SDLC/DCPJ/ VM, le 10.06.2015.

OCTOPUS CONFERENCE, JUNE 17th-19th 2015

Workshop 8: Radicalization on the Internet: the criminal justice perspective

Introduction:

General overview:

Terrorist use of internet and social media has increased dramatically over the recent years. Jihadist groups in particular have shown a sophisticated understanding of how social networks operate and have launched well organized social media campaigns to recruit followers, promote or glorify acts of terrorism and violent extremism.

Recent studies have shown that within four months more than forty six thousand twitter accounts have been used by supporters of the Islamic Stats (ISIS) and as much as 90 000 tweets and other social media responses are produced every day.

« In France, 930 French nationals and foreign residents who used to live in France are now involved in the jihad in Syria and in Iraq » recently stated the French Minister of Home Affairs. « Three hundred of them are already there, including 60 women. About 180 people have departed from Syria and 170 are in transit to the area. Two hundred and thirty have expressed ideas of leaving. To this total number of 930, we can add 36 persons who died over there » said the Minister of Home Affairs to the *JDD*. « That is the blunt reality » he added.

Never before has the official number of French participants in the jihad been so high. In July the French Ministry of Home Affairs had evaluated the number of people engaged in Islamic operations in the Middle-East to 800. A number that had increased by 56% in a few months: they were 500 in April. A year ago, in March 2013, only 50 French nationals had chosen the jihad.

Following the French terrorist attacks that targeted Paris, France, in January 2015, the cyber threats have unfolded through the messages advocating for terrorism and the messages of incitement to racial hatred and violence found on the social networks and various web platforms (videos in particular) and through the high number of cyber attacks against official and private French websites. The “cyberwar” has been an extension of the Parisian terrorist attacks, triggering a clash between opposite ideological movements: the group of hackers defending the jihadist websites against the group of hackers known as the Anonymous, both groups respectively diffusing under #OpCharlieHebdo and #Opfrance.

The PHAROS platform has been mobilized 24 hours a day since January 07th 2015. The statistical report shows a growth like never before of the visits of the website www.internet-signalement.gouv.fr. Before the attacks, the previous average volume of reporting was around 400 per day. Between January 07th 2015 and January 30th 2015, PHAROS has received 37 829 reporting, all categories of offences included. Around **29 000** reporting were related to the terrorist events. *Tweets* were overwhelmingly used, well ahead of Facebook messages.

The priority was set as a live reading of all the reportings in order to determine which ones should be treated as an emergency by the UCLAT.

A constant watchfulness aimed at the social networks has been set up with a permanent connection with the national contact point of the Central Service of Domestic Intelligence (SCRT).

The Bureau of the Internet of the Internet Section of the SDLC has constantly activated its restricted contacts within the Internet Service Providers (e.g. Twitter, Facebook, Google/Youtube, Dailymotion…).

The International Relations Office of the SDLC has kept records of every issued data preservation requests, mainly addressed to the US.

A special pre-emptive work has been set in order to detect videos advocating terrorism with major companies (i.e. Dailymotion, Youtube/Google, Wat TV/TF1), using a fingerprinting method of the original videos.

At the operational level:

After the attacks that targeted France on January 07th 2015, a series of attacks aiming at French targets was launched by cyber jihadists. The SDLC has maintained high vigilance regarding the evolution of the phenomenon and has mobilized all the DIPJ's and DRPJ's correspondents in order to organize the filing of complaints and to ease the technical feedback susceptible to provide guidance on methods of attacks and investigative leads to consider. An operational cooperation with the Gendarmerie Nationale has also been put together.

An alert on the European level with EC3 has also been issued. An investigation on the exploration of the so-called dark web is still ongoing.

The activation of the channels of international police cooperation is decisive as well.

The French national organization in the fight against radicalization on internet

1) PHAROS: What's Pharos?

With the increase of online offences and the subsequent rise of the number of victims, the French administration had decided to make available for the public a web portal that would enable internet users to report these offenses to the police.

In January 2009, this web portal was launched. It is available at the URL www.internet-signalement.gouv.fr. The web portal is run by a team of police and gendarmerie officers and non-commissioned officers who handle these reports in real time, within the frame of a platform called PHAROS who deals with all kind of offences (child exploitation, swindles, online racism, threats...).

All the reports are analyzed, cross-checked and sent to local or specialized police or gendarmerie forces.

Means of action:

The purpose of PHAROS is to **identify the administrators** of illicit websites or **perpetrators of deviant behaviors** (groomers, authors of racist statements…), if necessary by starting **legal proceedings**, and send all gathered information to the entity that will be in charge of arresting the perpetrators.

The PHAROS circular dated July 19th 2013 defines the platform as a cybercrime database for investigators, including profiles, nicknames, accounts of perpetrators and child abuse material website URLs. In addition this circular establishes the transmission protocol of legal proceedings.

Statistics:

PHAROS has received around **150 000** (one hundred fifty thousand) **reports in 2014**.

These reports rank as follows: Swindles and extortions (52%), **Child exploitation** (including child abuse material distribution and online grooming) **(12%)** and Racial hatred (11%).

2) Website blocking scheme:

The Article 12 of the law n°2014-1353 dated November 13th 2014 provides the possibility to block access to websites that distribute child abuse material or advocate terrorism. Technically, access to these websites will be prevented by Internet Service Providers, on the basis of a list drawn up by PHAROS.

Access is blocked at domain name level.

The other part of the scheme is to ask search engines (Google, Bing, Yahoo, Ask…) to remove all references to the websites included in the aforementioned list.

Section 6 of the Act n°2004-575 on Trust in the digital economy of June 21st 2004, as amended, provides for a phased arrangement, in which the blocking of websites only substitutes to the withdrawal of content

- The administrative authority must first ask the web host or the publisher to remove the content inciting to terrorism, advocating for terrorism or the child-pornography content ;
- The administrative authority simultaneously informs the Internet Access Providers (IAPs) without requesting the blocking of the concerned websites ;
- If the illegal content has not been removed by the web host or by the publisher within 24 hours, the administrative authority may require the IAPs to block the concerned websites without delay ;
- This procedure of subsidiarity and this 24-hour delay does not apply if the informations regarding the publisher are not available online: in that case, the administrative authority may directly notify to the IAPs the Internet addresses to which the access must be blocked.

The administrative authority may also communicate to the search engines the list of illegal websites in order for them to no longer appear among the search results (de-listing).

This entire plan is placed under the control of a qualified person, designated by the National Commission of Technology and Liberties (CNIL), and who belongs to that Commission. The qualified person receives the list of websites simultaneously as its transmission to the ISPs or to the search engines. It ensures the regularity of withdrawal requests and conditions of application, of update, of communication and of use of the list of websites to block. If it finds an irregularity, it may at any time recommand the administrative authority to end it. If the administrative authority does not follow the recommendation, the qualified person may refer to the competent administrative jurisdiction.

Internet users visiting blocked websites are redirected to a webpage from the Ministry of the Interior. The O.C.L.C.T.I.C. was designated as the administrative authority responsible for the transmission of the lists to the ISPs.

- Statistics:

This chart has been filled since March 2015: about fifty websites have been blocked to date.

In conclusion :

Furthermore, discussions are currently underway with Europol and its IRK project (Internet, Listing Unit).