Social Media INTELLIGENCE

Using Facebook, Twitter and other sites to combat organized crime

By **Tudoriu Constantin-Sorin** | Photos by The Associated Press

The international security environment has responded to the rapid development of the internet and mobile communications technology by developing a new intelligence domain — social media intelligence (SOCMINT). After the 2011 London riots, Sir David Omand, former director of the United Kingdom's Government Communications Headquarters, developed this new domain and defined it as a set of applications, techniques and capabilities obtained through the collection and use of social media.

In a 2005 video, Mark Zuckerberg described his goal for the social media platform that was to become Facebook as "[not] to make an online community, but sort of like a mirror for the real community that existed in real life." By 2018, social media platforms, along with the entire digital ecosystem, had outgrown this description.

OPPORTUNITIES AND LIMITATIONS

SOCMINT differs from open source intelligence (OSINT), which is produced from publicly available sources such as traditional media (newspapers, radio, television, etc.), public data (government reports, official data, etc.), web communities and personal reports. SOCMINT is the process of identifying, collecting, validating and analyzing data from social media sites and accounts using nonintrusive and/or intrusive methods to develop intelligence that reduces the unknown in the decision process. For law enforcement agencies, intelligence services and justice/legal institutions, SOCMINT provides real-time information on ongoing events filtered from the internet noise, making it useful for monitoring the processes of criminal acts, collecting evidence and predicting future events.

Social media has created the opportunity for interaction, without frontiers, between criminal structures and vulnerable individuals, and changed the paradigm for organized crime. There has been a shift from *omerta* (the Sicilian Mafia code of silence) to "cyber banging," defined by the Global Initiative Against Transnational Organized Crime as "exhibiting criminal power, recruiting members, or even acting directly against their enemies on social networks" because the code of silence was replaced by promoting or bragging about criminal services through social media platforms. Similar to how jihadists use the internet for conversion and recruitment, criminal groups recruit new members using social media platforms by promoting the luxury lifestyle, the gang's reputation and money.

In 2014, the website espresso.repubblica.it published a profile of the social network of Cosa Nostra scion Domenico Palazzotto, the Mafia boss of the Arenella district in Sicily. The article was titled "Mafia, the life on Facebook of the young godfather between selfies, limousines, luxury and insults to the police." It exposed the "values" of Sicily's new generation of criminal bosses. Palazzotto's Facebook page is a mix of ostentatious luxury and continuous bluster.

Members of Mexico's drug cartels have also been harnessing the power of the internet to run positive public relations campaigns, post selfies with their gold-plated assault rifles, scantily clad women and fast cars, and to "hunt down targets by tracking their movements on social media," according to a 2013 report on *Vice* magazine's website. Social media is empowering criminals and rewiring relations with potential new members or buyers. The Knights Templar (Caballeros Templarios, in Spanish) used to run a Facebook page under the pretense of being a small business, according to *Vice*.


INVESTIGACIÓN
CRIMINAL
AGENCIA DE
INVESTIGACIÓN
CRIMINAL

In 2005, law enforcement began detecting the online sharing by cartels of *narcomensajes* — short messages about the reasons for a killing — which later became narco videos used for propaganda. Some of the world's most ruthless drug cartels are voracious users of various digital platforms. The Sinaloa cartel, one of Mexico's most powerful crime groups, has a Twitter account (@carteidsinaloa) with 84,000 followers. A Twitter feed using the nickname of the cartel's now-jailed leader Joaquín "El Chapo" Guzman (@elchap0guzman) has 590,000 followers.

According to the Global Initiative, the "Twitter accounts of presumed Mexican drug traffickers have recently attracted the attention of international media as they give the opportunity to take a look at the lifestyles of the so-called 'narcojuniors,' the second generation of drug traffickers that have inherited the leadership of large criminal organizations." El Chapo's sons use multiple Twitter accounts, which, contrary to the generally low profile maintained by their father, engage in cyber banging and feature pictures of luxurious parties, women, exotic animals, cash and guns. Social media has provided organized crime groups with business and public relations opportunities and a quick way to communicate with members or potential buyers. From the Japanese Yakuza creating its own website to the cyber banging of next-generation Mexican cartel and Sicilian Mafia leaders, today's transnational organized crime (TOC) groups are visible on the internet and on social platforms because the users want to be known.

The difference between OSINT and SOCMINT is the difference between open source *exploration* and social media *exploitation*; it's the difference between *public* and *private*. For SOCMINT, there is debate over when it is legal or appropriate for agencies to use intrusive methods to collect information by entering the private space of individuals. To resolve the question of intrusive methods, Omand and his team established six principles to create a legal framework for the use of intrusive SOCMINT. According to an article by the British think tank Demos and co-authored by Omand, the "laws of war" for ethics in intelligence operations are: 1) there must be sufficient and sustainable cause; 2) there must be integrity of motive; 3) the methods used must be proportionate and necessary; 4) there must be the right authority, validated by external oversight; 5) recourse to secret intelligence must be a last resort if more open sources can be used; and 6) there must be a reasonable prospect of success.

Security agents guard a gate to the attorney general's office for organized crime as a convoy arrives carrying Damaso Lopez, nicknamed "El Licenciado," in Mexico City in 2017. Mexican prosecutors captured Lopez, one of the Sinaloa cartel leaders, after the arrest of Joaquín "El Chapo" Guzman.

SOCMINT uses the intelligence cycle — from planning and direction to collecting, processing and analyzing data — to produce the intelligence and disseminate it to the end users, who then use the information to plan and direct future intelligence gathering.

BEYOND THE CONVENTIONAL

The transition from an industrial society to an information society means that organized crime networks no longer exploit only the countries in which they originated; the networks have become extensions of the new, globalized world. TOC's exploitation of digital technology to enhance the efficiency and effectiveness of their operations can be compared to how youth behavior has changed with the expansion of the internet. When launched, Facebook, Twitter and Instagram planned to unite people, making geographic distance unimportant.

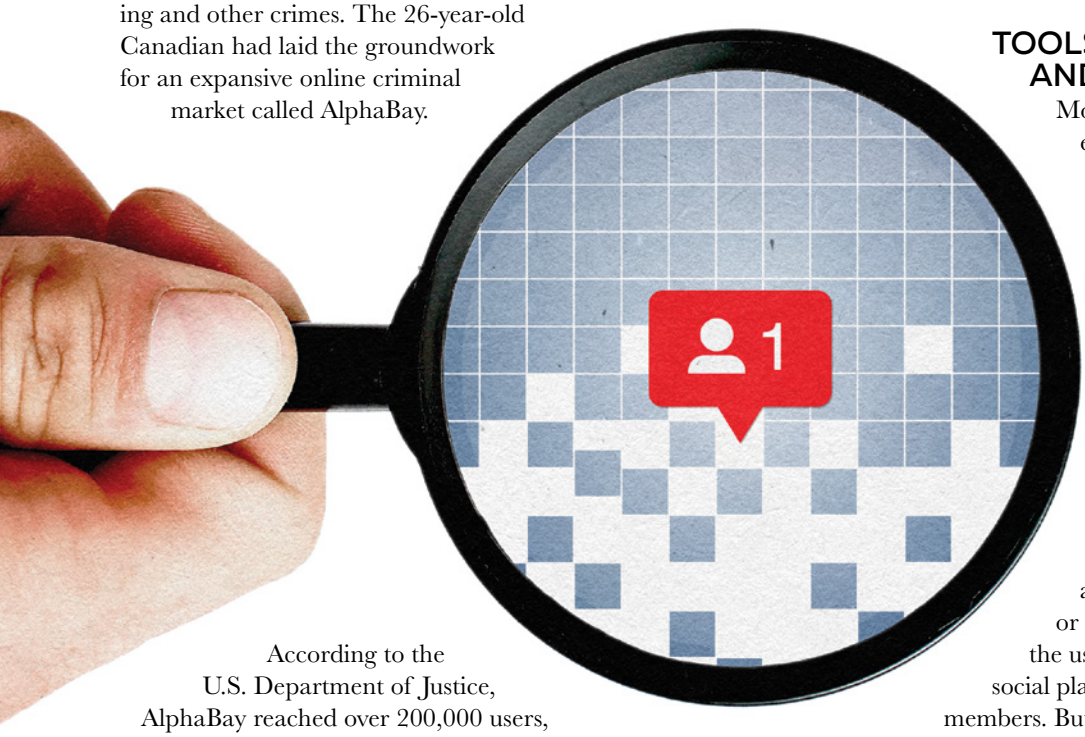
These bitcoin tokens were seized in Utah after U.S. prosecutors charged two men with conspiring to commit money laundering by selling more than $1 million in bitcoins to users of the black-market website Silk Road, which lets users buy illegal drugs anonymously.

But like a double-edged sword, they also managed to provide fertile ground for the promotion of violence. For example, the number of online games, many depicting graphic violence, has grown exponentially over the past 10 to 15 years, and YouTube is rife with channels extolling violence. In addition, in modern, digitalized society, individualism, relativism and instability make people more dependent and vulnerable, increasing their need for information to understand what they see online and what is happening around them. SOCMINT (which is able to identify online opinion) can play an important role against crime, particularly organized crime. Social media can be used in the fight against TOC but also can encourage aggressive behavior. This encouragement is known as a "primer effect," a concept theorized by American social psychologist Leonard Berkowitz, among others, whereby people's observations of crime lead them to think along similar lines and make comparable judgments, predisposing them to violence in interpersonal situations.

Which is the faster way to look for something: Go to the library? Or search the internet? Of course, nowadays a simple search of Facebook, Twitter, Instagram or the dark web returns a lot of information, including offers from TOC

groups that have set up shop on the internet. Let's compare the case of the Silk Road — perhaps the most well-known place online for anyone who wanted to purchase all sorts of illegal goods, ranging from illicit drugs to firearms, or even hitmen for hire — to the AlphaBay/Hansa Market case to see how intelligence can operate online.

Authorities took down Silk Road in 2013, but it was replaced almost immediately by new online marketplaces such as Silk Road 2, Agora and Evolution, where criminal vendors and buyers quickly resumed selling and buying illegal commodities. On behalf of the United States government, in 2017 Thai police arrested Alexandre Cazes in Bangkok on charges of narcotics distribution, identity theft, money laundering and other crimes. The 26-year-old Canadian had laid the groundwork for an expansive online criminal market called AlphaBay.



According to the U.S. Department of Justice, AlphaBay reached over 200,000 users, had 40,000 vendors for more than 250,000 listings for illegal drugs and toxic chemicals, and more than 100,000 listings for stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms and fraudulent services.

About the AlphaBay operation, Robert Wainwright, the executive director of Europol, said: "This can be frustrating, and we and our partners therefore decided to strategically exploit this criminal behavior by acting against two top markets in a coordinated strike to maximize disruptive impact." In the meantime, Dutch authorities, with the cooperation of international law enforcement, covertly seized the servers of Hansa Market, another large illicit darknet site. Instead of shutting down the site, Dutch police continued to run it covertly while monitoring the traffic. When AlphaBay was shut down, investigators saw an eightfold increase of users and, in a few weeks, collected information on high-value targets and delivery addresses for a large number of orders, which helped in other investigations.

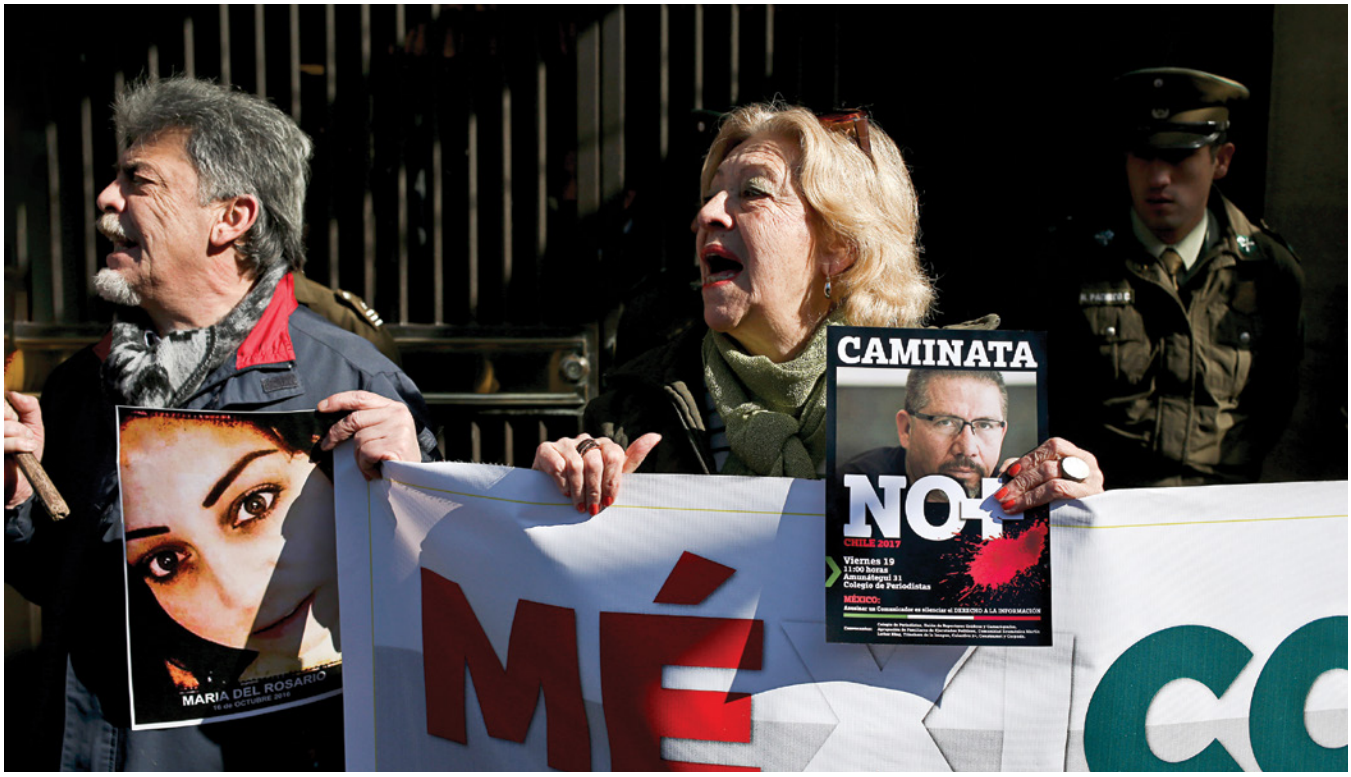
Unlike Silk Road, in the AlphaBay/Hansa Market case, law enforcement used intrusive online measures: going undercover by posing as criminals such as arms dealers in criminal forums, mining sites to reveal the identities of criminals who visit, tracking financial transactions, as well as traditional measures to track and physically prohibit the delivery of illicit goods such as drugs and weapons. About the successful operation, Europol's Wainwright said, "Addressing cyber crime and the use of information technology platforms for criminal purposes has become an important policing priority across the EU. The recent takedown in July 2017 of AlphaBay and Hansa, two of the largest darknet markets, is an example of how law enforcement can intervene to disrupt this environment."

TOOLS, METHODS AND TECHNIQUES

Monitoring, analyzing and extracting social networking data from TOC groups can provide valuable information about sites visited and used, reveal patterns to help understand complex relationships hidden in massive amounts of data, and detect fraud, transactions, and the scale and goals of criminal networks.

Avatars or fictitious accounts that are difficult or impossible to associate with the user are frequently used on social platforms by organized crime members. But by using intrusive measures like infiltration of accounts and fake identification, law enforcement can run online operations against criminal organizations. "Social media monitoring started in the world of marketing, allowing companies to track what people were saying about their brands, but with software that allows users to scan huge volumes of public postings on social media, police are starting to embrace it as well," National Public Radio said in an article about social media tools.

SOCMINT is the process of collecting and analyzing data gathered from across multiple social media sites and channels to understand users, identify influencers, monitor online conversations, mine customer sentiment and predict consumer behavior, among other purposes. To go beyond merely "listening," SOCMINT has myriad tools (because every social media platform and channel have unique features) that can be used in the intelligence analytical processes. Finding a person and mapping his or her online footprint is often used to establish the extent of a social media profile. Specialized software can create a



Chilean journalists in Santiago, Chile, protest the murder of Mexican journalist Javier Valdez, who wrote about drug trafficking and organized crime. He was slain in the northern state of Sinaloa, Mexico, long a hotbed of drug cartel activity.

profile from someone's presence on social media sites such as Facebook, Twitter, LinkedIn, Google+, YouTube and Instagram. Other tools can find and validate mail addresses, trace email and analyze traffic analysis or conduct screen-name investigations. There are tools, toolkits and apps to investigate websites.

SOCMINT was created to monitor "social media risk" after the riots in London and to detect trouble. Meanwhile, working with social media companies has opened new opportunities to law enforcement to geolocate and monitor users or content. Geolocating is an essential SOCMINT tool because members of criminal groups are often unaware of the functionalities of the applications they use and make mistakes. Based on observations and various studies, about half of the members of organized crime groups fail to disable geolocation for Twitter and Facebook postings, allowing online activity to be linked to a specific place, which in some cases is a prison from where a leader gives orders. Specific to TOC is a traditional hierarchy that, regardless of the form — in real life or on a digital network — contributes to maintaining loyalty. For SOCMINT, this hierarchy is an opportunity to identify and analyze how influence, respect or loyalty is represented online.

This relationship analysis uses SOCMINT tools such as Maltego, SocioSpyder, Visallo, Gephi and Ucinet to query public or private data sources to make sense of data and measure a person's relationships within the network. To understand behavior and determine influencers, law enforcement also mines blogging platforms for intelligence, infiltrates accounts through covert operations and works with visual blogs such as Instagram, SnapChat, Pinterest and Tumblr.

CONCLUSION

Globalization, the explosion of communications channels and the need to target new and richer markets brought about two major changes in TOC: criminal groups became more international, with cross-border crimes becoming increasingly frequent; and the groups have gradually shifted to a more businesslike approach, one vector of change being social media. TOC networks have turned to social media where dialogue is fast, effective, anonymous and encrypted, and as a result, law enforcement must deal with narco-twitters, cyber banging, cyber crime, human traffickers on the darknet and more.

Most TOC members are young and inexperienced, but have seen the benefits of social media, which is pervasive and impacts every aspect of modern life. Even if they do not directly use social media, organized crime groups are integrated into communities that share information about criminal activity online, which can be captured, analyzed and transformed into actionable intelligence by SOCMINT. For these reasons, SOCMINT must be seen as an opportunity for law enforcement to manage information in an increasingly intense online environment and a tool for planning operations that would be difficult to mount otherwise. □