Domestic Shield initiative, formerly known as Replicator 2, and Operation Clear Horizon and how JIATF's work intersects with and supports the drone focused executive orders that the Trump administration has issued?

Ross: I'll start with Operation Clear Horizon. Within 30 days of being established as JIATF-401 by SECWAR, we ran an exercise to look at all the services, and their programs of record for counter-UAS. We brought all of the services' equipment out to a location, and we flew really complex threat profiles. We threw Group 3 drones at them. Group 2 Drones. Group 1 drones controlled over radio frequency, LTE, GPS, and fiber-optically controlled drones. We flew the most advanced technology and profiles that we had seen on the battlefield in Ukraine against our countermeasures. In fact, the red team that we used for that came from 10th Special Forces Group who had just recently been in Ukraine and in eastern Poland, working against this problem. We did that so we could identify those areas where we have gaps or seams in our protective capability and then that allowed us to prioritize our efforts.

That helped to set the stage to get where we are today, and to build a more robust layered defense for counter-UAS. When I talk about the need for a common C2 and the requirement for physical effectors for Group 1 and Group 2 drones, that all came from Operation Clear Horizon and those lessons learned.

Domestic Shield started off as Replicator 2. Replicator 1 was the provision of one-way-attack drones and loiter munitions. We wanted to provide them across all the Department. Replicator 2 was a recognition that we needed to do the same thing on counter-UAS, and we needed to protect our critical infrastructure in the homeland and our power projection platforms. That effort started with reconciliation funding and was previously run by DIU [Defense Innovation Unit]. Right after JIATF-401 was established, it was transitioned to our team and became the Domestic Shield initiative. What we did with that problem is we looked at defense critical

infrastructure across the Department and we tiered it by priority based off what types of activities and operations they conduct to make sure that we understood what locations required the most protection. Then, we worked with the services. They conducted a survey of every one of our installations. Some would argue that when you identify a really good counter-UAS set of equipment, why don't you just give one to every installation? Well, that doesn't work well because all our installations are different; they're different sizes, different shapes, they've got different types of security forces. In some cases, we manage them with air force security forces. Sometimes on army bases, you just have MPs [Military Police] that are patrolling. In some cases in shipyards, you actually have contractors who are providing security. So, we needed some level of tailorability for counter-UAS at each of those installations. We worked closely with the services to conduct the surveys.

Those surveys told us the following: 'Based off what I'm protecting and the resources that I have available, here's what I require in terms of counter-UAS solutions.' We validated those against the systems that we've tested and evaluated across the Department, and if everything lines up, we're procuring those systems and we're delivering them at scale. It's important to note that none of our installations were completely uncovered. We're just making sure that as we continue to adapt to the evolving threat, we systematically and continuously update our counter-UAS posture with the most recent technology so we can keep pace.

CTC: JIATF-401 has accomplished a lot in 12 months. Where would you like to see the organization in a year?

Ross: My track record to predict the future is really poor, but I can tell you how we're approaching it today. When JIATF was stood up, we knew that it was going to be temporary. As a result, we need to be able to transition the functions we are providing back into the services and the COCOMs, and so for this short period of time, we are going to continue to sprint against the problem. I don't think that our defenses are static. We were just talking about Domestic Shield. I think we have to constantly evolve and mature to ensure resilience, redundancy, and creativity in our counter-UAS posture. That means everything from active patrolling to physical barriers to the counter-UAS measure that would serve as the last line of defense.

We talk about our power projection platforms—our CONUS bases/installations—the homeland is no longer sanctuary, so we have to be prepared to defend our power projection platforms inside the U.S. from nefarious drones. We need to get our formations from fort to port and into a combat theater if and when required. We're also going to continue to pursue emerging technology in conjunction with the services, which is specifically important for directed energy and layered kinetics as we integrate that into our countermeasures more robustly across the United States. That's how we project power. That's how we build a layered defense that gives our warfighters the tools they need to counter this threat.

CTC

Citations

- 1 Adam Scher, "Joint Interagency Task Force Integrates Skills, Creates Layered Counter-Drone Defense," U.S. Department of War, December 18, 2025.
- 2 Adam Scher, "Counter-UAS Marketplace Streamlines Acquisition, First Purchases Total \$13 Million," U.S. Department of War, April 15, 2026.
- 3 Editor's Note: "Memorandum for Senior Pentagon Leadership Commanders of the Combatant Commands," U.S. Secretary of Defense, July 10, 2025.
- 4 Nicholas Slayton, "Soldiers with the XVIII Airborne Corps are training with anti-drone rounds," Task and Purpose, April 14, 2026.

Remotely Coerced Violence: 764, The Com Network, and the Hybridization of Threats

By Marc-André Argentino and Angus Lindsay

This article examines 764 and the wider Com Network as a case study in remotely coerced violence and the hybridization of contemporary terrorist and violent extremist threats. It argues that nihilistic violent extremism is best understood as a victim-driven, youth-centered online ecosystem in which status, belonging, and identity are earned through the production, circulation, and escalation of harm. Drawing on case studies and an arrest dataset of 295 Com Network-linked offenders across 33 countries, this article shows how 764 and adjacent groups combine sadistic online exploitation, cybercrime, self-directed violence, animal abuse, school-violence threats, and terrorist or violent-extremist conduct. Ideological symbols drawn from neo-Nazism, occultism, and accelerationism are present, but usually function as aesthetic and performative resources rather than stable strategic commitments. This article cautions about the risks of mischaracterizing motivation, obscuring victim-perpetrator dynamics, and mistargeting interventions. The authors highlight that responses should integrate a systems approach of prevention and threat reduction that includes counterterrorism, child protection, online harm reduction, trauma-informed practice, and cross-jurisdictional cooperation to address the specific ecology of remotely coerced harm.

In the five years since Bradley Cadenhead founded 764, there has been a surge of media and scholarly reporting examining the nihilistic violent extremism (NVE) phenomenon. In part, this is related to a number of successful and foiled mass-casualty attacks¹ and violent extremist actors² who appear to be at least associated with the broader networks and subcultural spaces that intersect with Com Network groups such as 764, Maniac Murder Cult, and No Lives Matter (for example: Solomon Henderson,³ Jose Pagan,⁴ Arda Küçükyetim,⁵ etc.).⁶ The September 9, 2024, arrest of Dallas Humber⁷ and other core members of the Terrorgram Collective has also challenged understandings of contemporary violent extremism, with the emergence of the so-called “mixed, unstable, and unclear”⁸ or “salad-bar” ideologies.⁹ Recent debates around this ‘new’ form of violent extremism have often centered around the degree to which individuals and groups within online violent extremist networks adhere to a violent extremist ideology, with some researchers and analysts seeking to fit definitions of NVE into broader militant accelerationist categories.¹⁰ Previous research has revealed that so-described NVE groups appear to be influenced by these broader

militant accelerationist and neo-Nazi occultist ideologies¹¹ such as Order of Nine Angles (O9A),¹² which the Government of New Zealand formally designated as a terrorist entity in December 2025, with 764 (and others) defined as “nexions” of the group—which in O9A parlance refers to local, clandestine cells or independent groups.¹³ The Government of Canada listed the 764 group as a terrorist entity in December 2025 as well.¹⁴ By designating these groups as terrorist entities, these governments have assessed that the specific listed groups pursue goals that meet their respective legal definitions of terrorism. The authors do not read those designations as extending automatically to all NVE actors or to the broader milieu.¹⁵

Terrorist designations are an important tool for law enforcement and serve as public markers to recognize and communicate the threat posed by such groups. Because they are tied to legal definitions of terrorism, such designations necessarily center on the political, religious, or ideological motivations those definitions require. Here, the authors complement that lens by focusing on additional dimensions of the threat and argue that nihilistic violent extremism is characterized by six key elements:

- active participation in a specific online ecosystem (the edgesphere), organized around aesthetics, networked performance, and competitive identity work;
- status and belonging earned through the production and circulation of harm (‘clout chasing’);

Dr. Marc-André Argentino is the author of QAnon From Conspiracy Theory to New Religious Movement (2025), co-editor of Contemporary Far-Right Culture The Art, Music, and Everyday Practices of Violent Extremism (2025), and co-author of Dangerous Conspiracy Theories: When Bad Ideas Turn Violent (forthcoming 2026). His current research focuses on nihilistic violent extremism, youth radicalization to violence, and malevolent use of technology. Argentino is a Team Lead at the Government of Canada’s Canada Centre for Community Engagement and Prevention of Violence. The views expressed do not necessarily represent those of the Government of Canada.

Dr. Angus Lindsay is a critical criminologist and national security policy specialist researching digital violent extremism, far-right ecosystems, and emerging online subcultures. His recent work also explores digital racial capitalism, and contemporary far-right mobilization. Based in Aotearoa, New Zealand, he works across research and national security policy to strengthen approaches to counterterrorism, violent extremism, and digital harm reduction. The views expressed do not necessarily represent those of the Government of New Zealand.

© 2026 Marc-André Argentino, Angus Lindsay

- behavioral drivers of anomie, nihilism, and misanthropy;¹⁶
- the hybridization of harms, including the centrality of sadistic online exploitation;
- a limited or secondary role for ideology as a primary driver of mobilization;^a and,
- the absence of a coherent strategic end state.^b

As a hybridized threat,¹⁷ nihilistic violent extremism presents as part sexual violence, self-directed violence, and coercive control;^c part terrorism and violent extremism (with which it overlaps at the level of conduct and threshold, without being reducible to ideological terrorism); part school-safety and school violence; part extreme violence and animal abuse; and part cybercrime and organized cyber-harassment, whose potency lies in its agility and absence of a limiting ideology. Contrary to some understandings, the authors argue that nihilistic violent extremists are individuals and/or networks that actively encourage, promote, glorify, or engage in serious acts of violence and/or criminality with no specific end goal aside from the misanthropic aim of causing harm, chaos, and fear.¹⁸ Although the authors use NVE as an umbrella, the population

“As a hybridized threat, nihilistic violent extremism presents as part sexual violence, self-directed violence, and coercive control; part terrorism and violent extremism (with which it overlaps at the level of conduct and threshold, without being reducible to ideological terrorism); part school-safety and school violence; part extreme violence and animal abuse; and part cybercrime and organized cyber-harassment, whose potency lies in its agility and absence of a limiting ideology.”

- a Historically, assessments have privileged ideological content, doctrinal commitments, command-and-control indicators, and discernible operational planning as the primary discriminators between violent extremist ‘support’ activity and credible mobilization. In The Com Network ecosystems, however, the ecology of risk is frequently mediated through aesthetics, networked performance, and competitive identity work rather than stable ideological adherence. Legacy terrorist semiotics (logos, mottos, anthems, martyr iconography, stylistic templates, and archival propaganda fragments) can be instrumentally redeployed by nihilistic violent extremists without implying continuity of membership, lineage, or even sincere ideological identification with these entities.
- b The authors distinguish a diffuse, destruction-oriented impulse, which is often present, from a coherent strategic objective or governing project, which generally is not. ‘Burning it all down’ as nihilistic destruction for its own sake is not the same as the accelerationist pursuit of collapse as a route to a specified successor order.
- c A growing body of scholarship has argued that coercive control extends beyond intimate partnerships and can function within peer-based relationships, particularly in digital environments where surveillance, group conformity, and emotional domination are structurally enabled. This includes technologically facilitated coercive control, whereby digital tools such as messaging apps, GPS tracking, and social media platforms are used to surveil, isolate, harass, and manipulate. Within digital extremist spaces such as The Com, these dynamics become visible in how participants monitor one another’s behavior, enforce subcultural norms, and punish perceived disloyalty through emotional blackmail, exclusion, and extortion. What distinguishes coercive control within The Com Network is its decentralized peer-to-peer structure, embedded in layered subcultural hierarchies rather than formalized chains of command. Manipulation and coercion in The Com are driven by dynamics of social capital, aesthetic performance, and emotional dependency rather than ideological indoctrination or top-down orders. Victims and perpetrators in this ecosystem do not require formal authority to exert power. Instead, they cultivate influence through ‘clout chasing,’ leveraging emotional intimacy, shame, and the validation of disordered behaviors (such as self-harm and eating disorders) to manipulate and dominate peers. Molly Dragiewicz, Delanie Woodlock, Bridget Harris, and Claire Reid, “Technology Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms,” *Feminist Media Studies* 18:4 (2018): pp. 609-625; Molly Dragiewicz, Delanie Woodlock, Michael Salter, and Bridget A. Harris, “‘What’s Mum’s Password?’: Australian Mothers’ Perceptions of Children’s Involvement in Technology-Facilitated Coercive Control,” *Journal of Family Violence* 37:1 (2022): pp. 137-149; Anastasia Powell, Asher Flynn, and Sophie Hinds, *Technology-Facilitated Abuse: National Survey of Australian Adults’ Experiences, Research Report 12/2022* (Sydney: Australia’s National Research Organisation for Women’s Safety, 2022); Leena Malkki, Henrik Ali-Hokka, and Saija Benjamin, *Violence-Focused Online Communities, RADIA Brief 1/2025* (Helsinki: RADIA, University of Helsinki, 2025).

it covers is not homogeneous, and assigning a single motive to it obscures more than it reveals.

Adapting the role typologies developed for jihadi and right-wing milieus by Nesser and by Bjorgo,¹⁹ the authors distinguish at least four recurring roles: (1) leaders and senior coercive operators, who found groups, set norms, and direct or commission harm (for example, Cadenhead and Chai); (2) influencers and propagandists, who produce and brand content and incite others (for example, Finnigan); (3) groomers and extorters, who cultivate and coerce victims; and (4) directed followers, frequently minors, who carry out coerced or incentivized acts (for example, the Swedish offenders). These roles are fluid; individuals move between them, and a single actor may occupy several at once. They differ from classic terrorist roles in that status flows from documented harm rather than doctrinal commitment, and in the routine overlap between perpetrator and victim. Where statements in this article refer to motivation or ideology, they should be read as applying differentially across these roles.

What is Nihilistic Violent Extremism?

Among those at the core of this threat environment lies a deep-seated sense of anomie.²⁰ Individuals appear to characterize contemporary existence as broadly futile; they lack purpose and appear to experience emotional emptiness and despair. This anomie stems from an unstable social system, the breakdown of normative standards and values, and a lack of collective purpose or ideals at both the individual and community levels. These ‘anomic’ conditions are intensified in digital environments where many chronically online youths who experience loneliness,²¹ alienation, identity instability, social fragmentation, and weakened attachment to pro-social institutions in the offline world are immersed in networked digital subcultures that reward irony, transgression, and ever-escalating displays of anti-social behavior and harm. For those experiencing such anomic conditions, striving is considered useless, because there is no accepted definition of what is desirable.²²

Anomie is further accompanied by an ingrained nihilistic

orientation and driven by a misanthropic outlook that fuels a desire to destroy society, not reform it. This is not to say that ideology is completely absent, but that it does not appear to be a primary driver of the violence. Through the observation of online NVE subcultures and the detailed examination of court documents from cases of known NVEs, the authors have identified that ideology plays a secondary or tertiary role in shaping behavior. These conditions do not emerge in an ideological vacuum; they draw on fragments of pre-existing extremist traditions, most notably neo-Nazi accelerationism, the Order of Nine Angles, maniac culture and Saints Culture, and the celebration of mass-casualty perpetrators. In the authors' assessment, these traditions function less as a belief system adopted wholesale than as archives of transgression, elitism, occultism, and anti-humanism on which actors draw selectively. Instead, ideology acts more as a justification for violence and other criminal activity that is primarily driven by clout-seeking^d and individual grievances.²³ Taken together, these anomic and nihilistic orientations result in a bricolage of influences and ecosystems that collapses traditional moral and epistemic boundaries in order to justify violence as an end in itself.

NVE did not emerge in isolation; rather, it formed out of a transnational virtual network known as the edgesphere. The edgesphere²⁴ is composed of an ecosystem of online subcultures, fandoms, and digital communities that normalize, celebrate, and commodify violence, trauma, and sadism. Between 2018 and 2020, the edgesphere emerged on the fringes of the most extreme communities of chronically online youth.²⁵ The term edgesphere captures a broader ecosystem rather than any single group or platform, and is characterized by its fluid boundaries, the rapid formation and dissolution of constituent communities, and the progressive normalization of transgressive and harmful behavior among network participants. These milieus frequently overlap with designated violent extremist and terrorist networks, functioning both as radicalization pathways into NVE networks (like The Com) and as operational environments that drive victimization.^e

Status and belonging are conferred through the ability of individuals to shock, transgress, and escalate harm. This is most often observed through the curation of grotesque, violent, or otherwise transgressive visual content and videos with a recognizable style. Visual aesthetics are a foundational aspect of NVE communities, serving as a primary medium of identity and belonging. In NVE spaces, identity is performed through engaging in and sharing violent acts, thereby portraying a 'transgressive'

and 'deviant' character to peers. This results in the blurring of the boundaries between play, spectacle, and extremism in these online spaces. Representing oneself as a violent extremist actor and engaging with known terrorist/extremist ideologies (such as militant accelerationism) and content are not signs of ideological beliefs, but due to their symbolic function of asserting power and eliciting fear. In other words, while extremist ideologies are present in NVE networks, they are typically not the primary mobilizing factor for violence and other criminal behaviors.^f

As a hybridized threat, NVE manifests as conduct that includes sub-criminal, criminal, and national security threats.^g Critically, this is a victim-driven space, not a doctrinally driven one: what organizes activity is who is targeted and how harm is produced and displayed, rather than any shared ideological doctrine. As discussed above, participation is shaped less by coherent ideological drivers than by aesthetics, fandoms, subcultures, and a pervasive sense of anomie and misanthropy. Rather than confronting nihilism's philosophical challenge as a question of how one may create their own values in the absence of a shared sense of meaning, NVE collapses it into a justification for cruelty, domination, destruction, with the primary goal of gaining social currency in online networks. NVEs systematically targeted vulnerable individuals by grooming, extorting, coercing, and otherwise compelling them through force, or the threat of force, to engage demands that include, but are not limited to: online and in-person sexual acts, sextortion, sexual exploitation of siblings, self-harm, suicide,²⁶ harm to animals, threats of physical violence, murder, and mass casualty attacks. Individuals active in NVE networks must then capture and disseminate digital media as evidence of these acts to maintain access to these spaces, spread fear and chaos among their targets, gain notoriety in the network, and inspire others to engage in their own acts of violence and criminality.

The Com Network and 764

What is The Com Network?

Within the edgesphere is the transnational virtual network called "The Community," or The Com Network²⁷ for short. The Com Network functions as a central operational environment for a number of groups including but not limited to 764, No Lives Matter, and Maniac Murder Cult.²⁸ An important distinction is that The Com Network and its constituent groups are not interchangeable

d 'Clout,' notoriety, or popularity is the primary currency of The Com Network. Status is earned through the severity, visibility, and impact of actions. The more extreme the action, or the ability to extort others into taking action, the greater the attention and reputation an individual accrues within the network. The killing of another person confers the highest status. Manipulating a victim into suicide, producing viral footage of a member attacking strangers, and commissioning large-scale cybercrimes are similarly high-value acts within this social economy of attention.

e There are eight principal ecosystemic pathways that lead into the edgesphere: terrorist and violent extremist milieus, the true crime community, extreme trolling communities, cybercriminal ecosystems and groups, gore network and platforms, animal abuse milieus, sadistic online exploitation, and self-directed violence ecosystems. These ecosystems are not mutually exclusive; individuals frequently participate across multiple feeder communities simultaneously, and their cumulative exposure across these spaces accelerates radicalization trajectories and complicates threat assessment, prevention, and intervention efforts.

f Though not the main drivers, these conditions do not emerge in an ideological vacuum; rather they intersect and draw influence from fragments of pre-existing extremist traditions, most notably neo-Nazi accelerationist, esoteric and occultic network like the Order of Nine Angles, the Terrogram Collective, maniac culture, Saints Culture, and the celebration of perpetrators of mass casualty attacks. These racially and ethnically motivated violent extremist movements provide an important symbolic and cultural repertoire for some of the early groups that informs today's NVE ecosystem. However, in the authors' assessment, it does not necessarily act as a coherent belief system adopted wholesale, but as archives of transgression, elitism, occultism, violence, and anti-humanism.

g This is evident in networks linked to or emulating 764, No Lives Matter (NLM), and M.K.Y./M.M.C., where references to National Socialism, accelerationism, O9A, and 'collapse-oriented' thinking can appear alongside trolling, irony, and aesthetic performance. The result is not a coherent ideological project, but a flattened remix of extremist traditions in which violence is detached from strategic ends and recast as an end in itself. In this configuration, extremist elements function less as commitments than as symbolic resources used to generate shock, status, and belonging.

terms;²⁹ they are distinct entities^h with their own threat vectors, tactics, leadership structures, membership requirements,ⁱ and documented harms.^j Groups such as 764, No Lives Matter, and Maniac Murder Cult exemplify the network's most visible and dangerous elements, blending criminality with terrorist and extremist violence and fostering a competitive environment that escalates harm and undermines public safety. Using these terms interchangeably risks mischaracterizing the scope and nature of the NVE threat. Members in The Com Network³⁰ may simultaneously belong to multiple groups, and individual actors may operate or lead several groups concurrently.

The Com Network is organized around three primary pillars of criminal activity: cybercrime,^k sadistic online extortion,^l and offline violence.^m There is significant fluidity between these pillars, and individuals often participate in multiple simultaneously, wherein criminal services are regularly exchanged across pillars in furtherance of shared objectives.ⁿ The Com Network thrives on a culture of 'clout chasing,' where notoriety and influence are earned through increasingly extreme acts. Unlike traditional extremist organizations, participation is driven less by ideology and more by the pursuit of recognition, status, and belonging through

transgression.^o

What is 764?

764^p is an online group founded in 2020 by then 15-year-old Texan Bradley Cadenhead (also known as "Brad764") who named the group after his zip code. The group emerged from a previous group called CVLT³¹ (pronounced 'cult') and Gregg's Cult.³² 764 exists as a community within The Com Network, whose leaders and influencers seek to create agents of chaos who will mobilize adherents to carry out criminal, violent extremist, and terroristic acts on behalf of the group in order to increase the group's status within the milieu. Through the data they have unearthed in the open source, the authors assess that the 764 Network is comprised of a range of public and private online groups/chats that primarily target vulnerable youth (aged on average between 8 and 17 years).^q 764 also recruits members and victims from games with a primarily minor user base such as Roblox and Minecraft,³³ which are popular among 8- to 13-year-olds. They also focus on individuals from the 2SLGBTQIA+ community, individuals struggling with mental health issues (e.g., suicidal ideations or depression), disordered eating and self-harm communities,^r as well as gore³⁴ and extreme violence communities.^s Coercive control is a key feature of the

h The Com Network has both established legacy groups (referred to colloquially within the network as "oldgen" or "OG," active prior to 2021), mid-period groups ("midgen," 2022-2023), and newer entrants ("newgen," 2024 onward).

i Access to a group in The Com Network is predicated on committing a certain amount of criminal or violent extremist activity. For example, a prospective member may be required to complete five to six acts of vandalism, two to three acts of sadistic online extortion, one or two acts of animal crushing, or only a single stabbing or shooting. This tiered structure is not incidental; it functions as a deliberate pipeline, normalizing criminal participation at accessible entry points before escalating the commitment required for higher-status membership.

j Members document and disseminate their criminal acts as a form of cultural currency. Where acts target a specific individual, the resulting material is archived in a "LoreBook," a dedicated repository of personally identifiable information, extorted content, and documentation of acts carried out against the victim, published online for the purpose of ongoing harassment and blackmail.

k Cyber Com is the pillar known for cyber-criminal activities including SIM swapping, ransomware, swatting, and social engineering data theft. Notable incidents linked to Cyber Com include the Snowflake-related data breaches and the Scattered Spider intrusion network. Brian Krebs, "The Dark Nexus Between Harm Groups and 'The Com,'" Krebs on Security, September 13, 2024.

l Sextortion Com is the pillar within which members target vulnerable minors through grooming, sextortion, and coercion into producing child sexual abuse material (CSAM) and self-harm content. Victims' personal and sexually explicit information is compiled into digital archives known as "LoreBooks," used for blackmail, re-traumatization, and the accumulation of social standing within the network.

m Offline Com focuses on real-world criminal activity ranging from vandalism, tire slashings, and brickings, through to arson, random stabbings, terrorism, and bioterrorism.

n The fluidity between these pillars means that a member primarily active in Cyber Com may offer swatting or doxing services to a Sextortion Com actor, facilitating coercion of a minor. Similarly, national security threats and online child sexual exploitation regularly co-occur within the same digital spaces and among the same individuals. The harms of The Com Network are primarily online in origin but reliably produce offline consequences, including self-harm, suicide, child sexual exploitation, and real-world violence.

o Members, particularly younger ones, escalate their behavior not because they hold genuine ideological convictions, but because they seek online validation and recognition. There is clear competition among youth to outperform each other, and the perception of risk, including law enforcement intervention, is often treated as a badge of honor rather than a deterrent. To gain access to a named group's private servers or to be formally recruited, an individual must prove themselves by creating "content." In practice, this means committing and recording a crime. This requirement functions simultaneously as an initiation mechanism, a means of generating blackmail material that can be used to control the new recruit, and a way to build the notoriety and brand of a particular group.

p 764 is a network of individuals who seek to normalize/weaponize criminal activities such as animal torture, zoosadism, incest, self-harm, sextortion, and violent extremism as coercion tactics.

q 764 and adjacent Com Network groups and/or their threat actors are typically older teenagers and young adults, often only a few years older than their victims. Older individuals with interest in the network are not often accepted. However, some notable exceptions have been identified, with feared and respected members aging into their 20s and, in one case a middle-aged threat actor (Richard "Rabid" Densmore) acting within the network. This age dynamic presents new challenges to existing awareness models of child protection, in which children may be encouraged to view unknown adults, but not other children, as potential predators. This also contrasts popular views of traditional terrorist and violent extremist group dynamics, in which young members are often delegated to outreach or recruitment, but rarely lead large violent extremist groups themselves.

r 764 recruiters seek to exploit personal vulnerabilities of members and recruits by targeting individuals with existing grievances and/or vulnerabilities, whether rooted in mental health struggles, personal failures, or societal rejection. The pseudo-philosophical justifications of their nihilistic and misanthropic worldview paints violence as a transformative act, offering participants an escape from their perceived insignificance, as well as personal or social suffering.

s 764 threat actors manipulate victims into video recording or livestreaming acts of self-harm, real-world violent crimes, and child sexual exploitation. These streams and recorded videos are shared with either the abuser or a group of abusers who will watch the 'shows.' The threat actors then often share this content in online group forums or in digital archives they call "LoreBooks" to further traumatize the victims. Abusers control their victims through intimidation, including threats of violence, doxing, swatting, animal mutilation, extortion, and forced suicide. Victims are also shared between members as a form of 'punishment' for non-compliance.

network, where victims can also be controlled through social engineering, blackmail, and/or by crafting a false sense of belonging and acceptance.¹ Threat actors are often brought into the 764 ecosystem by being invited to join a private chat or forum with like-minded individuals (a blend of other abusers and victims being targeted and exploited).

The worldview of 764 incorporates elements of performance, as the group puts an emphasis on members and potential recruits to record attacks and share them as propaganda. As argued elsewhere, “performance is the cornerstone of the NVE milieu, where actions hold little value without an audience. Perpetrators stage their violence as performative acts meant for peer recognition.”^u Notoriety is achieved through violence and “spectacle rather than ideological argumentation.”³⁵ Joe Ondrak and Laura Vitelli developed the framework of participatory mimetic violent extremism to explain the performative and participatory nature of NVE. As they define it, “Participatory Memetic Violent Extremism (PMVE) is violence enacted as a symbolic statement of affiliation with or participation in groups that valorize violent or transgressive action, either as an end in itself or for its perceived social and cultural significance, in lieu of any clear strategic, political, or ideological goal.”^v Interestingly, this insight also aligns with a broader trend in other extremist movements (such as the Islamic State or the right-wing extremist groups) that weaponize media to show allegiance or to further ideological goals.

For 764 and other NVE groups, the recording and sharing of the action also tests an individual’s willingness and capacity to commit transgressive acts for the network. This content is not only meant to terrorize viewers but to create a shared mythology that binds participants together. It is an act called “clout chasing,” where they seek to gain notoriety through the acts they are willing to commit and share with each other.³⁶ Clout chasing has been an impactful motivator for members to commit violent acts for the group.³⁷ Each act of violence becomes part of a global collective narrative,

glorifying the perpetrator as a symbol of rebellion against societal norms; however, many 764 participants, particularly younger followers, appear to escalate their behavior not primarily because they hold settled ideological convictions, but because they seek online validation and recognition.^w As part of this clout chasing, there is clear competition among youth to outperform each other, and the perception of risk, including law enforcement intervention, is often treated as a badge of honor rather than a deterrent.^x To gain access to a named group’s private servers or to be formally recruited, an individual must prove themselves by creating ‘content,’ which in practice means committing and recording criminal activities. This requirement functions simultaneously as an initiation mechanism, as a means of generating blackmail material that can be used by members to control new recruits, alongside a mechanism to build notoriety and the brand of a particular group.^y

The hybridized influences of 764 present risks that are not necessarily present in the movements that inspire it. 764 borrows its aesthetics and tactics from established militant accelerationist and neo-Nazi occultist movements, including Siege culture, Atomwaffen Division, the Terrorgram Collective, the Order of Nine Angles, and Temple of Blood. Unlike those movements, however, it imposes none of their membership criteria: It neither restricts itself to a single racial identity, as neo-Nazi and accelerationist groups do, nor requires a defined religious or esoteric adherence, as groups such as the Islamic State do. This openness makes 764 appealing and accessible to a far wider demographic of disaffected youth.

Unlike most other violent extremist groups, 764 hardly ever discourages violence. For example, a violent right-wing extremist group would advocate violence against non-white peoples and only condone the targeting of white people under certain circumstances. From the perspective of 764, all violence is good, regardless of the background of the victims or perpetrators.³⁸ This makes 764 a clear and present danger to any young person targeted by threat actors in the network, including their family, friends, pets, peers, educators, and institutions seeking to combat this emerging threat.

Com Network Arrest Dataset

From February 1, 2020, to May 20, 2026, the authors have identified

t They will often create a fake relationship (an ‘e-romance’) to attract those feeling isolated, lost, or grappling with personal issues, and looking for attention and validation. In these instances, they gain victims’ personal information, sexually explicit images, and affection through gifts (e.g., Amazon deliveries, e-transfers, video game currency, or cryptocurrency transactions).

u “Within NVE milieus, sadism, gore, and aesthetics become forms of entertainment and drivers of humor and irony, while aesthetics borrowed from extremist or popular culture provide legitimacy through recognizability. Recognition and validation within these deviant peer groups establish hierarchy and influence. Thus, performance in NVE is not simply expressive but constitutive: It defines identity, sustains membership, and drives escalation.” Marc-André Argentino, “Beyond the Headlines: Arrest Data and Drivers of Nihilistic Violent Extremism in the Com Network,” *From the Depths*, September 18, 2025.

v “PMVE is a form of extremism that places an emphasis on violence as an end in itself, rather than as a means to further a political or ideological agenda. To PMVE communities, violent attacks are viewed as a symbolic rite that adds to a collective mythos based solely on socially transgressive action. Communities involved in PMVE often deploy a diffuse (and sometimes self-contradictory) combination of ideological and online culture symbols. These are used as references to signal subcultural participation rather than ideological affiliation. The use of in-group signaling combined with the symbolic nature of an attack itself means that actors without prior affiliation with PMVE communities can still carry out attacks in dialogue with these groups that can then be referenced in the future by others.” Joe Ondrak and Laura Vitelli, “Participatory Memetic Violence: Legend, Ostension, and Ideologically Diffuse Violence,” *Global Network on Extremism and Technology (GNET)*, December 18, 2025.

w NVEs prioritize scalability and privilege ease of replication over complex planning logistics. Rather than requiring prolonged ideological indoctrination (such as in religious or ideologically motivated violent extremists cells who may study doctrine or plan operations for months), NVE actors furnish ‘operation kits’ including instructional guides on: low-cost, high-impact attacks, including how to plan a knife attacks; how to plan a vehicle ramming, swatting and doxing, vehicular ramming attack; how to sadistically extort victims, and swatting and doxing guides. *Likes voor Leed: 764- en COM-netwerken, Misanthropisch/ Nihilistisch Gewelddadig Extremisme* (Apeldoorn, Netherlands: Nuance door Training & Advies, November 2025).

x The guiding strategic logic is to overwhelm systems through the sheer volume of attacks: a proliferation of low-sophistication, highly chaotic events, such as school shootings, viral animal-cruelty clips, and swatting campaigns that collectively strain law enforcement and social resilience, so that authorities expend resources faster than perpetrators expend effort.

y Nihilistic violent extremists weaponize the architecture of social media to locate highly suggestible users (typically adolescents seeking belonging, thrill, or meaning) and then subject them to escalating norm violations. This cycle creates a renewable pool of actors operating in influencer and groomer roles who weaponize the architecture of social media to locate highly suggestible users, producing a renewable pool of directed followers willing to conduct lone-actor violence under remote instruction.

295 arrests linked to The Com Network in 33 different countries.

Table 1: Countries with Identified Com Network Arrests, 2020-2026 (n = 33) (Source: Based on publicly available information, government and law enforcement press releases, and court records reviewed by the authors)

Australia	Austria	Belgium
Brazil	British Virgin Islands	Canada
Chile	Denmark	Egypt
Finland	France	Georgia
Germany	Greece	Iraq
Ireland	Italy	Latvia
Morocco	Netherlands	New Zealand
Norway	Peru	Portugal
Romania	Russia	Serbia
Singapore	Spain	Sweden
Turkey	United Kingdom	United States

The dataset represents a limited and incomplete picture about the true scale of the threat. Court records about Com Network arrests are often sealed and not made public due to the offenders being minors, the inclusions of child sexual exploitation material, the reality that several countries do not make publicly available court records, as well as the fact that not all countries use similar language to describe the threat or identify arrests or crimes as linked to The Com Network or nihilistic violent extremism. It is very likely that the scale of the threat, the breadth of global arrests, and the number of victims are grossly underrepresented here.

Based on this dataset, these 295 Com Network members have victimized a total of 5,375 individuals and entities. This includes at least 22 fatalities, 1,747 victims of sadistic online extortion,^z 1,754 victims of swatting,^{aa} 143 animals subjected to crushing, 1,633 victims of cybercrime, and 76 properties damaged. Of the 257 perpetrators whose gender was recorded, 94.9% (244) were identified as male, whereas 5.1% (13) were identified as female—meaning there is a 19:1 male-to-female ratio among cases where gender is known. The data also shows that for the 229 individuals out of 295 for whom their age is known, the median age is 19 years old, while the mean is 20.17. Importantly, this age data reflects the

age of the offender at arrest, however the authors have observed that the majority of these individuals were active within The Com Network for years prior to their arrest. This dynamic, and lack of visibility into arrests and court proceedings involving minors, likely means that the age picture offered here skews somewhat older. Year-on-year, the median age of arrested offenders is as follows:^{ab}

2020: 20
2021: 21.5
2022: 22
2023: 18
2024: 20
2025: 19
2026:^{ac} 19

In calculating the age of victims, the authors do not account for the age of victims of cybercrime, victims of animal crushing, victims of swatting, or properties damaged. Further, due to the majority of victims being minors and/or their demographic details not being included or available in public sources, the authors' dataset only accounts for the age of 251 victims. The overall mean age for victims of The Com Network is 14.33, while the median is 13 years old. The median age of known victims' year-on-year is as follows:

2020: n/a^{ad}
2021: 11.5
2022: 16
2023: 14
2024: 12
2025: 14
2026: 13

A methodological and conceptual caveat applies throughout this dataset: It records individuals by their legal status at the point of arrest and therefore counts them as offenders, which cannot capture the extent to which the same individuals may also have been victims. Given the dynamics described above, in which recruitment frequently proceeds through grooming, coercion, blackmail, and the exploitation of pre-existing vulnerability, it is likely that a portion of those recorded here as offenders were themselves subjected to coercion, exploitation, or abuse within these same networks, whether prior to or concurrent with their own offending. This is consistent with the authors' observation that many offenders were minors when they first entered these spaces, and with the victim-perpetrator dynamics evident in several of the case studies that follow. The authors do not attempt to disentangle these overlapping roles here, and their offender counts should not be read as implying that the individuals concerned were never victims. Rather, the authors signpost that, in a meaningful number of cases, offender and victim are not mutually exclusive categories and that this overlap is itself a defining feature of the NVE ecosystem.

A subset of the cases in this dataset have been prosecuted not through general criminal statutes alone, but under dedicated

^z "Sadistic online exploitation (SOE) reflects a significant shift in how risk and harm emerge for young people in digital spaces. Unlike other forms of exploitation, SOE manifests as primarily youth-driven, networked environments that are socially structured around harm itself, where demonstrated tolerance of, and participation in, harm function as mechanisms for group belonging and status. Within them, adolescents are not only the primary victims but also the primary active participants in harming others, achieving status through escalation. In these environments, harm spreads quickly, intensifies rapidly, and becomes increasingly difficult for participants to disengage from." *Advancing Response to Sadistic Online Exploitation in Networked Youth Environments* (Los Angeles: Thorn, 2026).

^{aa} Swatting is the practice of calling emergency services, usually through anonymized VoIP (voice over internet protocol) phone applications, and reporting false crimes intended to provoke an armed response by police. In many cases, the perpetrator will pretend to be the intended victim and tell authorities they are armed and intend to kill themselves or others.

^{ab} The age of the offenders is based on their age at their moment of arrest; however, based on the authors' review of the data and study of their digital footprints, the majority of these individuals were active within The Com Network for years prior to their arrest. Though this research is incomplete and ongoing, it is very likely that when they began offending, the majority of these individuals were themselves minors.

^{ac} Data from 2026 is based on arrests up to April 30.

^{ad} There is no publicly available demographic information about the victims of The Com Network in 2020 in the authors' dataset.

counterterrorism legislation, or charged with conduct that maps onto how most scholars and practitioners would define an act of terrorism. In the United States, Baron Cain Martin was charged with conspiring to provide material support to terrorists alongside child-exploitation and foreign-murder-conspiracy counts.³⁹ In Alabama, Carson Albert Butler was indicted on a state terrorism count in connection with a plot against a high school,⁴⁰ and in Florida, Jose Pagan Jr. was charged with terrorism and child-pornography offenses.⁴¹ In Canada, Jeffrey Roussel⁴² and Nevin Thunder Young⁴³ were each charged with participating in, facilitating, and committing an offense for a terrorist group, while an Edmonton-area youth was placed under a terrorism peace bond before being charged with further terrorism offenses.⁴⁴ In the United Kingdom, Cameron Finnigan (one of the cases explored in more detail below) pleaded guilty to offenses including possession of a document likely to be useful to a person committing or preparing an act of terrorism. In the Netherlands, the alleged founder of No Lives Matter is being prosecuted for terrorism,⁴⁵ with the Public Prosecution Service treating the group as a terrorist organization. And in Australia, a 16-year-old was charged under the Commonwealth Criminal Code with collecting and making documents likely to facilitate a terrorist act and with possessing violent extremist material.⁴⁶

These cases indicate that, although the conduct the authors describe is frequently prosecuted through child-exploitation, cybercrime, and ordinary violent-crime statutes, a growing number of NVE-linked actors are now being charged under terrorism law itself, a pattern consistent with the recent designation of 764 and affiliated groups as terrorist entities.

Two important caveats apply, however. First, the status of these matters varies: Some are allegations or indictments not yet tested at trial; others have resulted in convictions or guilty pleas, and preventive measures such as peace bonds are distinct from criminal charges. In addition, several individuals were charged in connection with affiliated Com Network groups, such as Maniac Murder Cult or No Lives Matter, rather than 764 specifically.

In a review of the 295 cases in the dataset, the authors have found that just because someone is arrested for crimes committed as part of The Com Network (or even being a member of 764) does not necessarily mean they are nihilistic violent extremists. This is, in part, a question of role: Cybercrime-focused or peripheral participants may sit within The Com without exhibiting the behavioral orientation the authors describe, whereas leaders, groomers, and directed perpetrators more often do. The data suggests that participation in The Com Network, or association with groups such as 764, is not in itself sufficient to classify an individual as a nihilistic violent extremist. Rather, cases vary in the extent to which they exhibit the elements set out above. In practice, this means asking of a given individual: Are they actively embedded in the edgesphere and its status economy, rather than transacting at its periphery; do they produce or circulate harm in order to earn standing ('clout'); is their conduct shaped by anomie, nihilism, and misanthropy rather than instrumental gain; do their harms hybridize across categories, including sadistic online exploitation; does ideology operate as justification and aesthetic rather than as the primary driver of their violence; and is their offending directed at no coherent strategic end state? Further, the case studies featured below have been included to illustrate the applications of the framework across a geographically diverse set of offenders and

offense types. Taken together, the cases suggest that the defining characteristics of NVE manifest across actors, roles, and contexts within the broader Com ecosystem.

764 Case Studies

Bradley Cadenhead (United States)

At the time of his offending, Bradley Chance Cadenhead was a minor in Texas with a documented history of violent ideation. In September 2018, at age 13, he was charged in juvenile court with making a terroristic threat^{ae} after stating he wanted to shoot up his junior high school and “carve pentagrams into the table and kill everyone.”⁴⁷ Teachers documented his fixation on firearms, silencers, and improvised explosives, with one expressing the concern that he was “building his courage up to do such things.”⁴⁸ In August 2019, Cadenhead threatened to kill his father and was sent to a psychiatric hospital followed by juvenile detention. A second hospitalization in early 2022 was triggered by a statement that he wanted to “kill them all.”⁴⁹ According to Cadenhead, he began consuming gore and torture imagery at age 10 “for the shock value,” began self-cutting at age 11, and met a co-conspirator through Minecraft with whom he launched the Discord server he named 764, accumulating “hundreds of torture videos” and between 200 and 400 followers.⁵⁰

As founder, moderator, and content curator of the Discord server, Cadenhead uploaded child sexual abuse material (CSAM) to attract and retain followers, while other users contributed further material into the same environment. He admitted that the sextortion of minors and other targets was “quite common,” and conducted both for money and, in his own words, for “power over the individuals.”⁵¹ Forensic examination of his devices recovered prepubescent CSAM, videos of adolescent victims, audio files referencing grooming, and operational accounts under multiple aliases.⁵²

The defining feature of Cadenhead’s offending was the coercive, ritualized control he exerted over victims. Pre-sentence findings establish that he directed individuals “to actually carve his initials and other references to him into their bodies as a form of homage,” with forensic imagery depicting victims cutting “Brad is a pedo” and “764” into their skin.⁵³ He described the group to investigators as “actually a self-described Cult,” with members idolizing him as its leader.⁵⁴ The District Attorney’s filing characterized the broader seized material as depicting infant sexual assault, child mutilation, torture and death, and human self-mutilation, and formally assessed the defendant as dangerous.⁵⁵ On May 16, 2023, Cadenhead aged 18 pleaded guilty to nine second-degree felony counts of Possession with Intent to Promote Child Pornography and received an aggregate sentence of up to 80 years.⁵⁶ Although Cadenhead was convicted on child-exploitation rather than terrorism or violent-extremism grounds, the network and ritualized online culture he founded have become the operational template for a successor generation of 764-aligned actors whose offending is now escalating from coercive online harm into terrorist and violent-extremist acts.

ae Terroristic threat is a discrete state criminal offense covering threats of violence made to place others in fear or to disrupt activity; it is distinct from, and should not be read as equivalent to, a federal terrorism charge or a formal domestic terrorism designation.

Ronndog “HokaMachine” Keefe (New Zealand)

At the time of his offending, Ronndog “HokaMachine” Keefe was a young New Zealander in his late teens to early 20s with no prior criminal history. His pathway into The Com Network appears to have begun with exposure to violent extremist material online, including footage from the Christchurch mosque attacks. In evidence before the Court, Keefe described encountering and sharing edited segments of this material within online gaming environments, including *Call of Duty*-related Discord servers, where such content was circulated as spectacle, detached from its real-world consequences.⁵⁷ Following exposure in these spaces, Keefe’s engagement deepened. Over a period of approximately two years (2022-2024), Keefe became immersed in online networks operating across platforms such as Discord, Instagram, and MEGA, using more than 20 distinct accounts and identities.⁵⁸ These environments exposed him to communities in which exploitation, transgression, and notoriety were both normalized and rewarded.

Keefe’s offending involved the large-scale distribution of child sexual exploitation material, including the creation and distribution of publicly accessible repositories containing thousands of files.⁵⁹ He also directly engaged in the grooming of minors. In one instance, Keefe communicated with a 13-year-old girl via social media platforms, including Snapchat, using deception, sexualized communication,⁶⁰ and incentives such as gaming tokens to solicit explicit material.⁶¹ Keefe also communicated with a young woman in the United States over an extended period who alerted authorities after Keefe repeatedly described his desire to carry out a mass-casualty attack to gain notoriety.⁶²

Keefe’s offending extended beyond child exploitation into violent extremist intent. Keefe possessed Christchurch attack content and expressed a desire to emulate high-profile acts of violence for recognition. When police executed a search warrant at Keefe’s Hastings home located in New Zealand’s Hawkes Bay, they located multiple bladed weapons in his bedroom, including a machete and bayonet.⁶³ Open-source reporting further indicates that he had written about being radicalized and framed his intended violence in religious terms, describing himself as a “soldier of Christ” and outlining plans to carry out a stabbing attack targeting members of the public.⁶⁴

Keefe later claimed that aspects of his offending were driven by coercion from members of the 764 network, describing experiences of online pressure and doxxing. However, this explanation was rejected by the court.⁶⁵ His communications instead reflected a desire to gain recognition within these environments, including emulating acts of mass violence that would attract public attention. Keefe pleaded guilty to 13 charges, including knowingly distributing child sexual exploitation material, exposing a young person to indecent material, and threats to kill. In 2025, Keefe was sentenced to five years and four months in prison and placed on the child sex offender register for eight years.

Taken together, Keefe’s trajectory illustrates how exposure to violent content, immersion in harmful online subcultures, and participation in networked environments of exploitation can converge into pathways of harm that blur traditional distinctions between criminality and extremism. His case demonstrates how NVE-linked ecosystems produce actors for whom violence, coercion, and notoriety are mutually reinforcing components of a single system of harm.

Cameron “ACID” Finnigan (United Kingdom)

Cameron “ACID” Finnigan was 18 years old and living with his adoptive parents at the time of his offending. Between late 2023 and March 2024, Finnigan became an active participant in 764, operating primarily through Telegram.⁶⁶ His offending involved the production and dissemination of violent propaganda with 764 imagery, including content depicting murder, mutilation, rape, self-harm, and extreme violence.⁶⁷ Like Keefe in New Zealand, Finnigan’s pathway into these environments appears to have been shaped by prolonged immersion in online subcultures where violent and exploitative content circulated alongside gaming, meme culture, and shock-oriented social interaction. In 764 channels, Finnigan boasted about the quality of his content creation, edited videos and graphics using the application called CapCut, and encouraged other 764 members to commit serious acts of violence and vandalism. During a period referred to as “Terror Week” within the network, he encouraged associates to target homeless people and discussed acts of violence in explicitly racialized and accelerationist terms.⁶⁸

Finnigan also self-identified as a “high-level extorter.” As such, he encouraged a vulnerable young woman to livestream her suicide in a 764-affiliated Telegram chat after she had sent him footage of her self-harming. Finnigan also shared this self-harm footage with the 764 Inferno chat group.⁶⁹ This dynamic mirrors patterns observed in the Keefe case, where vulnerable young people were manipulated and drawn into escalating cycles of coercion, humiliation, and violence within online networked environments. Finnigan also possessed the “NLM x MKY Kill Guide,” a document containing instructions for how to commit mass-casualty truck, knife, and firearm attacks.⁷⁰ Police also recovered indecent images of children, extremist propaganda, and evidence linking Finnigan to acts of vandalism and threatening graffiti.⁷¹

The sentencing remarks describe Finnigan as a socially isolated and vulnerable young person with a history of developmental trauma, bullying, mental health difficulties, and self-harm.⁷² Mirroring Keefe, psychiatric evidence described by the judge suggested that his involvement with 764 was driven by a desire for belonging, status, and social connection, alongside a fascination with violence and sadistic behavior.⁷³ The court accepted that 764 provided Finnigan with a sense of identity and purpose, but rejected claims that he had been unwillingly drawn into the network, concluding instead that he had occupied a prominent and active role within it.⁷⁴

Slain, Njae, and Chai (Sweden)

‘Slain764,’ ‘Njae764,’ and ‘Chai764’ were all part of a Swedish cell of The Com Network group No Lives Matter (NLM). These cases illustrate how Com Network groups like 764 and NLM within the NVE ecosystem blur distinctions between online and offline offending, exploitation/grooming and extremism, as well as direct and mediated forms of violence. As with the previous cases, the Swedish cases involve socially isolated youth immersed in online subcultures characterized by neo-Nazi occultist and accelerationist symbols, coercion, performative violence, and status-seeking behavior within networked chat environments.

The first case concerns a then 14-year-old boy associated with the alias ‘Slain764’ who on September 13, 2024, carried out an apparently unprovoked stabbing attack against an elderly man in Hässelby, Stockholm.⁷⁵ Swedish court records and media reporting state the attack was livestreamed and shared in 764 and No Lives

Matter-affiliated chat groups.⁷⁶ According to court records, the suspect identified the user ‘Chai764’ as the individual who coerced and blackmailed him into carrying out the attack, recalling that Chai reassured him that, as a minor, he had effectively no serious consequences to fear and should simply go ahead.^{af} Slain764 also described the broader group, which he had been embedded in for two to three years, as one of his only experiences of belonging, into which he had ultimately been manipulated to commit serious violence against another person.⁷⁷ In April 2025, Solna District Court found in a *bevistalan*^{ag} proceeding that the boy had committed attempted murder.⁷⁸ The case reflects several recurring dynamics observed across NVE spaces: youth participation, accelerationist and performative violence, and the transformation of violence into networked social capital through recording and dissemination. As with Finnigan’s propaganda production and Keefe’s notoriety-driven aspirations, the attack appears embedded within a broader culture of transgression, spectacle, and recognition-seeking rather than a clearly articulated political objective.

The second case also concerns a then 14-year-old boy who, on January 4, 2025, attacked a 55-year-old woman with a knife in the Trandared district of Borås, livestreaming the assault on Discord⁷⁹ to viewers in 764-affiliated chat spaces.⁸⁰ The victim, who was walking her dog, sustained life-threatening injuries but survived; the boy, who went by the username ‘Njae764,’ was arrested the same evening on the basis of tips received about the livestream.^{ah} Forensic examination of the offender’s devices recovered MKY-claimed murder videos from 2021, Order of Nine Angles and No Lives Matter imagery, and mass-murderer reference material.⁸¹ In subsequent police interrogation, as reported in the Swedish press, he stated that he had felt pressured into committing the attack by persons he had encountered online and recalled that livestream viewers had urged him in real time to follow through.⁸² In chat records reviewed by the authors, the stabbing was a substitute for a tire slashing that the group had deemed insufficient to grant Njae membership, instead demanding that he find a human target.⁸³ The perpetrator described his motivation as a desire to feel belonging within the group, which over a period of online immersion had

“What unifies these cases is not a shared ideology but a shared ecosystem, a shared status economy in which standing is earned by producing and circulating harm, a shared behavioral orientation in anomie, nihilism, and misanthropy, and a shared reliance on sadistic online exploitation and coercive control as the means through which that harm is enacted.”

progressively convinced him to act. In May 2025, Borås tingsrätt (Borås District Court) found in a *bevistalan* that he had committed the act but did not rule it attempted murder; in July 2025, the Hovrätten för Västra Sverige (The Court of Appeal for Western Sweden) upheld that finding on the prosecution’s appeal.⁸⁴

The third case concerns an 18-year-old man (alias ‘Chai764’), who according to Swedish prosecutors occupied a highly prominent position within 764 and No Lives Matter.⁸⁵ Active within the network from the age of 15, he was first convicted in 2024 in connection with the attempted online inducement of a 13-year-old boy to livestream his own suicide, and was identified by SVT’s investigative documentary series *Dödens chattrum* (2025) as the most serious Swedish 764 perpetrator before the courts.⁸⁶ In May 2026, prosecutors in Umeå filed a superseding indictment charging him with 77 offenses allegedly committed online between 2023 and 2025, including attempted murder, incitement to suicide, rape, aggravated child sexual exploitation, aggravated child sexual abuse, and aggravated cruelty to animals.⁸⁷ Court records document Chai’s coercion of a Swedish child victim via Discord, in which the victim was directed, under threat of being doxxed to their school, to cut themselves on camera.⁸⁸ Beyond his documented coercion of the ‘Slain764’ attacker, prosecutors allege ‘Chai764’ also coerced victims in Australia and Germany into severe self-harm and sexual abuse. Swedish prosecutors have framed the case as a potential “pilot case” for determining whether serious violent offenses can be committed remotely via online networks and successfully prosecuted.⁸⁹

The Swedish cases demonstrate the breadth of behaviors emerging within NVE-linked environments. Violence within these ecosystems is rarely overtly ideological; it is performative, socially reinforced, done for acceptance and a desire for friendships, and embedded within online networks centered on status acquisition, exploitation, and transgression. They further illustrate how these environments produce both acts of public, performative violence and diffuse forms of coercive, digitally mediated harm, in some instances within a single connected ecosystem, complicating traditional distinctions between criminality, violent extremism, child sexual exploitation and abuse, and online abuse more broadly.

af Chai is likely making reference to HVB (*hem för vård eller boende*), which is the Swedish juvenile residential care system – the placement minors go to in lieu of prison – since under-15s in Sweden cannot be criminally prosecuted in the ordinary sense. Chai’s message to the 14-year-old was effectively: ‘You’re a kid, the worst that can happen to you is a stint in a youth home, stop overthinking it, just go through with the attack.’ This is not the first case, but a consistent pattern within NVE milieus, whereby perpetrators or those coercing individuals into violence will regularly leverage the fact that those under the age of criminal responsibility in their countries will not be held accountable or held to lighter consequences for their violent crimes.

ag A *bevistalan* (loosely, an evidentiary trial) is a Swedish proceeding used to establish, on the criminal standard of proof, whether a person under the age of criminal responsibility (15 in Sweden) committed an act, without imposing a criminal penalty.

ah According to Telegram chat records reviewed by the authors, members of the group to which Njae belonged claimed to have reported him to law enforcement purely for amusement (“for the lolz”). That an offender was exposed to authorities by his own peers, and for entertainment rather than conscience, underscores how unstable the boundary between insider and target can be within these groups. This goes against what is traditionally understood about in-group dynamics where being part of the in-group in most terrorist and violent extremist groups provides protection, whereas in these groups, insiders can turn on one of their own at any given time.

Conclusion

Taken together, the cases of Cadenhead, Keefe, Finnigan, Slain, Njae, and Chai demonstrate that the proposed dimensions of NVE do not manifest uniformly across actors and that the role an individual occupies shapes how they present. Cadenhead, as a leader and content curator, anchored his offending in coercive sexual exploitation and cult-style charismatic authority, with violent-extremist imagery operating as ambient decor. Keefe, an aspirational follower seeking notoriety, and Finnigan, an influencer, propagandist, and self-described 'high-level extorter,' combined prolonged immersion in shock subcultures with aspirational and propaganda-producing engagement with accelerationist material. The Swedish cases span the role spectrum. At one end are directed followers: the minors known as Slain764 and Njae764, who were coerced through networked pressure into committing acts of in-person violence. At the other is Chai764, a senior coercive operator who industrialized the manipulation of vulnerable minors across multiple jurisdictions. What unifies these cases is not a shared ideology but a shared ecosystem, a shared status economy in which standing is earned by producing and circulating harm, a shared behavioral orientation in anomie, nihilism, and misanthropy, and a shared reliance on sadistic online exploitation and coercive control as the means through which that harm is enacted. The roles differ; the underlying logic of recognition through harm does not.

The most consistent finding across the case studies is that ideology in NVE spaces is fluid, performative, and primarily symbolic. Neo-Nazi imagery, occultist iconography, accelerationist slogans, and references to mass-casualty attackers function as currency through which status, transgression, and group membership are signaled, rather than as coherent political programs pursued through violence. This stands in marked contrast to the operating logic of militant accelerationism as developed in the lineage of James Mason, the Atomwaffen Division, the Base, and the Terrorgram Collective, where the production and consumption of ideological texts, the articulation of strategic end states, and the cultivation of doctrinal cadres remain central organizing principles. Militant accelerationism is structured around racialized in-groups and out-groups; NVE is not. The NVE ecosystem is racially and culturally diverse,^{ai} and actors within it routinely espouse neo-Nazi views and adopt Nazi aesthetics irrespective of their own non-white identities.

The collapse of NVE and militant accelerationism into a single analytical category, as has increasingly occurred in some research

and operational settings, risks committing three substantive errors, even where assessors are diligent. First, it increases the risk of mischaracterizing motivation, by treating ideological signaling as though it were ideological commitment. (Organizations whose mandate is tied to ideology can and do assess deeper drivers; the point is that collapsing the categories makes such errors more likely, not inevitable.) Secondly, it risks mistargeting intervention, prioritizing approaches to prevention, deterrence, and response that center on ideology and narrative, where there is instead a need for greater focus on, and investment in, approaches that prioritize youth safeguarding, online harm reduction, and victim-centered responses to coercive control. Thirdly, it risks obscuring victimization. Given the centrality of victim-perpetrator cycles in these milieus, in which many actors are first groomed, coerced, or exploited before going on to perpetrate harm themselves, NVE actors are frequently both perpetrators and products of the ecosystems through which they offend. The prevention field has begun to address such pathways through trauma-informed practice, building on findings that a substantial share of perpetrators were exposed to violence or victimization earlier in life. The gap is more pronounced in security and enforcement settings, where victim-perpetrator dynamics remain under-incorporated, and this is precisely an area where comparison and collaboration across NVE and accelerationist violent extremism could prove valuable.

Instead of conflating, or treating, these two phenomena into a single analytical category, the Participatory Memetic Violent Extremism (PMVE) framing developed by Ondrak and Vitelli is more helpful when it comes to NVE cases. One important reason is because those cases can then also be viewed in relation to the literature on youth subcultural deviance, transgression, and edgework. Read alongside trauma-informed practice, this lens also helps explain why transgression and edgework are so reinforcing: For many participants, staged violence and risk-taking meet needs created by victimization, anomie, an absent sense of personal safety, and a desire for control. Seen this way, the performative production of harm is not only a route to status but also a maladaptive response to vulnerability, which is why effective responses run through child protection and clinical support as much as through security. Reading NVE through these lenses recovers what terrorist designations obscure: that we are looking at a coercive online youth subculture in which the production and circulation of harm is both the mechanism of belonging and the medium of status, and within which the symbols of violent extremism are deployed because they are the most transgressive symbols available, not because their bearers seek the political worlds those symbols originally described. Taking this seriously has substantial implications for child protection on platforms such as Discord and Roblox, the training of educators and clinicians, and cross-jurisdictional cooperation on remotely coerced violence, which the authors argue, are the more urgent next frontiers for research. **CTC**

ai This dataset remains an active research instrument. Beyond the descriptive distributions reported here, the authors intend to expand it to further examine for the behavioral and developmental correlates of escalation; for platform-migration pathways that recur across cases, such as the progression from open gaming environments (for example, Roblox and Minecraft) into encrypted and ephemeral messaging channels; and for the relationship between offender age, charge severity, and sentencing outcomes across the 33 jurisdictions represented in the data.

Citations

- 1 Peter Smith, Cat Cadenhead, and Clara Broekaert, "True Crime Community: Understanding the Depths of Digital Fandom and Performative Violence," *CTC Sentinel* 19:2 (2026).
- 2 Mackenzie B. Hart, "'Less than a Speck of Dirt': Exploring the Manifestos of Nihilistic Violent Extremists," Behavioral Sciences of Terrorism and Political Aggression (online), March 6, 2026, pp. 1-20.
- 3 Phoebe Petrovic, "Madison and Nashville School Shooters Appear to Have Crossed Paths in Online Extremist Communities," ProPublica, January 24, 2025; "Nashville Shooter's Manifesto Reveals Inspiration Drawn from the Online Far-Right," Global Project Against Hate and Extremism, January 23, 2025.
- 4 "Wimauma Teen Tied to Neo-Nazi Satanic Group, Charged with Terrorism, Child Porn," Maryland Coordination and Analysis Center, February 5, 2026; Joe Espy and Joey Swanson, "Teen Linked to Neo-Nazi Satanic Hate Group Accused of Planning Mass Shooting at Wimauma Church: HCSO," Fox 13 News (Tampa Bay), February 4, 2026.
- 5 "Turkish Attacker Steeped in Neo-Nazism and Online Gaming Culture," Global Project Against Hate and Extremism, August 14, 2024; Graham Macklin, "Evaluating 'Transnationalism' as an Analytical Lens for Understanding REMVE Terrorism," *CTC Sentinel* 17:11 (2024).
- 6 Jacob Ware, "A Terrorism of Vengeance," Lawfare, December 16, 2025.
- 7 "Leaders of Transnational Terrorist Group Charged with Soliciting Hate Crimes, Soliciting the Murder of Federal Officials, and Conspiring to Provide Material Support to Terrorists," U.S. Department of Justice, September 9, 2024.
- 8 Alexander Meleagrou-Hitchens and Moustafa Ayad, *The Age of Incoherence? Understanding Mixed and Unclear Ideology Extremism* (Washington, D.C.: Program on Extremism, George Washington University, and National Counterterrorism Innovation, Technology, and Education Center, 2023); Stephane J. Baele, "Critical Reflexions on 'Composite,' 'Fused,' or 'Mixed, Unclear and Unstable' Extremist Ideologies (and Concepts)," VOX-Pol, October 15, 2025.
- 9 Max Taylor, Ethel Quayle, and John Horgan, "Radicalisation in Coercive Online Communities: A Research Note," *Perspectives on Terrorism* 20:1 (2026); Che Tibby, "Incoherent Violent Extremism in a New Zealand Cohort," Journal of Policing, Intelligence and Counter Terrorism (online), March 5, 2026.
- 10 Karl Roberts and Claudia Wallner, *Beyond Ideological Categories: Mixed Ideologies and What They Mean for Preventing and Countering Violent Extremism* (Brussels: Radicalisation Awareness Network, 2023).
- 11 Peter Smith, *Com/764: Transnational Abuse, Extortion, and Cybercrime Networks Targeting Youth* (Toronto: Canadian Anti-Hate Network, August 2025).
- 12 Marc-André Argentino, Barrett G., and M.B. Tyler, "764: The Intersection of Terrorism, Violent Extremism, and Child Sexual Exploitation," Global Network on Extremism and Technology (GNET), January 19, 2024.
- 13 "Statements of Cases to Designate Terrorist Entities, December 2025," New Zealand Police, December 2025; Daveed Gartenstein-Ross and Emelie Chace-Donahue, "The Order of Nine Angles: Cosmology, Practice & Movement," *Studies in Conflict and Terrorism* 48 (2025): pp. 1,214-1,234.
- 14 "Government of Canada Lists Four New Terrorist Entities," Public Safety Canada, December 10, 2025.
- 15 Bjorn Ihler, "What M/NVE Is – and What It Isn't," Revontulet, May 3, 2026.
- 16 Cécile Rousseau, Diana Miconi, Cindy Ngoy, and Ghayda Hassan, "Ideological and Nihilistic Violence in Adolescents Referred to a Specialized Clinic for Violent Extremism," *Canadian Journal of Criminology and Criminal Justice* 67:2 (2025): pp. 30-48; *Spotting the Signs: Recognizing and Responding to Subcultures of Nihilistic Violence* (London: Institute for Strategic Dialogue, 2025).
- 17 Leena Malkki, Henrik Ali-Hokka, and Saija Benjamin, *Violence-Focused Online Communities, RADIA Brief 1/2025* (Helsinki: RADIA, University of Helsinki, 2025).
- 18 Marc-André Argentino and Angus Lindsay, "Schrödinger's Terrorism: Is It or Is It Not in the Box?" From The Depths, January 30, 2026.
- 19 Tore Bjørgo, "Conceptualizing Diversity among Violent Extremists: A Typology and a Model for Explaining Change" in Milan Obaidi and Jonas Kunst eds., *The Cambridge Handbook of the Psychology of Violent Extremism* (Cambridge: Cambridge University Press, 2025), pp. 78-79; Petter Nesser, *Islamist Terrorism in Europe: A History* (New York: Oxford University Press, 2018).
- 20 Émile Durkheim, *Suicide: A study in sociology* (New York: Routledge, J. A. Spaulding & G. Simpson, Trans., 1951) (original work published in 1897).
- 21 Ellyn Maese and Zacc Ritter, "Youth, Loneliness and Political Violence in the U.S.," Gallup News, December 3, 2025.
- 22 Hart.
- 23 Richard Connor, "How Grievance Turns to Violence in a Mass Shooter's Mind," Deutsche Welle, April 21, 2026.
- 24 *How the Edgesphere Uses AI-Generated Visual Content to Glorify, Promote, and Humanize Violence* (New York: Graphika, 2026).
- 25 Felix Neumann, "The Development of Nihilistic Violence: Terrorism without a Goal?" Konrad-Adenauer-Stiftung, January 8, 2026.
- 26 Mike Levine, "'10 Minutes of Murder': Why One Family Is Speaking Out about the Online Extremist Network 764," ABC News, November 18, 2025.
- 27 "Project COMPASS," Europol, accessed May 28, 2026.
- 28 Marc-André Argentino, Barrett Gay, and Matt Bastin, "Nihilism and Terror: How M.K.Y. Is Redefining Terrorism, Recruitment, and Mass Violence," *CTC Sentinel* 17:8 (2024): pp. 22-29.
- 29 Beth Daviess, *764 and The Com: Misconceptions and Guidance, DVERT Center Quick Look* (Arlington, VA: CNA, 2026).
- 30 *HCSS Focus: Het Com-netwerk* (The Hague: The Hague Centre for Strategic Studies, 2026).
- 31 United States v. Rane, No. 2:25-cr-00040, Indictment (C.D. Cal.).
- 32 "Five Leaders of 'Greggy's Cult' Charged with Sexually Exploiting Children on the Internet," U.S. Department of Justice, December 2, 2025.
- 33 "764 Terrorist Network: Individual from Québec City Area Charged," Royal Canadian Mounted Police, April 22, 2026.
- 34 Ali Fisher and Arthur Bradley, *Gore and Violent Extremism: An Explorative Analysis of the Use of Gore Websites for Hosting and Sharing Extremist and Terrorist Content* (Dublin: VOX-Pol Network of Excellence, 2025).
- 35 Marc-André Argentino, "Beyond the Headlines: Arrest Data and Drivers of Nihilistic Violent Extremism in the Com Network," From The Depths, September 18, 2025.
- 36 Marc-André Argentino, "Chasing Clout: How Com Networks Turn Violence into Social Currency," From The Depths, October 25, 2024.
- 37 "Com-Groepen: Nihilistisch en Sadistisch Geweld in Anonieme Chatgroepen," Nederlands Jeugdinstituut, accessed May 28, 2026.
- 38 Hart.
- 39 "Arizona Leader of Violent Extremist Network '764' Charged with Running a Child Exploitation Enterprise, Supporting Terrorists, Producing and Distributing Child Pornography, and Other Crimes," U.S. Department of Justice, October 30, 2025.
- 40 "Athens teen indicted on terrorism, attempted murder charges in plot targeting high school," Maryland Coordination and Analysis Center, December 5, 2025.
- 41 "Wimauma teen tied to Neo-Nazi satanic group, charged with terrorism, child porn," Maryland Coordination and Analysis Center, February 5, 2026.
- 42 "764 terrorist network: individual from Québec City area charged," Royal Canadian Mounted Police, April 22, 2026.
- 43 "Winnipeg resident charged with terrorism-related offences," Manitoba RCMP, March 18, 2025.
- 44 "Alberta youth arrested for terrorism-related offence," Royal Canadian Mounted Police, May 29, 2025.
- 45 Haro Kraak, "[Justin B. allegedly incited young people to self-harm, murder, and extortion through the terrorist group No Lives Matter,]" deVolkskrant, October 28, 2025.
- 46 "NSW JCTT charges young person with terrorism offences," Australian Federal Police, March 25, 2026.
- 47 Appended Stephenville PD juvenile narratives (Case 18-00014452) in State of Texas v. Bradley Chance Cadenhead, Cause No. 22CRDC-00016, 266th Judicial District Court, Erath County, Texas, May 24, 2023.
- 48 Ibid.
- 49 Pre-Sentence Investigation State of Texas v. Bradley Chance Cadenhead.
- 50 Ibid.
- 51 Stephenville PD forensic supplement (23/06/2022) State of Texas v. Bradley Chance Cadenhead.
- 52 Pre-Sentence Investigation State of Texas v. Bradley Chance Cadenhead.
- 53 Ibid.
- 54 District Attorney's Statement of Fact cover page State of Texas v. Bradley Chance Cadenhead.
- 55 Judgment of Conviction State of Texas v. Bradley Chance Cadenhead.
- 56 Ibid.
- 57 Notes of Judge R J Earwaker on Sentencing CRI-2024-020-002908 [2025] NZDC 31614.
- 58 Ruling of Judge R J Earwaker [On Permanent Name Suppression] CRI-2024-

- 020-002908 [2026] NZDC 3634.
- 59 Notes of Judge R J Earwaker on Sentencing CRI-2024-020-002908 [2025] NZDC 31614.
- 60 Melissa S. de Roos, Elza Veldhuizen-Ochodničanová, and Laura Veldhuizen-Ochodničanová, "Of Lolitas and Jailbait: An Exploration of Incel Discourse Surrounding Sex with Minors," *Journal of Sex Research* (online), March 12, 2026.
- 61 Ibid.
- 62 R v Keefe, Ruling of Judge R J Earwaker on Permanent Name Suppression, CRI-2024-020-002908, [2026] NZDC 3634 (Napier District Court, February 27, 2026).
- 63 Ibid.
- 64 "Man Dubbed 'National Security Threat' Identified," *Otago Daily Times* (syndicated from RNZ), February 27, 2026; "Hawke's Bay Man Ronndog Keefe Named as Planner of Mass Killing and Distributor of Child Sexual Exploitation Material," *RNZ*, February 27, 2026.
- 65 Ibid.
- 66 R v Finnigan, Sentencing Remarks (UK Judiciary, January 2025), p. 4.
- 67 Ibid., p. 5.
- 68 Ibid., pp. 5-6.
- 69 Ibid., pp. 7, 15.
- 70 Ibid., p. 8.
- 71 Ibid., pp. 9-11.
- 72 Ibid., pp. 13-14.
- 73 Ibid., p. 14.
- 74 Ibid., p. 11.
- 75 "14-åring pojke knivhögg 82-årig man i ryggen – skyldig till mordförsök," *SVT Nyheter*, April 14, 2025; "Flera svenska ungdomar drivande i sadistnätverket 764," *SVT Uppdrag granskning*, April 2025.
- 76 Solna tingsrätt, mål nr. B 1768-25; Erik Glaad, "764-attack med kniv anses inte vara mordförsök," *Expo*, May 19, 2025.
- 77 Solna tingsrätt, mål nr. B 1768-25; "18-åring från Umeå åtalas för flera grova brott – kopplas till 764-gruppen," *SVT Nyheter*, May 8, 2026.
- 78 Solna tingsrätt, bevistalan ruling, mål nr. B 1768-25, April 2025.
- 79 "14-åring greps för knivattack i Borås – radikaliserades av 'No lives matter,'" *SVT Uppdrag granskning*, April 2, 2025.
- 80 "Flera svenska ungdomar drivande i sadistnätverket 764."
- 81 Borås tingsrätt, mål nr. B 39-25; Glaad.
- 82 "14-åring greps för knivattack i Borås – radikaliserades av 'No lives matter.'"
- 83 Ibid.; "Dödens chatttrum – svenskarna i 764," *SVT Uppdrag granskning*, three-part series, April 2025.
- 84 "Hovrätten ändrar dom för 764-kopplat knivdåd," *Expo*, July 2025; Borås tingsrätt, bevistalan ruling, mål nr. B 39-25, May 19, 2025; Hovrätten för Västra Sverige, ruling on appeal, July 2025.
- 85 Umeå tingsrätt, mål nr. B 953-23; "Man i Umeå åtalad för flera grova brott över internet," *Åklagarmyndigheten [Swedish Prosecution Authority]*, May 6, 2026.
- 86 "18-åring från Umeå åtalas för flera grova brott – kopplas till 764-gruppen;" "Dödens chatttrum – svenskarna i 764."
- 87 Ibid.
- 88 Umeå tingsrätt, mål nr. B 953-23.
- 89 Ibid.