

Cyberbanging: When Criminal Reality and Virtual Reality Meet

François Haut^A

In March 2013, two NYPD officers, photographs of whom had been published on Instagram with “Wanted” notices, were offered up for judgment and prosecution by gangbangers. The label read: “The 50z wants these pigs’ heads,” and prospective candidates for the murder were encouraged to “empty their magazine into them.” This is *cyberbanging*.

In France, there is much talk of cybercrime, less about *cybertactivism*. There is never any mention of *cyberbanging: gangbanging* on the Internet.

Gangbanging is the criminogenic activity of criminal street gangs. *Cyberbanging* is the convergence of the virtual world with the tangible criminality of these criminal gangs.

The criminal world is generally associated with being discreet and secretive, and holding conspiratorial meetings. This is not the case with criminal gangs, and never has been. They have always had a high profile, because each gang-member has to permanently demonstrate his pride in belonging to his gang. Such demonstrations are everywhere, including now on the Internet.

On *Facebook* and *Twitter*, as well as on *Instagram*, *YouTube*, and *MySpace*, we see it all the time: gang-members who are completely at ease with revealing their faces as they show the symbols of gang membership, brandishing firearms, sharing drugs, wads of banknotes, and girls.

It is true that we live in an open digital world, but gang-members as a section of the population operate with a degree of

transparency that would surprise the most committed Internet geek, as they terrorize the population in their neighborhoods and conduct their ruthless wars. These have been a reality for years.

We are faced, therefore, with a paradox: criminal activities which require great secrecy in order to succeed, alongside an outlandish need for notoriety for the individual or for the group to which he belongs.

This produces a virtual image of gang life—almost an intimate portrait—which might lead non-members to believe that they are almost a part of it. It can be a short step for noninitiates.

We can also see the benefits of mass awareness in terms of increased “prestige” for individuals, and the degree to which it reinforces the attractions of gang life, but we can also appreciate the intrinsic risks for those who are dazzled by it.

In order to understand this phenomenon, we will first provide an overview of the social media used, then what is found there and why. We will then look at the criminogenic effects of cyberbanging, and finally, what it means for combatting gangs violence.

I - A Brief Typology of Social Networks

While gangs have long used the Internet in the form of websites, the appearance of social networks has given them the opportunity to develop their imagination in other directions.

^A Head of the Department for the study of the Contemporary Criminal Menace, Université Panthéon-Assas, Paris

Under the heading “social network,” we find diverse means of communication which, in broad terms, use the Internet: magazines, forums, blogs, micro-blogs, wikis, podcasts, photo-, video-, and music-sharing sites, to mention a few. The list is almost infinite.

Access to these social networks is made easier with a smartphone, more than using a computer, but this also varies depending on the applications used.

They can be placed in the following broad categories:

- collaborative sites, like *Wikipedia*;
- blogs, forums requiring a password, and micro-blogs, which are often open (for example, *Twitter*);
- information sites, like *Leakernet* and *Digg*;
- video and photo sites, like *YouTube*, *Flickr*, *Instagram*;
- networking software, like *Facebook* and *LinkedIn*;
- computer games, like *World of Warcraft*, or system-specific ones, such as *Grand Theft Auto* and *Call of Juarez*;
- virtual worlds, like *Second Life*; and
- systems comparable to conventional telephony, like *Skype* and *Viber*.

These different social networks are not used in the same way or for the same purposes, and only some are used by criminal street-gangs.

These are evidently *MySpace*, the oldest network, which goes back to 2003, *Facebook*, *Twitter*, *Instagram*, *YouTube*, and *Flickr*. But new competitors are appearing, such as *Google+*, or thematic ones, which are also of interest to the gangs.

To these we must add a separate category—softwares that enable research into what is being said on the networks. This is clearly important for gangs, who enjoy

measuring the impact of their communications, of whatever kind.

One example is *WhoTalking*, which provides instantaneous information on what is happening on the most commonly-used networks, across the world, on any subject, and in any language.

For example, when a while back we entered the search term “Secte Abdoulaïe” into *WhoTalking*, we were able to find very specific information about the activities of that large north of Paris gang of the 1990s (and probably later), as well as photographs of some of their “heroes.” The document entitled “Sarcelles Storie” (*sic*), retraces their exploits, and gives details of their specialties, the areas of operation, and the periods of activity of “notorious” gang-members... all as told by one of the gang-members. A trip down Memory Lane! Very informative...

II - Developing Influential Communications

Gangs have always needed to make themselves known and express themselves, for a range of reasons. Communications have, therefore, always been an important aspect of this type of organized crime.

At the gregarious level, there is a need to show how powerful the group is, its domination of its neighborhood or territory, to make it known what the gang has done, or what its goals are. Intimidate...

For individuals, it is a matter of showing one’s courage by challenging enemies, of earning respect, or establishing one’s reputation.

This influential type of communication has been seen everywhere in the form of graffiti. It happens all over the world with this relatively simplistic and spontaneous criminality.

In Los Angeles, graffiti is known as the “journal of the street” and gang-bangers—as well as cops—were used to “read the walls” to understand what was going on. Graffiti can still be found in the streets there, but in general, the police and community associations clean them off after photographing them and adding them to a database, when resources allow, since they still represent useful information.

If not replacing graffiti, cyberspace widens and boosts the impact of this communication, without noticeably changing its fundamentals or its aims.

The objective is the same: to transmit information which enhances the group and its members, and let everybody know, especially their enemies, of their mood, intentions, and grievances. Communications may include photos or videos in which they show their weapons in order to demonstrate their strength, but sometimes might also show that a girl from an enemy gang has become the girl-friend of a member of their gang. This is a kind of provocation or intimidation.

They aim to give out information about recent developments involving the gang, the territories it has won, the successes it has had in its operations, and it is often the case that such communications take the form of a “gangsta rap,” performed by a rapper in the group, whose job it is to send out messages.

Gang-members also use social media to make it known that they are part of a particular gang, in order to back up their personal reputation, or to secure their place in the group by relating their part in some violent act, or by reporting imminent danger, either from the police or some other source.

While their objective is clearly the same as that of the graffiti, social networks

do have a fundamental difference: the speed and simultaneous nature of their broadcasting.

In order to read graffiti, you have to walk in front of it, even if that does not happen by chance; yet the Internet is immediate and inclusive. You can be sure that the information will reach all, or nearly all, intended recipients immediately.

Large-scale social media are used to channel influential communications from gangs, but so too are all other means of transmission, including, of course, verbal exchanges between people via *Skype* or *Viber*, which are said to be discreet, and more difficult to intercept than the telephone...especially if you keep changing your software, or use protection such as a VPN (virtual private networks) and encryption! All of these enhance criminal activities.

III - Tools for Criminogenic Gang Activities

Gangs have always followed technical developments in their criminal activities, either to use them, or to make a profit from them.

We have seen them equip themselves with pagers or beepers, which were used as tools for organizing the distribution of narcotics as much as for communication.

We have seen them steal and clone early cell-phones, those without SIM cards, in order to sell them or rent them out, but also to organize their operations while using somebody else as cover.

We have seen them use the first Internet telephony systems, with *MagicJack* devices.

Gangs have always been on the lookout for ways to keep in touch in order to coordinate their actions and organize their own protection.

The networks on the Internet have changed the nature of the relationship: not only can gang-members swiftly communicate with each other, but they can also undertake group communication both within their own group and in relation to their enemies, and indeed to wider society—for some, this communication can become genuinely addictive.

Those most “hooked” on it are known as “Facebook *drillers*.” In gang slang, to “drill” means to kill someone.

As soon as he wakes up, the *driller* goes on Facebook and gives free rein to his innate violence, starting by insulting people he hardly knows, or people in rival gangs. It is much easier to do this online than face to face. Then another person saves a screenshot of the message and begins to circulate it. Very soon, the whole criminal galaxy knows about it.

The person insulted must respond in order to save face. At this point, things can degenerate quickly, crossing over from the virtual world to become a reality on the street.

This addiction among those relatively under-occupied people also leads to what is known as *cyber-bullying*: harassment or intimidation carried out using social networks. There is also *sexting*, which involves adding violent sexual images or videos to abusive messages. This is daily life for many gang-members, made much easier because there is hardly any risk.

But there are also some ways in which activity on social networks crosses over into real action—what is known on the west coast of the United States as *flocking*. This is based on the same principle as a “flash mob,” whereby gang-members meet up at a location sent to them via a *tweet* or an text message, in order to commit a criminal act, often what is known as *swarming*, in which, for instance, a

store is looted of its entire stock.

In contrast, accolades glorifying the gang are more readily expressed through “gangsta rap” in its aggressive, provoking form.

“Gangsta rap” is the mass broadcasting of gang subculture. Before, there was only MTV, with all its limitations. Now, with *YouTube* or *DailyMotion*, and the easiness of making a recording, it is possible to reach millions of people in a few hours, almost single-handed. This is what is known as a “viral” effect...that can lead to bloody confrontations too.

This, for example, is the story of “Li'l JoJo” and “Chief Keef,” in Chicago:

To put it simply, the person known as “Chief Keef” posted a “rap” telling how wonderful his gang was (*the Black Disciples Nationals*), which went “viral,” scoring more than two million views on *YouTube*, and making a lot of money.

“Li'l JoJo” is 18, slightly older than “Chief Keef.” He is a member of a rival gang, the *Insane BDK (Black Disciples Killers)*, and probably through jealousy, he put out a very aggressive piece about the *Black Disciples*, which was very insulting toward “Chief Keef”: he said that he had had sex with “Chief Keef’s” mother.

The next afternoon, “JoJo” posted a video of himself and members of his gang in a car, heading towards “Keef’s” territory, in which someone is heard to say, “I’m going to kill him.” A few hours later, shortly after indicating where he was in a tweet, “Li'l JoJo” was gunned down in a burst of automatic fire.

Yes, indeed, being a rapper, even a young one, is a dangerous and risky business, and there are many examples of murder being treated as something to

show off about. According to available data, at least 63 rappers have met a violent end, or have died of an overdose, which comes as no surprise.

“Chief Keef” also sent a tweet making fun of “JoJo” after his death, a lack of “respect,” sparking off a wave of violence that lasted months and killed a large proportion of the 500 people who died in gang confrontations in Chicago’s wars in 2013.

Gang violence is learned on the street from birth, but is now improved on the Internet through video games in which the player spends whole days killing people. There are no personal consequences, due, most notably, to the fact that in the game he has several “lives” rather than the single chance he has in real life.

Apart from immediate violence, social networks are also an important means of running money-making operations.

There are sites where gang-members can hang out virtually, such as *TheHoodUp.com* (a meeting place for every “Hood”) and discuss issues, make deals, and establish alliances, either regionally or nationally, in private chat rooms.

Social networks also allow a considerable widening of the recruitment pool for gang-members, and enable them to spread as they conquer new markets.

Although it was film and television series about gangs that first acted as recruiters for them, the effect is more obvious with social networks, which allow a lot more than just “publicity.” The interactive communication now possible aids the process such that candidates already have a very clear idea of what gang life is like, to the point that they even think they are in some way already part of one, not to mention the “dress code”...In this way, recruitment and the commitment to action is much more natural.

We will not discuss here the details of the money-making activities of the gangs, where nothing can be excluded, but it is readily understandable that social networks facilitate all manner of trafficking and dealing.

We have in mind the drug trade, of course, but a newer activity is developing on the West Coast, and it seems ready to spread. Los Angeles is not just a movie and a gang capital; it is also a huge commercial port, turned toward Asia. A noticeable recent trend has been the arrival of large quantities of counterfeit goods of all kinds, and gangs are working hard to gain control of that market. The use of social networks supports this low-risk, weakly-sanctioned diversification in many ways.

In the same way as gangs often have their own rappers, some have their taggers, who themselves need to spread the word about their “exploits.” Social networks offer them the means to do so.

Finally, social networks enable gangs to protect themselves from the police by allowing all gang-members to have real time information about its operations and movements.

IV - In the Fight Against Gangs, are Social Networks a Challenge or an Opportunity?

The number and variety of social networks might lead us to think that we are faced with a multiplier effect applied to a form of criminality which is already difficult to combat, and would make the problem impossible to solve. In fact, the dangers of these networks cut both ways.

In using the Internet, various traces are left behind, which often make it possible to track down the author of a message, or the real holder of an account, such as on

Facebook. This is especially true since those involved openly announce themselves, their aim being to assert themselves.

Thus today, the police patrol the Internet just as they patrol the streets.

In order to do this, they have a range of widely available as well as professional tools at their disposal. These have allowed them to refine criminal intelligence, and gain advanced knowledge of a crime, sometimes even to the point of preventing incidents from occurring in the first place.

These tools, which are themselves evolving very quickly, include:

WhoTalking, which we have already mentioned;

Wheretweeting or *Echosec* which takes geo-thematic approaches; and

SnapTrends, a commercial application, also geographical, but going far beyond just the fight against gangs.

This police work on the Internet is rather successful.

These include arrests. For example, in New York, in April 2013, 41 gang-members were arrested for cocaine trafficking. They had all put photos of themselves on social networks with rolls of banknotes and luxury watches. But the case still took nearly a year to succeed.

Police social media watch can also prevent irreparable damage from occurring. This is what happened in Chicago (you will remember “Chief Keef”). Sometime after the death of “Li'l JoJo,” a 12-year-old boy posted some derogatory comments online about him. The police immediately put him under protection away from his home. The next day, gunmen came and circled around his house. They were arrested, which possibly prevented another murder.

Similarly, the FBI was able to close down a ring for recruiting very young prosti-

tutes set up by a gang in Fairfax, Virginia. The gang-members would generally spot them on *Facebook*, since it is a network designed for making “friends,” and unsurprisingly, it was easy for them to approach their victims. It was generally quite simple given that the language used by all sectors of the population, especially the young one, is usually very crude on this medium. After that incident, the FBI produced a set of documents for parents, with information on the genuine danger posed by using these virtual networks without any kind of precaution.

In Cincinnati and other cities, a specialized division keeps dozens of sites under surveillance, and does not hesitate to intimidate the gangsters by telling them exactly what they did the day before...

But things evolve quickly. For example, there is a software which allows photos to be sent that then disappear automatically after they are viewed: *SnapChat*. If this were to become widely used and spread to text and videos, it might well pose a new problem for the authorities.

However, given the speed of developments, softwares allowing *SnapChat* content to be saved came out almost immediately, such as *SnapChatSave* and *SnapHack*.

On the other hand, the aim of the gangs is to achieve notoriety and glory, which pushes them to be as widely visible as possible. This requires that information lasts and can continue being circulated.

We are, therefore, in a complex vicious circle in which the quantity of instantaneously available information is without doubt the greatest obstacle.

There remain, finally, activities on the Internet that are not intended to be visible, on the Dark Web, for example—activities which will take some time to uncover because these *gangbangers* have far more resources than is generally believed.