The Use of Social Networks by Criminal Gangs

Thomas Legrain

Thomas Legrain is a strategy, communication, and lobbying consultant (http://www.thomas-legrain-conseil.com). A graduate of ESSEC, with a DEA in Market Finance and Bank Management from the Sorbonne and qualified member of the French Actuary Institute, Thomas Legrain was a participant in the 64th "Defense Policy" national session at the HEDN. Thomas Legrain is the author of the Routard guide on Economic Intelligence.

Contact: tlegrain@tlconseil.com

Reports by the French ministry of the interior, the European Union and the UN are unanimous: cybercrime is the scourge of the twenty-first century. While hacking has been a very familiar form of online crime to the authorities since the arrival of the Internet, there are now other rival forms of such crime, ones that come directly from the real world. Unlike hackers, these criminals are already active in "real life." The Internet and social networks simply act as marketing relays that contribute to developing their activities and increasing their influence.

Even though the list of online criminality is long, in our comparative analysis we will focus on three categories of cybercriminals: hackers, cyber-jihadists and the mafia 2.0. While a distinction can be made between the different types of criminality, the three categories of criminal gangs share one thing in common: they all have very organized networks that make it possible to manage a virtual space from far away as well as thousands of followers throughout the world. These organizations are thus able to act simultaneously in different places, following a similar procedure predefined by those at the highest level. When this is combined with cyberspace's anonymity and viral nature, we have a rather terrifying phenomenon that is able to develop almost outside of any police or legal control.

The recent attacks in Paris have put the issue of surveillance of these latent criminals active on social networks back on the agenda: how can these potential terrorists be detected prior to their taking action? At what point will they act? Even though they often act alone, as lone wolves, how do they interact on social networks with the criminal organizations that influence them? These remain open questions.

The Internet and social networks are excellent propaganda and proselytizing tools. The communication strategy of cybercriminals is often similar to that of a brand. For lawbreakers on the Internet, every social network has a well-defined

doi: 10.18278/ijc.4.1.2

function: image networks (Facebook, Instagram, Pinterest) are different from influence networks (Twitter, Messenger).

The best knowledge of the ways in which criminals and criminal gangs operate online should make it possible to better understand their psychology and better grasp their methods of operation, with the goal of gaining the upper hand over these Internet kingpins.

SOCIAL NETWORKS: A DEVELOPMENT IMPOSSIBLE TO CONTROL

The explosion of social networks was a real windfall for criminals and terrorists who now have an international and free platform available to them, allowing them to affect thousands of individuals with just a few clicks. Marketing effectiveness, determined by GRP (Gross Rating Point)[1], is optimal.

Hidden by a degree of anonymity, cybercriminals can freely communicate through a multitude of dedicated accounts, difficult to censor and with a potentially exponential viral nature. Thanks to social networks, criminals can remain in constant contact with members of their organization and lead globalized activities.

To plan and fight effectively, this phenomenon makes it difficult to implement a response at the legislative level as well as the level of justice and law enforcement.

SOCIAL NETWORKS: WHAT LEVERS, WHAT STRATEGIES?

Criminal gangs make distinctions between the social networks. The choice of interface points to the strategy they seek to implement: reputation, recruitment, or influence. These three development levers refer to established and often complementary marketing theories. Even though images have undeniable symbolic strength, moral affiliation has become a major issue. To reach this goal, what better way than by focused rhetoric, which in modern advertising terms is called "storytelling"?[2]

In just a few word, Pierre Conreaux, chief executive and co-founder of WalterMelon btp (a consulting & coaching agency), explains what storytelling is in a very instructive slideshare: *"Storytelling, is making our brand into a story; it creates interest and affiliation, appeals to the emotions and encourages commitment, and also allows for interaction."* This procedure comes directly from the world of cinematography and has been gradually taken up by the marketing industry, which sees it as an innovative way to address an audience.

1 The average number of advertising contacts obtained based on 100 persons of the target market.

2 Storytelling literally means "telling a story." The expression refers to a method used in communication based on a narrative structure of language comparable to that of fairy tales and stories.

Because criminal organizations have done a good job understanding these marketing issues and the benefit of "storytelling," Al-Qaida, ISIS, the Camorra, and Anonymous have become major brands in the criminality sector.

To create preference and loyalty, recruit new members, or increase their notoriety, criminal gangs have exploited the marketing possibilities presented by social networks, in the same way as any other major distribution brand.

For each of the forms of cybercrime studied below, we will see how and through which social networks they have successfully risen to become, both on the web and in the field, the stars of the criminal world.

I. HACKERS, CYBER-JIHADISTS, AND MAFIA 2.0: BETWEEN ANARCHY, TERROR, AND BUSINESS

A. Hackers: Seeking a Challenge

By means of two cyberspaces that exist parallel to the Internet (TOR or VPN), hackers are developing increasingly better performing and more discrete pirating techniques. Phishing, spamming, or infection through a Trojan horse enable these crooks to exploit the personal data of Internet users (bank account, passwords, photos, and so forth) after gaining access. Social networks have facilitated cyber-attacks. Facebook and the other places for chatting online are interfaces web users prefer for exchanging or posting confidential information. Users are not always aware just how insecure this space is.

While computer attacks have existed since the appearance of automatic transaction systems, social networks have created a new kind of hacking: "ethical" hacking. Through their actions, some cybercriminals such as White Hats or members of Anonymous seek to reveal security holes, the goal being not to exploit them but to expose them.

These groups gained prominence when they took action against pedophile websites or criminals with malicious Facebook or Twitter accounts (stalkers, jihadists). The Charlie Hebdo operation launched on January 9, 2015 by Anynomous under the hashtag #OpCharlieHebdo is one example. The hacking took place in two phases: a warning video was uploaded to YouTube on Friday evening (January 9, 2015); three days later, hundreds of Islamist propaganda sites were "taken down." Pro-jihadist hackers were quick to respond: they pirated several school and company websites. All the sites pirated by pro-jihadists displayed slogans such as *"You are racism (sic)!," "You are the Terrorist (sic) of the world," or even "I am muslim (sic) and I am not Charlie." Three flags accompanied the pirated page: French, Israeli and American."*[3]

3 http://tempsreel.nouvelobs.com/charlie-hebdo/20150113.OBS9841/anonymous-et-hackers-islamistes-s-affrontent-au-nom-de-charlie-hebdo.html

These acts of vengeance positioned these organizations as "cyber-vigilantes." Even though it seems natural to be sympathetic towards these Internet "protectors," this image is the result of a well-thought-out strategy. Emblematic groups like Anonymous and UGNazi have established values, a charter, and targets. They have a real "brand platform" adopted by all members, with strict rules to follow. As an example, Anonymous implemented an internal communication strategy based on partitioning theory: one Anonymous member only knows the identity of three other members and only communicates with these three people, which allows them to keep their actions secure.

Whether they are well intentioned or malicious, hackers are driven by the enjoyment of taking on the challenge. Breaking through the limits of a system and raising their skills to another level are challenges they seek every day. Tim Jordan and Paul Taylor, from the University of London, have just published the first sociological study on hackers. Their conclusions concur with our initial analyses. The testimony by one of the interviewees affirms the characteristics we ascribe to them. *"I only do this because I feel good, better than with anything else. The rush of adrenaline that I get when I try to escape the authorities, the chills I feel after writing a program that does something people thought was impossible, and the possibility of being socially related with other hackers is all very thrilling."*

These cybercriminals dare to be seen because they are not ashamed of their actions and consider themselves as "Internet heroes." This "social communication" is a paradox in terms of their brand DNA. Indeed, anonymity is sometimes a prerequisite for their existence. This "double game" between visibility and anonymity denotes a provocative personality, one that elicits curiosity, a fact they are well aware of and which they seek out.

From a more metaphoric analytical angle, the portrait that follows presents an Identikit picture of the typical hacker.

If hackers were...

a book

"Time for Outrage!" by Stéphane Hessel.

a social network

Facebook: a Mecca for secrets between web users. This image social network is finally a top choice for hackers. The mass of web users there allows them to hide themselves more easily. This interface satisfies their desire for "discrete visibility."

B. Cyber-jihadists: evil psychologists

According to the Belgian newspaper *La Libre Belgique*, a study by the University of Milan, done between July 1 and October 22, 2014,[4] concluded that Belgium is the country from which the majority of propaganda in favor of ISIS is sent out to social networks (31% of Arabic-speaking messages posted in Belgium are in favor of this terrorist organization compared to 20% in France, 19.7% in Iraq, and 7.6% in Syria). Surveillance of the movement's activity is increasing in every country, but ISIS has already launched a counter-offensive by distributing to its members throughout the world a social network manual to avoid, among other things, leaks that would make it possible to geo-locate the jihadists. Online training "by ISIS" is being organized, which confirms the desire of cyber-jihadists to use the Internet as the main lever for their propaganda. Social networks demonstrate their modernism and organization.

But the most concerning phenomena appeared after the Charlie Hebdo attack. Two hundred students refused to respect the minute of silence due to terrorist sympathies, and there were hundreds of tweets advocating terrorism with the hashtag #jesuiskouachi and #jesuiscoulibaly ... An article in *Le Figaro* dated November 18, 2014 spoke very correctly of *"bedroom radicalization."* Influenced by the Internet, several potential extremist young people have been identified throughout France. Most are, however, not believed to be young jihadists ready to act. This capacity to believe in conspiracy theories and position themselves on the side of the enemy reveals the degree of influence these terrorist organizations hold today thanks to social networks.

Social networks have become fishponds from which Islamist representatives can easily recruit. Operations to appeal through Facebook or Twitter are fairly simple to implement. In addition, recruiters do not even have to go find their victims; some come directly to them! With photos and selfies of smiling friends, jihad presented as a stay at a summer camp, propaganda videos showing jihadists as heroes, and so forth, terrorists very easily use the misunderstanding and naïveté of the very young to convert them.[5] This is what has led many French people to go participate in jihad in Syria.

"Buzz is dead, long live influence,"[6] said Vincent Ducrey, Luc Chatel's former Internet advisor when he was spokesperson for the Fillon government. Much more effective than simply "buzz," influence marketing is a long-term strategy based on the study of consumer and web user behavior.

---

4 http://www.lalibre.be/actu/belgique/la-belgique-terre-de-propagande-pour-daech-infographie-547e001c3570a0fe4c974cd1

5 Study by Memri (The Middle East Media Research Institute).

6 Arthur Orfrey, "Les réseaux sociaux, ou l'art de contrôler les masses," Epoch Times, [n.d.] http://www.epochtimes.fr/front/14/10/28/n3510420/les-reseaux-sociaux-ou-lart-de-controler-les-masses.htm.

The main strength of influence marketing resides in its ability to draw a crowd.

The study "Experimental Evidence of Massive-scale Contagion through Social Networks" demonstrates the influences of discourse (positive or negative) on individual behavior. For example, when the flow of positive messages posted on social networks decreases, people produce fewer positive expressions. The opposite is equally true. According to our understanding, this study may explain the influence cyber-jihadists can have on "fragile" web users. Social networks allow messages to be constructed in an extremely personalized way. The psychological strength of the prospect is a major criterion in recruitment. Terrorists are conducting a well-run personalization strategy based on five myths (or five profiles of young prospects). This classification is the result of advanced sociological work.

THE FIVE PROFILES IDENTIFIED BY ISIS AS BEING "READY TO BELIEVE AND COMMIT"[7]

1. The heroic knight: a person who needs recognition.
2. Mother Theresa, or a person who becomes involved in humanitarian causes. A feminine target more sensitive to horrible events and intended to do jobs related to humanitarian work.
3. The wingman: a person in search of an identity. He wants to belong to a community (observed in teenager behavior).
4. The Call of Duty: a primarily masculine target audience that wants to fight. These young people have often been rejected by the army (the weak catch up to the strong, to regain their dignity).
5. Zeus or a person who seeks to be all-powerful. An individual without any limits. He consistently exhibits extreme behavior and takes risks (drug addiction, speeding, unprotected sex, and so forth).

Every individual does not automatically fall into one of these categories. Some can have character traits belonging to several categories. However, this typology is an essential base of communication for cyber-jihadists. Manipulation is a basic principle: an intelligent mix of visibility and storytelling.

Strongly symbolic, the following portrait paints a precise psychological profile of terrorists 2.0.

7 Bouzar, Dounia, Christophe Caupenne, Sulayman Valsan, "La Métamorphose opérée chez le jeune par les nouveaux discours terroristes," CPDSI, November 2014. Accessed at http://www.bouzar-expertises.fr/images/docs/METAMORPHOSE.pdf.

If cyber-terrorists were...

a book

"The Crowd: A Study of the Popular Mind," by Gustave Le Bon

a social network

Twitter: quick and effective. More so than YouTube, which has become an important platform for jihadist groups and their supporters, Twitter has had the greatest success with terrorists. Twitter has been seen to be more effective than Facebook for disseminating their propaganda and enabling internal communication. The use of Twitter by terrorists is in line with a recent media tendency to consistently sacrifice cross-checking and in-depth analysis for the benefit of real-time coverage. A skillful mix of Facebook/Twitter enables these malicious psychologists to conduct a strategy that simultaneously involves image and influence.

C. MAFIA 2.0: ME, MYSELF, AND I

Mafia organizations dedicate a significant portion of their activities to their image. Social networks allow them to post their laid-back attitude, lifestyle, and victories, as well as spread their warning message. On social networks such as Facebook and Instagram, several figures from these organizations regularly post outrageous photos that display their luxurious lifestyle or the latest weapons they have acquired. Aside from these ostentatious behaviors, which often lead to their arrest, these bandits have taken to social networks to give themselves yet another illegal platform. Drug or weapons traffickers often use a virtual currency called Bitcoin to carry out a transaction. This currency is untraceable, because transfers are made on the web in complete anonymity (VPN and TOR networks). Aside from financial transactions on the web, traffickers use the Internet and social networks as a parallel logistics platform.

Social Networks: Between Business and E-Reputation

While they belong to well-identified collectives which they promote in a consistent way, these individuals are not in the habit of speaking "in the name" of their group. People talk about Broly Banderas and Manuel Nino Spagnuolo but very little of the Order of the Temple or the Camorra. In addition, they create Facebook accounts that bear their mark. These "stars" are individuals and not

organizations, unlike hackers and terrorists. It is another sign of these criminals' egocentricity. The marketing organized around their actions is to serve their individual ambition. This leads to statements that are not uniform, but instead extreme, since they are based on one-upmanship. Provocation is at the heart of their activity. Obviously, the social networks best suited to their methods of operation are image social networks (Facebook, Instagram).

Whether they chose these networks by chance or due to a careful strategy, an IFOP study from 2013 shows they have reason to do so. Indeed, the image social networks are the most popular among web users. Some lead in their category and others are quickly growing; they are among the social networks that have experienced the greatest growth from one year to the next (Facebook is No. 1 and Instagram moved up nine places to the twelfth position). This positioning makes it possible to receive significant media coverage when the time comes.

In brief,

If drug traffickers 2.0 were...

an advertising slogan

"Because I'm worth it" (L'Oreal).

a social network

Instagram: the images speak for themselves.

CONCLUSION

The three categories of cybercriminals we have studied represent just a minority of web users. However, their power of influence is substantial.

With regard to these three types of criminal networks, there is a need to gain the upper hand on (future) cyber-victims. While the terrorists conduct a strategy related to analyzing the lifestyles and psychological condition of their target audience, the mafia continue to exert psychological pressure through the personal accounts of their scapegoats, and hackers rely on the naïveté of their victims in order to "push them to make a mistake" (supplying their bank card code or other confidential data). The exploitation of psychological weaknesses varies from one network to the next, but is a basic principle in their strategy.

The difference can be found in their varying objectives. The terrorists aim to enlarge their network and draw "the crowd" into a radical and fighter ideology.

This is not the case for the mafia and hacker groups which, by exploiting web users' naïveté, are only concerned with enriching their community. Recruiting candidates is not a priority. The psychological functioning of the target web user, outside of the scope of the operation targeted, does not interest them.

"Before making proposals to change the world or regulate it, it is important to understand it. It is therefore necessary to study the behavior of individuals and groups. Then, more normative elements can be drawn out to make recommendations. The modern macro view is to a degree micro-based," Jean Tirole.

The terrorist attacks perpetrated in France in 2015 pushed Manuel Valls and François Hollande to take a proactive approach with regard to cybercrime. Several solutions to be "effective immediately" were unveiled. These included 2,680 jobs created over three years within the ministries of the Interior, an additional 425 million Euros to better equip law enforcement, the study of a bill in March on intelligence services, 60 additional Muslim chaplains in prisons, 5 districts dedicated to bringing together incarcerated radicalized persons, a file created to identify persons convicted of terrorism, and a website created to inform the general public concerning ways to fight against jihadist recruitment.

All of these announcements sound like the authorities have become aware (belatedly) of the need to act. While these provisions aim to impede extremist terrorist groups from forming and acting within the country, the authorities must, as they seek to anticipate actions, be able to counterattack on the web, the starting point for sectarian excess. Manuel Valls broached a consideration of these questions when he was minster of the Interior. According to him, to be effective, it behooves the French police to be able to make use of social networks. For 2025, he wanted a police force 3.0. "*The police and the gendarmerie must make the technological leap required of them.*" Beyond national boundaries, European unity in planning strategies to be implemented will be one of the challenges in the months to come.

SOURCES

Internet site references were all accessed between the end of 2014 and the beginning of 2015.

Reports, Scholarly Works, Studies

Botton, Marcel. *Les hommes politiques sont des marques comme les autres*. Paris: Editions du moment, 2008.

Bouzar, Dounia, Christophe Caupenne, and Sulayman Valsan. "La métamorphose opérée chez le jeune par les nouveaux discours terroristes." CPDSI, November 2014. Accessed at http://www.bouzar-expertises.fr/images/docs/METAMORPHOSE.pdf.

Hessel, Stéphane. *Time for Outrage: Indignez-vous!* New York: Twelve Books, 2011.

IFOP. "Les réseaux sociaux et les français en 2013." Paris: IFOP, 2013.

LeBon, Gustave. *The Crowd: A Study of the Popular Mind.* New York: Dover, 2002.

Lemieux, Vincent. *Les réseaux criminels*. Ottawa, Canada: Gendarmerie royale du Canada, 2003. Accessed at http://cpc.phippsinc.com/cpclib/pdf/56312f.pdf.

Internet Sites

A., Yassine. "L'activité d'Anders Breivik dans les médias sociaux," July 25, 2011, http://www.ya-graphic.com/2011/07/263-activite-anders-behring-breivik-dans-les-medias-sociaux.

Aigrault, Valentin, Tony Fabri, Jean-Michel Hansen, "Le faux compte Twitter qui incrimine un élu," July 24, 2014, http://www.ouest-france.fr/le-faux-compte-twitter-qui-incrimine-un-elu-2723712.

Alonso, Pierre. "Le djihad digital natives," Slate.fr, August 13 2013, http://www.slate.fr/story/76308/djihad-digital-native-al-qaida-aqmi-aqpa.

Berger, J. M. "How Iraqi Militants are Gaming Twitter," The Atlantic, June 16, 2014, http://qz.com/221981/a-rebel-army-in-iraq-is-putting-corporate-social-media-mavens-to-shame.

Black Hat USA. "Black Hat USA 2013 Briefings," http://www.blackhat.com/us-13/briefings.html#Lau.

Brandy, Grégor. "Twitter, le nouveau réseau social préféré des terroristes," Slate.fr, May 15, 2014, http://www.slate.fr/monde/87121/twitter-prefere-terroristes.

Braun, Elisa. "Les réseaux sociaux: une nouvelle arme de guerre," July 17, 2014, http://www.rslnmag.fr/post/2014/07/17/les-reseaux-sociaux-une-nouvelle-arme-de-guerre-.aspx.

Bret and Lejeune, "Les causes de la cybercriminalité," March 31, 2011, http://why.cybercrim.over-blog.com.

Cahen, Muriel. "Intrusion dans un système informatique," May 1, 2009, http://www.legavox.fr/blog/murielle-cahen/intrusion-dans-systeme-informatique-hacking-314.htm#.VFzQevmG8m0.

Cassely, Jean-Laurent. "Un Facebook des terroristes, ... créé par une agence de renseignements américaine," Slate.fr, June 27, 2014, http://www.slate.fr/story/89123/agence-renseignements-facebook-terroristes.

Chafiol-Chaumont, Florence. "Réseaux Sociaux: terrain béni pour les usurpateurs d'identité," Huffingtonpost.fr, March 21, 2013, http://www.huffingtonpost.fr/florence-chafiolchaumont/usurpation-identite-reseaux-sociaux_b_2916506.html.

Chalancon, Cécile. "Attaque des shebaabs à Nairobi: le djihad passe par Twitter," Slate.fr, September 22, 2013, http://www.slate.fr/monde/78040/kenya-nairobi-attaque-shebaab-live-twitter.

Champagne, Aurélie. "Narcotrafiquant est selfie comme les autres," Novel Obs, November 22, 2013, http://rue89.nouvelobs.com/2013/11/22/narco-trafiquant-est-selfie-comme-les-autres-247742.

Col, Pierre. "Europl a crée un groupe de travail pour lutter contre la cybercriminalité internationale," September 17, 2014, http://www.zdnet.fr/actualites/europol-a-cree-un-groupe-de-travail-pour-lutter-contre-la-cybercriminalite-internationale-39806505.htm.

Comité de la Convention Cybercriminalité. "Convention sur la cybercriminalité," November 23, 2001, Conseil de l'Europe, STE 185, http://conventions.coe.int/treaty/fr/Treaties/Html/185.htm.

Criminel 2.0, http://www.ikone-web.com/criminel-2-0.

De Douet, Marie. "Les terroristes à l'assaut des réseaux sociaux," Le Point, April 6, 2012, http://www.lepoint.fr/monde/les-terroristes-a-l-assaut-des-reseaux-sociaux-06-04-2012-1449043_24.php.

Editorial staff, "Les narcotrafiquants sur les réseaux sociaux," October 27, 2014, http://www.mensquare.com/menly/pop-life/164643-narcotrafiquants-reseaux-sociaux.

Editorial staff of Zdnet.fr. "La loi SOPA-PIPA suspendue: l'Union Européenne ne bloquera jamais internet," January 23, 2012, http://www.zdnet.fr/actualites/loi-sopa-pipa-suspendue-l-union-europeenne-ne-bloquera-jamais-internet-39767733.htm.

FBI. "Social Network Analysis," October 2013, http:www.fbi.gov/stats-services/publications/law-enforcement-bulletin/2013/March/social-network-analysis.

Garot, Pierre-Emmanuel. "Au Chili, la police traque les délinquants sur les réseaux sociaux," France TV, July 17, 2014, http://polynesie.la1ere.fr/2014/07/17/au-chili-la-police-traque-les-delinquants-sur-les-reseaux-sociaux-170017.html.

Government of France. Law No. 2011-267, March 14, 2011, Article 2, LOPSI 2, http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=F0FFD1715CDAF3B75B4D524C5907D5D3.tpdjo11v_2?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000023709201&dateTexte=20131231&categorieLien=id#LEGIARTI000023709201.

Government of France. "Protéger les internautes - Rapport sur la cybercriminalité," Groupe de travail interministériel sur la lutte contre la cybercriminalité, February 2014, http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf.

Hamm, Camille. "Anders Behring Breivik, entre pratiques branchées et influences ringard," July 27, 2011, http://www.cafebabel.fr/article/anders-behring-breivik-entre-pratiques-branchees-et-influences-ringardes.html.

Huffington Post / AFP. "Attentat au Kenya: l'attaque d'un centre commercial à Nairobi se poursuit," – September 22, 2013, http://www.huffingtonpost.fr/2013/09/22/kenya-attaque-centre-commercial-nairobi-se-poursuit_n_3971818.html.

Huyghe, François-Bernard. "Djihadistes irakiens, réseaux sociaux et images," June 22, 2014, http://www.huyghe.fr/actu_1240.htm.

INHESJ, 2013. http://www.inhesj.fr/sites/default/files/defis1-v3.pdf.

Inspire 7, Fall 2011. Accessed at https://azelin.files.wordpress.com/2011/09/inspire-magazine-7.pdf.

Inspire 12, March 14, 2014, http://www.memri.fr/2014/03/18/le-xiie-numero-de-inspire-special-voitures-piegees-manuel-de-fabrication-et-liste-de-cibles-aux-etats-unis-au-royaume-uni-et-en-france.

Jaulmes, Adrien. "Le son des épées, les islamistes radicaux changent de langage," June 27, 2014, http://www.h24info.ma/monde/moyen-orient/le-son-des-epees-les-islamistes-radicaux-changent-de-langage/24947.

JORF No. 0281 of December 5, 2014, Text No. 89 – "Décret du 4 décembre 2014 portant nomination du préfet chargé de la lutte contre les cybermenaces - Jean-Yves Latournerie," http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029837986.

JORF No. 0298 of December 26, 2014, page 22224 – text No. 1 – "Décret n°2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion,"http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=

JORFTEXT000029958091&dateTexte&categorieLien=id.

Karayan, Raphaël. "La fermeture de Megaupload signe l'échec des lois antipiratage," L'Express, January 20, 2012, http://lexpansion.lexpress.fr/high-tech/la-fermeture-de-megaupload-signe-l-echec-des-lois-antipiratage_1385229.html.

Lamande, Emmanuel. "Les cybergendarmes sur les traces de vos supports numériques,"January2014, http://www.globalsecuritymag.fr/Les-cybergendarmes-sur-les-traces,20140115,42265.html.

Le Douaran, Marie. "Marketing et réseaux sociaux : la communication de pro des djihadistes de l'EIIL," L'Express, June 19, 2014, http://www.lexpress.fr/actualite/monde/proche-moyen-orient/marketing-et-reseaux-sociaux-la-communication-de-pro-des-djihadistes-de-l-eiil_1552390.html.

Lemaire, Eric. AXA Guide, www.axaprevention.fr/Documents/fichiers_pdf/AXA_GUIDE_BSN.pdf.

Malbrunot, Georges. "'Inspire': le premier magazine en ligne en anglais d'Al-Qaïda," Le Figaro, July 2, 2010, http://blog.lefigaro.fr/malbrunot/2010/07/inspire-le-premier-magazine-en.html.

Malmstrom, Cécile. "L'Europe doit se doter des meilleurs outils contre le terrorisme," L'Express, January 15, 2014, http://www.lexpress.fr/actualite/monde/europe/l-europe-doit-se-doter-de-meilleurs-outils-contre-le-terrorisme_1314455.html#zyZq6CQG5G5kq3ts.99.

Miklaszewski, Jim, and Courtney Kube. "New Video Shows Al-Qaïda Leaders Addressing Dozens of Militants," NBC News, June 27, 2014, http://www.nbcnews.com/news/world/new-video-shows-al-qaeda-leaders-addressing-dozens-militants-n81546.

Miller, Joel. "Iraq Blocks Facebook and Twitter in Bid to Restrict Isis," BBC News, June 16, 2014, http://www.bbc.com/news/technology-27869112.

MIT. "How to Detect Criminal Gangs using Mobile Phone Data," *MIT Technology Review* (April 2014), http://www.technologyreview.com/view/526471/how-to-detect-criminal-gangs-using-mobile-phone-data.

Niedercorn, Franck. "Quand le big data prédira l'avenir," October 1, 2013, http://www.lesechos.fr/01/10/2013/LesEchos/21533-046-ECH_quand-le---big-data---predira-l-avenir.htm.

Ropars, Fabian. "Tous les chiffres 2014 sur l'utilisation d'internet, du mobile et des médias sociaux dans le monde," January 8, 2014, http://www.blogdumoderateur.com/chiffres-2014-mobile-internet-medias-sociaux.

Rosso, Romain. "Daesh mise sur nos faiblesses," L'Express, October 2, 2014, http://www.lexpress.fr/actualite/monde/proche-moyen-orient/daech-mise-sur-nos-faiblesses_1603400.html.

Rossoor, Benjamin. "Réputation: l'influence de la minorité en psychologie sociale," http://www.webreport.fr/reputation-influence-minorite-psychologie-sociale.

Sallon, Hélène. "En Irak l'EIIL décuple la terreur grâce à internet," Le Monde, June 16, 2014, http://www.lemonde.fr/proche-orient/article/2014/06/16/en-irak-l-eiil-decuple-la-terreur-grace-a-internet_4438941_3218.html.

Saume, Julien. "Les cyberattaques bientôt considées comme acte de guerre par l'OTAN," September 4, 2014, http://www.latribune.fr/actualites/economie/international/20140904trib0fdbd09da/les-cyberattaques-bientot-considerees-comme-acte-de-guerre-par-l-otan.html.

Senecat, Adrien. "Humour de djihadistes: la guerre sainte a aussi ses lolcats," L'Express, June 17, 2014, http://www.lexpress.fr/actualite/societe/humour-de-djihadistes-la-guerre-sainte-a-aussi-ses-lolcats_1550845.html#Utm3dFQJ7i0xZZBk.99.

Senecat, Adrien. "Le djihad 3.0 des Français partis en Syrie," L'Express, June 21, 2014, http://www.lexpress.fr/actualite/societe/le-djihad-3-0-des-francais-partis-en-syrie_1551982.html#7I1PG6m1FWxmUI6s.99.

Source AFP. "Un député UMP victime d'une usurpation d'identité sur Twitter," February 7, 2013. http://www.lepoint.fr/politique/un-depute-ump-victime-d-une-usurpation-d-identite-sur-twitter-07-02-2013-1625054_20.php.

Staff writer, 20 Minutes. "Les nouveaux boss de la mafia friment sur le web," August 4, 2014, http://www.20min.ch/ro/news/insolite/story/Les-nouveaux-boss-de-la-mafia-friment-sur-le-web-10931767.

Staff writer, Islamic News. "Une musulmane arrêtée pour avoir lu *Inspire* revue d'al Qaeda," 2013, http://www.islamic-news.info/2013/10/musulmane-arretee-avoir-lu-inspire-revue-dal-qaeda.

Staff writer, L'Express. "Arrestation du hacker français du Twitter d'Obama," L'Express, March 24, 2010, http://lexpansion.lexpress.fr/high-tech/arrestation-du-hacker-francais-du-twitter-d-obama_1409977.html.

Staff writer, La Rédaction, "Les Réseaux Sociaux vont ils vaincre le crime," July 4, 2014, http://www.rtflash.fr/reseaux-sociaux-vont-ils-vaincre-crime/article.

Staff writer, Le Parisien. "La mafia étend sa toile," February 10, 2013, http://www.leparisien.fr/espace-premium/actu/la-mafia-etend-sa-toile-10-02-2013-2555019.php.

Staff writer, Lesechos.fr. "Facebook, le réseau social des terrorists," October 22, 2012, http://www.lesechos.fr/22/10/2012/lesechos.fr/0202341232799_facebook--le-reseau-social-des-terroristes.htm.

Staff writer, Terrafemina, "La social TV ou quand les réseaux sociaux prennent d'assaut le petit écran," February 10, 2014, http://www.terrafemina.com/culture/culture-web/articles/37097-la-social-tv-ou-quand-les-reseaux-sociaux-prennent-dassaut-le-petit-ecran.html.

Staff writer, Viruslist. "Les hackers et la loi," http://www.viruslist.com/fr/hackers/info?chapter=162426945.

Studer, Camille. "Les géants du web et la cybercriminalité," June 30, 2014, http://www.infoguerre.fr/infolabo/geants-du-web-et-la-cybercriminalite-5466.

Telesatellite, "La télévision reste le média préféré des français pour s'informer," January 22, 2013, http://www.telesatellite.com/actu/42020-la-television-reste-le-media-privilegie-des-francais-pour-informer.html.

Tregouet, René. "Les réseaux sociaux vont-ils vaincre le crime?," http://www.rtflash.fr/reseaux-sociaux-vont-ils-vaincre-crime/article.

UNODC. "The Use of the Internet for Terrorist Purposes," 2012, http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

Walid, Tamara. "Puissance des médias sociaux," http://expo2020dubai.ae/fr/hello_2020/article/the_power_of_social_media.

We are Social Agency. "Social, Digital Mobile Around The World," January 2014, http://fr.slideshare.net/wearesocialsg/social-digital-mobile-around-the-world-january-2014?ref=http://www.blogdumoderateur.com/chiffres-2014-mobile-internet-medias-sociaux.

Weimann, Gabriel. "New Terrorism and new Media - Wilson Center, Commons Lab, 2014, http://www.wilsoncenter.org/sites/default/files/STIP_140501_new_terrorism_F.pdf.

Wikipédia, "Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication," http://fr.wikipedia.org/wiki/Office_central_de_lutte_contre_la_criminalit%C3%A9_li%C3%A9e_aux_technologies_de_l%27information_et_de_la_communication.

Social networks

Twitter

Al-Kanadi, Abdulmalik: https://twitter.com/al_kanadi

Thompson, David
https://twitter.com/_DavidThomson/status/535439228176699392/photo/1

Place Beauvau: https://twitter.com/Place_Beauvau

Police Nationale: https://twitter.com/PNationale.

Préfecture de police: https://twitter.com/prefpolice

Facebook

Guagliun, E.
https://www.facebook.com/pages/E-Guagliun-E-Stu-Rion/150298304982686?fref=ts

Manuel, Nino: https://www.facebook.com/ninomanuel.spagnuolo.3

Anonymous, Official Francophone: https://www.facebook.com/pages/Anonymous-officiel-francophone/249485455090652

Anonymous: https://www.facebook.com/OffiziellAnonymousPage?fref=ts