

Investigating Converging and International Criminal Markets

In many parts of the world, multiple criminal markets operate, and sometimes even converge, in the same space, which complicates criminal investigations. Criminal organizations often operate international, which makes tracing their activities and defying members, command structures, and affiliates time-consuming.

Especially for detecting patterns and intent to prevent further illicit activities requires getting actionable insights based on collected and analyzed OSINT data.



CRIMINAL MARKETS ARE HIGHLY DYNAMIC

Often converging with other criminal markets, with international operating criminal organizations as main market players.

POLY-CRIMINALITY

Major criminal organizations operate across multiple illicit business lines using the profit of one business activity (e.g., weapons trade) to finance another business line (such as operating meth labs).

Organized crime groups across the world involved in human trafficking are often also involved in the drugs trade, illegal fishing, environmental crimes, arms trafficking, maritime piracy, or tobacco smuggling.



40%

Engage in more than one main criminal activity



INTERNATIONAL DIMENSION AND MOBILITY

Criminal organizations purchase goods or services from each other internationally to boost their business, using online (dark web) marketplaces to buy and sell illicit goods and services using encrypted communications and payment solutions.

Since these criminal organizations operate in different criminal markets, they are not in direct competition with each other, such as a drug syndicate buying weapons from an arms trafficking network.

Large criminal enterprises often have specialized in-house services (e.g., document forgery), that they also sell to other crime groups.



7 out of 10

Are typically active in more than three countries

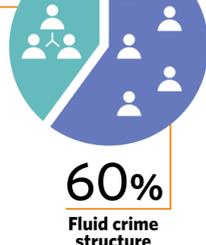
STRUCTURE AND COMPOSITION

The majority of criminal organizations in the EU have a fluid structure in contrast to hierarchical structured criminal enterprises.

These loosely organized criminal networks collaborate with individual threat actors and groups to promote their shared criminal objectives, which makes their operations more complex and difficult to detect.

40%

Hierarchical structure



60%

Fluid crime structure

The largest market players in criminal markets are criminal networks that are very well organized and engage in serious and organized crime.

In this networked ecosystem, cooperation between criminal network members is fluid and systematic, serving the common goal of generating as much profit as possible.



Criminal networks easily adapt to new circumstances in the environment they operate in, turning obstacles into business opportunities.

During COVID-19, the flow of drugs across countries reduced sharply, but the shortage of Covid-related medical products provided new opportunities for illicit profits.

ORGANIZED CRIME RINGS

Cybercrime has become a major source of income for criminal networks, costing the global economy \$445B annually. Cyberattacks are conducted by well-organized crime rings that operate internationally.

Know-how and hacker tools are shared on the dark web, with stolen data put up for sale on dark web message boards and marketplaces.

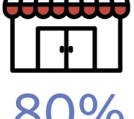


80%

Of cyber-attacks are driven by organized crime rings, in which data, tools, and expertise are widely shared.

LEGAL BUSINESS STRUCTURES

The lines between criminal networks and legitimate business can be blurred, with a legitimate business generating income for rendered services (banking, legal advice) and crime networks using the legitimate business to e.g., launder illicit profits or using the legitimate business as a front.



80%

Use legal business structures for their criminal activities.

CHALLENGES OF INVESTIGATING CRIMINAL MARKETS AND THEIR PLAYERS

International operating and converging criminal organizations complicate joint efforts due to diverging legal frameworks. Criminal markets quickly adapt to changes in the ecosystem in which they operate.

By identifying key nodes in criminal networks, investigators can take action to disrupt multiple criminal activities simultaneously, forcing such networks to go out of business.



Members and affiliates of criminal networks often interact with service providers and brokers in key roles, which complicates criminal investigations.



Interactions and cooperation between criminal market players are fluid, systematic, and profit-driven, making them hard to trace for law enforcement.

60%

of the criminal organizations in the EU engage in corruption and 38% in drugs



Criminal market players use encrypted communications and social media to network and exchange information between them, and to buy/sell illegal goods, which complicates investigations.



The use of violence and corruption are the main features of criminal organizations and can be the result of growing competition or can be marketed as a service on dark web platforms and encrypted communication apps.

CRIMINAL PROCESS CHAIN

When investigating criminal markets and the main market players dominating such markets, investigators focus on three main aspects of the criminal process chain: acquisition, money flows, and facilitating goods and services. Collecting and analyzing OSINT data is crucial to analyze criminal markets, detect patterns, identify players, and solve crimes, and prevent criminal activities.

This requires a versatile and automated tool to collect and analyze OSINT data based on search parameters for quick and efficient actionable insights for follow-up. Using Artificial Intelligence and smart Machine Learning and Natural Language Processing algorithms.

Such a platform should achieve the following for supporting comprehensive investigations:



Identity Resolution

Following the digital footprints of criminal market players with a single identifier using a one-click search.



Location Intelligence

Collecting and analyzing location-based OSINT data using interactive maps with one click.



Secure Online Investigations

Providing anonymous and safe browsing on the surface, deep, and dark web in order to collect critical insights and act in real-time.



Regulatory Compliance

Collecting and analyzing only data from publicly accessible sources to ensure the authenticity and preservation of digital evidence.

To discover how your organization can benefit from Cobwebs Web Intelligence Platform contact us today.

[Book a Demo >](#)

Cobwebs Technologies

Cobwebs Technologies is a worldwide leader in web intelligence. Our innovative solutions are tailored to the operational needs of national security agencies and the private sector, identifying threats with just one click.

Cobwebs solutions were designed by our intelligence and security experts as vital tools for the collection and analysis of data from all web layers: social media, open, deep and dark web. Our web intelligence platform monitors these vast sources of data to reveal hidden leads and generate insights.

Our exclusive technology extracts targeted intelligence from big data using the latest machine learning algorithms, automatically generating intelligent insights.