PIRACY ORGANIZED CRIME

How Global Piracy Networks Became Organized Crime Syndicates – And What Needs to be Done About it

A Joint Report by

Digital Citizens Alliance and IP House

DIGITALCITIZENSALLIANCE
a safer internet is a better internet

IP HOUSE

April 2026

Table of Contents

Executive Summary

If any aspect of the movie classic The Godfather ever accurately depicted La Cosa Nostra, those days are long over, undone by a Congress and law enforcement that finally acknowledged: organized crime wasn't a myth—it was a sophisticated criminal threat that existing laws couldn't effectively reach.

That recognition led to new laws, including the Racketeer Influenced and Corrupt Organizations Act, which gave law enforcement new tools to target criminal organizations and judges the discretion to impose long prison terms. By the 1980s, the so-called Five Families began a slow descent into also-ran status.

Organized crime didn't disappear. A diminished La Cosa Nostra now competes with Russian, Eastern European, and Asian syndicates for control of human trafficking, cyber fraud, and violence-for-hire. Mexican cartels flood American communities with fentanyl, methamphetamine, and cocaine. These organizations differ in structure and tactics but share the same DNA: profit as the motive, diversification as strategy, shell companies to mask operations, and money laundering to move illicit gains.

Now, a new flavor of organized crime has emerged: global piracy networks.

This isn't your grandfather's organized crime—centralized, hierarchical, and territorial. In 2026, organized crime is digital, decentralized, and borderless. The vast majority operate outside of the United States, creating enforcement challenges for law enforcement. But one thing hasn't changed: the focus on illicit profits, by any means and at any cost.

There have been indications since 2009 that organized crime and piracy networks have intersected, bringing together two illicit groups that flourish through diversification. And in recent years, law enforcement in the United Kingdom, Italy, Spain, and Southeast Asia have reported increasing interconnections between piracy and organized crime.

This report, entitled "Organized. Piracy. Crime.", based on a joint investigation by the Digital Citizens Alliance and IP House, is the first to pull together the full global picture of how closely connected organized crime and piracy networks have become. It also paints a picture of sophisticated piracy networks copying, and in many cases, refining the playbook (shell companies, money laundering, diversification) of organized crime.

This report is based on interviews with law enforcement agencies across the globe, a review of criminal cases that revealed links between piracy operations and known organized crime entities, as well as previous reports and news investigations. The sum total of this output details how piracy operators evolved from selling bootleg DVDs to sophisticated global networks leveraging stolen content to build a multibillion-dollar criminal ecosystem. And like their predecessors in organized crime, they ventured into drug trafficking, human trafficking, weapons smuggling, and other crimes.

In addition, the investigation shows how organized criminal networks have embraced piracy as an additional revenue stream. In notable cases, the criminal networks have morphed into the other, with the net result being substantial harm.

The evidence is substantial:

- European authorities in November 2024 dismantled what investigators called the continent's largest piracy operation - a network that generated $3.5 billion annually. When police executed coordinated raids across eleven countries, they seized not only $1.9 million in cryptocurrency and $46,000 in cash, but also drugs and weapons.
- In Spain, Operation Fake exposed a piracy enterprise that combined content theft with cryptocurrency mining, property fraud, drug trafficking, and industrial-scale money laundering—resulting in 30 arrests and $12.7 million in frozen assets. In addition, a law enforcement initiative named Operation Atria exposed piracy revenues moving through the same clandestine payment networks used for Iranian human smuggling and embargo evasion.
- Italy's Camorra—one of the nation's most powerful crime syndicates—targeted piracy networks, attracted by high margins, low risk, and a business model mirroring their traditional rackets. "The link with organized crime is quite explicit, between

dummy accounts and payments made via disposable Postepay cards, and is still the subject of investigations," reported Italian publication Money. "In Italy, millions of subscribed users are estimated, with as many enlisted as sellers and assistants (with advertisements even present on Facebook)." A former piracy operator turned informant, in an interview on Italian television, warned: "Those who pay for IPTV are funding the Camorra."

- In the United States, the KickassTorrents prosecution was pursued under racketeering and money-laundering frameworks, with prosecutors emphasizing the scale and organization of the operation. Similarly, the Sparks Group case invoked organized crime offenses and statutes, as enforcement agencies characterized the piracy network as a sophisticated transnational enterprise.

These revelations mark a fundamental shift. Over the past decade, investigations documented how piracy operators spread malware, facilitated credit card theft, and enabled terrorists to broadcast in the United States. But this is the first report to show how piracy networks have transformed into organized crime syndicates—meeting definitional criteria established by INTERPOL, Europol, and the United Nations.

If it operates like organized crime, launders money like organized crime, and diversifies into other criminalities like organized crime—it is organized crime.

The implications are urgent. Unlike other forms of organized crime, there is no cohesive national or global effort to combat piracy syndicates. Congress only made large-scale illicit streaming a felony in 2020. Law enforcement lacks adequate tools to target overseas operators who steal from Americans, infect their devices with malware, and fund the trafficking of human beings.

Those living overseas where organized crime and digital piracy have melded understand this better than those far removed from their activities. In countries such as the Philippines, Brazil, and India, a large majority of citizens recognize the links. Sixty nine percent of respondents in Brazil, 67 percent in India, and 63 percent in the Philippines connect the dots between organized crime and piracy, according to a global research study commissioned by the Digital Citizens Alliance and IP House. In other markets, such as the United

States (42 percent) and Spain (48 percent), for example, there remains less of a recognition of the role that organized crimes in digital piracy. Combined, over 5,000 respondents were surveyed across these countries.

The implication is difficult to ignore. In parts of the world where piracy flourishes, the public recognizes the criminal structures behind them. Yet in the markets that drive the demand for digital content and possess the greatest enforcement resources, the organized crime dimension of piracy remains less widely acknowledged.

That partly explains how digital organized crime thrives as it exploits fundamental asymmetries. Criminals operate across dozens of jurisdictions simultaneously while law enforcement remains bound by national boundaries, competing priorities, and resource limitations. And criminal networks can pivot to new technologies, platforms, and jurisdictions within days. Legislative responses take months or years.

Decades ago, U.S. policymakers faced similar challenges with La Cosa Nostra. They could continue with inadequate tools, or they could recognize the threat and respond accordingly. They chose to act.

Now, Congress and law enforcement must consider how to protect Americans. Their options are rooted in two principles. The first is stepped-up enforcement and stiffer penalties for those who engage in digital crimes. And the second is blocking overseas criminals from being able to operate in the United States so they can no longer prey on Americans—who are the most targeted across the globe.

As piracy operators expand their criminal enterprises to include drug trafficking, human trafficking, and terrorism financing, we are asking law enforcement to bring a knife to a digital gunfight.

It's time to change that.

Piracy to Drug Trafficking and More

From Bootlegs to Billions

Criminals didn't go from profiting off pirated content to drug trafficking, human trafficking, money laundering for global organized crime syndicates overnight. It unfolded over two decades as piracy operators discovered that stolen content was just the beginning.

First came advertising revenue—profits from hosting stolen movies, TV shows, games, and music on ad-supported platforms. Then subscription models emerged, offering ad-free experiences for monthly fees. Some operations grew to shocking scale: the November 2024 European pay-TV network served more than 22 million subscribers across multiple countries, generating $288 million monthly.

The European pay-TV network investigation uncovered a highly organized criminal structure with distinct roles: technical administrators managed server infrastructure from the Netherlands, Romania, and Hong Kong; resellers distributed subscriptions through pyramid-like networks; and enforcers used encrypted communications to coordinate operations while employing false identities to register phone numbers, credit cards, and server rentals.

Comparable compartmentalization appeared in the Japanese Manga Mura case as well. Once one of the country's most notorious piracy platforms, Manga Mura monetized massive traffic through advertising and reportedly explored premium membership models before its closure. At its peak, it drew nearly 100 million monthly visits, turning pirated manga into an industrial-scale traffic and monetization engine. Investigations into Manga Mura revealed a distributed and evasive infrastructure model, with the piracy platform leveraging overseas hosting arrangements and mirrored or externally sourced image-

1 Mainichi / Tokyo Court damages award / civil judgment
2 Japan Agency for Cultural Affairs piracy report / Manga Mura structure and impact
3 Japanese OSINT / technical reconstruction of Manga Mura infrastructure
"漫画村は…海外のサーバーに身を置いていた…本来のサーバーの場所を隠ぺいして調べづらくするように構成されていました"
("Manga Mura was placed on overseas servers and configured to conceal the true server location, making investigation difficult.")
4 AIPPI / Cloudflare Liability Case Summary

storage systems rather than centralized domestic servers. The site repeatedly shifted technical infrastructure and used obfuscation measures to frustrate attribution, maintaining operations for years until its shutdown in 2018.

What the European pay-TV and Japanese Manga Mura cases illustrate is not simply scale. It illustrates maturation. Much like a diverse organized crime network, these European piracy operators did not follow a single commercial script. The arc, from ads to subscriptions to full-service criminal infrastructure, isn't conjecture, was documented in case after case. As storefront subscription platforms expanded through the mid-2010s, a second tier of operators emerged almost simultaneously, those who did not want the storefront, only the engine behind it. This was the onset of Piracy-as-a-Service, where some groups sold subscriptions, while others sold the content and the technical infrastructure that made the sale of subscriptions possible.

Traditional organized crime groups perfected this insulation decades ago. In Cosa Nostra, capos directed while soldiers absorbed operational risk. The Camorra distributed logistics, enforcement, and laundering across compartmentalized crews while leadership remained buffered. 'Ndrangheta clans separated procurement, transport, and financial movement across trusted cells, shielding the command layer from direct attribution.

Digital piracy enterprises adopted the same logic not in violence, but in design. No single layer exposes the whole. No single arrest necessarily collapses the system. Command remains insulated behind corporate fronts and technical intermediaries. The structure is disciplined and the cushioning of principals, the deliberate insulation of those who profit most, is the clearest sign of an organized enterprise.

But criminals always want more.

Piracy operators began partnering with malware distributors, exposing users to ransomware, identity theft, and device hijacking. A 2022 Digital Citizens Alliance report captured a ransomware attack in real time after investigators clicked on an advertisement. When malware revenue proved lucrative, operators discovered another opportunity: exploiting the credit card information subscribers had willingly provided.

Another DCA investigation found a troubling correlation between piracy and credit card fraud, with a finding that Internet users who signed up for a piracy subscription service using a credit card were 4 times more likely to report unwanted credit card purchases than those who said they don't visit piracy websites and apps. In all, 72 percent of those who used a credit card to sign up for a piracy service reported credit card fraud.

In 2023 and 2024, U.S. and international investigators uncovered what became known as the BadBox and BadBox 2.0 botnet. Off-brand Android streaming devices, marketed to consumers as inexpensive gateways to free movies and TV shows, arrived preloaded with malware. The FBI and cybersecurity analysts concluded that more than one million devices worldwide had been silently enrolled into a residential proxy network that enabled them to take over a device of an unknowing person to reroute criminal traffic and enabled ad fraud.

The pattern repeated in subscription-based IPTV investigations such as the BOS IPTV case spanning India, Canada, and the United States. Court documents and investigative reporting described how subscriber databases — names, email addresses, payment credentials — were harvested and repurposed. The customer list was not merely for billing. It became a resource for phishing operations, identity theft, and broader financial fraud. Piracy revenue expanded into data monetization.

There is a high reward: piracy profit margins exceed those of drug trafficking, yet penalties remain lower and prosecution rates minimal. The high profit margins enable criminal organizations to invest heavily in cutting-edge technologies including encrypted communications, cryptocurrency, artificial intelligence, and blockchain analysis evasion. Many law enforcement agencies lack equivalent technical capabilities or expertise.

The economics explain the escalation.

As mentioned, the IPTV network dismantled by European authorities served 22 million subscribers and generated an estimated $288 million a month in revenues. Similarly, when Chinese prosecutors concluded the Jiangsu "pirated links" case in 2023, they documented nearly 400 million RMB in advertising revenue generated over several years through app-based interception of licensed streams. Prosecutors in

Brazil, in cases linked to the MeuPlayer streaming network, described piracy revenue functioning alongside drug trafficking activity, with weapons recovered during enforcement actions.

A Canadian investigation of the sale of illicit IPTV subscriptions led law enforcement to Éric Grenier, who, according to Piracy Monitor, was "seen associating with members of the Hells Angels. He also had past involvement in the adult entertainment industry, earning him the nickname "Quebec's Hugh Hefner." In 2014, Grenier sentenced to five years imprisonment in the US on cocaine smuggling charges."

European IPTV investigations led authorities to seize not only servers and cryptocurrency but also narcotics and firearms. Operation Atria, in Spain, exposed a different, more financial convergence. Spanish authorities detailed how subscription revenues were allegedly funneled through a web of front businesses, including kebab shops and small retail outlets used as cash collection points. Prosecutors described layering techniques that included *hawala*-style informal value transfer systems, shell companies, fragmented deposits, and rapid conversion into cryptocurrency before redistribution across borders. The laundering typology mirrored methods long associated with organized crime groups: high-turnover cash fronts, structured deposits, and transnational value movement designed to obscure beneficial ownership.

Digital piracy does not simply coexist with organized crime; in documented cases it shares infrastructure, financial channels, and personnel.

The result is digital organized crime not only survives but thrives, generating tens of billions of dollars annually while facing minimal effective enforcement. This is the environment in which piracy networks operate and why they have transformed into sophisticated transnational organized crime syndicates.

This blurring of lines—where piracy operators diversify into other crimes while drug traffickers and human traffickers invest in piracy—should alarm law enforcement, policymakers, and anyone concerned with public safety.

Human Trafficking and Forced Labor

There is a growing acknowledgement within global law enforcement officials of the links between piracy networks and human trafficking and child sexual exploitation. Some of those suspicions point to convergence of piracy networks with human trafficking operations in Southeast Asia. This is an area that demands additional investigation.

Let's start with what has been said. A British law enforcement official, Detective Sergeant James Woodcock of the North East Regional Organised Crime Unit, stated that "illegal streaming services that supply entertainment and sports content via modified boxes, firesticks, and subscriptions help fund wider organised crime such as human trafficking, child sexual exploitation, drug supply and other sinister crimes."

In addition, Interpol stated, "Criminals behind pirate sites can be part of organized crime groups. They can use the proceeds to fund other illegal activities, such as illegal online gambling, online sexual exploitation, drug trafficking, arms smuggling, and money laundering." Officials in Sweden, Europol, and other UK law enforcement organizations echo these assertions about the connections between piracy and heinous crimes.

Now let's turn to what is suspected but not publicly documented: piracy operations in large-scale compounds in Myanmar and Cambodia, where an estimated 220,000 are held in and forced to work on online criminal operations. The United Nations Office on Drugs and Crime estimates that between 2020 and 2024, victims lost approximately $75 billion to Southeast Asian cyber scam operations run by transnational criminal organizations.

Those compounds are described by UN agencies and regional investigators as "polycriminal" infrastructures — operations capable of running multiple illicit revenue lines under one roof. While the public record does not definitively establish that digital piracy is a core activity inside these compounds, given what is known to occur – telecom fraud, illegal online gambling, cryptocurrency laundering,

investment scams – there is justifiable concern that piracy operations are included within this criminal structure.

The reason for that concern is two-fold. First, the technical architecture is compatible: The server farms, VPN tunnels, SIM-box arrays, VoIP routing systems, shell companies, and crypto payment rails enable scam call centers may also be powering IPTV subscription panels. Second, large-scale piracy platforms have thrived for years in parts of Southeast Asia with minimal custodial risk. Criminal indictments were rare. Prison sentences rarer still. The economic signal was clear — high margins, low exposure.

Vietnam illustrates the point. For years, globally trafficked piracy platforms operated from Vietnamese infrastructure while enforcement largely consisted of administrative measures or domain disruption. It was only in 2023 that a significant commercial streaming piracy case moved forward criminally, marking a shift from tolerance to prosecution. Prior to that inflection point, piracy rarely carried the deterrent weight associated with organized crime statutes.

In that enforcement environment, underreporting becomes structurally likely. When law enforcement frameworks prioritize telecom fraud, narcotics, and trafficking and when piracy is not systematically charged as a serious criminal offense it may remain secondary in indictments or omitted altogether. That does not mean it is absent. It means it may not be captured with the same prosecutorial visibility.

Given the human scope of these compounds and ease by which digital crimes can occur in those regions, this is an investigative area that requires additional investigation, something Digital Citizens and IP House intend to undertake.

Drug Trafficking and Narcotics Organizations

> n Brazil, law enforcement investigations revealed what prosecutors described as piracy serving as "Plan B" for organized crime—used by drug traffickers to bolster profits, purchase weapons, and expand operations when revenue streams faced disruption.

Brazilian authorities found that criminal networks involved in narcotics trafficking were simultaneously operating piracy rings, using the lower-risk, high-profit piracy operations to supplement drug revenues. When authorities raid piracy operations in Brazil, they regularly discover firearms and evidence of weapons smuggling alongside counterfeit media production facilities.

In Mexico, blockchain analysis of cryptocurrency transactions revealed financial ties between drug cartels and the same payment networks used by illicit IPTV operations. A 2024 Chainalysis investigation documented how organized crime groups, including those operating IPTV piracy networks, increasingly rely on cryptocurrency to facilitate cross-border transactions while obscuring financial trails.

In Canada, the operator of Arubox—a subscription-based IPTV service—was investigated not only for signal theft but also for money laundering and export control violations. His conviction for cocaine trafficking underscored that piracy had become a tool for actors deeply embedded in traditional criminal networks.

Spain's Operation Fake, led by Spanish National Police and Europol, revealed a similar convergence. Charging documents examined whether the IPTV enterprise headed by José Luis Huertas ("Juanillo") had received early seed capital linked to narco-connected family networks in southern Spain. Investigators scrutinized the use of a private aircraft allegedly associated with cocaine transport routes that was also used to move and distribute illicit IPTV set-top boxes across European corridors. Narcotics trafficking charges were not part of the piracy convictions themselves, but investigators documented significant overlap between the piracy network's distribution logistics and established cocaine aviation routes.

In Operation Atria, Spanish authorities uncovered laundering patterns familiar to narcotics enforcement long before digital piracy emerged. IPTV revenues were allegedly funneled through small front businesses, including kebab shops and retail outlets functioning as high-cash turnover nodes. Funds were layered through informal *hawala-style* transfers, shell corporations, fragmented deposits, and cryptocurrency conversions before moving offshore. The typology mirrored classic organized crime laundering playbooks: break the cash, move the value, blur the origin.

Digital piracy offers organized crime groups something narcotics cannot: recurring subscription income with lower sentencing exposure and global reach. When trafficking networks diversify, piracy is a logical addition. It requires servers instead of smuggling routes, reseller panels instead of street distributors, and encrypted messaging instead of radio chatter. But the hierarchy, the insulation of principals, and the shared financial conduits remain strikingly familiar.

Weapons Trafficking

The November 2024 European piracy takedown yielded weapons during raids across multiple countries—evidence that these operations maintain armed security or engage in weapons trading. The presence of firearms in piracy operations mirrors patterns seen in drug trafficking organizations, where weapons serve both to protect criminal infrastructure and as a separate profit center.

Digital piracy is often described as non-violent. The documented seizures suggest something more complicated. In certain jurisdictions, piracy revenues flow through networks already accustomed to carrying firearms.

In Brazil, federal operations targeting IPTV networks linked to groups such as MeuPlayer resulted in the seizure of pistols and ammunition alongside servers and subscription ledgers. Investigators described digital piracy infrastructure and weapons stockpiles occupying the same operational footprint. The streaming panels generated recurring income. The firearms protected territory and personnel.

In parts of Latin America, law enforcement officials have publicly acknowledged that when piracy operations are raided, firearms are often present. The explanation is straightforward: where organized criminal groups control territory or distribution networks, weapons follow revenue. Firearms change the risk profile. A piracy operation that includes weapons is not merely infringing intellectual property. It signals organized capability — the potential for violence, coercion, and territorial enforcement.

The Global Initiative Against Transnational Organized Crime notes that intellectual property theft, including piracy, has evolved into a highly structured form of organized crime that frequently overlaps with arms trafficking networks.

Terrorist Financing and Promotion

Recent investigations in India illustrate how the digital piracy infrastructure can also become a channel for ideological dissemination and potential extremist influence. In 2024, Indian authorities arrested Mohammed Murtuza Ali, a developer from Jalandhar, accused of operating an unauthorized IPTV service known as BOS IPTV. According to investigators, the platform distributed thousands of premium television channels including foreign broadcasts without authorization and allegedly reached close to five million users. But the piracy charges soon proved to be only part of the investigation.

Officials from the Gujarat Cyber Crime Cell stated publicly that investigators were examining whether the network had also been used to distribute extremist or radicalizing content through the same unauthorized streaming infrastructure. The Gujarat Cyber Crime Cell noted that authorities were investigating links between the suspect and Pakistani nationals involved in content distribution and were attempting to identify the overseas servers used to transmit the material into India. Investigators also indicated that the platform may have been connected to a broader piracy syndicate operating across Pakistan, Syria, and parts of the Middle East, raising concerns that the same IPTV networks used for piracy could potentially be leveraged to disseminate propaganda or ideological messaging.

The case, which is still pending, illustrates an uncomfortable reality confronting law-enforcement agencies worldwide: once a large piracy network exists with global servers, subscriber databases, payment channels, and encrypted communication systems, it can be repurposed for more than just stolen entertainment. The same infrastructure capable of delivering pirated films or sports broadcasts can just as easily distribute extremist propaganda, or other illicit content at scale.

This is precisely why digital piracy should be viewed as a distribution infrastructure, one that can be exploited by criminal groups, extremist networks, or hybrid bad actors operating across borders.

Yet even as piracy networks evolve into digital infrastructures capable of carrying extremist propaganda or cybercrime operations, the roots of the business remain deeply connected to older forms of illicit media distribution. Long before IPTV servers and encrypted streaming panels existed, organized crime groups built their profits through the physical trade of counterfeit DVDs, bootleg music, and pirated software discs—a market that provided the financial and logistical foundation for today's digital piracy economy.

In the United States these piracy networks had enabled terrorist organizations not only to raise funds but to circumvent broadcast bans in the United States.

Al-Manar, the television network of Hezbollah, was designated a "Specially Designated Global Terrorist entity" and banned by the United States in 2004. A government spokesman said the decision reflected "its incitement of terrorist activity." Yet a 2020 Digital Citizens Alliance report documented how Al-Manar circumvented that ban by broadcasting on piracy platforms—reaching American audiences through illegal IPTV services that carry the channel despite its terrorist designation.

The connections run deeper. A 2009 RAND Corporation study provided compelling evidence that terrorist groups have used piracy proceeds to finance operations:

The Barakat Network: Operating in the Tri-Border Area of Brazil, Argentina, and Paraguay—a known haven for criminal groups and Islamic terrorist organizations—Assad Ahmad Barakat ran a criminal syndicate engaged in piracy from its inception. The network used funds from piracy and other crimes to transfer at least $3.5 million to Hezbollah. The U.S. government designated Barakat as a specially designated global terrorist in 2004.

D-Company: India's most wanted criminal, Dawood Ibrahim, controls D-Company, which transformed from an organized crime syndicate into a terrorist organization after orchestrating the 1993 Mumbai bombings that killed more than 257 people. The RAND study found substantial evidence that D-Company used film piracy proceeds to fund terrorist activities. Named a global terrorist by the U.S. government in 2003, Ibrahim operates from hiding, likely in Pakistan.

Provisional Irish Republican Army: The PIRA engaged in counterfeiting and piracy to finance operations during decades of political violence. After the 1998 peace agreement, the organization leveraged its criminal infrastructure to expand organized crime activities, with film piracy serving as a consistent revenue source.

Convergence with Illegal Gambling and Online Fraud

Law enforcement investigations have documented convergence between piracy operations and illegal online gambling. The 2024 UNODC threat analysis noted that cases examined highlight how illegal online casino operators have diversified business lines to include cyber-enabled fraud, cryptocurrency-based money laundering services, and intellectual property theft including IPTV piracy.

In the Philippines, what were legally registered as Philippine Offshore Gaming Operators turned out to be fronts for massive scam and trafficking operations. A March 2024 raid on a POGO facility in Bamban, Tarlac rescued more than 800 Filipinos and foreign nationals being held in what authorities described as a scam hub operating crypto and romance scams while also managing IPTV piracy services. The convergence of these criminal activities under single organizational structures shows how modern organized crime operates across multiple illicit markets simultaneously.

Nordic authorities have raised concerns about links between piracy and organized crime involved in trafficking and drugs. Viaplay Group's Danish CEO stated , "We are losing money on piracy, but more importantly, piracy is run by ringleaders who use the money for trafficking, drugs."

Money Laundering Operations and Financial Crime Connections

Modern piracy networks have become increasingly sophisticated in money laundering operations, often exceeding the capabilities of traditional organized crime.

In Southeast Asia, UNODC reports document industrial-scale money laundering through underground banking systems, cryptocurrency solutions, and sophisticated financial technologies. These networks take advantage of vulnerabilities in financial systems across Cambodia, Laos, Malaysia, Thailand, and Vietnam, as well as financial hubs like Singapore and Hong Kong. Laundered funds from operations such as piracy, fraud, and other cyber-enabled crimes flow into real estate investments globally, including in the United Kingdom, other European countries, Canada, and the United States.

The November 2024 European takedown revealed criminal use of cryptocurrency mixing services, layered wallet structures, shell companies registered with false identities, and encrypted communications to obscure financial flows.

As mentioned earlier, authorities seized $1.9 million in cryptocurrency and tens of thousands in cash, but investigators described the digital ecosystem as far larger. As one Eurojust official noted, this was "not a streaming service, it was a financial architecture."

But cryptocurrency wallets are only one layer of the laundering story.

In the United States, the prosecution of Bill Omar Carrasquillo ("Omi in a Hellcat") revealed how piracy revenue converts into visible assets. Federal prosecutors alleged that his IPTV service, Gears TV, generated tens of millions of dollars in unlawful subscription revenue over several years. Court filings detail how proceeds were routed through shell

companies and layered bank accounts before being used to purchase luxury vehicles, multiple properties, jewelry, and commercial real estate. In sentencing proceedings, prosecutors emphasized that the defendant "treated piracy as a business enterprise," reinvesting illicit proceeds in assets designed to legitimize wealth. The laundering model was traditional in structure — shell entities, layered deposits, asset conversion — but powered by recurring digital subscription revenue.

The Z-Library indictment (United States v. Shulman et al.) alleged millions in global revenue routed through cryptocurrency wallets, mirror domains, offshore hosting, and fragmented payment processors. Investigators described an ecosystem designed to "evade detection and frustrate asset tracing." When domains were seized, new ones appeared. When wallets were frozen, others activated. The platform's financial resilience mirrored adaptive laundering models seen in narcotics enterprises, except the revenue began in encrypted digital rails rather than bulk cash.

In Spain's Operation Atria, investigators traced IPTV revenues estimated in the tens of millions of euros through informal remittance systems resembling *hawala* networks. Funds were allegedly laundered through small front businesses — including kebab shops and retail outlets — functioning as high-cash aggregation points. Deposits were fragmented, layered, converted into cryptocurrency, and redistributed across jurisdictions. Spanish prosecutors described the structure as "characteristic of organized criminal concealment," noting the deliberate separation between subscriber payments and beneficial ownership.

Similarly, Spanish authorities examined IPTV subscription flows allegedly linked to shell corporations and cross-border financial channels historically associated with narcotics laundering. Investigative filings scrutinized whether early seed capital had connections to narco-linked networks. While narcotics convictions were not secured in the piracy case itself, the laundering typology — shell entities, layered transfers, aviation logistics overlapping trafficking corridors — reflected organized crime financial behavior.

The Jetflicks case in the United States (United States v. Dallmann et al.) involved subscription revenue generated through automated ingestion systems serving tens of thousands of paying users. Court documents detailed coordinated financial management, server leasing contracts, payment processors, and shell structures. Prosecutors characterized the operation as "an unlawful streaming service operating at

commercial scale," not a hobbyist piracy ring. The money moved through structured accounts rather than physical cash exchanges — a digital analogue to traditional layering.

Canada's investigation into individuals associated with Arubox similarly involved cryptocurrency tracing and export violations, with financial scrutiny extending beyond signal theft. The operator's separate cocaine trafficking conviction underscored the overlap between digital piracy income and traditional criminal revenue streams. Prosecutors examined how subscription payments and other illicit proceeds flowed through overlapping financial conduits.

Even infrastructure-level cases illustrate the point. The 2019 dismantling of Xtream Codes, a middleware provider serving thousands of IPTV resellers, revealed revenue fragmentation across global reseller panels, layered subscription gateways, and distributed hosting infrastructure. While exact revenue totals were not fully public, European authorities treated the case as a transnational financial enterprise, coordinating asset freezes across multiple jurisdictions.

Across these cases, the laundering mechanisms repeat with striking consistency:

- Shell companies registered under false or layered identities
- Cryptocurrency wallets fragmented across hundreds of addresses
- Use of mixing services and privacy-enhancing exchanges
- High-cash front businesses to aggregate and structure deposits
- Informal remittance systems resembling *hawala*
- Rapid cross-border digital transfers designed to outrun enforcement
- Conversion of digital proceeds into hard assets — vehicles, real estate, luxury goods

The architecture mirrors traditional organized crime laundering — layering, integration, concealment — but it operates at digital velocity.

Drug proceeds traditionally move in bulk cash before entering the financial system. Piracy proceeds are born digital. Subscription payments convert instantly into cryptocurrency. Wallets fragment revenue into distributed nodes. Funds cross continents in minutes. As one federal prosecutor observed in a U.S. IPTV case, "This was not piracy for convenience. It was piracy for profit."

Organized Crime Structure of Piracy Networks

Major piracy networks operate through modular structures that surpass traditional organized crime in sophistication. Rather than hierarchical pyramids where removing leadership collapses the organization, digital crime syndicates function as loosely coupled networks of semi-autonomous cells.

Each cell handles specific functions—content sourcing, technical infrastructure, payment processing, customer support, reseller management—operating independently enough that compromising one doesn't expose others.

This compartmentalization borrows from terrorist organization models and drug cartel structures, where operational security demands that participants know only what's necessary for their role. The November 2024 European takedown revealed this clearly: server administrators in the Netherlands and Romania maintained core infrastructure. Reseller coordinators in Italy and Croatia handled subscription distribution. Separate actors managed cryptocurrency wallets under false identities. Customer support operated through encrypted channels. Each role was isolated. Leadership, if identifiable at all, sat several layers removed.

The SPARKS Group divided source acquisition, encoding, and distribution into insulated units. KickassTorrents (United States v. Vaulin) separated hosting, advertising revenue, and domain control across jurisdictions. Z-Library segmented mirrors, hosting, and payment rails so that domain seizures did not end operations. Xtream Codes insulated middleware developers from thousands of downstream IPTV resellers.

This is not pyramid criminality. It is cellular resilience.

Note: There is a U.S.-based Sparks Group that is different from this entity cited in the report.

Piracy Franchise Model

Perhaps the most significant evolution is piracy-as-a-service.

Sophisticated piracy rings no longer operate individual sites—they sell complete turnkey solutions to operators worldwide. These kits include pre-configured streaming panels, massive content libraries, payment system integrations, subscriber management tools, and customer support templates.

The 2019 takedown of Xtream Codes in Italy marked the inflection point. Investigators discovered a middleware platform powering thousands of IPTV brands worldwide. Xtream did not market to viewers. It marketed to entrepreneurs. For a fee, operators received authentication APIs, billing panels, reseller tiers, and real-time stream control tools. When servers were seized, entire continents saw IPTV outages, proof that a hidden wholesale layer had been feeding the retail illusion.

This model mirrors software-as-a-service businesses, but with criminal intent. The core operation insulates itself by functioning as a wholesaler to hundreds of retail-level operators. When law enforcement shuts down a franchise, dozens continue operating.

This model creates rapid global expansion while maintaining operational security. A central organization in Eastern Europe can have franchisees operating in Asia, South America, Africa, and North America simultaneously, each tailored to local languages, payment preferences, and content demands. The franchisees assume most of the risk of detection and prosecution, while the core operation remains largely invisible.

Anonymous Leadership

Traditional organized crime eventually revealed its leadership. Law enforcement identified John Gotti, Pablo Escobar, El Chapo Guzmán. Even the most sophisticated criminal organizations operated through identifiable human networks that persistent investigation could penetrate. Once leadership was known, targeted prosecution, asset seizure, and extradition became possible.

Digital organized crime has often achieved what eluded traditional crime families for generations: leadership anonymity. Through encrypted communications platforms, layered cryptocurrency transactions, darknet marketplaces, false identity documents, and compartmentalized operations, many piracy syndicates operate without identifiable leadership structures. Law enforcement investigators pursuing these networks often cannot determine who controls operations.

Communication flows through Telegram, Signal, or custom encrypted channels. Instructions appear but sources remain unknown. Bitcoin and privacy coins like Monero move through multiple wallets and mixing services before destination. Shell companies register using stolen identities or nominees in jurisdictions with minimal oversight. Technical administrators communicate solely through screen names, never revealing real identities even to close collaborators.

This represents an evolution beyond traditional organized crime models. When RICO prosecutions dismantled La Cosa Nostra families, they did so by identifying and charging leadership. But how do you charge someone you cannot identify? How do you extradite someone whose location remains unknown? How do you seize assets you cannot trace? Digital organized crime has created a fundamental asymmetry where law enforcement's most powerful tools prove inadequate.

Consider how long it took to unmask the alleged operator of KickassTorrents in United States v. Vaulin. The platform operated for years, serving millions of users globally, generating millions in advertising revenue, while its founder hid behind the alias "tirm."

Investigators did not identify him through a cooperating witness or visible hierarchy, as in traditional mafia cases. They identified him through digital forensic correlation — an IP address tied to an iTunes transaction, domain registration records, and advertising contracts. The trail was technical, not human.

In the Z-Library prosecution (United States v. Shulman et al.), leadership did not surface through an internal defector or intercepted meeting. Authorities relied on coordinated domain seizures, blockchain tracing, hosting records, and cross-border cooperation to attribute control to specific individuals operating under layers of anonymity. Even then, the platform's mirrored infrastructure continued functioning, illustrating how distributed architecture protects leadership.

Digital piracy operators often govern through infrastructure instead of territory.

Physical Production to Digital Distribution

Modern IPTV piracy requires no physical production. Content originates from compromised streaming accounts, insider leaks, or screen captures. Distribution occurs through internet streaming—impossible to intercept physically. Payments process through cryptocurrency—difficult to trace and seize. Customers never meet sellers, sellers never meet suppliers, suppliers may not know ultimate sources. The entire supply chain exists in digital space, creating minimal physical footprint that law enforcement can target.

This shift dramatically reduces operational risks while increasing scale potential. A physical DVD counterfeiting operation might produce hundreds of thousands of discs, requiring warehouses, trucks, and distribution networks vulnerable to detection. A digital piracy operation can serve millions of concurrent users from a handful of servers that can relocate to new hosting providers within hours of enforcement action.

Advanced Piracy Networks = Organized Crime

Law enforcement bodies such as UNODC, INTERPOL, and EUROPOL define organized crime by:

- **Structure:** Hierarchical or network-based organizational models—piracy networks show both, with technical administrators, content providers, payment processors, resellers, and customer support operating in coordinated fashion.
- **Scale:** Significant revenue streams—piracy generates an estimated 40 billion dollars globally, with individual operations earning hundreds of millions annually.
- **Cross-border activity:** Operations spanning multiple countries and jurisdictions—piracy takedowns regularly involve coordination among 10 to 18 countries, with infrastructure distributed across continents.
- **Profit motivation:** Financial gain as the primary driver—piracy operations exist solely to generate illegal profits, with no ideological or political motivations.
- **Serious crimes:** Involvement in activities beyond the primary criminal enterprise—as Chapter 1 documented, piracy networks actively engage in drug trafficking, human trafficking, weapons smuggling, terrorism financing, and money laundering.
- **Duration:** Ongoing criminal enterprises rather than isolated acts—many piracy networks operate for years or decades, continuously adapting to enforcement efforts.
- **Violence and intimidation:** Use of force to protect operations and eliminate competition—weapons seizures during piracy raids and documented connections to violent criminal organizations reflect this element.
- **Corruption:** Co-opting public officials and law enforcement—many piracy networks operate with protection from corrupt officials in jurisdictions providing safe harbor.

Digital piracy networks meet every criterion. The question is not whether they qualify as organized crime. The question is what to do about it.

Thwarting Organized Piracy Requires New Enforcement Tools

> n 1970, Congress recognized that organized crime required new approaches. The result was legislation that fundamentally changed what law enforcement could accomplish against sophisticated criminal enterprises.

Today, piracy networks have evolved into transnational organized crime syndicates meeting every legal definition while engaging in serious violent crimes including drug trafficking, human trafficking, weapons smuggling, and terrorism financing. Yet these operations face enforcement frameworks designed for a pre-digital era.

The choice before policymakers is fundamentally the same one their predecessors faced fifty years ago. They can continue to provide law enforcement with inadequate tools, watching criminal enterprises grow more sophisticated and more dangerous.

Or they can recognize the threat and respond accordingly.

There are two actionable steps Congress can take:

- Adopt the approach taken by more than 50 countries: Blocking criminal piracy networks from being able to operate in the United States. Site-blocking is a legal mechanism that allows courts to order internet service providers to prevent websites—typically overseas piracy platforms that operate beyond the reach of domestic law enforcement. This action would only apply to piracy networks operating overseas that law enforcement can't reach.
- When a piracy operation is based in a jurisdiction that won't cooperate with takedown requests or extradition, traditional enforcement becomes challenging. Site-blocking addresses this by targeting the demand side: rather than trying to shut down a server in Eastern Europe or Southeast Asia, authorities can require ISPs within their own borders to block the domain names or IP addresses associated with piracy services. The

United Kingdom, Australia, France, Germany, Italy, Spain, and most of the European Union have implemented some form of site-blocking, often through a process that requires a judge to approve it.

- The United States remains a notable outlier among developed nations in lacking a site-blocking framework—a gap that allows overseas piracy operators to target American users while facing no practical barrier to market access. As IP House wrote in a 2025 report sponsored by Digital Citizens, "Thousands of blocking orders have been executed in more than 50 countries, so any real shortcoming or defect in the process would have clearly surfaced and resulted in concrete examples of failed or inappropriate blocks. Indeed, there is a highly motivated and well-funded cadre of site-blocking critics scouring the record and scrutinizing these cases for any hint of a problem. But no such obvious examples exist."
- Congress can also strengthen the laws that govern illegal piracy. Lawmakers in 2020 took an important step with passage of legislation that make piracy streaming a felony. However, the thresholds and penalties remain modest compared to other organized crime offenses. Congress could lower the threshold for felony prosecution, increase maximum sentences for repeat offenders or operations linked to other criminal activity, and create sentencing enhancements when piracy is conducted as part of an organized criminal enterprise or when proceeds fund other serious crimes like drug trafficking or human trafficking.
- Since piracy operations depend on payment processors, advertising networks, hosting providers, and others, Congress could also require payment processors to terminate relationships with merchants identified as piracy operations, similar to existing requirements for illegal gambling and expand the Treasury Department's authority to designate foreign piracy operations, when warranted, as "primary money laundering concerns," cutting them off from the U.S. financial system.

These are reasonable steps lawmakers could take to give law enforcement and the administration more effective tools to combat organized piracy networks. These recommendations are based on the findings of this report, which leave no room for doubt about what piracy networks have become. The only question is whether we will act on that knowledge.

How We Got Here

Naples, 2019: A whistleblower tips off authorities to an illicit IPTV service in the suburb of Miano, churning out an estimated €6 million annually in pirated TV subscriptions. The revelation causes a stir not only among law enforcement but also in the local underworld. Investigators learn that Camorra clans have been circling the operation, eager to invest in this high-margin, low-risk racket. After all, what could be more attractive to a mafia don than a criminal venture that yields big profits without turf wars or bloodshed? The business model offers everything mob bosses crave – lucrative returns, minimal violence, and plausible deniability behind a veil of technology.

When police finally moved in, they treated the IPTV ring itself as an organized crime group. In the ensuing takedown, codenamed Operation Eclipse, Italian prosecutors charged the pirates under the same statutes used for Mafia gangs, invoking the organized crime conspiracy law alongside piracy offenses. Nearly two dozen suspects were identified operating more than 200 servers across Europe, streaming hijacked content to an estimated 5 million viewers, a criminal enterprise of "well-skilled criminals" that mirrored a Mafia-style operation in structure and scale. And in the United States, the infamous KickassTorrents case a few years earlier had unfolded similarly: investigators from the FBI's International Organized Crime unit (IOC-2) helped build a case that the world's most-visited piracy site was, at its core, an organized criminal conspiracy to launder millions in illicit ad revenue. Digital piracy, long dismissed as a mere civil IP issue, was now being prosecuted as organized crime.

How Did We Get Here?

To understand why multi-national piracy rings are being painted with the same brush as the Camorra or Cosa Nostra, we must first understand how the very definition of organized crime evolved. The term "organized crime" wasn't born in a courtroom or statute; it germinated in the streets. In 19th-century New York and Chicago, it described the urban gangs that ran bootlegging, gambling, extortion. By the mid-20th century, criminologists formalized the concept as Organized Crime Groups (OCGs): structured, continuous networks that pursue profit through serious crime. Still, for decades this concept remained tied to the familiar specters of the drug cartel, the mob family, the triad. It wasn't until 1970, with the U.S. Organized Crime Control Act, that the term gained a legal definition: "the unlawful activities of a highly organized, disciplined association". Thirty years later, the world's nations agreed on a broader standard.

The United Nations Convention Against Transnational Organized Crime (2000) defined an "organized criminal group" as "a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing serious crimes to obtain, directly or indirectly, a financial or material benefit." This UN definition, at least three members, some continuity over time, and a profit-driven serious crime, became the benchmark. INTERPOL echoed similar criteria: a group of individuals, loosely or tightly organized, with continuity of structure and the goal of profit through illegal activities. EUROPOL added familiar mafioso touches like the use of violence, corruption, or infiltration of the legal economy.

How We Got Here (Cont'd)

Those definitions, forged in an age of heroin trafficking and extortion rackets, anchored law enforcement for decades. They assumed syndicates with guns and territories, a world still analog. None explicitly foresaw server farms hijacking movies, or pirate apps on phones. The Internet was simply not on the radar when policymakers imagined organized crime. But by the 2010s, this blind spot was impossible to ignore. Cybercrime was exploding, and organized crime was digitizing. In 2010, the UK's Serious and Organized Crime Strategy became one of the first national policies to explicitly classify cybercrime as a core organized crime threat. UNODC's cybercrime module observed that "piracy rings now operate like digital franchises," with obscured finances, interchangeable roles, and coordination via encrypted apps. The traditional hallmarks of mob enterprises – structure, intent, continuity, and scale – were now manifest in the cyber realm. In short, the definitions finally began to catch up with the new players.

Why do Definitions Matter?

How we define a crime determines how we fight it. "You can't criminalize what you can't define," notes Dr. David Shepherd, a former financial investigator and now a senior lecturer in economic crime. If piracy networks slip through the definitional cracks, regarded as mere civil-law nuisances rather than economic crime machines, they also slip through enforcement gaps. Definitions shape priorities.

The law often lags technology; definitions must catch up before authorities can uniformly classify piracy kingpins as "mobsters" and hit them with the same arsenal of statutes. And legally, there's a gap: many jurisdictions don't have a clear threshold for when a piracy operation graduates from a copyright issue to an organized crime issue. Some police agencies still consider all piracy as a matter for civil courts or minor fines, a legacy mindset that doesn't account for the new realities.

Signs point to greater official recognition of piracy as part of the organized crime networks. The UK, as noted, already pegs major piracy under "cyber-enabled economic crime" in its National Crime Agency assessments. Internationally, efforts like INTERPOL's newly launched Stop Online Piracy (I-SOP) initiative indicate that global law enforcement now views large-scale piracy as a serious transnational crime to be tackled with multi-country operations, not cease-and-desist letters. And if digital piracy continues to serve as a financial engine for traditional gangs or as a gateway crime for tech-savvy youths to become cyber-crime bosses, the case for treating it on par with other organized crimes will only strengthen. As UNODC suggests, many piracy rings function like franchises of a shadow economy.

The debate over labeling digital piracy as "organized crime" is not a mere matter of semantics; it's about strategic clarity in protecting markets and the public. Yes, a spectrum exists – from small-scale bootleggers to sprawling syndicates – and not every case warrants the heavy artillery of anti-OCG measures. But many pirate operations do meet the international criteria of organized criminal enterprises. It's time our laws and investigations shine a light on it, as brightly and unflinchingly as they have on the traditional mob. Only then can we close the gap between the piracy operators of old and of now and confront this new breed of criminal enterprise on its own terms.

Spain: Intersection of Piracy & Organized Crime

Spain has become one of Europe's most persistent hotspots for digital piracy. In the early 2010s, Spanish users topped global charts in accessing illicit films, music, and live TV. Although public attitudes have shifted and enforcement has gradually tightened, piracy remains deeply embedded in the digital underground.

Spain's digital infrastructure, proximity to entrenched narcotrafficking routes, and privileged access to EU-wide hosting and payment frameworks have made it a strategic launchpad for IPTV piracy operations. The same logistical corridors once dominated by cocaine and hashish smuggling have been repurposed by digital piracy syndicates to enable encrypted signal theft, server obfuscation, and transnational laundering.

Law enforcement operations have exposed the connections. In one of the IPTV bust operations, Operation Fake, content redistribution hubs and crypto-funded laundering routes were embedded in trafficking strongholds like Galicia and Las Palmas. Another operation, Operation Atria, exposed piracy revenues moving through the same clandestine remittance networks used for Iranian human smuggling and embargo evasion.

These cases underscore a key evolution: digital piracy in Spain has become structurally enmeshed within polycriminal networks where telecommunication fraud, trafficking logistics, and financial subversion intersect to produce resilient illicit enterprises. Spain, undoubtedly, has become a site of evolution, where traditional forms of organized crime, smuggling, counterfeiting, and fraud have intersected with tech-enabled piracy ventures.

Between 2019 and 2021, Spain witnessed a growing string of piracy investigations that blurred the boundaries between digital infringement and organized criminality. Law enforcement units, particularly those under the Policía Nacional's IP and Economic Crimes Division, reported that piracy revenues were not merely flowing into encrypted wallets or crypto exchanges. In several cases, they were being laundered alongside profits from drug trafficking, weapons smuggling, and immigration rackets.

For years, Spanish courts largely pursued these actors under copyright statutes. Operation Fake was a turning point. It was one of Spain's first major IPTV investigations where authorities framed piracy not only as a copyright offense but as part of a criminal enterprise with transnational scope10a What set this case apart was the discovery that the syndicate had also used advanced satellite-capture and signal-decryption technologies, operated content capture hubs, and monetized stolen content on 16 different websites, all while allegedly laundering the proceeds through offshore mechanisms10c. Authorities traced the operation's roots back to 2015—underscoring just how long such networks can persist beneath the radar.

Operation Fake served as a template for future Spanish enforcement strategies. It showed the value of treating piracy not as an isolated tech crime but as part of a polycriminal ecosystem—one that can't be dismantled without tackling the financial structures and parallel crimes that sustain it. It also marked a shift in language: Spanish police statements began referring to IPTV as an "entramado criminal" and judges were urged to consider broader charges like fraud, laundering, and economic crime.

Spain: Intersection of Piracy & Organized Crime (Cont'd)

Through Operation Fake, charges filed included IP crimes (unauthorized content distribution), money laundering through real estate, vehicles, crypto mining, and shell companies, electricity fraud for powering six illegal mining centers, drug trafficking via private aircraft, organized crime participation, and counterfeit manufacturing through fake luxury auto workshops. It culminated in coordinated raids across nine Spanish provinces. The final tally was striking: 11 arrests, 16 interrogations, 47 property searches, 48,000 illegal set-top boxes seized, and the dismantling of seven servers—four located in Spain, three abroad. Police also froze assets exceeding €6 million and uncovered a user base of roughly 2 million customers.

Appendix

These tables are Organized by the Organized-crime characteristic most clearly illustrated by each case. The final row in every table is dynamic by design: it highlights the specific overlap that makes the case analytically useful - weapons recovery, drug linkage, terror-finance risk, laundering architecture, or corporate-style hierarchy.

Cases Where Organized Crime Statutes Were Invoked or Organized Crime Units / IOC Were Involved

Defining criterion: piracy cases in which Organized-crime statutes, Organized-crime units, or enterprise-style prosecution tools were central to the enforcement posture.

KickassTorrents / Artem Vaulin	
Category	**Details / Highlights**
Criminal Type	Large-scale torrent platform prosecuted as a transnational criminal enterprise, with conspiracy and money-laundering counts layered onto copyright charges.
Illicit Revenue	US$12.5-US$22 million in annual ad revenue; platform value estimated above US$50 million; more than US$1 billion in infringing content distributed.
Modus Operandi	Indexed torrent files and magnet links at global scale, rotated domains and servers across jurisdictions, and monetized massive traffic through ad brokers.
Money Laundering / Financial Concealment	Advertising proceeds routed through offshore accounts and shell entities, including the Cryptoneat front, to obscure beneficial ownership and revenue flows.
Tech Tools Used	BitTorrent infrastructure, rotating domains, offshore servers, privacy masking, platform admin panels, and layered hosting across multiple countries.
Law Enforcement	DOJ, HSI, IRS-CI, IOC-2, Polish Border Guard and prosecutors, with supporting seizures in Canada, Latvia, and Italy.
Charges Filed	Criminal copyright conspiracy, substantive criminal copyright infringement, and conspiracy to commit money laundering.
Evidence Base	DOJ criminal complaint, IRS financial tracing, domain records, Apple and Facebook account data, and international server seizures.

KickassTorrents / Artem Vaulin	
Category	**Details / Highlights**
Why It Matters	Early U.S. precedent for treating a piracy platform as Organized cyber-financial crime rather than a mere copyright nuisance.
Overlap with Organized Crime Statutes / IOC Involvement	Investigation was coordinated through IOC-2 and pursued using enterprise-style conspiracy and laundering charges normally associated with serious Organized crime.

SPARKS Group / Operation Global Screen	
Category	**Details / Highlights**
Criminal Type	Upstream warez network prosecuted as an international criminal conspiracy focused on pre-release theft and scene distribution.
Illicit Revenue / Harm	Tens of millions of dollars in studio losses; the operation supplied pirated releases covering much of the major-studio slate between 2011 and 2020.
Modus Operandi	Acquired screeners and discs before release, cracked protections, encoded files, and pushed them through FTP topsites, IRC channels, and downstream P2P ecosystems.
Organizational Structure	Clear division of labor across acquisition, cracking, encoding, metadata, hosting, and dissemination, operating across multiple continents.
Tech Tools Used	FTP topsites, IRC distribution channels, bulletproof hosting, encrypted communications, scene release tooling, and globally distributed servers.
Law Enforcement	SDNY, DOJ Organized-crime components, HSI El Dorado Task Force, U.S. Postal Inspection Service, Europol, and Eurojust.
Charges Filed	Wire fraud conspiracy, criminal copyright conspiracy, substantive copyright counts, and forfeiture actions.
Evidence Base	SDNY indictment, Eurojust coordination notes, international server seizures, and studio leak tracing.
Why It Matters	Marked a turning point in U.S. enforcement by treating upstream piracy as Organized cybercrime and hitting the supply layer, not just downstream mirrors.
Overlap with Organized Crime Framing	First known warez prosecution handled through DOJ Organized-crime channels, with the network characterized as a coordinated transnational criminal conspiracy.

Note: There is a U.S.-based Sparks Group that is different from this entity cited in the report.

Operation Eclipse / Xtream Codes	
Category	**Details / Highlights**
Criminal Type	Commercial IPTV infrastructure framed in Italy as an Organized criminal group using mafia-style conspiracy statutes.
Illicit Revenue	Approximately EUR 2 million in monthly turnover from an estimated 5 million users in Italy alone.
Modus Operandi	Stole and decrypted premium pay-TV feeds, redistributed them through the proprietary Xtream Codes platform, and sold cut-rate subscriptions through a reseller ecosystem.
Organizational Structure	Technicians, resellers, money handlers, and platform operators functioned in a clear chain of roles across 200+ servers and multiple European jurisdictions.
Tech Tools Used	Custom Xtream Codes software, retransmission stations, decryption infrastructure, payment processors, and a server network spread across Europe.
Law Enforcement	Rome Public Prosecutor, Italian cyber and anti-mafia authorities, Europol, Eurojust, and partner agencies across France, the Netherlands, Germany, Bulgaria, and Greece.
Charges Filed	Organized crime conspiracy, illegal digital broadcasting, circumvention of technological protection measures, and related financial-crime inquiries.
Evidence Base	Italian prosecutorial statements, Europol and Eurojust coordination records, and server/payment takedown data.
Why It Matters	Landmark European case that explicitly moved IPTV piracy into the Organized-crime category and helped reframe later enforcement actions.
Overlap with Mafia / OCG Structure	Authorities explicitly described the operation as an OCG, and later intelligence showed Camorra interest in controlling similar piracy revenues.

Flawless IPTV	
Category	**Details / Highlights**
Criminal Type	Large-scale commercial IPTV enterprise prosecuted in the UK through fraud and serious-crime frameworks rather than as a narrow copyright case.
Illicit Revenue	More than GBP 7.2 million from at least 50,000 customers and resellers buying illicit Premier League and premium-TV subscriptions.
Modus Operandi	Sold subscriptions under multiple aliases, delivered streams through modified apps and set-top boxes, and maintained dedicated customer-support operations.
Fraud / Financial Controls	Revenue was concealed through multiple payment accounts and laundering activity; POCA confiscation mechanisms were central to the enforcement strategy.
Tech Tools Used	Modified streaming apps, reseller portals, hacked broadcast access, and account compromise techniques used to maintain feed quality.
Law Enforcement	Premier League investigators, FACT, Trading Standards, regional police forces, and the North West Regional Organized Crime Unit.
Charges Filed	Conspiracy to defraud, money laundering, contempt-related financial violations, and associated computer misuse allegations.
Evidence Base	Trial records, sentencing remarks, financial evidence, and enforcement reporting from UK agencies and rightsholders.
Why It Matters	Set the modern UK benchmark for serious sentencing in piracy cases and demonstrated that Organized-crime tools can produce far heavier consequences than IP statutes alone.
Overlap with Serious-Crime Enforcement	Led by Organized-crime units and prosecuted as a fraud enterprise, not a low-level streaming offence.

Arubox / Stocker IPTV	
Category	**Details / Highlights**
Criminal Type	Pirate IPTV operation embedded in a broader Organized-crime portfolio involving prescription-drug trafficking, laundering, and telecom fraud.
Illicit Revenue	At least CA$2 million over roughly 3.5 years from around 7,000 subscribers in Quebec alone, with additional offshore exposure possible.
Modus Operandi	Sold pre-configured Formuler Z boxes and illicit access codes carrying 3,500+ channels, while using overlapping personnel and logistics for other black-market activity.
Money Laundering	Piracy proceeds and drug proceeds allegedly moved through shell companies, bank transfers, and property-of-crime concealment mechanisms.
Tech Tools Used	Preloaded IPTV boxes, subscriber panels, offshore domains, support channels, and concealed streaming infrastructure.
Law Enforcement	Surete du Quebec Organized-crime and cybercrime units, financial-crime specialists, telecom complainants, and cross-border tracking support.
Charges Filed	Conspiracy to defraud, theft of telecommunication service, trafficking in illicit devices, laundering proceeds of crime, and trafficking in prescription drugs.
Evidence Base	Subscriber lists, payment records, seized devices, telecom complaints, international flight history, and court filings.
Why It Matters	Rare Canadian example where IPTV piracy was openly prosecuted as part of a polycriminal Organized enterprise rather than as a standalone signal-theft matter.
Overlap with Drug-Trafficking and Organized-Crime Portfolio	Same network and money channels were used for IPTV sales and prescription-drug trafficking, giving prosecutors a credible criminal-organization narrative.

Cases With Firearms Recovery and Drug-Trafficking Linkage

Defining criterion: piracy investigations where raids surfaced firearms, ammunition, narcotics indicators, or other evidence of convergence with traditional trafficking ecosystems.

Operation Takedown / Kratos / Europa	
Category	**Details / Highlights**
Criminal Type	Mass-scale subscription IPTV super-network operating as a high-value Organized digital fraud enterprise with armed and narcotics-linked indicators.
Illicit Revenue	Approximately EUR 250 million per month, or nearly EUR 3 billion annually, from around 22 million users worldwide.
Modus Operandi	Captured and redistributed premium TV and streaming content through mirrored domains, cloned streaming servers, reseller layers, and 80+ IPTV control panels.
Money Laundering / Financial Concealment	Used cryptocurrency billing, forged identities, and distributed infrastructure to hide revenues and obscure operational roles.
Tech Tools Used	1,400+ servers, mirrored websites, IPTV panels, encrypted communications, cloned streaming nodes, and false-identity registration.
Law Enforcement	Italian Postal and Communications Police, Catania prosecutors, Europol, Eurojust, and partner agencies across 15 countries.
Charges Filed	Criminal conspiracy, IT intrusion, computer fraud, money laundering, and illegal broadcast piracy.
Evidence Base	Eurojust and Europol statements, multi-country raid data, and supporting enforcement coverage.
Why It Matters	One of the largest piracy busts ever recorded, showing that major IPTV rings now operate at Organized-crime revenue scale.
Overlap with Weapons and Narcotics Recovery	Raids yielded firearms, narcotics indicators, crypto assets, and other contraband - clear signs that the piracy platform sat within a wider trafficking environment.

MeuPlayer IPTV	
Category	**Details / Highlights**
Criminal Type	App-based IPTV operation prosecuted through money-laundering and Organized-crime lenses, with weapons and narcotics indicators recovered in raids.
Illicit Revenue	More than R$3.2 million processed through over 5,000 individual deposits linked to illicit IPTV subscriptions.
Modus Operandi	Distributed pirate IPTV through Android and Windows apps, collected thousands of small payments, and routed proceeds through front companies to disguise origin.
Money Laundering	Used a sham hosting company and personal investments, including a Porsche and real estate, to transform streaming revenue into legitimate-seeming wealth.
Tech Tools Used	Pirate streaming apps, bank-transfer aggregation, Windows and Android clients, and structured account networks.
Law Enforcement	Brazilian federal and state police, Sao Paulo financial-crime court actors, and Operation 404 enforcement partners.
Charges Filed	Money laundering convictions first, with copyright and criminal-enterprise matters pursued separately.
Evidence Base	Banking records, app-distribution evidence, seizures of firearms and ammunition, and court findings from Sao Paulo.
Why It Matters	Strongest Latin American example of piracy revenue moving through armed criminal ecosystems and being targeted through financial-crime law.
Overlap with Firearms and Drug-Nexus Indicators	Firearms and ammunition were seized, and prosecutors described piracy as supplementary revenue within criminal environments already tied to narcotics activity.

Cases Which Overlap with Organized Crime Characteristics / IOC Indicators.

Manga Mura / Romi Hoshino	
Category	**Details / Highlights**
Criminal Type	Industrial-scale manga piracy platform operated as a highly organized digital infringement enterprise, monetizing stolen copyrighted works through ad-driven traffic and premium platform features.
Illicit Revenue	Exact illicit revenue undisclosed publicly; platform drew nearly 100 million monthly visits at peak. Linked to approximately US $2.1 billion (¥320 billion) in estimated industry harm. Tokyo court later awarded US $11 million+ (¥1.7 billion) in civil damages against operator.
Modus Operandi	Aggregated and displayed pirated manga through a centralized reader interface designed to mimic legitimate digital reading platforms; monetized traffic through advertising and reportedly explored premium/paying user models.
Money Laundering / Financial Concealment	Advertising and platform monetization structures remain only partially disclosed publicly; available reporting indicates ad-based monetization and attempted premium models, though no proven laundering scheme was publicly established.
Tech Tools Used	Offshore hosting providers, mirrored image/CDN-style storage systems, proxy/redirect infrastructure, obfuscated backend routing, domain shifting, and web-reader interface optimized for frictionless mass consumption.
Law Enforcement	Japanese publishers and anti-piracy groups initiated technical tracing efforts; investigation progressed with Japanese law enforcement and international cooperation culminating in arrest of operator in the Philippines and extradition to Japan.
Charges Filed	Criminal copyright infringement charges in Japan; subsequent civil actions by major publishers resulted in record damages award. Operator convicted and sentenced to imprisonment.
Evidence Base	Traffic analytics, publisher investigations, hosting/server tracing, payment and advertising monetization records, technical forensic analysis, operator attribution evidence, and extradition/arrest records.
Why It Matters	Landmark Asian case demonstrating that non-IPTV digital piracy can reach industrial scale with infrastructure, monetization, and evasive sophistication resembling organized cyber-financial enterprises.
Overlap with Organized Crime Characteristics / IOC Indicators	The operation exhibited multiple hallmarks of organized digital criminality: sustained profit motive, industrial monetization, distributed international infrastructure, operational evasion, jurisdictional arbitrage, prolonged continuity, and sophisticated technical compartmentalization.

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 IP House

IP House is a global one-stop-shop intellectual property protection and enforcement company dedicated to safeguarding innovation by protecting brands from counterfeiting, piracy, and all forms of IP theft. Through its integrated online-to-offline enforcement model, IP House delivers end-to-end brand protection services—combining proactive marketplace assessment and online monitoring with strategic threat and intelligence analysis. Its capabilities include notice and takedown programs, test purchases and controlled buys, people and asset tracing, covert surveillance, and on-the-ground enforcement operations designed to disrupt illicit networks at scale.

IP House collaborates with law enforcement and regulatory authorities worldwide, supporting coordinated action across jurisdictions. The team spans North America, Latin America, Europe, Africa, Asia Pacific, and the Middle East operating around the clock to detect, monitor, and address IP infringement wherever and whenever it occurs. The result is a truly global approach to IP enforcement that protects innovation, reinforces compliance across markets, and holds bad actors accountable. IP House is committed to preserving the value and safety of authentic products for brands, creators, and consumers worldwide.