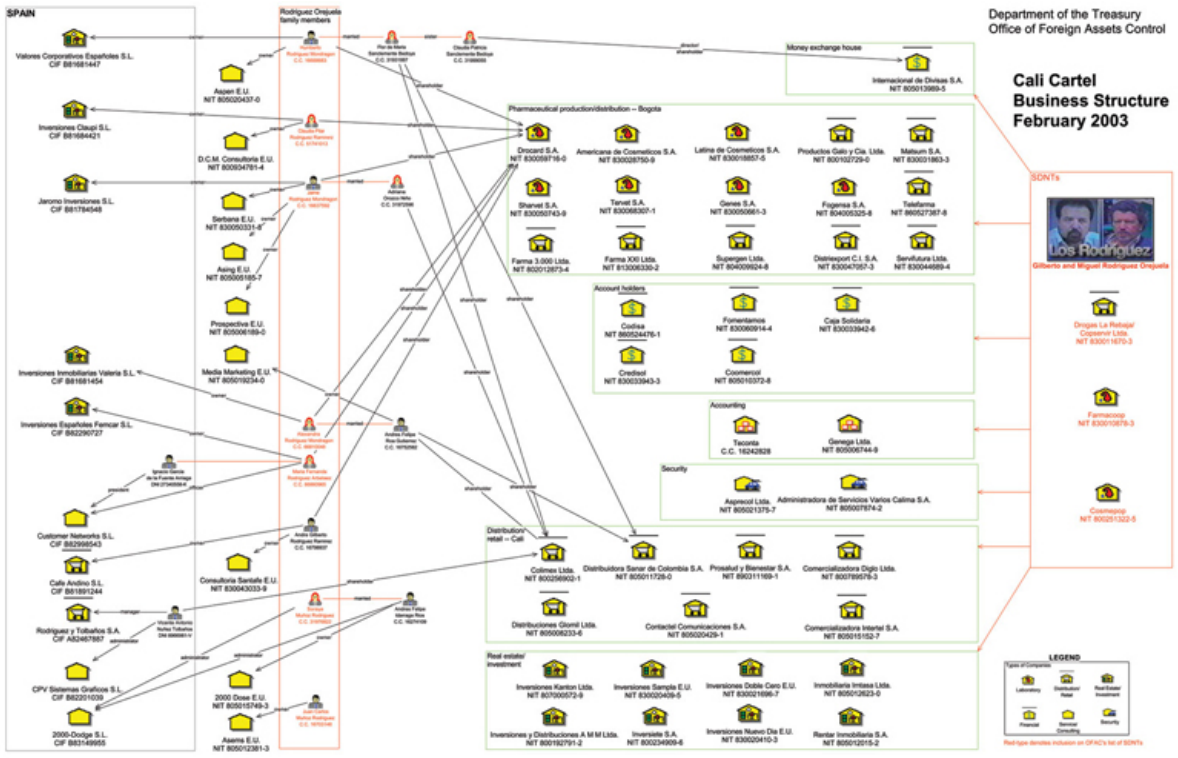
Formulas that drive Google, Klout, Facebook help researchers understand organized cybercrime

April 14 2015



This chart, which outlines the structure and hierarchy of the Cali drug cartel, was generated by the U.S. Department of the Treasury in 2003. Today, Drexel researchers are using social network analysis tools to get a better look at the structure of organized crime in cyberspace.

Notorious gangsters Al Capone and Carlo Gambino were famously done in by tax evasion charges. John Gotti, the "Teflon Don" was given up by a confidant. While the criminal masterminds of today are conducting their nefarious business online, the key to taking them down depends on understanding how they organize and where to squeeze them. Researchers from Drexel University's Privacy, Security and Automation Lab are searching for that pressure point by studying the activity of cybercrime forums. Their findings could guide the next generation of "Untouchables."

As part of National Science Foundation-funded research, Rachel Greenstadt, PhD, an associate professor in the College of Computing & Informatics and director of the lab; Vaibhav Garg, PhD, a former postdoctoral researcher at PSAL, Rebekah Overdorf a doctoral researcher in the lab; and their associate Sadia Afroz from the University of California – Berkeley; broke down several years-worth of conversations between members of four cybercrime forums that were anonymously made public a few years ago.

"We tried to answer the question 'what does organized crime really mean in cyberspace?'" said Garg. "To understand how criminals are 'organized' with people halfway around the world."

Using six centrality-finding formulas, whose variations are part of the the algorithms running Google's search engine, Klout's ranking system and Facebook's analytics, the team produced visual representations of the forums' organization.

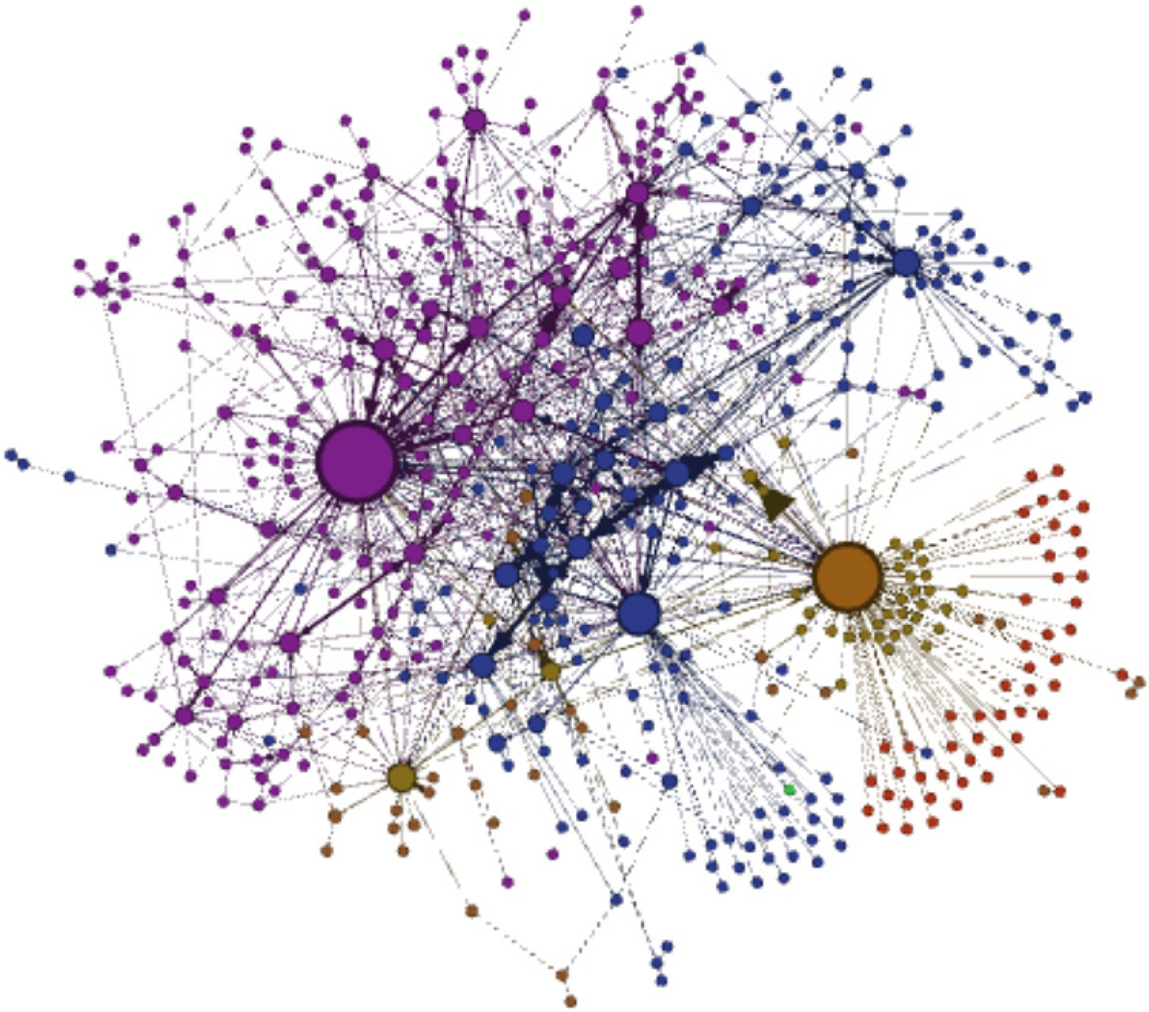
The formulas measure the relative connectedness of any one member in a network to other members. On the Internet a higher score in these analyses might mean a higher page ranking in a Google search. Among social networks, it could equate to a better Klout score.

In a cybercrime forum it could point out the leaders. The calculation tallies the number of people a person is directly linked to via a conversation or a transaction—with some stretching of the imagination, the exercise is not unlike a cybercrime version of the parlor game "Six Degrees of Kevin Bacon."

More connected cybercriminals hold a great deal of power in cybercrime forums because they are able to interact directly with a number of other members without going through an intermediary. Adding another person to an interaction begins to erode trust—and in a forum where people are operating anonymously trust is a commodity in short supply.

"The main challenge to cybercriminal organization is the lack of trust among peers," Overdorf said. "It limits group size and the efficiency of transactions."

By generating maps of the connections within the forums, the team found that online criminal operatives organize in two distinct communities—both of which will look familiar to any criminologist.



This social network graph which was generated from messages sent between members of a cybercrime forum called Carders, was created by researchers from Drexel's Privacy, Security and Automation Lab. It illustrates the "gang-like" structure that exists in cybercrime forums. The larger dots are the "most connected" members of each group, but the group sizes appear to be limited to just over 100 members and there is little interconnection between groups.

"We see these members arranging into groups that resemble gangs and mobs," Overdorf said. "This description has to do with their size, the

distribution of their leadership and how they conduct business in the forum."

Gangs in cyberspace sound a lot like the ones operating in cities for generations. They have one central leader who makes all the decisions for the gang. As a unit, they tend not to have a fixed goal, but will shift their operation to take advantage of the opportunities at hand.

"Gangs seem to go after whatever they can get their hands on," Garg said. "One day it could be stolen credit cards, the next, its bot nets. It's a more quick-and-dirty operation, relatively speaking."

Because of their two-tier hierarchy, gangs are limited in size. The team observed that a central leader could only maintain functional, trusted connections with about 150 members. This number is significant among cyber scholars and sociologists, who call it the Dunbar Number. It's shown to be the maximum number of meaningful relationships one person can actively maintain—a theory that informs everything from Facebook's news feed to the size of corporate offices.

By contrast, the cybercrime "mobs" that the team observed had hundreds or even thousands of members divided into multiple sub-groups each operating within a particular illegal revenue stream. This is roughly equivalent to the organizational structure of mafia or cosa nostra groups. For example, a group of 800 members of the forum called "Carders" primarily discussed drugs. A mob that included 1,447 members in the "L33tCrew" forum handled stolen Apple devices. Instead of having just one central leader, like a gang, several members of the mob share relatively equal centrality rankings.

To get from Dunbar's 150 to the thousand-member mobs that the Drexel researchers observed, it requires this broad distribution of leadership. And for this to occur there must be a system in place for earning trust

and punishing those who violate it.

The trope of becoming a "made man," or earning trust by performing a task to show loyalty, is central to the existence of organized crime. Joining the "family" in the parlance of organized crime, means the person is trusted.

In organized cybercrime, members earn trust by having positive transactions; meaning they deliver the goods they've promised. When they don't deliver or deliver bad or faulty products, they can be banned from the group. Members can also be banned if it is discovered that they have duplicate accounts, in an attempt to manipulate the market for their goods or otherwise deceive members of the forum.

This social network graph, created by researchers in Drexel's Privacy, Security and Automation Lab, depicts the messages sent between members. This graph illustrates a "mob-like" organization structure that exists in the cybercrime forum Carders. The larger green dots are the "most connected" or "most central" members of the group. The fact that there are several larger dots indicates a distribution of leadership that allows the network to expand.

Being kicked out of the group isn't as final a penalty in organized cybercrime as the, often fatal, recourse doled out to the mafia's "moles,"

"rats" and "stoolies." Cyber operators can simply rejoin or use an undetected duplicate account to gain admittance.

The challenge that this fickle formulation of trust poses for law enforcement is that while it might be relatively easy to gain admittance to a forum, it wouldn't be efficient to attempt to identify perpetrators. Few forum members would trust another member's identity, even within the context of the forum duplicate accounts are quite common. Trust is based on transactions, so that's where the team's research would advise law enforcement to make its move.

"We saw sub groups that specialized in everything from stolen credit card numbers, to drugs, to stolen hardware," Garg said. "But each forum shares a common characteristic: the e-currency it used. Some accepted payment on Paypal, other used WMZ or PSC for transactions, but every cybercriminal needs a way to get their money."

This situation could be a point of vulnerability for organized cybercriminals—and one that could be exploited by law enforcement, according to the researchers.

"There is a bottleneck with the currencies—even cyber criminals need to have a way to clean their money," Garg said. "E-currency companies already have the ability to collect information on who is using their product, if they are made to enforce laws or divulge criminal activities to authorities, it could be a way to catch cybercriminals or at least limit their activity."

Garg notes that this method could also clarify the murkiness of international laws regarding cybercrime. If a cybercriminal is tracked to another country, it may be difficult to extradite them in order to prosecute. But if law enforcement follows the money trail—much like the federal agents reeling in Capone in 1920s—it might be possible to

bring even the cagiest of organized cybercriminals to justice.

The group recently presented its findings at the Financial Cryptography and Data Security Conference. It is part of a series of investigations based on the forum data, that also includes a study on how to identify duplicate accounts and how erosion of trust can be used to grind cybercrime commerce to a halt.

Provided by Drexel University