FIGHTING GANG VIOLENCE
LEVERAGING SOCIAL MEDIA

White Paper
Violence in urban and suburban neighborhoods, particularly in minority communities and those of limited socioeconomic means, has been a concern for decades. With the dominance and growing impact of social media, gang violence is now instigated through these virtual social spaces, resulting in criminal acts such as shootings. Gangs make their mark by provoking violence and threats via social media platforms. Gang affiliates exploit their online presence to promote gang identity and gain notoriety.

Gang members are extremely active online, leaving digital footprints that can be traced and used in criminal investigations. This allows law enforcement agencies to harness data collected from social media to identify gang members and their planned actions to prevent crime.

In this white paper, you will learn more about:

• Gang network
• Gang violence
• Gangs on social media
• WEBINT and HUMINT solutions

“SOME 33,000 VIOLENT STREET GANGS, MOTORCYCLE GANGS, AND PRISON GANGS ARE CRIMINALLY ACTIVE IN THE U.S. TODAY. MANY ARE SOPHISTICATED AND WELL ORGANIZED; ALL USE VIOLENCE TO CONTROL NEIGHBORHOODS AND BOOST THEIR ILLEGAL MONEY-MAKING ACTIVITIES, WHICH INCLUDE ROBBERY, DRUG AND GUN TRAFFICKING, PROSTITUTION AND HUMAN TRAFFICKING, AND FRAUD. MANY GANG MEMBERS CONTINUE TO COMMIT CRIMES EVEN AFTER BEING SENT TO JAIL.”

Federal Bureau of Investigation
To better understand gang violence, we first need to understand the intricacies of gang networks using social network analysis. Utilizing WEBINT tools for reconstructing profiles based on data derived from social networks, a gang, its leaders, core members, and associates can be visualized for criminal investigations regarding gang violence. Image 1 below represents such a visualization. The correlation between a gang member and locations, names, email addresses, types of drugs (grey icons featuring a syringe with the name of the drug next to it), organizations, workplaces, calendars, etc. are mapped. Based on this visualization, law enforcement can identify the structure, hierarchy, and main activities (in this case the buying, selling, and dealing of drugs).

In the peer-reviewed journal Crime Law and Social Change, the paper “Technology and conflict: Group processes and collective violence in the Internet era” was published that described the inner workings and dynamics of gangs. The diagram below represents the cycle of gang violence.

![Figure 2 - Cycle of Gang Violence](image)
The cycle of gang violence is often triggered by poverty and institutional racism. Once a gang is joined, a gang member gets a sense of belonging and security. Gang members like to embrace “Street Culture” and violence as part of their new social status. Combined with peer pressure, all this makes at-risk youths especially susceptible to join gangs. Once gangs are formed, they start to act and react close to the territories of other gangs, which is a fertile ground for escalation of violence. Gangs vary in size, conflict history with other gangs, street code, online presence, technological skills, and propensity for violence and crime. The reaction to violent acts can be intervention, de-escalation, or retaliation.

**GANGS ON SOCIAL MEDIA**

Overall, social media is playing a primary or secondary role in the radicalization of extremists and the mobilization of street gangs. Terrorists use social media platforms in various ways, including to consume and spread extremist narratives, create sharable content, and/or communicate with like-minded individuals. With the exponential growth of social media, user-to-user platforms have become an important factor in the radicalization and mobilization of extremists and gang members in recent years. According to a study in 2016, the social media use of extremists has grown dramatically since 2005 (START Research Brief).

![Figure 3 - Social Media Use among U.S. Extremists, 2005-2016](image-url)
With social media becoming a venue for publicizing violent attacks by gangs against civilians or rival gang members, the online presence of gang members has increased gang crimes. It only takes one post, tweet, share, or retweet to instigate a violent crime. While social media platforms are boosting their security measures to reduce online hate crimes and resulting in gang crimes, law enforcement must cope with online and offline gang violence. Police in various cities are taking comprehensive measures and investing data-driven solutions to address escalating gang violence triggered by social media. Recognizing gang violence online gives law enforcement a chance to tackle active and violent gangs.

Gangs operate in the real world, but also have an extensive social media presence. Social media have profoundly changed gang activity in the United States. According to a new report, “the Gang Book” by the Chicago Crime Commission, social media often appear to amplify and speed up the cycle of aggression and violence. Social media has become a rapid vehicle for violence with real consequences. Law enforcement worldwide are now paying attention to “cyber banging”. Rival gang members often follow and even friend each other on social media to exchange insults. Killed gang members are memorialized online, making their deaths fuel for online feuds. Some gangs also use private groups and privacy settings on social media platforms for marketing their drugs and firearms.

Figure 4 shows the main types of drugs that were discussed on social media by e.g., buyers, sellers, dealers, and gangs. These data were collected and processed by an AI-powered WEBINT solution in real-time. (Cobwebs Technologies)
Law enforcement officers are looking for innovative technologies that can crunch data on social media platforms for getting actionable and intelligent insights. Concrete intelligence must be collected and processed from the emerging and evolving activities of gangs on social media. Such solutions must provide entity association, hashtag monitoring, facial recognition of possible suspects, guidance in correlating one social media user to the next, etc. When fighting gangs, human (HUMINT) and artificial (AI) blend together to keep violence off the streets and off social media platforms.

There are thousands of online information sources that can be leveraged for collecting data. However, it is often complicated to determine the starting point of a search and where relevant data can be found. By using a predictive artificial intelligence program, likely perpetrators of violence can be identified by mining and analyzing data collected from social media accounts. This real-time monitoring of potential crimes and violence generates automated alerts of suspicious or violent activities; these alerts must be issued as soon as these happen.
WEBINT AND VIRTUAL HUMINT

To fight gang violence, investigators need to analyze vast volumes of data originating from multiple web and social media sources. Content that contributes to the investigations is found and accessed online or through real, live individuals. By creating and using avatars (virtual agents), investigators can gather data from various open and human sources on the web. Intelligence agencies can now collect data from various virtual HUMINT sources online using tools to gather intelligence. They can work anonymously thanks to a global proxy infrastructure without their cover being blown. The ability to mask themselves provides the key to securely browse platforms to extract data such as IP addresses and other key identifiers.

“THE CALL TO ACTION FOR LAW ENFORCEMENT AGENCIES THROUGHOUT THE UNITED STATES AND GLOBALLY IS TO MAKE THE MOST OF INNOVATIVE TECHNOLOGIES SUCH AS WEBINT AI-POWERED PLATFORMS THAT CRUNCH SOCIAL MEDIA PLATFORMS’ DATA AND CHURN IT OUT INTO ACTIONABLE AND INTELLIGENT INSIGHTS. PREVENTION OF VIOLENT CRIME, MURDER, DESECRATION OF FAMILIES, NEIGHBORHOODS AND EVEN VIOLENT ATTACKS AGAINST YOUTH AND CHILDREN IS NOW POSSIBLE.”

Udi Levy, CEO of Cobwebs Technologies

Figure 3 - Cobwebs Safe Web Browsing Tool
Cobwebs Technologies assists analysts in the creation, management, and maintenance of essential information collected by avatars over time. The smart technology supports these processes by utilizing worldwide proxy services and adhering to proper intelligence methodologies for safe web browsing utilizing advanced automation services. The system provides analysts with relevant and critical data in real-time. The AI-powered WEBINT platform with machine learning algorithms enables analysts to identify and classify gang members and their activities on social media. By analyzing the profile of each gang member, investigators were able to understand their social status within the hierarchy and structure of the gang, identifying the gang leaders. Through monitoring their profiles and activities, the analysts receive live alerts relating to those members' activities and locations. By showing connection types, their relevance to targets, and the nature of their relationships, the collected critical data helps to locate targets, and to collect more information about each gang member for more in-depth profiling.

The smart analysis tools integrate all the data mined from various sources and conducts an automated and predictive analysis on gang members, connecting all the dots to recognize patterns and revealing hidden links to generate even further insights. Similar to traditional methods where intelligence operatives gained the trust of their suspect, analysts can engage with suspects online to gain their trust and uncover crucial intelligence. Leveraging AI and machine-learning algorithms, the WEBINT platform provides advanced virtual intelligence capabilities coupled with traditional HUMINT methods to gather all necessary information automatically and in real-time.

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.