HOSTILE SIGNALS

How Piracy Platforms Give Terrorist Organizations and State Adversaries a Back Door into American Homes

An Investigative Report by

DIGITALCITIZENSALLIANCE
a safer internet is a better internet

risk3sixty

September 2026

Table of Contents

Executive Summary

Terrorist organizations and state adversaries - including Hezbollah, Hamas, the Houthis, and the Iran-backed militants Kata'ib Hezbollah, organizations that have launched attacks on U.S. targets and are collectively responsible for the deaths of hundreds of Americans - are reaching U.S. audiences through the same illicit piracy streaming services that supply bootlegged movies, TV shows, and sports, a joint Digital Citizens/risk3sixty investigation has found.

Each of these terrorist organizations is subject to sanctions, or a federal domain seizure meant to keep their propaganda programming out of the United States. Piracy platforms have put it back with U.S.-based connections that can be accessed for about $15 a month. A piracy subscription has restored what two decades of federal action removed.

National security officials, policymakers and citizens alike should be concerned. Piracy platforms have created a new avenue for terrorist organizations and state adversaries to distribute recruitment messaging to U.S. audiences, including content intended to inspire acts of violence.

The 2026 Annual Threat Assessment by the Director of National Intelligence warned that adversaries are prioritizing the spread of propaganda in the United States: "In response to setbacks to their capabilities that have mitigated the threat of large-scale, complex attacks and reinforced the regional focus of the largest groups, Islamist terrorists have shifted attention to executing information operations to spread propaganda and inspire or enable individuals located in or with access to the West."

There is precedent for that concern. Ali Kourani, a naturalized U.S. citizen living in the Bronx, was convicted in 2019 on eight counts for conducting surveillance on New York targets - federal buildings, JFK Airport, National Guard armories - on behalf of Hezbollah's Islamic Jihad Organization. Federal prosecutors pointed the court to the propaganda on Kourani's laptop, including video published by Al-Manar, which he had searched for and followed, as evidence of his violent intentions and the risk he would return to terrorism. He was sentenced to 40 years.

At the heart of this investigation is the U.S. government's post 9/11 efforts to keep terrorist organizations and other state actors from being able to attack, finance, recruit within, or otherwise project influence into the country.

When Hezbollah's Al-Manar was stripped of its U.S. satellite feed in 2004, a State Department spokesperson put the rationale in these terms: "We don't see why here or anywhere else a terrorist organization should be allowed to spread its hatred and incitement through the television airwaves." Two years later, a man prosecutors called "Hezbollah's man in New York City" was arrested for conspiring to violate the International Emergency Economic Powers Act by providing New York-area customers with the Hezbollah-operated channel. Javed Iqbal was convicted in 2008 of providing material support to a foreign terrorist organization and sentenced to 69 months in prison.

The United States and other Western governments methodically blocked satellite, cable, and social-media distribution of adversaries from digitally invading their borders.

Piracy operators provide a platform for banned or sanctioned broadcasters that a website cannot. Content from terror organizations may be findable online by someone determined to locate it - but no one stumbles onto Al-Manar's website.

The extent to which piracy networks enable terrorist organizations to bypass U.S. restrictions was not fully known until this investigation. As part of the Digital Citizens/risk3sixty investigation, researchers surveyed piracy-based IPTV provider sites and checked each for the presence of channels tied to designated terrorist organizations or hostile foreign states. The investigation found numerous instances of piracy IPTV services carrying these broadcast outlets.

Every service was reached through a U.S.-based Internet connection.

This investigation examined 25 piracy platforms and found terrorist broadcasters on 17 of them (68 percent). Given that there are thousands of piracy storefronts in the United States, that raises the possibility that the broadcast outlets of terrorist-affiliated broadcasters and other U.S. adversaries are widely available across platforms.

Al-Manar, the broadcast outlet of Hezbollah, which has a long history of attacking American targets and is responsible for at least 291 U.S. deaths over decades, is carried by all 17 piracy platforms identified to allowing carriage.

It is important to note that access doesn't equate to viewership. And terrorist organizations continually look for ways to influence and even radicalize Americans. For example, a 2018 Digital Citizens report revealed how social media platforms such as Google+ became a haven for ISIS to recruit members and post graphic content.

At their peak of conventional satellite distribution, Al-Manar claimed a worldwide daily audience of roughly 10 million, while Al-Aqsa TV was estimated in 2010 to reach 20 million viewers across Europe, the Middle East, and North Africa.

When European regulators moved against Al-Aqsa's satellite distribution, the station itself said the action would cost it 70 percent of its audience. Although those estimates were not independently audited, they demonstrate the scale these broadcasters could achieve when given access to international distribution infrastructure.

They also illustrate why alternative distribution channels matter. Restrictions that remove these broadcasters from conventional satellite and cable systems can reduce their potential audience; carriage on illicit piracy services provides another means of distribution that can potentially restore some of that lost access by placing the channels back into television packages available to U.S. subscribers.

This is also not the only national security threat piracy poses. In recent months, there has been growing alarm about how threat actors such as China and Russia are gaining control – through piracy devices pre-loaded with malware among other ways - of Americans' home devices to launch attacks. Residential proxy networks hinder U.S. law enforcement and national security agencies tracking criminals and terrorists.

It should not be lost on anyone that piracy enables U.S. adversaries to both skirt a ban on broadcasting their ideology into the United States *and* launch cyberattacks against the country. That is quite an effective use of piracy by foreign adversaries with stated goals to do harm to the United States.

These findings reinforce the need for the United States to adopt measures to prevent overseas piracy networks from operating in the country.

Piracy presents a spectrum of risks: to consumers, who are baited to watch free content so their devices can be infected with malware; to national security, as state actors and criminals exploit piracy devices to take over millions of American devices and use them to wage cyberattacks against the United States; and now, evidence that terrorist organizations and other adversaries have regained access to U.S. homes.

There is a potential solution. Site-blocking is a legal process to block foreign websites from accessing the United States. While it's generally designed to combat infringers, it could address the problem of terrorist-linked broadcasters being distributed through piracy services by disrupting the piracy networks that carry their content.

The 25th anniversary of the 9/11 attacks is days away. It should be a reminder that vigilance in all ways - whether guarding against physical attacks or blocking adversaries from being able to spread propaganda - is critically important.

Foreign Adversaries Leveraging Piracy Against the United States

The organizations that control the terrorist broadcasters cited in this report are responsible for the deaths of at least 376 American citizens and service members in individually documented attacks. That figure excludes the Pentagon's separate assessment that at least 603 U.S. personnel were killed in Iraq between 2003 and 2011 by Iran-backed militias, including Kata'ib Hezbollah, owner of Aletejah TV. Hezbollah also initiated a hostage-taking campaign that ultimately held an estimated 25 Americans, including some who were murdered.

It was the 9/11 attacks that prompted the U.S. government to block these organizations' domestic access. Just weeks after the 2001 attacks, an executive order gave Treasury the authority to block the property and transactions of anyone who commits, threatens, or supports terrorism - the same authority Treasury would use, in 2006, to designate Al-Manar a Specially Designated Global Terrorist entity.

This instrument was never limited to money and weapons. From the outset, U.S. policymakers treated a terrorist organization's ability to broadcast as a threat.

It wasn't just the United States. A French court in December 2004 ordered Eutelsat to stop carrying Al-Manar within 48 hours. In March 2005, Dutch regulators forced New Skies Satellites to drop it for lacking a Dutch license, at a Brussels meeting where EU regulators agreed to step up action against broadcasts inciting hatred.

Less than a decade later, Eutelsat and Intelsat stopped carrying several Iranian channels. Over time, other outlets tied to organizations deemed terrorists, such as Al-Aqsa TV (Hamas), were added to the U.S. banned list. Similarly, when Iran-aligned Iraqi militia media and Iranian state outlets moved onto the open web, the Department of Justice seized Aletejah's domains in September 2020 and, in June 2021, 33 domains operated by the Islamic Radio and Television Union network.

What these actions did not anticipate is the emergence of piracy operators. Just as piracy networks illicitly bundle together movies and TV shows they don't have the right to distribute, terrorist organizations and others can circumvent the practical effect of broadcast restrictions when banned channels are bundled together with hundreds or thousands of stations on a piracy service.

Piracy services don't supply availability; they supply placement. These channels sit in the same lineup as the sports and movies the subscriber paid for.

That placement is exactly what U.S. regulators, prosecutors, and satellite carriers have denied these outlets for the past two decades. Piracy operators have handed them back the channel space the U.S. government took away.

Earlier Digital Citizens research focused primarily on the threat to American users posed by piracy operators. What started as research into how piracy content is used as bait to infect devices and exploit credit card information grew into an exploration of how the piracy ecosystem had grown into a $2 billion enterprise that mimics organized crime behavior.

But in 2026, there are new concerns about how piracy can pose a national and economic security threat. In January 2026, when one of the world's largest residential proxy networks was dismantled, it was discovered that 550 threat groups, including state-sponsored actors from Russia, China, and Iran, relied upon it to launch cyberattacks. A residential proxy network routes Internet traffic through real devices - home computers, phones, routers - that belong to ordinary people, rather than through servers sitting in a data center. In many cases those Internet connections are harvested by bad actors through networks infected by compromised piracy devices.

State and state-linked actors use residential proxy networks to camouflage their attacks by routing intrusion traffic or espionage-related reconnaissance through ordinary Americans' home IP addresses. The FBI has identified streaming devices advertised as unlocked or offering free content as an indicator of infection by malware that enrolls home connections into exactly those networks.

This report focuses on how piracy sites provide the means to get around these restrictions. Digital Citizens and cyber investigation firm risk3sixty identified known terrorist organizations and other U.S. adversaries and known piracy IPTV services.

risk3sixty investigators signed up for piracy services to gain access to thousands of live channels and tens of thousands of videos on demand. Investigators used a U.S.-based connection throughout. Each accessible service's channel list was checked against broadcast outlets tied to designated terrorist organizations or hostile foreign states.

Those broadcast outlets fall into two categories. The tiers below represent the legal status of each as well as the organizations by category:

Tier 1 — Designated Terrorist Entity, Banned Outright: The platform itself, or its parent organization, is a U.S.-designated Foreign Terrorist Organization (FTO) or Specially Designated Global Terrorist entity. Piracy access to a Tier 1 outlet constitutes a circumvention of a terrorism-related broadcast ban.

Al-Manar TV — Lebanon (Hezbollah)

Ownership / Affiliation: Owned and operated by Hezbollah as its official satellite broadcaster. Al-Manar anchors are documented reading official Hezbollah ("Islamic Resistance") combat communiqués live on air - evidence the channel functions as a direct operational mouthpiece for the organization, not merely a sympathetic outlet.

U.S. Deaths Linked to Affiliated Terrorist Organization: At least 291 deaths, from 1983 to 2007.

Legal Basis for Restriction: Added to the State Department's Terrorist Exclusion List in December 2004; separately designated a Specially Designated Global Terrorist entity by the U.S. Treasury Department on March 23, 2006, under Executive Order 13224. Treasury's designation cited Al-Manar's role raising funds for Hezbollah, publicizing recruitment calls, and employing Hezbollah operatives under cover of the broadcaster.

Al-Manar is a full-production, 24-hour satellite network with anchors, field reporting, and original programming, all framed through Hezbollah's ideological messaging. It is the original benchmark case for U.S. terrorist-broadcaster designation and remains widely available via regional satellites, Internet streaming, and - as documented in this report's access testing - U.S.-accessible piracy IPTV services.

Documented Piracy Access (U.S.): The most-carried banned outlet in this review. Found on numerous piracy IPTV services accessed during platform testing, including Belitvision, FomnyBox, Fosto IPTV, Freeintertv, Glow IPTV, Lion OTT, Online-television, OTTOcean, PixelPulse IPTV, Public IPTV, Rapid Live, RapidIPTV Stream, Sansat VIP, Smarter IPTV, TVIVU, Wish IPTV.

Al-Aqsa TV — Gaza (Hamas)

Ownership / Affiliation: Owned and operated by Hamas as its primary broadcast outlet.

U.S. Deaths Linked to Affiliated Terrorist Organization: An estimated 71 deaths, from 1993 to 2023.

Legal Basis for Restriction: Hamas has been a U.S.-designated Foreign Terrorist Organization since 1997. Al-Aqsa TV is separately designated in its own right: on March 18, 2010, the U.S. Treasury Department designated Al-Aqsa Television and the affiliated Islamic National Bank as Specially Designated Global Terrorists under Executive Order 13224, blocking any assets under U.S. jurisdiction and prohibiting U.S. persons from transacting with them. In announcing the action, Treasury stated that it would not distinguish between a business financed and controlled by a terrorist group, such as Al-Aqsa Television, and the terrorist group itself.

Al-Aqsa TV has served as a central tool for Hamas governance and mobilization in Gaza, including news coverage, ideological programming, and children's programming that has drawn international condemnation. Despite repeated strikes on its production facilities across multiple conflicts, the station has consistently resumed broadcasting within hours or days from mobile or improvised locations.

Documented Piracy Access (U.S.): Belitvision, Lion OTT

Al-Masirah — Yemen (Houthis / Ansar Allah)

Ownership / Affiliation: Houthi-affiliated network headquartered in Beirut; chairman Mohammad Abdulsalam serves as the group's chief negotiator and spokesperson.

Threat to U.S. Forces and Commerce: Houthi forces have conducted sustained missile and drone attacks against U.S. Navy vessels and personnel in the Red Sea and Gulf of Aden since November 2023 and have targeted more than 100 merchant vessels transiting the corridor. Al-Masirah aired a Sana'a rally in which children pledged to serve as soldiers of Abdul-Malik al-Houthi, praised martyrdom, and recited the 'Death to America' slogan."

Legal Basis for Restriction: The Houthi movement (Ansar Allah) was redesignated a Foreign Terrorist Organization by the State Department on March 4, 2025, reversing a prior removal. Treasury's accompanying March 2025 sanctions package targeted Houthi leadership and affiliated media figures, including Al-Masirah's chairman.

Al-Masirah, operating in close coordination with Hezbollah's media apparatus, serves as the official mouthpiece for Houthi governance in Sana'a, broadcasting battlefield footage, political speeches, and anti-Western messaging to domestic and international audiences.

Documented Piracy Access (U.S.): Belitvision, Lion OTT, Online-television, OTTOcean, PixelPulse IPTV, Public IPTV, Sansat VIP, TVIVU, Wish IPTV

Aletejah TV — Iraq (Kata'ib Hezbollah)

Ownership / Affiliation: Owned and operated by Kata'ib Hezbollah as a project of the militia's media office.

"Death to America."

— On-air chant, Aletejah TV broadcast, carried via the piracy service OTTOcean.

U.S. Deaths Linked to Affiliated Terrorist Organization: At least 14 deaths, from 2011 to 2024.

Legal Basis for Restriction: Kata'ib Hezbollah has been a U.S.-designated FTO and Specially Designated National since July 2, 2009. The Department of Justice seized the Aletejahtv.com and Aletejahtv.org domains, along with the militia's own kataibhezbollah.com domain, in fall 2020, for operating without the Treasury Department license required of a designated entity's U.S.-based services.

Aletejah is one of the more developed outlets within Iran's Islamic Radio and Television Union (IRTVU) network, an IRGC-linked umbrella that supports militia-run media across Iraq. Its direct ownership by an FTO-designated militia places it on firmer legal footing than other IRTVU-linked channels that lack a direct FTO nexus.

Documented Piracy Access (U.S.): OTTOcean

Tier 2 — Sanctioned / Domain-Seized, Not Terrorist-Designated: The platform or its parent has been targeted by Treasury Department Office of Foreign Assets Control sanctions and/or DOJ domain seizure, but the outlet itself does not appear on the banned list. Piracy access to a Tier 2 outlet constitutes evasion of a sanctions or enforcement action.

Al-Alam TV — Iran (Islamic Republic of Iran Broadcasting)

Ownership / Affiliation: Arabic-language satellite news channel launched in 2003 and operated by the Islamic Republic of Iran Broadcasting World Service, the international arm of Iran's state broadcasting monopoly.

Legal Basis for Restriction: Al-Alam's parent, IRIB, was designated by the U.S. Treasury Department on February 6, 2013 under Executive Order 13628, for restricting or denying the free flow of information to or from the Iranian people, an action authorized by the Iran Threat Reduction and Syria Human Rights Act of 2012 that placed IRIB on the Specially Designated Nationals and Blocked Persons List, blocking its assets under U.S. jurisdiction and prohibiting U.S. persons from transacting with it. The Department of Justice seized Al-Alam's domain on June 22, 2021, as one of 33 websites used by the Iranian Islamic Radio and Television Union.

Documented Piracy Access (U.S.): FomnyBox, Freeintertv, Online-television, OTTOcean, Public IPTV, TVIVU

Al-Ghadeer TV — Iraq (Badr Organization)

Ownership / Affiliation: Owned by the Badr Organization, a political party with an armed wing formally integrated into Iraq's state-sanctioned Popular Mobilization Forces (PMF).

"Their blood will not go in vain, and we will certainly avenge them. Those who yesterday were sending car bombs and suicide bombers have today returned to send missiles."

— On-air speaker, Al-Ghadeer TV, in coverage of a Popular Mobilization Forces commemoration event framed around the "Saudi American aggression."

Legal Basis for Restriction: Department of Justice seized Al-Ghadeer's domain, alghadeer.tv, on November 4, 2020, as one of 27 domains found to be operating on behalf of Iran's Islamic Revolutionary Guard Corps in violation of the International Emergency Economic Powers Act and the Iranian Transactions and Sanctions Regulations. The IRGC has been a designated Foreign Terrorist Organization since April 2019. According to the seizure affidavit, Al-Ghadeer's site carried anti-U.S. and anti-Israel content and pro-Iranian messaging, including opposition to U.S. sanctions. The designation runs through the IRGC rather than through the channel's owner, which is why Al-Ghadeer falls short of the Tier 1 standard.

Documented Piracy Access (U.S.): OTTOcean

The Piracy Sites That Let Foreign Adversaries Broadcast into the U.S.

It is not surprising that piracy platforms don't hesitate to give terrorist organizations the ability to broadcast into American homes. After all, these are the same networks that steal content to offer to users – only to then infect those users' devices with malware because illicit actors pay them to do so. And most of the piracy operators are overseas, so their primary interest in the United States is financial.

In the case of piracy, crime pays – well. It's a $2 billion illicit ecosystem. Here are the most prominent sites found during the investigation:

Sansat VIP

Claims to have operated since 2015 across a dozen-plus domains, with wildly inconsistent scale claims (100,000 channels on one storefront, 20,000+ on another). The credit-based reseller economy ($65 for 60 credits up to $3,500 for 6,000 credits, plus a $35/year retail tier) is the important detail - it means the entity actually carrying Al-Manar is the upstream server operator, while hundreds of resellers who may never look at the channel list are the customer-facing side of the brand. There are indications that the platform traces to Chinese IPTV-panel wholesalers.

Wish IPTV

Targets francophone and Anglo-Irish markets (Ireland, France, Belgium, Canada, UK, US). Infrastructure is the textbook profile: Namecheap registration plus Cloudflare fronting. The registrant is shielded behind a privacy proxy based in Iceland, and ScamAdviser scored the site 17/100, flagging it as a likely "façade."

Lion OTT

The most commercially developed. It has an Android app rather than relying on third-party players, and precise inventory figures (19,635 live channels, 98,207 movies, 24,343 series). It's the only platform here with documented enforcement action - Australian ISPs reportedly sent warning letters to subscribers. It carries Al-Manar, Al-Aqsa TV, and Al-Masirah simultaneously.

Smarter IPTV

The "Smarters" branding is a deliberate free ride on IPTV Smarters Pro, a widely used legitimate player app.

PixelPulse IPTV

The 50,000-channel, 200,000-VOD claim is the highest figure of any platform reviewed. Its site includes a fake "PixelPulse TV®" trademark and "Anti-Freeze™" branding – reflecting a consistent pattern among IPTV sites of lifting legitimate-business visual grammar – SSL badges, money-back guarantees, "official website" language – to try to add legitimacy.

Glow IPTV

Main storefront claims 18,000+ channels and 80,000+ VOD, but a reseller listing describes a much smaller 7,000-channel package priced $10–$170 broken into sports tiers by country. It includes designated channels within an 'Arab Countries' package alongside numerous other channels.

Fosto IPTV

Not a subscription server but an activation-code app, the successor to the Volka/Wolf family - a reseller states that after problems with Wolf, Wolf X, and Wolf Pro, the same operator launched Fosto as a replacement. Volka was a prominent illegal IPTV app in France explicitly identified as unauthorized for Canal+, RMC Sport, and beIN Sports content. This rebrand-after-enforcement pattern connects directly to France's Arcom regime, which can now order ISPs to DNS-block illegal IPTV platforms.

Belitvision

It claims 31,000+ channels and 170,000+ titles. Its listed contact number carries a U.S. country code, and support runs through a plain Gmail address, which is inconsistent with its Belgian presentation. It is a three-designated-channel carrier (Al-Manar, Al-Aqsa TV, Al-Masirah).

Rapid Live

The numbered subdomains found on some variants (www15.rapidiptv.org) of Rapid piracy sites are evidence the operator has burned through more than a dozen prior host configurations, likely an answer to domain seizure and DNS blocking.

OTTOcean

It has the most extensive domain sprawl with ten-plus storefronts. Because OTTOcean carries both Aletejah and Al-Ghadeer - outlets whose own domains DOJ has already seized - it presents the clearest documented overlap between a piracy storefront and programming the Department has previously moved against.

These piracy networks are now providing a distribution pathway between banned broadcasters and U.S. viewers. Where operators knowingly distribute content from designated terrorist entities in violation of applicable law, their conduct warrants scrutiny by U.S. authorities.

The Path Forward

Piracy networks can be a novel way for broadcasters tied to terrorist organizations to get around a ban on reaching the U.S. audiences. Confronting it requires a multi-pronged approach. As demonstrated in this report, piracy enables some of the most well-known and dangerous terrorist organizations to broadcast into the United States. It's another avenue to spread their ideology and potentially recruit Americans. The 2026 Annual Threat Assessment underscores why that is so dangerous.

By 2016, the FBI reported several hundred open Islamic State–related investigations across all 50 states. The George Washington University Program on Extremism has since catalogued 246 individuals charged in U.S. courts on Islamic State–related offenses, with 1 in 4 of them accused of plotting domestic attacks.

The legal architecture built after 9/11 to keep designated terrorist entities out of American commerce already exists but has never been pointed at the piracy distribution channels this report documents. The recommendations below start with what federal agencies and private intermediaries can do under authority they already hold, and end with the legislative remedy now before Congress.

Treasury Sanctions Advisory. Al-Manar and Al-Aqsa TV are Specially Designated Global Terrorist entities. Under Executive Order 13224, U.S. persons are prohibited from transacting in their property and interests in property.

That prohibition is not theoretical: in 2008, Javed Iqbal was convicted of providing material support to a foreign terrorist organization for delivering Al-Manar to New York-area customers. What has changed since Iqbal is scale.

Treasury regularly issues sector-specific advisories alerting industries to sanctions exposure. An advisory directed at piracy operators, resellers, and the payment processors and hosting providers that serve them would put the industry on notice that carriage of Specially Designated Global Terrorist-owned broadcasters creates sanctions exposure.

Justice Department Domain Seizures. DOJ has taken down this programming before. It seized Kata'ib Hezbollah's Aletejah domains in September 2020, alghadeer.tv that November as one of 27 Iranian

Islamic Revolutionary Guards domains, and dozens more in June 2021. Those cases were straightforward: a designated entity cannot obtain U.S. domain services without a Treasury Department license. Piracy storefronts are harder. They aren't designated entities, so any case turns on what operators knew and kept carrying. But the predicate now exists - named services, named channels, confirmed U.S. access.

DOJ and the FBI should determine which operators fall within U.S. jurisdiction, put them and their registrars, hosts, and payment processors on formal notice, and seize where carriage continues afterward. No new statutory authority is needed.

Site-blocking Legislation. Site-blocking is a legal process to block access from the United States to foreign websites. While it's generally designed to combat infringers, it could address the problem of terrorist-linked broadcasters being distributed through piracy services by disrupting the piracy networks that carry their content.

Proposals before Congress focus on a judicially supervised remedy aimed only at large-scale foreign piracy operations. Under the frameworks under discussion, a copyright owner must first persuade a U.S. district court that a foreign site is dedicated to infringement before it may seek an order directing service providers to restrict access. It's worth underscoring that while copyright owners drive the petition process, if the result is the blocking of piracy sites carrying the outlets of terrorist organizations, then site-blocking leads to a national security benefit.

In 2024, Digital Citizens and IP House, a leading IP enforcement organization, conducted a study of how site blocking had been enacted in over 50 countries. It found that in those countries, site-blocking is successful and proportionate and does not harm Internet safety.

The organizations behind these broadcasters have found a distribution channel that federal policy did not anticipate. Closing it does not require reinventing U.S. policy. It requires pointing the tools already built - sanctions authority and domain seizure - at a distribution channel they were never aimed at and giving courts the site-blocking authority to reach platforms that sit beyond U.S. law enforcement.

"Never Forget" became the enduring rallying cry for those who experienced the 9/11 attacks. It's also a reminder to never let the terrorists back in, in any form.

Methodology

- **Platform-access testing.** Researchers from risk3sixty examined 25 piracy-based IPTV provider websites and attempted to access each one's channel catalog through whatever sign-up process the service offered - a free trial, a paid subscription, or open registration - using a U.S.-based connection throughout. Each accessible service's channel list was checked against broadcast outlets tied to designated terrorist organizations or hostile foreign states.

- **Broadcast content review.** Where terrorist-linked or hostile-state channels were identified on a piracy service, translated broadcast segments and publicly reported statements from those same outlets were reviewed to characterize the nature of the content being distributed separately from, and in addition to, the access-testing exercise.

- **Every broadcast-content citation** is content aired directly by catalogued platforms named in the reviewed source material, including Al-Manar, Al-Aqsa TV, Al-Masirah, Aletejah, or Al-Ghadeer.

Methodology Footnote: U.S. Deaths Attributed to Terrorist Organizations Cited

The figure of at least 376 U.S. deaths is a composite assembled by Digital Citizens from individually documented attacks attributed to three of the four organizations whose broadcasters appear in this report: Hezbollah (at least 291 deaths, 1983–2007), Hamas (an estimated 71 deaths, 1993–2023), and Kata'ib Hezbollah (at least 14 deaths, 2011–2024). No U.S. deaths are attributed here to the Houthis, whose attacks on American vessels and personnel in the Red Sea and Gulf of Aden since November 2023 have not, to our knowledge, produced confirmed U.S. fatalities. The 376 total should therefore be read as covering three organizations, not all four.

The component figures are drawn from different kinds of sources, which apply different attribution standards. The Hezbollah figure rests principally on S.Res. 784 (118th Congress), introduced July 31, 2024, which enumerates Hezbollah attacks on Americans, and on contemporaneous accounts of the 1983 Beirut barracks and embassy bombings. The Hamas figure draws on the Department of State's October 2025 statement marking the second anniversary of the October 7 attack and on a tally maintained by the American Jewish Committee. The Kata'ib Hezbollah figure draws on organizational profiles maintained by the Wilson Center and United Against Nuclear Iran. Where sources conflicted, we used the lower figure. Where an attack was attributed to an organization by some sources and to an affiliate or umbrella coalition by others, we counted it only where the primary source named the organization directly.

This composite is deliberately conservative and is separate from — and does not incorporate — the Department of Defense's assessment that at least 603 U.S. personnel were killed in Iraq between 2003 and 2011 by Iran-backed militants, a category that includes Kata'ib Hezbollah. Because DoD's assessment covers a coalition of militias rather than named organizations, folding it into the composite would risk double-counting the Kata'ib Hezbollah figure while attributing to that group deaths caused by others. The two numbers are reported separately for that reason.

Relevant Links:

https://5g.wilsoncenter.org/article/profiles-irans-militia-allies-iraq

https://www.unitedagainstnuclearіran.com/report/kataib-hezbollah

https://www.state.gov/releases/office-of-the-spokesperson/2025/10/two-year-anniversary-of-october-7th-attack

https://www.ajc.org/news/how-many-americans-have-been-killed-by-hamas-before-and-after-october-7

https://www.congress.gov/118/bills/sres784/BILLS-118sres784is.htm

https://www.globalsecurity.org/security/ops/1983beirut.htm

Appendix A: Piracy IPTV Access Testing — Site Examples

Here is the list of piracy platforms reviewed that carried broadcast outlets affiliated with designated terrorist organizations or foreign adversaries. Services were accessed via a U.S.-based connection from May through August 2026.

Service	Terror/Hostile-State Content Found
Belitvision	Al-Aqsa, Al-Manar, Al-Masirah
FomnyBox	Al-Alam, Al-Manar
Fosto IPTV	Al-Manar TV
Freeintertv	Al-Alam, Al-Manar
Lion OTT	Al-Aqsa, Al-Manar, Al-Masirah
Online-television	Al-Alam, Al-Manar, Al-Masirah
OTTOcean	Al-Alam, Aletejah, Al-Ghadeer, Al-Manar, Al-Masirah
PixelPulse IPTV	Al-Manar TV, Al-Masirah
Public IPTV	Al-Alam, Al-Manar, Al-Masirah
Rapid Live	Al-Manar TV
RapidIPTV Stream	Al-Manar
Sansat VIP	Al-Manar, Al-Masirah
Smarter IPTV	Al-Manar
TVIVU	Al-Alam, Al-Manar, Al-Masirah
Wish IPTV	Al-Manar, Al-Masirah
Glow IPTV	Al-Manar
Icanlive	Al-Alam, Al-Manar

About Digital Citizens Alliance

The Digital Citizens Alliance is a nonprofit, 501(c)(6) organization that is a consumer-oriented coalition focused on educating the public and policymakers on the threats that consumers face on the Internet. Digital Citizens wants to create a dialogue on the importance for Internet stakeholders—individuals, government, and industry—to make the Web a safer place. Based in Washington, DC, the Digital Citizens Alliance counts among its supporters: private citizens, the health, pharmaceutical, and creative industries, as well as online safety experts and other communities focused on Internet safety. Visit us at www.digitalcitizensalliance.org.

About risk3sixty

risk3sixty is an elite boutique cybersecurity firm headquartered in the greater Atlanta area, serving clients nationwide with continuous threat exposure management (CTEM), threat intelligence, and proactive security services through its Armada Proactive Services practice.

Unlike software-only exposure management platforms that bury teams in unvalidated alerts, Armada embeds senior practitioners who run continuous threat intelligence, manually exploit findings to prove what's actually dangerous, and stay on every exposure until it's closed for good.

In addition, risk3sixty offers a comprehensive suite of services for CISOs, including internal audit, compliance, and GRC program optimization. Learn more about risk3sixty's proactive services at armada.risk3sixty.com