

CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

September 2, 2025



Influence Operations and Conflict Escalation in South Asia

Insikt Group identified two influence operation networks supporting India and Pakistan during their April–May 2025 conflict, which we respectively track as Hidden Charkha and Khyber Defender.

Both networks intervened at every phase of the conflict, presenting a blueprint of two influence operation networks supporting adversarial, nuclear-armed countries attempting to control escalation.

Future kinetic conflict between India and Pakistan will likely continue featuring large-scale influence operations to erode diplomatic support, political credibility, and perceptions of military superiority.

Executive Summary

Insikt Group documented two large-scale, state-aligned influence operation networks supporting India and Pakistan, respectively, during the India-Pakistan conflict of April and May 2025; we track these networks as Hidden Charkha (pro-India) and Khyber Defender (pro-Pakistan). These networks are very likely motivated by patriotism and are almost certainly aligned with India's and Pakistan's domestic and foreign policy objectives, respectively. Both networks intervened at every phase of conflict escalation between the April 22, 2025, Pahalgam terror attack and the ceasefire announcement on May 10, 2025, presenting a blueprint of the TTPs and narratives employed by two separate influence operation networks supporting adversarial, nuclear-armed countries attempting to control escalation and garner popular and diplomatic support for limited conventional kinetic actions.

Each network consistently attempted to frame India or Pakistan, respectively, as maintaining superior technological and military capabilities — and therefore the implied ability for each respective country to exercise tactical restraint — as proof of having the moral high ground, and hence having domestic and international support. The networks also attempted to undermine India's and Pakistan's claims of military preparedness by amplifying forged military documents and exaggerating the impact of claimed cyberattacks to highlight vulnerabilities.

Despite their efforts, both networks were almost certainly unsuccessful in shaping public opinion, as measured by their lack of organic engagement on social media, their inability to break out of patriotic echo chambers, and their recurrent use of generative AI to produce visual content, which very likely undermines their credibility. Nevertheless, analyzing narratives produced by both networks can provide defenders with valuable insights into the role of influence operations (IOs) during conflict escalation. Organizations operating in conflict zones should proactively track mentions of their brand or key personnel in influence narratives to proactively mitigate against reputational damages.

Key Findings

- Hidden Charkha is a pro-India network active since at least 2021 that is almost certainly aligned with the Indian government and operating in the Indian Standard Time (IST) timezone. Khyber Defender is a pro-Pakistan network active since at least 2020 that is almost certainly aligned with the Pakistani government.
- Both networks were active during the India-Pakistan conflict following the Pahalgam terror attacks on April 22, 2025, and very likely attempted to support the governments of India and Pakistan, respectively, at different phases of conflict escalation.
- Initially, both networks attempted to stake claims and counterclaims to attribute the Pahalgam attacks as acts of state-sponsored terrorism from India or Pakistan. The networks then attempted to undermine senior political figures in each country, in addition to amplifying nationalist and patriotic sentiment domestically while suppressing dissenting opinions on social media.
- Hidden Charkha and Khyber Defender closely supported and criticized each country's kinetic military operations (Operation Sindoor and Operation Bunyan-Al-Marsous, respectively) and claimed each respective country was demonstrating tactical restraint and technological superiority.
- Following the ceasefire announcement on May 10, 2025, Hidden Charkha accused Pakistan, and Khyber Defender accused India, of violating the ceasefire, as both networks attempted to shape international perceptions on the outcome of the conflict and reassert claims of technological superiority.

Table of Contents

Two Networks	4
Hidden Charkha	5
Attribution	6
Objectives	6
Assets and TTPs	8
Khyber Defender	9
Attribution	9
Objectives	10
Assets and TTPs	12
Influence Operations and Conflict Escalation	13
Background	14
Initial Attribution Claims	14
Political Pressure and National Unity	17
Diplomatic Escalation and Media Reactions	19
Military Preparedness and Forged Documents	21
Supporting Kinetic Escalation	22
Initial Escalation and Retaliatory Framing	23
Responses to Operation Sindoor	24
Responses to Operation Bunyan-Al-Marsous	26
Supporting Cyber Escalation	28
Ceasefire and Aftermath	30
Mitigations	32
Outlook	32

Two Networks

Insikt Group identified two major influence networks engaging in coordinated inauthentic behavior (CIB) during the India-Pakistan conflict in late April and early May 2025: Hidden Charkha, a pro-India network, and Khyber Defender, a pro-Pakistan network (**Figure 1**). These networks illustrate how influence operations can be employed symmetrically during crises in an attempt to shape public perception in both domestic and foreign spheres, as well as in an attempt to manage escalation. Their behavior during the 2025 India-Pakistan standoff serves as a rare example of influence operations operating in tandem with kinetic and cyber escalation between rival nuclear-armed states. It also demonstrates the role of patriotic sentiment in aligning non-state influence actors with nation-state wartime objectives.

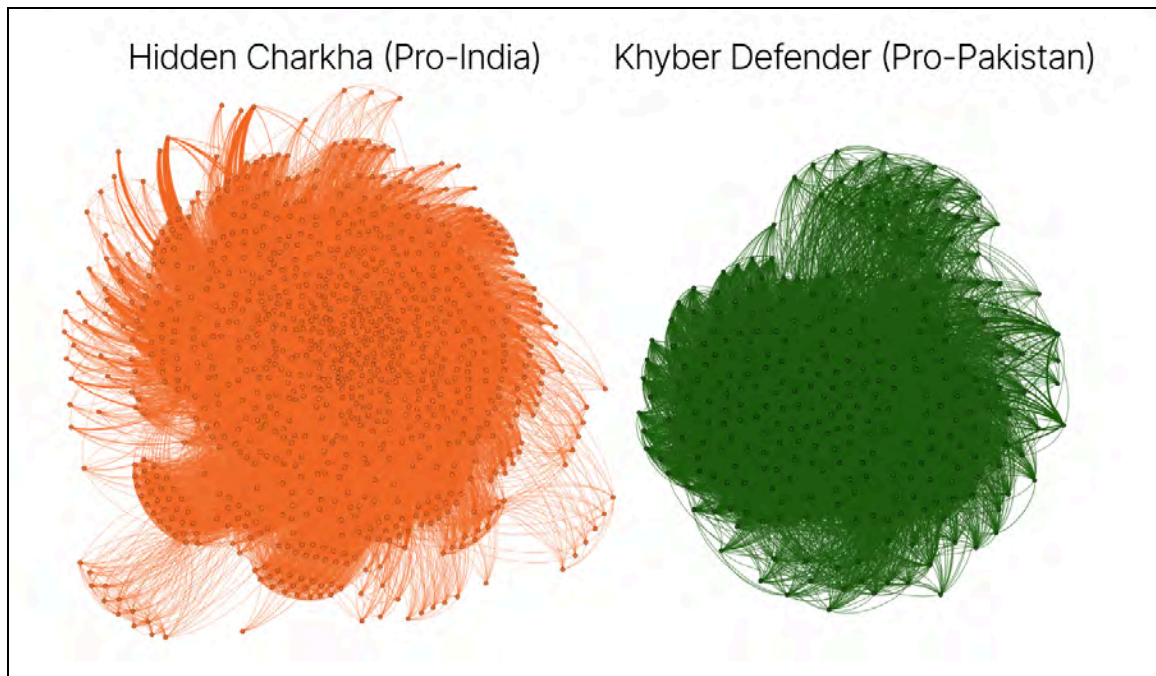


Figure 1: Hidden Charkha and Khyber Defender network graphs (Source: Recorded Future)¹

Both networks very likely operate to support and amplify pro-India and pro-Pakistan narratives on social media. These networks mainly promote pro-government messaging to domestic audiences in local languages and have seen sharp increases in activity during major domestic political events in each country (**Figure 2**). Hidden Charkha activity surged in November 2024 to commemorate the November 26, 2008, terrorist attacks in Mumbai; it also surged in January 2024 during [farmer protests](#) in India. Khyber Defender activity surged on April 15, 2025, when the Washington Post [revealed](#) that terrorist groups smuggled US weapons left in Afghanistan into Pakistan, as well as in July 2024, following Pakistani media coverage of “Operation Goldsmith,” an [alleged operation](#) by foreign actors to restore former Prime Minister Imran Khan. Both networks also prioritize narratives promoting national unity and

¹ **Figure 1** contains social network graphs of inauthentic social media accounts affiliated with Hidden Charkha (left) and Khyber Defender (right) posting identical content.

counter-insurgency operations in contested regions, such as the Balochistan province and Jammu and Kashmir (J&K), while undermining separatist movements operating in them.

In addition to domestic messaging, these networks also very likely support the aforementioned governments' foreign policy and diplomatic objectives, including undermining each respective government's rivals at global diplomatic events such as the United Nations (UN) General Assembly (UNGA). The pro-India Hidden Charkha network also likely supported [transnational repression](#) efforts by targeting Sikh separatists abroad, as well as by promoting content accusing Canada and the US of facilitating perceived Khalistani extremism.²

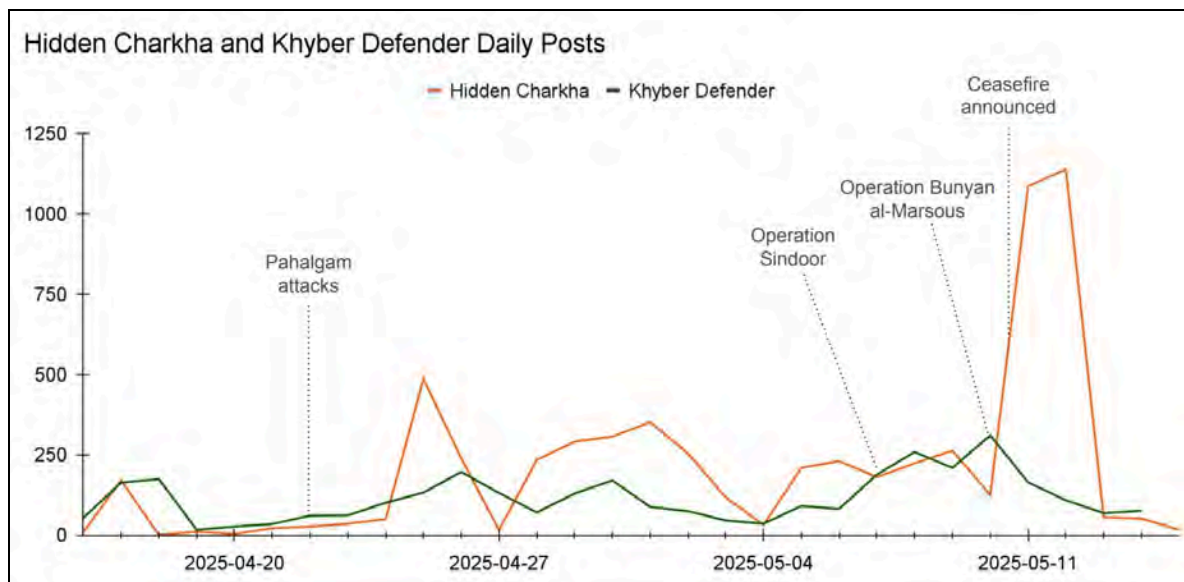


Figure 2: Hidden Charkha and Khyber Defender daily posting since January 2024 (Source: Recorded Future)

In addition to their size (over 900 inauthentic accounts affiliated with Hidden Charkha and over 300 affiliated with Khyber Defender), these networks are remarkably similar in terms of TTPs: They use hashtags to amplify content and manipulate trending topics, produce visual content inhouse, impersonate local and international news outlets, and use AI to generate content aimed at international audiences.

Hidden Charkha

Hidden Charkha is a covert influence network identified by Insikt Group in April 2025 disseminating pro-India influence content. We identified over 900 inauthentic accounts as part of this network, which has been active since at least 2021. Insikt Group assesses that Hidden Charkha's narratives are almost certainly aligned with the Indian government's geopolitical objectives, which include promoting

² Since India and Pakistan's independence from Britain in 1947, Sikh separatist movements have [called](#) for the creation of an independent homeland named "Khalistan." The Indian government has designated multiple Khalistani activists and groups as national security threats, and Canadian intelligence services have [accused](#) India of [assassinating](#) a prominent Sikh activist in British Columbia in 2023. In 2023 and 2024, Khalistani activists published threatening language [targeting](#) Air India, Indian stock exchanges, and Indian airports, and [called](#) for a "lockdown" of India's diplomatic missions in Canada.

pro-India narratives to international audiences, undermining pro-Pakistani narratives and positions, and targeting Khalistani separatist groups. We also observed the network producing influence content accusing the US and Canada of harboring Khalistani activists.

Attribution

Using pattern-of-life (PoL) analysis, Insikt Group assesses that Hidden Charkha's operators are likely based in India Standard Time (IST) locations, although we were unable to attribute this activity to a specific entity. Based on the network's posting patterns over the last two years, Hidden Charkha operators very likely follow typical 9-5 work schedules, with a pause around lunch (12:00-13:00) and reduced posting between 18:00-9:00 (**Figure 3**).

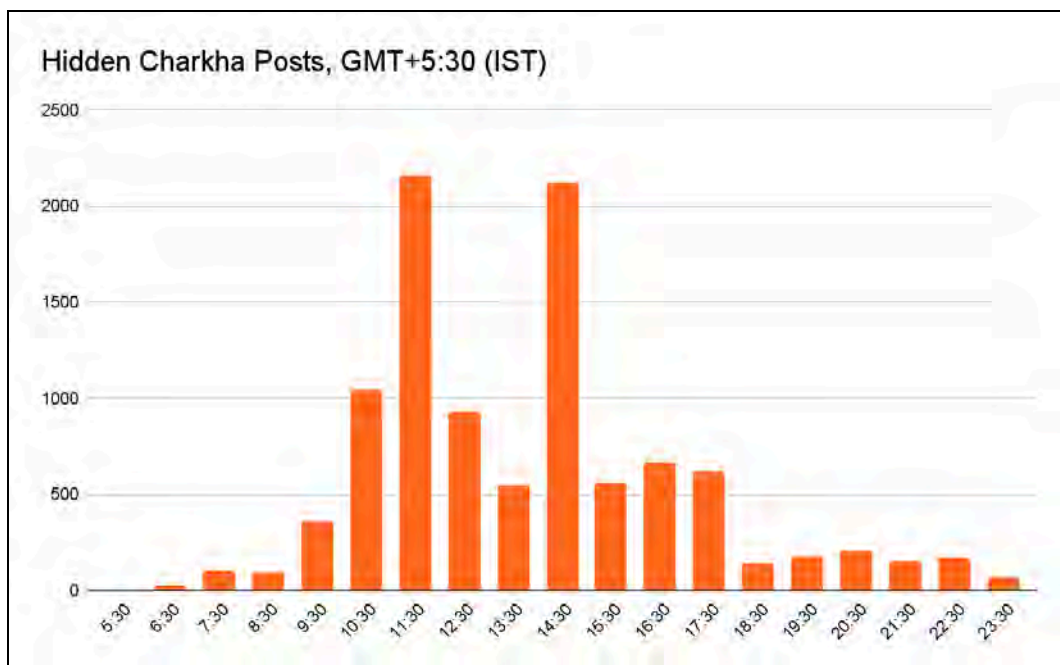


Figure 3: Hourly Hidden Charkha posting activity, GMT+5:30 (Source: Recorded Future)

Objectives

Hidden Charkha's content and narratives almost certainly seek to fulfill the following influence objectives:

- **Praise Indian political leaders** in addition to law enforcement and counter-terrorism units such as the Central Reserve Police Force (CRPF), and the National Security Guard (NSG), as well as highlight India's progress in sectors like defense manufacturing, semiconductors, AI, and transport infrastructure (**Figures 4, 5, and 6**). Accounts frequently promoted such content using hashtags like #MadeInIndia and #SelfReliantIndia.
- **Boost India's diplomatic standing** at events like the 79th UNGA in October 2024 and India's leadership of the G20 summit in 2023, using hashtags like #g20india and #g20_in_kashmir.

- **Defuse polarizing events** and support government responses such as the Muzaffarnagar school incident in September 2023, criminal law reforms in January and February 2024, major farmer protests in February and March 2024, and the November 2024 anniversary of the 2008 Mumbai terrorist attacks using hashtags like #NeverForget2611.

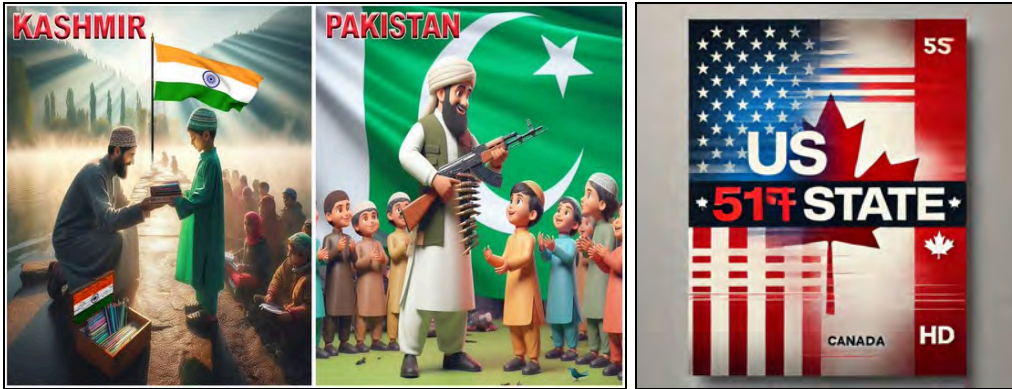
Insikt Group identified pro-India content posted by Hidden Charkha accounts likely generated using OpenAI's DALL-E 2 model and typically depicting India's economic success in sectors such as defense, manufacturing, and infrastructure.



Figures 4, 5, and 6: AI-generated images used in Hidden Charkha content (Source: Recorded Future)

Hidden Charkha's principal targets abroad are the following:

- **Pakistani Government:** Prior to the Pahalgam attacks, the network perpetuated narratives depicting Pakistan as sponsoring terrorism (**Figures 7 and 8**), often claiming the Pakistani government was complicit in the 2008 Mumbai attacks (also known as "26/11") [perpetrated](#) by the terrorist group Lashkar-e-Taiba (LeT), a position [also taken](#) by the Indian government.
- **Canadian Government:** Hidden Charkha repeatedly promotes content accusing the Canadian government of harboring Khalistani separatists, an issue that has driven a wedge between India and Canada and led to a [deterioration](#) in diplomatic relations (both countries have since [pledged](#) to mend relations over the issue at the 2025 G7 summit). The network has repeatedly blamed the Canadian government for sponsoring "Khalistani terrorism" and has amplified narratives calling for Canada to become a US state, using the hashtag #51state (**Figure 9**).
- **US Government:** Similar to Canada, Hidden Charkha promotes content targeting the US over its perceived tolerance for Khalistani activists residing in the country, mirroring Indian government [requests](#) for the US to list Sikh separatists as terror groups. Hidden Charkha accounts have also accused the US of funding "Pakistan-sponsored terrorists" and conducting transnational killings in reaction to US media outlets [attributing](#) an "assassination plot" targeting Khalistani activists in the US to India's Research and Analysis Wing (RAW).



Figures 7, 8, and 9: Hidden Charkha images referencing Pakistan, the US, and Canada (Source: Recorded Future)

Assets and TTPs

Hidden Charkha accounts are likely inauthentic but use multiple methods to hide or obscure their true identities while masquerading as legitimate users from India. Hidden Charkha account profiles almost certainly use profile pictures created by a generative adversarial network (GAN) generative model (**Figures 10 and 11**), or use stolen or generic profile pictures. Some of the network's most active accounts also employ AI-generated profile pictures, but obstruct faces to avoid being detected as AI-generated content, often by using veils or other kinds of objects, such as a building corner (**Figures 12, 13, and 14**).



Figures 10 and 11: GAN-generated profile pictures used by Hidden Charkha accounts (Source: Social Media)



Figures 12, 13, and 14: Similar AI-generated profile pictures used by Hidden Charkha accounts (Source: Social Media)

Insikt Group also identified Hidden Charkha accounts attempting to brand themselves as purported media outlets, using names such as "Daily Dose News" (@DdnDose), "NewsMasterIndia" (@NewsMasterIndia), and "NewsFreak" (@_peacekeeper2), with some accounts advertising

themselves as fact-checking organizations. One of the Hidden Charkha accounts branded as a fact-checking organization linked to *countermisinformation[.]com* in its bio, a website claiming to be “an initiative to combat the spread of disinformation against India by global media.”

Khyber Defender

Khyber Defender is a covert influence network identified by Insikt Group in May 2025; it has been disseminating pro-Pakistan influence content since at least 2020. Insikt Group assesses that Khyber Defender’s narratives are almost certainly aligned with the Pakistani government’s foreign and domestic policy goals, which include undermining the Indian government and nationalist movements in Balochistan, supporting Pakistan’s foreign policy regarding Afghanistan and the Israel-Hamas war, and lobbying the Pakistani government on topics like agriculture and public health.

Attribution

Insikt Group attributes Khyber Defender content with high confidence to Team 64, a Pakistani company and activist collective based in Khyber Pakhtunkhwa province. Insikt Group identified Khyber Defender accounts publishing large volumes of Urdu-language content, including Team 64’s logo (**Figures 15 and 16**), in addition to a number of likely inauthentic accounts [openly admitting](#) to posting “on behalf” of the company. Team 64 almost certainly has a current [Facebook page](#) and a [YouTube channel](#), the latter of which links to the social media handle @zeeshanhoti, which we assess is likely linked to Zeeshan Hoti, the President of the Provincial Youth Assembly in Khyber Pakhtunkhwa (KPK). However, we were unable to ascertain Hoti’s exact level of involvement in Team 64 or whether the KPK coordinates with the Pakistani central government.

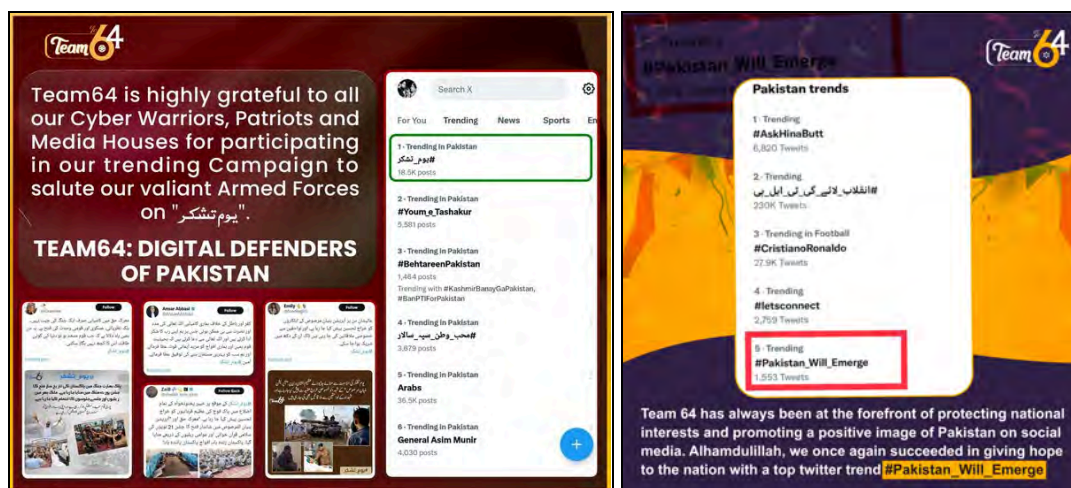


Figure 15: Team 64’s logo (Source: [Facebook](#))



Figure 16: Khyber Defender content using Team 64's logo (Source: Social Media)

In late May 2025, accounts linked to Khyber Defender published graphics using the #Team64 hashtag, calling Team64 the "digital defenders of Pakistan," thanking "all our Cyber Warriors, Patriots and Media Houses," and including a screenshot of Pakistan's top trending hashtags (Figure 17). Previous Khyber Defender and Team64 posts have also openly admitted to amplifying hashtags to reach Pakistan's top trends, such as #Pakistan_Will_Emerge in January 2023 (Figure 18).



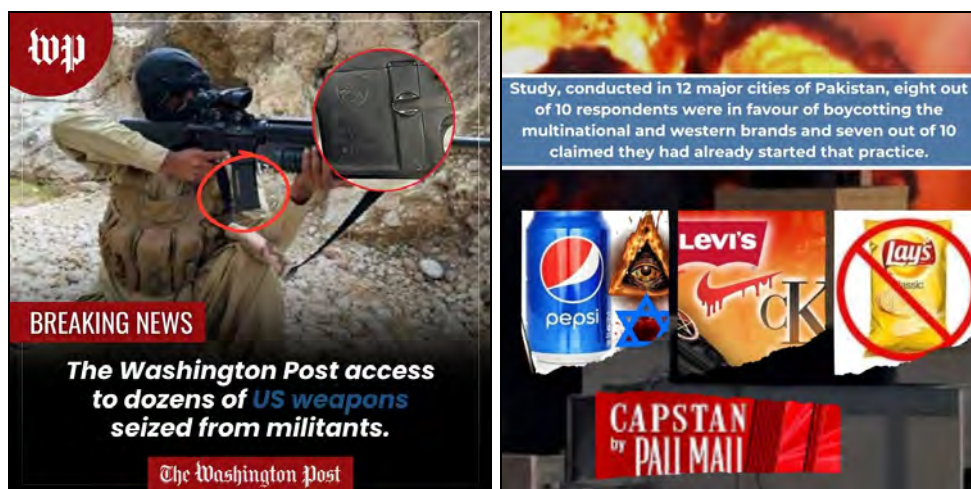
Figures 17 and 18: Graphic published by Khyber Defender accounts on May 16, 2025 (left), and January 2023 (right) (Source: Social Media)

Objectives

The majority of Khyber Defender content has focused on supporting Pakistan's geopolitical objectives and foreign policy, including by:

- Undermining the Indian government**, including by attempting to erode India's diplomatic standing (including at the 2023 UNGA, also targeted by Hidden Charkha; Khyber Defender used hashtags like #UNGA78 and #unga2023), deflecting accusations around alleged Pakistani state-sponsored terrorism, and sustaining pro-Pakistan sentiment in contested regions like J&K. Pakistani diplomats have [repeatedly](#) denied India's accusations at the UN.

- **Blaming the US for regional instability**, which includes criticizing the 2021 US withdrawal from Afghanistan. Notably, the network posted graphics impersonating The Washington Post (**Figure 19**) [based](#) on a real article describing the flow of US weapons to terror groups such as the Pakistani Taliban Movement (Tehrik-e Taliban Pakistan, TTP). Khyber Defender accounts stated that “American weapons are no longer symbols of partnership—they're assets in the hands of extremists.” Following the Taliban's return to power, the TTP has [surged attacks](#) against Pakistani military and law enforcement targets, which Pakistani leaders have [attributed](#) to US and NATO forces exiting Afghanistan in August 2021.
- **Supporting Palestine** by calling for the boycott of US companies and consumer brands operating in Israel during the Israel-Hamas war, using hashtags like #9MonthsofGenocide (**Figure 20**). The Pakistani government has consistently [sided](#) against Israel during the conflict, with Pakistan's National Assembly passing a unanimous resolution condemning Israel's “heinous waves of atrocities” in Gaza.



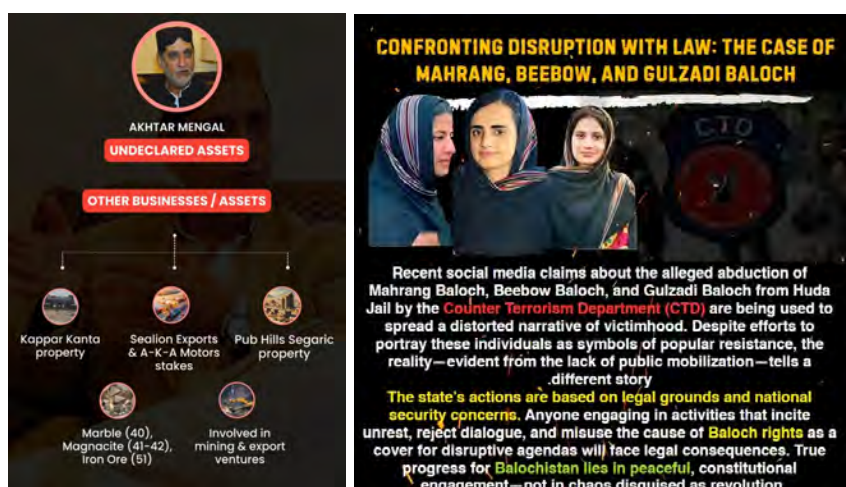
Figures 19 and 20: Khyber Defender content impersonating the Washington Post and calling for the boycott of US companies operating in Israel (Source: Social Media)

Khyber Defender almost certainly targets domestic Pakistani audiences in English and Urdu in pursuit of the following objectives:

- **Undermine Baloch nationalist and separatist movements** like Akhtar Mengal's Balochistan National Party (BNP-M; **Figure 21**), insurgent groups like the Balochistan Liberation Army (BLA), and the Balochistan Liberation Front (BLF), in addition to human rights groups like Dr Marhrang Baloch's Baloch Unity Committee (BYC; **Figure 22**). These objectives mirror the Pakistani government's crackdown on pro-Baloch movements and insurgents, as Pakistan [designated](#) the BLA a terrorist group in 2006 and has been accused of [cracking down](#) on peaceful protests by BYC and BNP-M supporters. In July 2025, Pakistani authorities reportedly [placed](#) Akhtar Mengal on a no-fly list.
- **Erode domestic support for Imran Khan** and the Pakistan Tehreek-e-Insaf (PTI) political party by accusing PTI of “collaborating” with Baloch separatist groups to form terror plots and alleging Imran Khan of being corrupt. Khan was [sentenced](#) to fourteen years in prison in January 2025

after being detained since 2023 over alleged corruption charges. The Pakistani government also [attempted](#) to ban PTI in 2024. Khyber Defender accounts previously expressed their support for Khan during his tenure as Prime Minister, but changed their narratives after he was deposed in April 2022, supporting our assessment that these accounts are operating in alignment with the Pakistani government.

- **Lobby the Pakistani government** over economic policy, including asking for an increase in wheat prices to support farmers, using hashtags such as #کسان_کا_ساتھ_دو ("Support the farmer") and #ریٹ_نہیں_تو_فصل_نہیں ("No fair rate, no crop"), and raising the tax rate on tobacco products to support public health. The Pakistani government decided in February 2025 to [abolish](#) minimum support prices for wheat, creating [economic concerns](#) for farmers; additionally, the government has also [continued raising](#) tobacco taxation levels to meet World Health Organization (WHO) standards.



Figures 21 and 22: Khyber Defender content targeting Akhtar Mengal and Dr. Mahrang Baloch
(Source: Social Media)

Assets and TTPs

The majority of Khyber Defender's accounts are very likely inauthentic, given their use of ["follow-for-follow"](#) tactics to accrue followers, stolen profile pictures, and common traits shared between accounts, such as the use of similar bios and specific emojis. Many Khyber Defender accounts have likely accrued significant followings by participating in inauthentic "follow-for-follow" networks, which involve following many accounts to receive many reciprocal followers.

Influence Operations and Conflict Escalation

Insikt Group assesses that Hidden Charkha and Khyber Defender both participated in influence activities aligned with India's and Pakistan's broader efforts to shape domestic and international public opinion and deflect blame following the Pahalgam attacks. This influence activity aligned with India and Pakistan characterized their kinetic reprisals as legitimate and proportionate, effectively attempting to assert control over conflict escalation. Based on content published during the India-Pakistan conflict between April 22 and May 15, 2025, these networks almost certainly attempted to do the following:

- **Rapidly establish control over attribution narratives over the Pahalgam attacks** and legitimize claims using government and news sources
- **Increase domestic political pressure on perceived adversarial public officials and erode trust in adversary leadership** while promoting narratives of unity domestically
- **Undermine the rival's diplomatic standing** and counter or support international media reports on the conflict
- **Erode trust in adversary military preparedness** by amplifying almost certainly forged military documents that reportedly showed a lack of morale and equipment malfunctions
- **Frame military retaliation as justified and securing the moral high ground** by promoting narratives of a disproportionate response by their adversary
- **Drive domestic and international support for conventional kinetic operations by amplifying operational successes**, establishing narratives of technological superiority, countering adversarial claims of failure, and promoting patriotic sentiment
- **Exaggerate the impact of cyberattacks on adversary infrastructure** by echoing claims from hacktivist groups and national media outlets
- **Claim military and cyber operations as successes post-ceasefire** while highlighting any ceasefire violations, undermining their adversary on the international stage, and reaffirming their own technological sophistication

In spite of each network's attempts, organic social media engagement with their campaigns during the conflict's time period was minimal, very likely denoting a failure to effectively shape public opinion. These networks also very likely failed to escape their national media echo chambers and likely reinforced existing messaging targeting like-minded activists and patriotic actors. Additionally, based on available data, Insikt Group is unable to establish whether these networks are operating under direct government supervision or control, limiting arguments of causal links between the Indian and Pakistani governments' strategies during the conflict and narratives published by Hidden Charkha and Khyber Defender.

Nevertheless, narratives promoted by both influence networks to support conflict escalation almost certainly demonstrate how nationalist or patriotic sentiment can align network operators with nation-state influence objectives and provide informational support in times of kinetic warfare.

Background

On April 22, 2025, gunmen [shot and killed](#) 26 tourists at a resort near Pahalgam in India-controlled Kashmir. The attack was initially claimed by The Resistance Front (TRF), an alleged proxy of the Pakistani terrorist organization Lashkar-e-Taiba (LeT), which has been designated as a terrorist group by the [Indian](#), [Pakistani](#), and [US](#) governments since 2001. Initial reactions in both countries included [deflecting blame](#) onto the other and mounting domestic political pressure to identify responsible parties in government. Diplomatic tensions soared after both countries [instituted](#) reciprocal diplomatic sanctions and [appealed](#) to foreign world leaders and international bodies. Escalating tensions along the Line of Control (LoC) border [culminated](#) with India's Operation Sindoor on May 7, 2025, which included strikes on LeT-linked facilities in Pakistan, and Pakistan's retaliation starting May 8, 2025, subsequently expanded under Operation Bunyan-Al-Marsous on May 10, 2025, shortly before a US-brokered ceasefire was announced later the same day.

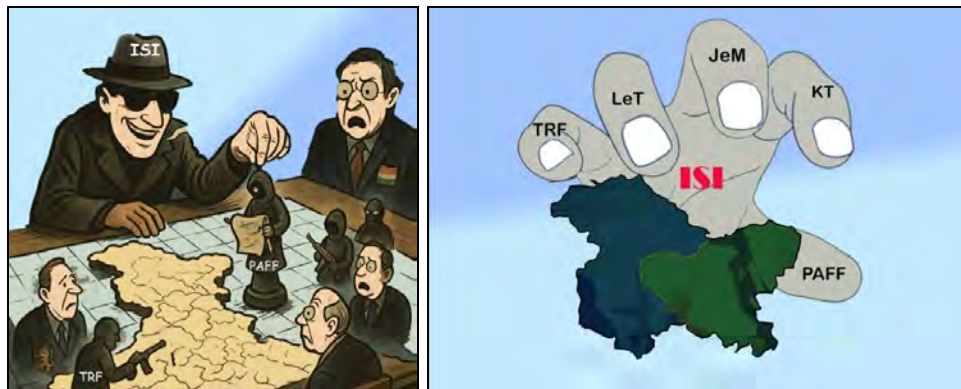
Initial Attribution Claims

Between April 22 and 25, 2025, both networks reacted rapidly to the attack to establish opposing attribution narratives (**Figure 23**), each framing the Pahalgam attack as state-sponsored terrorism by India or Pakistan. This activity almost certainly aimed to undermine the respective government's credibility among international audiences while simultaneously inoculating domestic audiences against hostile messaging, particularly in [contested](#) regions like Jammu and Kashmir.



Figure 23: Timeline of Hidden Charkha and Khyber Defender activity following the Pahalgam attacks
(Source: Recorded Future)

Within two hours of the Pahalgam attacks, Hidden Charkha accounts began attributing them to Pakistan. Accounts blamed the attacks on “Pak sponsored terrorists,” using hashtags like #pahalgamattack and #TerrorStatePakistan. By April 23, 2025, Hidden Charkha accounts began posting previously unseen (and therefore likely purpose-made) visual content accusing Pakistan’s Inter-Services Intelligence (ISI) of sponsoring LeT and calling TRF a “thinly veiled proxy” of LeT (**Figures 24 and 25**).



Figures 24 and 25: Visual content posted by Hidden Charkha accounts following the Pahalgam attacks
(Source: Recorded Future)

On April 22, 2025, at approximately 20:43 Karachi time, Khyber Defender accounts began coordinated posting of the #indianfalseflag hashtag. Initial posts attempted to counter claims [made](#) by Indian media outlets attributing the attacks to Pakistan. Accounts drew comparisons to the February 14, 2019, attacks in Puwalma, claiming that the two attacks were false flags and followed the “same script, same timing, same agenda.” On April 24, 2025, Khyber Defender accounts continued calling the Pahalgam attack a “scripted move” and an example of the Indian government’s “false flags, timed perfectly with global optics, to serve political agendas,” using hashtags like #IndianPropagandaExposed (**Figure 26**) and #IndiaFalseFlagKing (**Figure 27**).



Figures 26 and 27: Visual content posted by Khyber Defender accounts following the Pahalgam attacks
(Source: Recorded Future)

On April 25, Khyber Defender accounts also amplified images (**Figure 28**) purportedly stating a denial of responsibility for the Pahalgam attacks by the TRF. The statement, originally issued on a Telegram channel allegedly operated by TRF, denies the group's involvement in the attacks, citing a "cyber intrusion" by "Indian cyber-intelligence operatives." Starting May 30, 2025, the Telegram channel also began publishing screenshots of likely inauthentic documents purportedly sourced from India's Research and Analysis Wing (RAW). These documents allegedly show that the attack had been orchestrated by the Indian government.



Figure 28: Alleged statement of denial by TRF amplified by Khyber Defender accounts
(Source: Recorded Future)

Starting April 25, both networks attempted to legitimize their attribution claims by amplifying government and news sources. Hidden Charkha accounts began posting headlines from Indian national news outlets that provided evidence attributing the attacks to Pakistan (**Figures 29 and 30**); however, the narrative's credibility among international audiences was very likely [undermined](#) by a rising echo-chamber effect in Indian media, as outlets amplified unverified claims and suffered from circular reporting. In contrast, Khyber Defender attempted to validate its claims by repeatedly posting clips directly sourced from the Pakistan Armed Forces' Inter-Services Public Relations (ISPR) press conferences with Director General Ahmed Shareef Chaudhry (**Figure 31**).



Figures 29 and 30: Hidden Charkha content amplifying headlines from Indian news outlets reportedly confirming attribution to Pakistan (Source: Recorded Future)



Figure 31: Khyber Defender content amplifying ISPR press conferences (Source: Recorded Future)

Political Pressure and National Unity

Following the establishment of initial attribution claims, both networks attempted to erode trust in adversary leadership while simultaneously promoting unity at home and suppressing dissent from domestic political rivals.

Hidden Charkha attempted to undermine the perceived credibility of Pakistani officials by using quotes and supporting screenshots from Indian news outlets. Hidden Charkha initially amplified claims by former Pakistani officer and journalist [Adil Raja](#) that Pakistan Army chief General Asim Munir had ordered the Pahalgam attacks, using screenshots of an April 24, 2025, India Today article that [claimed](#) Munir was “desperate for a mini-war with India.” Other attempts to undermine General Munir included using quotes by former Pentagon official Michael Rubin [calling](#) Munir a “terrorist” in an interview with Indian media outlet ANI. Hidden Charkha accounts later targeted Pakistan’s Minister of Defense

Khawaja Asif, claiming the minister had confessed that “we [Pakistan] did the dirty work of funding & training terrorists for 3 decades.”

On April 25, Khyber Defender accounts began targeting India's National Security Advisor Ajit Doval using the hashtag #sackajitdoval, claiming that the Pahalgam attacks were an “intelligence disaster” for India and that “there are increasing calls for Ajit Doval and his colleagues to step down.” The network's narratives almost certainly attempted to capitalize on mounting domestic criticism in the aftermath of the attacks, such as from the Shiv Sena (UBT) party, which also [qualified](#) the Pahalgam attacks as an “intelligence failure” and criticized Doval on April 24, 2025.



Figures 32 and 33: Khyber Defender content calling for Ajit Doval to be fired (Source: Recorded Future)

While mounting pressure on adversary public officials, the networks simultaneously began posting narratives promoting unity, patriotism, and nationalist sentiment in their respective countries. Hidden Charkha, for example, focused on highlighting national and regional unity by posting content using hashtags like #KashmirRejectsTerrorism and #StandWithIndia, as well as visual content promoting unity in J&K using the #jmkumr hashtag (**Figure 34**). Conversely, Khyber Defender accounts amplified official messages from Pakistani officials like General Munir's “Pakistan Hamesha Zindabad” (“Pakistan Forever Alive”) slogan, or images of national unity using hashtags like #Pakistan_is_our_pride (**Figure 35**).



Figures 34 and 35: Hidden Charkha (left) and Khyber Defender (right) content promoting regional unity and nationalist sentiment (Source: Recorded Future)

Conversely, both networks also sought to suppress dissent by questioning the loyalty of domestic political rivals. For instance, Hidden Charkha promoted the [#राहुल_देशद्रोही_है](#) ("Rahul is a traitor") hashtag to label Rahul Gandhi, the [opposition leader](#) in India's Lok Sabha house of parliament, a terrorist "sympathizer." This narrative mirrors the animosity of the Bharatiya Janata Party (BJP) toward Gandhi, with BJP spokesman Pradeep Bhandari accusing Gandhi of "undermining India's progress" in December 2024. Similarly, Khyber Defender accounts used the hashtag [#PTM_Supports_Terrorism](#) to accuse the Pashtun Tahafuz Movement (PTM), a human rights organization [defending](#) Pashtun rights in Pakistan, of supporting Indian narratives on the Pahalgam attacks and called on Pashtuns to support Pakistan by stating "Proud Pashtun brothers! Understand the game of the enemies and support your state."

Diplomatic Escalation and Media Reactions

Governments typically use bilateral or multilateral diplomatic statements and communications during emerging conflicts as a mechanism for de-escalation or signalling foreign policy intent. Governments will hold press conferences or issue public statements, and they are increasingly using social media to promote these communications. Covert influence operations targeting social media users are likewise [increasingly being used](#) to shape narratives and drive diplomatic outcomes, particularly as diplomats themselves have been leveraged by nation-states like [China](#) and [Russia](#) as part of their broader influence ecosystems.

Both Hidden Charkha and Khyber Defender demonstrated a strong intent to shape international public opinion and promote their respective countries' diplomatic standing while undermining the opposite country. Hidden Charkha was almost certainly more proactive than Khyber Defender in amplifying influence content signalling diplomatic escalation, reflecting India's retaliatory measures in the immediate aftermath of the Pahalgam attack, while the latter kept a more reactive approach to India's diplomatic actions.

On April 23, 2025, diplomatic tensions between India and Pakistan rapidly [escalated](#) following India's decision to suspend the 1960 Indus Waters Treaty (IWT), among other measures like visa bans and border closures. The treaty, which governs water distribution between India and Pakistan in the Indus river basin, was [declared](#) a national security risk by Indian Foreign Secretary Vikram Misri after the Pahalgam attack. Following the IWT suspension, both networks attempted to appeal to international audiences and international diplomatic bodies; however, Hidden Charkha displayed greater intent to undermine Pakistan at diplomatic forums like the UN Security Council (UNSC).

Hidden Charkha accounts initially amplified Foreign Secretary Misri's announcement of the measures as "decisive" action by the Indian government (**Figure 36**). Meanwhile, Khyber Defender accounts reacted strongly against the suspension of the IWT, amplifying Pakistani government statements that the move [was](#) a "red line" and a "direct threat" to Pakistan (**Figure 37**), echoing an April 24, 2025, statement by Pakistan's National Security Committee [calling](#) the decision an "act of war." Khyber Defender accounts also attempted to frame the treaty's suspension as India violating international norms, stating that "It's time the global community took notice" and using the hashtag [#indiaemptythreats](#).



Figures 36 and 37: Hidden Charkha (left) content covering India's diplomatic measures and Khyber Defender (right) Urdu-language content framing the IWT suspension as contrary to international norms (Source: Recorded Future)

Hidden Charkha was particularly focused on undermining Pakistan's standing at the UN, a tactic not generally observed by Khyber Defender accounts regarding India. Starting April 30, 2025, Hidden Charkha accounts accused Pakistan's Foreign Minister Ishaq Dar of pressuring the UNSC to drop mentions of TRF from an official statement on the Pahalgam attacks (**Figure 38**). On May 5, 2025, following Pakistan's [demand](#) for a closed-door consultation at the UNSC, Hidden Charkha accounts attempted to undermine Pakistan's appeal to the UNSC over India's suspension of the IWT, accusing it of "playing the victim." On May 9, the pro-India network claimed that the UNSC had "rejected Pakistan's false flag narrative," and published likely inauthentic images depicting world leaders declaring their support for India as well as content using the hashtag #TerrorHasNoBorders (**Figure 39**).



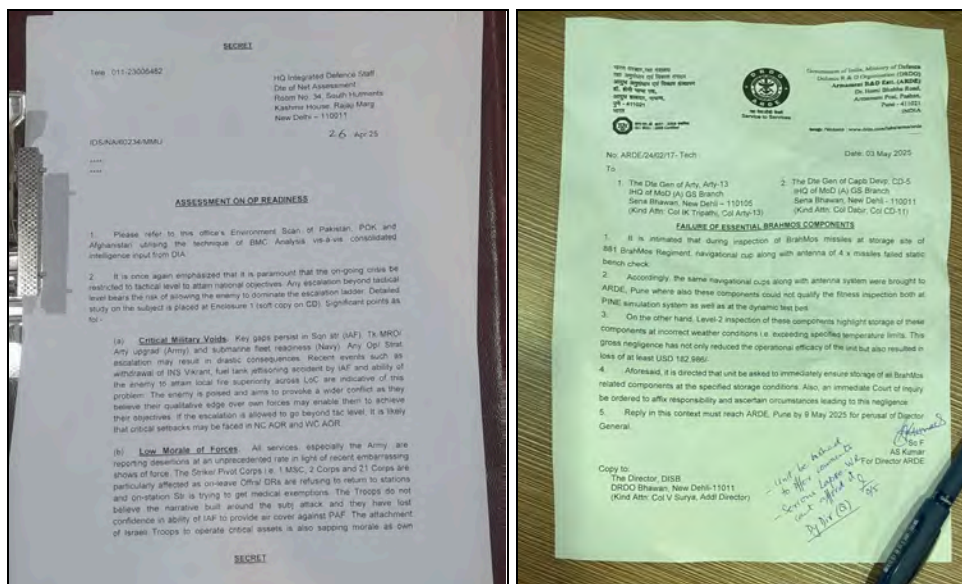
Figures 38 and 39: Hidden Charkha content seeking to undermine Pakistan at the UNSC (Source: Recorded Future)

In tandem with posting content aimed at supporting diplomatic measures by each country, the networks also reacted to international reporting on the emerging conflict. Of the two networks, Hidden Charkha also adopted a more aggressive stance against international media reporting by using the #stopwhitewashing and #MediaBias hashtags to accuse international media outlets, including the New York Times, Al Jazeera, and BBC, of naming the Pahalgam attackers "militants" — instead of terrorists — thereby legitimizing the TRF's attack. In contrast, Khyber Defender accounts praised the New York

Times' coverage of General Munir, by stating, for example, that the May 5, 2025, [article](#) by the newspaper was "absolutely correct."

Military Preparedness and Forged Documents

Following initial attribution claims and escalating diplomatic tensions, Khyber Defender focused on eroding the Indian public's trust in New Delhi's military preparedness by circulating almost certainly forged documents. Starting April 28, 2025, Khyber Defender accounts amplified alleged leaked documents from the Indian Integrated Defense Staff headquarters reporting on the Indian Army's reportedly low morale and increasing desertion rates (**Figure 40**). On May 5, 2025, Khyber Defender accounts amplified alleged leaked documents from India's Defense and Research and Development Organization's (DRDO) [Armament Research and Development Establishment \(ARDE\)](#) questioning the "operational efficacy" of the 881 Missile Regiment's BrahMos cruise missiles due to gross negligence in storage conditions (**Figure 41**). Both documents are almost certainly inauthentic and make verifiably false or non-credible claims, such as that "Israeli Troops" operating Indian Air Force (IAF) equipment was undermining morale or that "any uncontrolled escalation has the potential to set [our] own economy back by 50 years."



Figures 40 and 41: Images claiming to depict leaked Indian defense documents, amplified by Khyber Defender accounts (Source: Recorded Future)

Insikt Group assesses that the first known source of the documents is likely an anonymous pro-Pakistani social media account (@War_Analysts), which posted at least one of the two documents (**Figure 41**) before the Khyber Defender accounts. The account also published other likely inauthentic documents, such as a diplomatic complaint [from](#) the Israeli Embassy in New Delhi to the Indian government over an alleged case of sexual assault by Indian Special Forces on a member of the Israeli Defence Forces during a military exercise, a report [alerting](#) to T-90 ammunition shortages in the Indian Army, and an emergency procurement [request](#) for AK-203 rifles and other equipment from Russia.

Supporting Kinetic Escalation

On May 7, 2025, India began Operation Sindoor, which involved missile and airstrikes on [suspected](#) terrorist (including LeT) infrastructure in Pakistan-administered Kashmir and Punjab, Pakistan. On May 10, 2025, Pakistan [responded](#) with Operation Bunyan-Al-Marsous, which targeted Indian military installations in Northern India.³ In tandem with these conventional kinetic operations, both Hidden Charkha and Khyber Defender increased their operational tempo (**Figure 42**) and attempted to support specific armed forces by publishing content almost certainly intended to justify military action, deter further kinetic actions by establishing perceived technological superiority, and forge patriotic sentiment.

Operation Sindoor [represented](#) a major expansion from India's last kinetic actions against Pakistan in response to the 2019 Pulwama terror attack, and New Delhi very likely sought to calibrate its operations to minimize chances of uncontrolled escalation. Conversely, Pakistan — which has suffered [repeated](#) military defeats against its more [well-equipped](#) neighbor — very likely sought to capitalize on battlefield successes to present itself as a peer adversary not easily deterred. During the conflict, Hidden Charkha portrayed Operation Sindoor as precise, internationally supported, and strategically restrained, which Khyber Defender countered with claims of Indian losses and Pakistan's retaliatory capabilities during Operation Bunyan-Al-Marsous. Both networks emphasized technological superiority and weapon precision to support public perceptions of tactical restraint. They did this by promoting each respective country's weapons' effectiveness while discrediting the other country's systems in an attempt to paint retaliatory strikes as disproportionate and indiscriminate. Accounts consistently highlighted the precision of their respective country's military attacks, as well as any civilian casualties inflicted by the adversary, by sharing images and footage of military strikes, likely to complicate battle damage assessments and downplay the impact of the other country's actions, while appealing to international audiences and strengthening patriotic sentiment domestically.

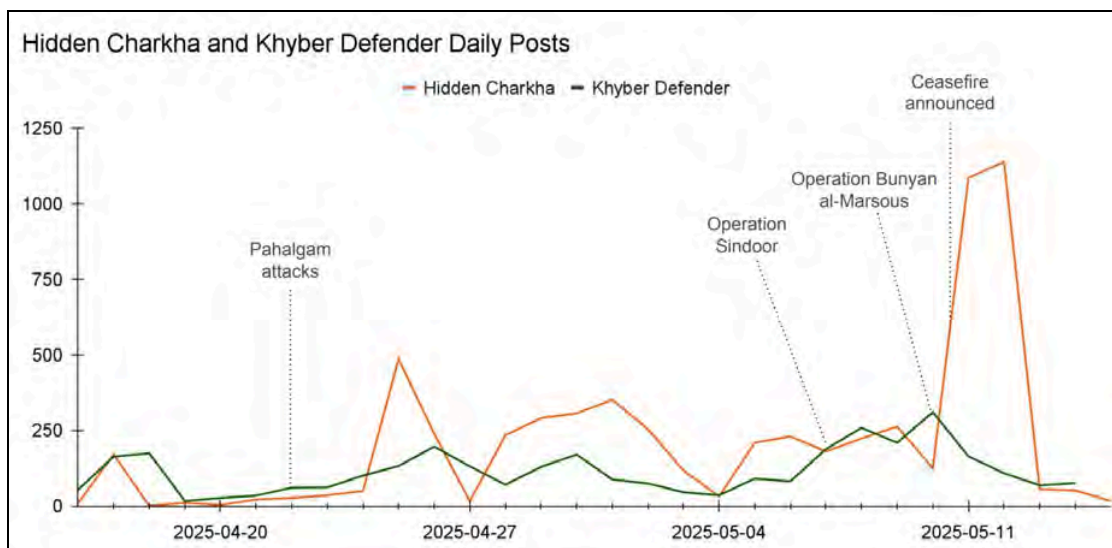


Figure 42: Increased operational tempo by both networks following kinetic escalation (Source: Recorded Future)

³ Insikt Group's Global Issues team covered these kinetic exchanges in daily situational reports, published in the Geopolitical Intelligence Module.

Initial Escalation and Retaliatory Framing

Prior to the launch of Operation Sindoor, both networks documented rising military escalation along the LoC in J&K. They also framed the military maneuvers of each other's respective country as provocations, while establishing such maneuvers as a clear justification for the other country's retaliation.

Both networks also made claims and counterclaims concerning shows of strength along the LoC. For example, Hidden Charkha accounts called Pakistan's May 3, 2025, [Abdali missile tests](#) an attempt to "divert attention from its role in the Pahalgam massacre." Meanwhile, very likely inauthentic images shared by Khyber Defender (**Figures 43 and 44**) attempted to justify military retaliation and deter further escalation by posting images with captions such as "We dare you" and "Pakistan will retaliate disproportionately." Khyber Defender also documented the Pakistani Army shooting down Indian Unmanned Aerial Vehicles (UAVs) and criticized Indian Rafale sweeps along the LoC.



Figures 43 and 44: Images shared by Khyber Defender prior to Operation Sindoor
(Source: Recorded Future, Social Media)

As soon as April 24, 2025, Khyber Defender accounts began repeatedly posting content attempting to establish a red line for kinetic escalation (using the hashtag #pakistanismyredline) and lauding its military preparedness, praising the Pakistani Air Force (PAF) using hashtags like #pafreadytorespond. The network also shared AI-generated images (**Figures 45 and 46**), which were likely made using OpenAI's GPT-4o (based on the [model's distinct](#) "sepia" or "yellow-tint" style also found in these images), showing military preparedness, such as portraying Pakistani F-16s in the style of traditional wartime propaganda. Khyber Defender accounts also began amplifying narratives of the Pakistani armed forces' technological superiority early in the conflict, stating, for example, that Pakistani JF-17s "outclass" India's "vintage MiGs," and that "Our AWACS & missile tech ensure dominance. No propaganda can hide this asymmetry."



Figures 45 and 46: AI-generated images shared by Khyber Defender
(Source: Recorded Future)

Responses to Operation Sindoor

Following the Indian military's launch of "Operation Sindoor" on May 7, 2025, Hidden Charkha accounts increased their operational tempo to justify military action, amplify and often exaggerate Indian military successes, discredit Pakistani counter-narratives, and generally celebrate the operation as a success.

Hidden Charkha praised the Indian Armed Forces' military capabilities and coordination, demonstrating intimate knowledge of India's military capabilities after years of posting content praising India's defense systems. Starting May 7, 2025, the network lauded the effectiveness of India's Akash and SCALP missiles, Dassault Rafale fighter jets, and Bofors L-70 and Zu-23mm anti-aircraft guns. The network also issued strong denials to counter initial Pakistani media reports that Pakistani forces shot down Indian Rafales. The network also highlighted Pakistan's loss of military equipment. On May 8, 2025, Hidden Charkha began posting claims that Indian S-400 air defense systems had downed two Pakistani JF-17s and a J-20C. The network later amplified reports of Pakistani equipment being destroyed, such as an AWACS aircraft and an F-16 squadron at Bholari airbase and Shapar and Bayraktar drones at Murid airbase, in addition to claiming that Chinese-made missiles, such as PL-15 and HQ-9 air-to-air missiles, were ineffective (**Figure 47**).



Figures 47 and 48: Images shared by Hidden Charkha covering Operation Sindoor (Source: Recorded Future)

Following Operation Sindoor, Hidden Charkha amplified narratives painting the military operation as a justified escalation and proportional response to the Pahalgam attack. On May 12, 2025, Hidden Charkha accounts amplified graphics posted by the Indian Ministry of Defense (MoD) Additional Directorate General of Public Information (ADG-PI) on social media, with accounts claiming that “India showed exemplary Strategic Restraint. #OperationSindoor was powerful yet measured, targeting only terror infrastructures, avoiding escalation.” Other accounts posted content claiming that Operation Sindoor had international approval, including sharing graphics originally from Indian news outlets that [claimed](#) US Secretary of Defense Pete Hegseth “backed” Operation Sindoor (**Figure 49**), [as well as](#) Afghanistan’s former Vice President Amrullah Saleh (**Figure 50**). Hidden Charkha likely attempted to amplify nationalist sentiment during Operation Sindoor by consistently using the hashtags #pahalgamavenged and #satyamevjayate, with the latter [being](#) India’s official national motto (“truth alone triumphs”).



Figures 49 and 50: Graphics published by Hidden Charkha accounts justifying Operation Sindoor (Source: Recorded Future)

In line with the network’s previous aggressive stance toward international media, at least one account posted an attempted community note in response to French media outlet France24, claiming that its reporting attempted to “protect the reputation of China’s rotten and outdated weapons.” On May 20,

2025, Hidden Charkha accounts posted content celebrating Operation Sindoor as a success, [dubbing](#) a BJP rally in Baramulla (located in India-controlled J&K) a “shining moment of unity, patriotism, and victory,” very likely attempting to reinforce patriotic narratives among audiences in contested regions.

During the early stages of Operation Sindoor, Khyber Defender accounts very likely attempted to capitalize on Pakistan’s [alleged downing](#) of Rafales and Israeli drones to spring counter-claims undermining Indian narratives of technological superiority (calling India’s claims “big talk” and a “bluff”) and attract international attention to the conflict. Starting May 7, 2025, Khyber Defender began posting content covering the reported downing of Indian Rafales by the PAF using PL-15 missiles (**Figure 51**), as well as amplified alleged imagery of the wreckage. On May 9, 2025, Khyber Defender accounts claimed that India’s loss of Rafale fighter jets had “sparked disbelief and mockery in French media” (**Figure 52**).



Figures 51 and 52: Khyber Defender content covering the reported Rafale downings by the PAF on May 7–9, 2025 (Source: Recorded Future)

Responses to Operation Bunyan-AI-Marsous

Following initial counter-claims to India’s Operation Sindoor, Khyber Defender pivoted to promoting Pakistan’s Operation Bunyan-AI-Marsous beginning on May 10, 2025. Similar to Hidden Charkha, Khyber Defender also attempted to exaggerate the PAF’s operational success and amplify nationalist sentiment (**Figures 53 and 54**), naming the operation “a symbol of national resolve and unmatched defense capability.” On May 10, 2025, the network claimed that PAF JF-17s had successfully “neutralized” an Indian S-400 using hypersonic missiles.



Figures 53 and 54: Khyber Defender content promoting Operation Bunyan-Al-Marsous (Source: Recorded Future)

Similar to Hidden Charkha, Khyber Defender accounts also amplified images and footage of alleged destruction of Indian military installations (**Figures 55 and 56**) to demonstrate precise strikes and tactical restraint, including purported footage showing the destruction of Indian Brahmos missile storage units in Beas and Nagrota. On May 10, 2025, Khyber Defender accounts also promoted the success of Fatah missiles in posts that allegedly revealed the “destruction of key Indian facilities.”



Figures 55 and 56: Footage of Pakistani missile strikes shared by Khyber Defender accounts (Source: Recorded Future)

On May 11, 2025, Hidden Charkha accounts attempted to paint Pakistan's actions as indiscriminate, accusing Pakistan of [shelling and killing](#) civilians in Poonch, J&K province, on May 8, 2025. Accounts posted AI-generated images containing slogans like “All Eyes on Poonch” (reusing international slogans like “[All Eyes on Rafah](#)” in the Israel-Gaza conflict), as seen in **Figures 57 and 58**, almost certainly to appeal to international audiences and call for the suspension of international aid to Pakistan by using the hashtag #frombeggingtobombing (**Figure 59**). Pakistan Prime Minister Shehbaz Sharif [announced](#) in January 2025 that the country would receive \$20 billion in loans from the World Bank over the coming decade, making this substantial financial aid a likely target of pro-Indian influence narratives.



Figures 57, 58, and 59: AI-generated images posted by Hidden Charkha accounts on May 11, 2025
(Source: Recorded Future)

Supporting Cyber Escalation

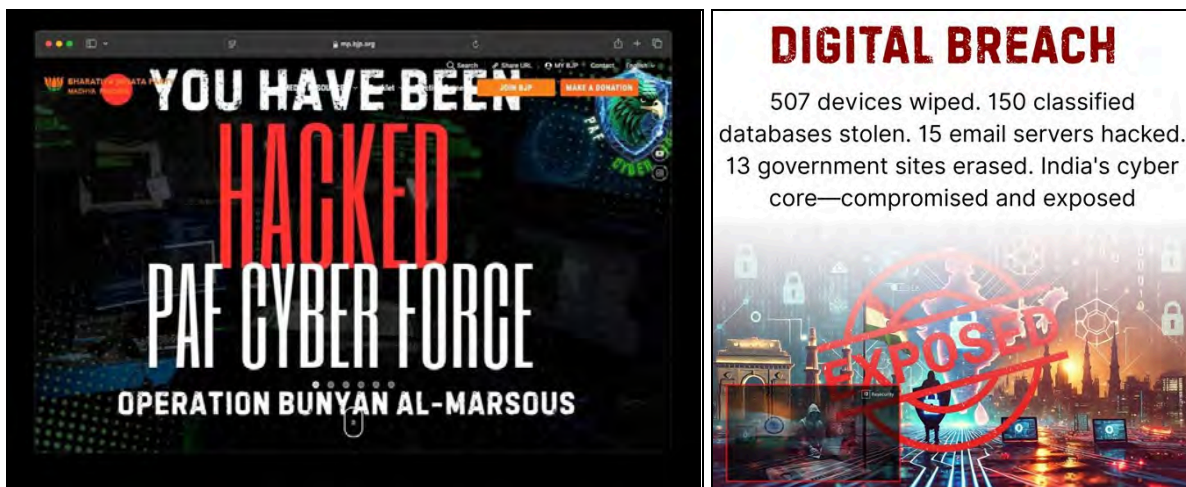
Insikt Group observed limited instances of Hidden Charkha and Khyber Defender amplifying claims of cyber attacks targeting India and Pakistan by hacktivist and state-sponsored threat actors following the Pahalgam attack. These networks almost certainly attempted to amplify the effectiveness and impact of hacktivist and state-sponsored [cyberattacks](#) to strengthen nationalist sentiment in the midst of kinetic escalation between the two countries, but often amplified unconfirmed claims by national media outlets and low-credibility hacktivist groups.

Both networks included unconfirmed claims on social media as part of their posts. On May 6, 2025, Hidden Charkha accounts amplified Indian Cyber Force (ICF)'s unconfirmed claims on social media that the hacktivist group had compromised "over 1,000+ cameras" in Pakistan, allegedly gaining access to surveillance footage in government facilities, industrial zones, private corporations, schools, and banks. One Hidden Charkha account amplifying the video lauded "Indian hackers' precision" while stating that "when you plot terror, expect cyber firepower!" likely in an attempt to capitalize on ICF's claims to amplify nationalist sentiment (**Figure 60**).



Figure 60: Hidden Charkha post amplifying a video from Indian Cyber Force claiming to have compromised surveillance cameras in Pakistan (Source: Recorded Future)

Khyber Defender accounts also almost certainly attempted to amplify unconfirmed claims of cyber attacks on Indian government infrastructure. On May 10, 2025, Khyber Defender accounts posted screenshots depicting a defaced website affiliated with the BJP alongside text stating that the website had been compromised by the PAF's "Cyber Force" (likely [in reference](#) to the PAF's Cyber Command) as part of Operation Bunyan-Al-Marsous (**Figure 61**). One account also very likely attempted to exaggerate the effects of cyberattacks by claiming, for example, that "India's cyber core" (**Figure 62**) and "70% of [India's] Northern grid" had been compromised, using hashtags like #infrastructureblackout, #griddownindia, #scadahacked, #powercollapse, and #logisticsparalyzed. The claim likely refers to [unconfirmed reports](#) by Pakistani media that Pakistani armed forces had compromised Maharashtra State Electricity Transmission Company (MAHATRANSCO), a major state-owned electricity transmission company. Khyber Defender accounts also claimed successful cyberattacks against Hindustan Aeronautics Limited, the Unique Identification Authority of India (UIDAI), the IAF, and the Election Commission of Maharashtra. The attacks remain unconfirmed in their scope and impact.

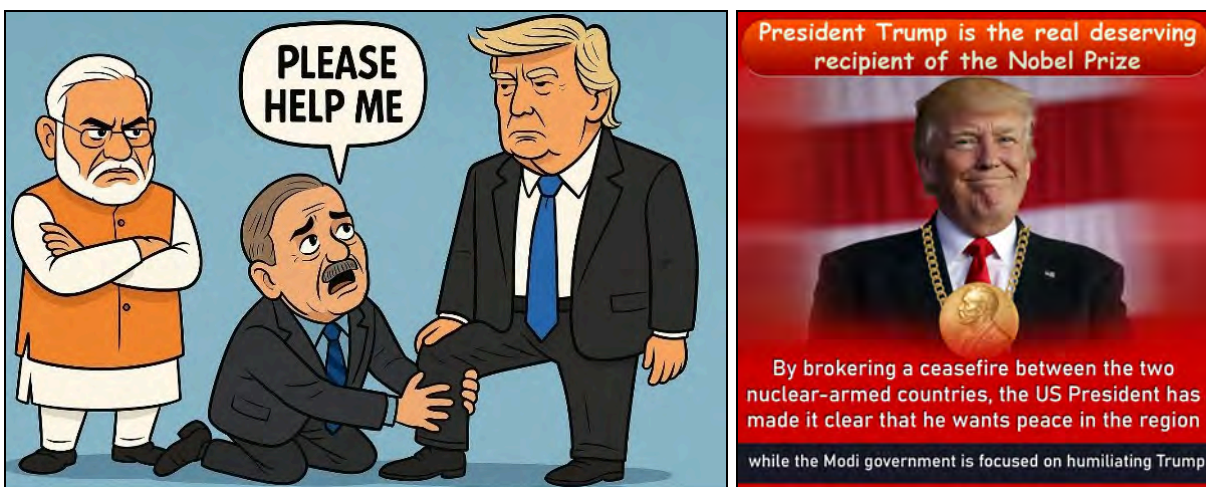


Figures 61 and 62: Khyber Defender content amplifying data breaches targeting the Indian government (Source: Recorded Future)

Ceasefire and Aftermath

As conventional kinetic operations escalated between May 7 and 10, 2025, members of the international community [sought](#) to [intervene](#) in an [effort](#) to [reduce](#) tensions and encourage restraint. On May 10, 2025, India and Pakistan [announced](#) a US-brokered ceasefire, shortly after the beginning of Pakistan's Operation Bunyan-Al-Marsous. As the ceasefire took hold, Hidden Charkha greatly increased its operational tempo, and Khyber Defender maintained the operational tempo seen during the kinetic escalation phases of the conflict. Both networks attempted to rapidly establish narratives promoting India and Pakistan's respective military successes and technological sophistication and to undermine either India or Pakistan on the global stage. Both networks also promoted the #ceasefireviolation hashtag in the immediate days following the announcement to accuse either India or Pakistan of violating the agreement, echoing [similar accusations](#) made by both governments.

Both Hidden Charkha and Khyber Defender attempted to exploit the US's diplomatic intervention in brokering the ceasefire agreement to further undermine India's or Pakistan's international and diplomatic credibility. Hidden Charkha accounts accused Pakistan of asking the US to broker the ceasefire in the face of mounting military failures, while attempting to gauge Indian social media users' sentiment on the ceasefire (**Figure 63**). Meanwhile, Khyber Defender praised US President Donald Trump for brokering the agreement, calling for him to receive a Nobel Peace Prize (using hashtags like #trumpfornobel and #trump_nobel_peace), as seen in **Figure 64**.⁴ Khyber Defender accounts also accused India's "elites" of "mocking" and "ridiculing" Trump's ceasefire (which allegedly shows their intent to prolong the conflict), while the pro-Pakistani network likely attempted to curry favor with the US president.



Figures 63 and 64: Hidden Charkha (left) and Khyber Defender (right) content following the announcement of a US-brokered ceasefire agreement (Source: Recorded Future)

⁴ On June 21, 2025, the Pakistani government actually [nominated](#) President Trump for the Nobel Peace Prize.

Despite the ceasefire agreement, both Hidden Charkha and Khyber Defender continued attempting to assert the technological superiority of India and Pakistan, respectively, and used the conflict's aftermath as proof of the other country's relative lack of military sophistication. Hidden Charkha accounts reported that Chinese defense companies' stock prices fell following the ceasefire after promoting narratives questioning the effectiveness of Chinese-made equipment used by Pakistan's armed forces, such as PL-15 missiles, which were made by Zhuzhou Hongda Electronics (Figure 65), and J-10 fighter jets, which were made by AVIC Chengdu (Figure 66). Meanwhile, Khyber Defender accounts amplified a speech by Pakistani PM Shehbaz Sharif to state that "the Air Force's use of modern technology sent a lasting warning the adversary will remember for generations" and attempted to undermine confidence in Rafale jets made by French company Dassault Aviation (Figure 67).



Figures 65 and 66: Screenshot of Chinese defense stocks following the ceasefire announcement posted by Hidden Charkha accounts (Source: Recorded Future)



Figure 67: Image shared by Khyber Defender accounts attempting to ridicule Indian Rafale jets (Source: Recorded Future)

Mitigations

- Customers can use the following queries to monitor Hidden Charkha and Khyber Defender activity, leveraging Recorded Future AI to summarize and track emerging narratives.
- Businesses operating in India and Pakistan should monitor ongoing influence narratives to understand national sentiment on major political and geopolitical issues, and track narratives perpetuated by CIB networks to measure attempts at managing conflict escalation.
- International news media outlets covering emerging conflicts should monitor influence content from known influence networks attempting to abuse their brand. Such abuse increases reputational risks and erodes consumer trust, potentially deterring advertisers and inflicting financial harm on the impersonated organizations.
- Governments tracking regional conflicts should monitor local and regional influence networks to track amplified narratives supporting conflict escalation during kinetic combat operations. Understanding influence networks' TTPs and narratives increases governments' resilience against the convergence of geopolitical, cyber, and influence threats.

Outlook

Hidden Charkha and Khyber Defender will almost certainly continue operating in alignment with the domestic and foreign policy objectives of the Indian and Pakistani governments, respectively. While Insikt Group was unable to determine the exact degree of state control or affiliation with these networks, we assess that patriotic sentiment will remain an important driver in aligning future campaigns with their governments, even if these networks are operated by non-state-sponsored threat actors.

Should a new kinetic conflict emerge between India and Pakistan, we expect these networks to resume the operational tempo observed during the standoff in April and May 2025, which amounted to over 1,000 posts daily at its peak. The networks will almost certainly continue amplifying narratives and content from national media outlets and government PR entities, in addition to opportunistically amplifying and exaggerating misleading claims and forged documents seeded by prominent social media accounts and hacktivist groups. While the networks were almost certainly unsuccessful in shaping domestic or international public opinion, the adoption of new procedures, such as using generative AI to generate original text and visual content, will likely help these networks cross language barriers and design consistent, more engaging content.

At a more strategic level, Hidden Charkha and Khyber Defender's activity during an escalating kinetic conflict demonstrates the potential role of covert influence networks in inflating operational success, strengthening national cohesion, and establishing a moral high ground to frame conventional kinetic actions as justified defensive operations. Influence networks can help reinforce perceptions of technological superiority and precise military capabilities by demonstrating each state's ability to conduct restrained, proportional strikes, which is almost certainly necessary for maintaining

international credibility and diplomatic support. Conversely, covert influence networks will also likely be used to undermine adversary narratives concerning tactical outcomes (such as airstrikes or downing enemy aircraft), cloud the online information environment, complicate battle damage assessment, and counter attribution claims on terrorist attacks.

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

Learn more at recordedfuture.com