Visualizing Criminal Networks

White Paper

COBWEBS TECHNOLOGIES

Introduction

Organized crime networks are billion-dollar businesses operating in many crime areas. As a general rule, organized criminal networks are involved in many different types of criminal activities spanning several countries. These activities may include trafficking in people, drugs, illicit goods and weapons, armed robbery, counterfeiting, and money laundering. With revenues estimated in the billions, criminal networks have operating models, long-term strategies, hierarchies, and even strategic alliances, all aimed at generating maximum profit with minimum risk.

As part of its global strategy on organized and emerging crime, INTERPOL made the identification of criminal networks, major figures engaged in serious transnational crime, and associated criminal networks and their key activities a top priority. Its five-year strategy consists of enabling member countries to target and disrupt transnational criminal networks by identifying, analyzing and responding to emerging criminal threats.

But these-criminal networks pose a huge problem for judicial and enforcement agents due to their complexity and obfuscation. In most countries, outdated methodologies and concepts are used that cannot analyze huge criminal networks. Investigating and prosecuting crime today require computational tools for processing, analyzing, and visualizing vast amounts of data.

In this white paper, you will learn more about:

- Criminal networks
- Visualization of criminal networks
- WEBINT platform

Visualization of Criminal Networks

"We're learning new insights about individuals by taking very specific physical events, let's say like a string of robberies, and identifying huge spikes of activity during that same period of time. We can then create a dynamic spring layout (a series of nodes that represent possible members of criminal networks) and analyze how those members interact and shape their interconnections over time."

Emilio Ferrara | Researcher at Indiana University's School of Informatics and Computing

Criminal Networks

The FBI defines a criminal network as a group of individuals with an identified hierarchy, or comparable structure, engaged in significant criminal activity. These networks often engage in multiple criminal activities and have extensive supporting networks. Members of these networks often operate transnationally for the purpose of obtaining power, influence, and financial gains. (Global Initiative against Transnational Organized Crime).

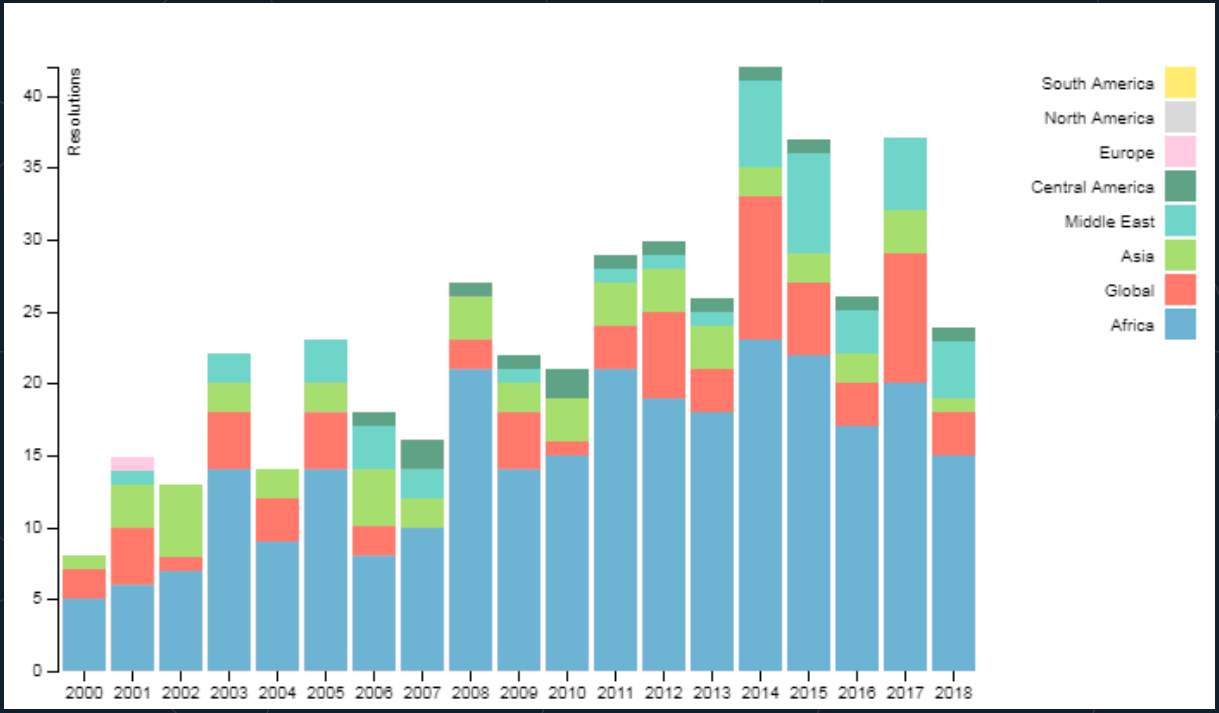

Figure 1 - Organized Crime and Illicit Flows

Visualization of Criminal Networks

By visualizing a criminal network, investigators can extract core information such as the flow of information in the network, who controls that network, what coordination patterns are there, and how information is executed and concealed in a criminal network. Since criminal networks evolve over time, so do their structure and relationships. This makes monitoring criminal networks challenging since these changing patterns make it difficult to analyze the degree of violence of the various groups and subgroups powerful actors who dominate the network.

Network visualization (also known as graph visualization or link analysis) is the process of visually presenting networks of connected entities in a schematic form, such as shown below. The image shows objects (nodes) and the relationships (edges) between them. These objects could be people, computers, or buildings, while the corresponding relationships could be group member ties and Internet connections. The connections are denoted as positive ties for criminal partnerships, or negative ties for hostile relationships. The betweenness and closeness of nodes are measured to identify the key players in a criminal network. This network visualization below shows a criminal network in Italy based on a case study using unique cell phones and phone calls. (Indiana University Bloomington).

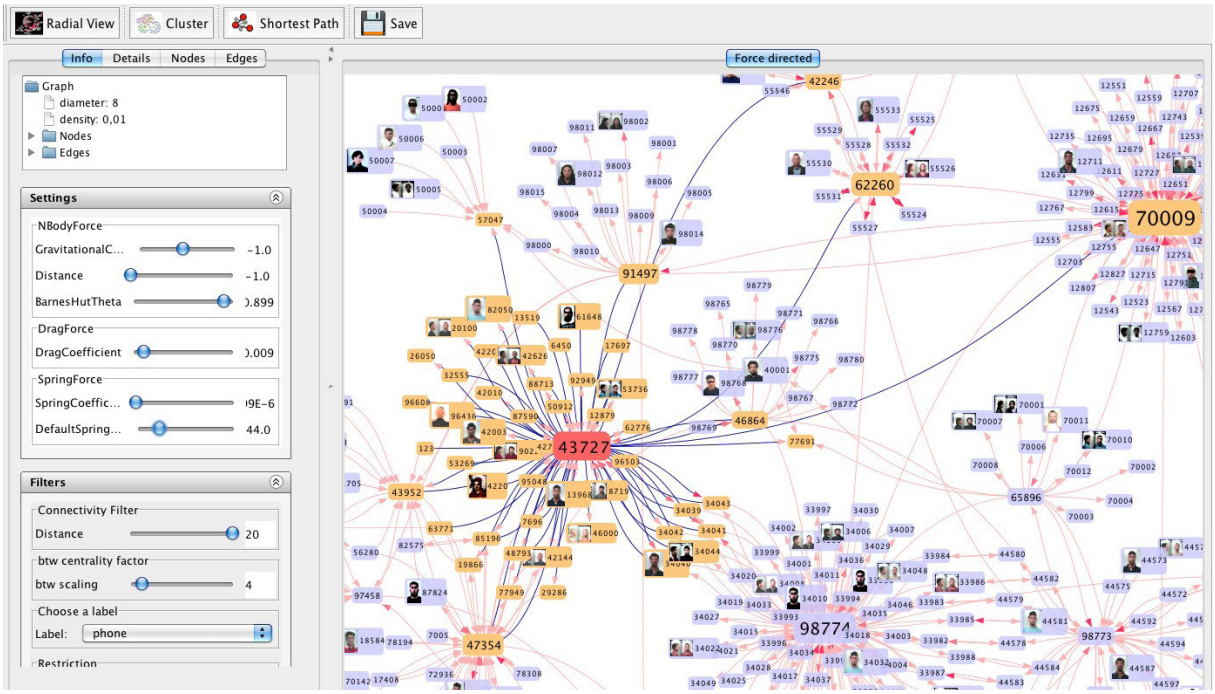

Figure 2 - Example of a visualized criminal network

Visualization of criminal networks with WEBINT solutions

"Law enforcement and government agencies use WEBINT solutions for predictive analysis, face recognition technology, and social media intelligence to gain insight into criminal networks, their members, and associates to target them. With predictive data indicating the sentiment, motives and geo-locations of these members and associates, these criminal networks can be visualized, identifying each member with an individual profile, location, and behavior pattern, and place in the network's hierarchy."

Omri Timianker | President of Cobwebs Technologies

In order to reveal the inner workings of criminal organizations, an AI-powered WEBINT platform using machine-learning algorithms is needed. Robust artificial intelligence algorithms are able to expose an entire network of conspiring actors in the planning and execution of violent crimes, terror, and cybercrime. Machine learning and deep learning technologies connect the dots between the various members. This allows investigators to learn the names, faces, locations, and hidden messages woven into the coded language of each member's communication. The solution scans the internet and relevant mobile apps for predefined keywords, terms, and entities.

Filling in the gaps of information required to prevent crime and terror, and resolve investigations is complicated due to the sheer volume of infinite online data. Between social media activity, mobile chat apps, and the dark web's obfuscated and encrypted communication, identifying critical pieces of information has become an inherent aspect of criminal investigations. AI allows terrorist, criminal and cybercrime organizations to be identified, geo-located, and prosecuted to prevent escalation of events in real-time as well as taking place in the future.

Only AI-driven solutions can detect and analyze structured and unstructured data (such as texts, pictures, and social media posts) effectively. Such a platform can visualize anonymous target details, conduct automatic searches, and analyze objectives, groups, and locations. This enables law enforcement to get into the structure and operations of criminal networks, their individual members, interactions, locations, and intent. Such a platform must use machine-learning algorithms developed with methodologies that meet the requirements of law enforcement agencies globally. It enables organized crime investigators to harvest and evaluate data from a wide variety of sources to generate profound and insightful takeaways and receive notifications of suspicious behavioral or communication patterns of a criminal network. This simplifies the complex investigations of cross-border organized crime dramatically.

The AI-powered WEBINT solution of Cobwebs Technologies

The WEBINT platform of Cobwebs Technologies turns intelligent information into actionable Insights. Law enforcement uses the platform to effectively reduce terror, violent crimes, drug trafficking, and cybercrime. Since the AI-driven software integrates seamlessly and agile and user-friendly, cases are investigated and solved at an exponentially faster rate. Visualizing the intricate pattern of connected places, people, items, faces, and dispersed data related to specific criminal networks, the powerful AI technology extracts intelligent insights on criminal collaboration and presents the bigger picture to investigators. The platform enables investigators to save precious time, and to acquire the necessary documents for legal action against criminals (e.g., warrants, subpoenas, and court orders) to prevent future crime.

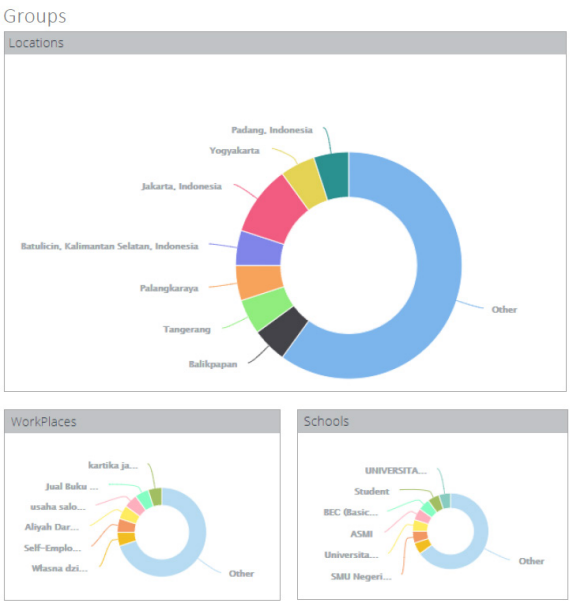

Figure 3 - Group analysis

The three screenshots on the left are the result of monitoring the dark web, in this case focusing on terrorist cells. The first screenshot shows groups active in specific cities, such as Jakarta, Indonesia. Based on correlated data, this might indicate an active terror cell. The next screenshot gives a breakdown of workplaces. Some of those are known by law enforcement as being a hotbed for criminal activities. Schools are another important metric. Certain universities are known to radicalize students, as terror attacks in the past have shown.

The WEBINT solution of Cobwebs Technologies uses AI and machine-learning algorithms to collect and analyze data from a wide range of sources, including the dark web. The powerful platform detects and analyzes the digital footprints that terror, criminals, and threat actors leave behind, even on the dark web.

By monitoring social media platforms and message boards on the surface, deep and dark web, discussions about specific topics can be de-anonymized, and this data can be used for e.g., identifying a crime organization or terror group, and for preventing acts of violence. (See Figure 4 below)

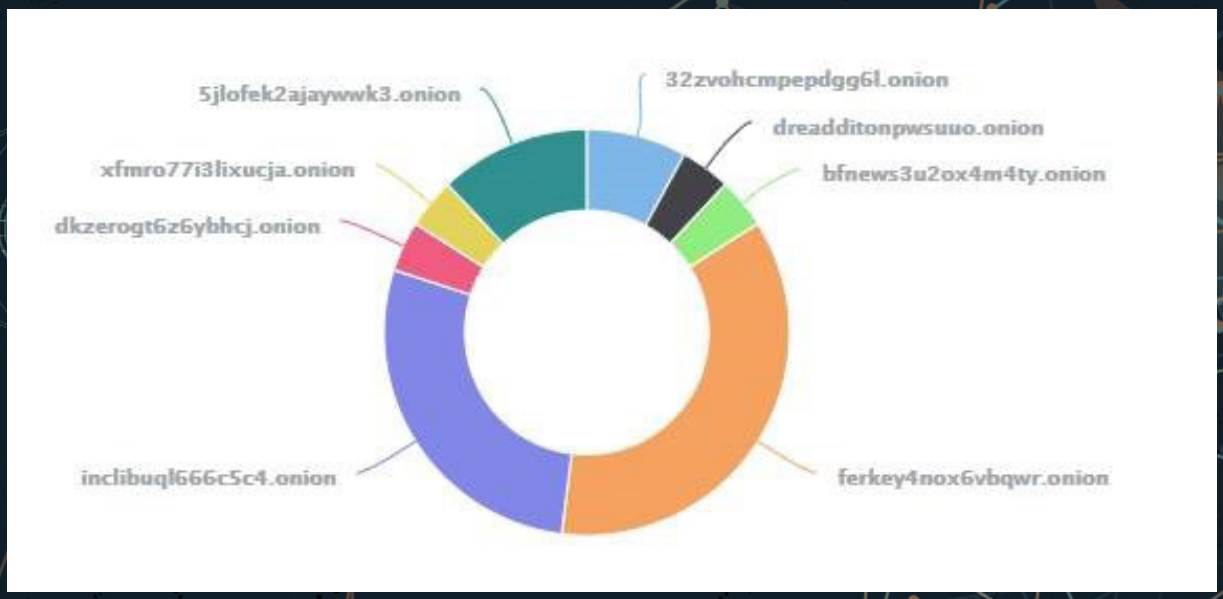

Figure 4 – Dark web sources discussing guns

The extraction of critical data helps to identify criminal networks, generate critical clues and leads, geo-locate those networks and their members, and tag online content within those networks. This way, sensitive information is detected by analyzing vast amounts of data. The facial and image recognition capability, word and text identification of predefined keywords and entities with advanced NLP (Natural Language Processing), deciphering the relevance, reliability, accuracy and even sentiment of data, real-time notifications of vital insights for optimal response times in critically time-sensitive situations are now a reality. National security agencies and government organizations, as well as law enforcement and border control, employ the cutting-edge technologies and services of Cobwebs Technologies to battle and prevent organized crime.

About Cobwebs Technologies

Cobwebs Technologies is a global leader in Web Intelligence providing innovative solutions tailored to operational needs of the public and the private sectors by identifying threats and generating insights in real-time.

The Company's advanced artificial intelligence and machine learning algorithms deliver powerful threat intelligence by deciphering the intricacies of web layers and analyzing the complex details of structured and unstructured data. Its web intelligence platform monitors these vast sources of data for revealing hidden clues and generating insights for intelligence-enhanced security to keep the world safer.

Ready to learn more about our platform?
Visit www.cobwebs.com or reach out
to a local sales representative.