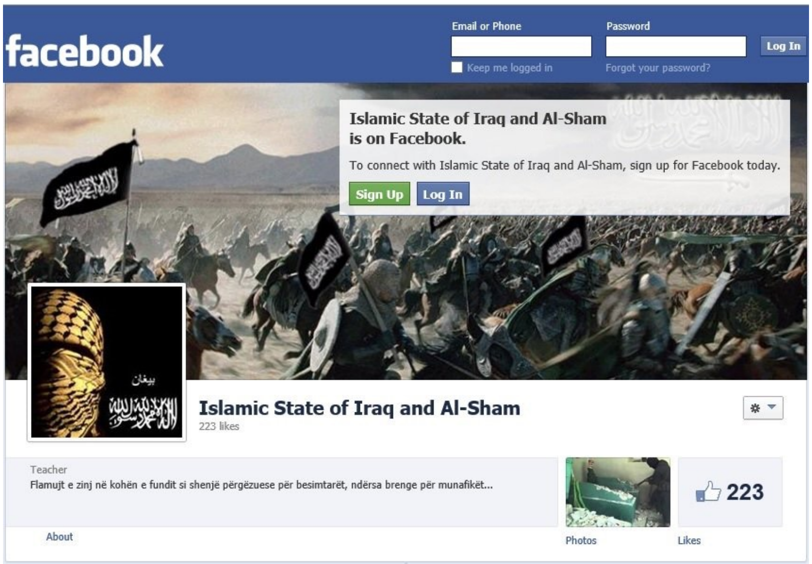
The EU after November 13th : war to the virtual accounts of a false God



Islamic State of Iraq and Al-Sham is on Facebook.

To connect with Islamic State of Iraq and Al-Sham, sign up for Facebook today.

Islamic State of Iraq and Al-Sham

Teacher

Flamujt e zinj në kohën e fundit si shenjë përgëzuese për besimtarët, ndërsa brenge për munafikët...

Imagine that your God would speak to you through his Facebook account. Imagine that he would dissuade you that the only good and acceptable way to respect him and accomplish his precepts it is to join a State that proclaimed itself in his name. To fight with an army whose supreme chief is not visibly known by almost any of his servants. To leave your family. To learn the military art. To systematically punish those who are unfaithful. To attack your own homeland. To die by killing in his name.

In the aftermath of the attacks of November 13th, France, in no uncertain terms, declared war to the Islamic State. The EU immediately showed its full solidarity and its support to the cause.

But, which kind of "war" are we really going to fight ?
The traditional battle arrays have been completely reshaped in today's world. The virtual accounts of a false God are the new enemies. Twitter, Facebook, Telegram and Youtube are the new battlefields. Tweets, videos, chats, posts, pictures and hacks are the new arms. Hackers sometimes become the new protagonists, the new guardians of our security.

An open war declaration has been submitted to all the virtual accounts of a God who becomes only an instrument, undressed of his own religion. Thus turning into a false God. An open war declaration has been submitted to his extreme and distorted precepts, to his power of persuasion and to his essential means of communication.

"Allah bless Twitter and Telegram, the strength of the holy war", the Italian Journal *Il Fatto Quotidiano* reported, by quoting the words of a jihadist Twitter account.

Internet is an accessible and practical platform, websites and social networks are free and attractive. The so called ***"imam Google"*** is pointed out to be the first recruiter and the main preacher. The **radicalisation** has assumed a ***"pocket-format"***. Smartphones and computers are the main channels through which radicalism is diffused, especially among young people who constitute the most vulnerable category. The actions of propaganda and recruitment actually seem to be undertaken more in front of digital screens than inside mosques. Internet is the main tool responsible for the feeding of the row of the IS and the glorification of its successes.

One month of conversations in **Facebook and Skype** was enough for Abou Bilel al-Firansi, affiliate to the IS and holding close ties to Abu Bakr al-Baghdadi, to persuade Mélodie, a 20-year-old Muslim convert from Toulouse. To deceive her with false promises, to marry her and to organise her travel to Syria. The only reason why Mélodie finally never saw the Syrian land it is because a French journalist was hidden behind her. The newspapers, however, are full of stories of young Mélodies who discover the power and the "attractiveness" of the IS on the web and dream to become part of it. And Many of them already succeeded : *"This is OUR youth that has turned against us"* affirmed Commissioner Avramopoulos on November 18th.

The process envisages precise and logic steps : showing the glory of the IS ; getting in contact with those who show little interest for what it is shared on the web ; keeping narrow and direct communications ; painting the image of a correct and attractive alternative life. After the arrival in the "holy" land : arabic courses and military training.

The Facebook account we spoke about, moreover, is nothing else than one single ring of a virtual chain of similar accounts (and the same could easily be made on Twitter or any other social). A virtual chain that constitutes a **platform for the communications** and also for the strategic and technical **planification** and organisation of attacks.

The use of **Twitter** accounts is usually related with other and more secure social media platforms : once the first contacts are established, the conversations are shifted to encrypted softwares, hidden platforms from the prying eyes of the intelligence services.

Telegram is one of those, giving the possibility to invite contacts to join "secret chats". Chats using end-to-end encryption, leaving no trace on the server, having a self-destruct timer and not allowing forwarding. One of the other apps considered among the most secure by the IS is **Signal** that before sending the messages, applies to them mathematical formulas that only the receiving device is able to decode and read.

"For the communications it is important that you use PGP even though it takes more time, it is more secure". The PGP (Pretty-Good-Privacy) is an **encryption software** and this is a message received by Sid Ahmed Ghlam, who was planning terrorist attacks in two churches in Villejuif, France.

In order to communicate in a secure way, also very basic tools such as **emails** are exploited. Sometimes, indeed, it is sufficient to apply very banal but at the same time efficient strategies. According to the lawyer in charge to defend the victims of the shooting at the Jewish Hypercacher supermarket (Paris, January 2015), the attacker, Amedy

Coulibaly, would have simply used the drafts of an electronic mail system to communicate with one of the mind behind the attack located in Syria. While writing up a message those systems imply its automatic storage in the draft folder. Thus, by knowing user name and password and thanks to the fact that mailboxes are accessible from any electronic device, it becomes easy to communicate without practically sending any message.

The web is not only the place for propaganda and communication. The web is also the place where it is possible to make money transactions with virtual coins such as **BitCoins**, that allow the possession and the transfer of money anonymously and without the need of third party verification : easy way to obtain anonymous financing or to make anonymous transfer to militants also abroad. The web is also the place where it is possible to buy any kind of illegal product, arms included, by deploying the **deep web**.

The *nbcnews* recently reported the concerns of the FBI Director, James Comey, about an IS that is constantly increasing its ability to "go dark". Many news have declared the come back of the **Cyber Caliphate**, a group of hackers affiliated to the IS, that would have recently forwarded informations about US military personnel, and the set up of a **24-hours Jihadi Help Desk** whose main aim is to deliver and diffuse instructions on how to encrypt and secure communications.

The digital dimension of the conflict, profoundly impalpable but such fundamental and efficient, has thus pushed the EU institutions and other actors to accelerate the development of new actions measures and strategies.

In the resolution of 25 November 2015 on the prevention of radicalisation and recruitment of European citizens by terrorist organisations, the European Parliament has addressed numerous measures to the **prevention of the radicalisation online**.

The Parliament, by recalling the **legal responsibility** of **internet and social media companies** and **service providers** to cooperate with Member States authorities to eliminate illegal contents, it also invites **Member States to consider legal actions**, including criminal prosecuting against those who refuse to act in line with administrative or judicial requests.

"Refusal or failure by internet platforms to cooperate should be considered as an act of complicity" .

A systemic and stronger collaboration between public and private entities is necessary : it is fundamental that the freedom of expression is not killed and sometimes it is not easy and immediate to define illegal content. On December 3rd, the Commissioners Avramopoulos (Migration, Home Affairs and Citizenship) and Jourová (Justice, Consumers and Gender Equality) launched the **EU Internet Forum** that brought together EU Interior Ministers, high-level representatives of major internet companies (Ask.fm, Facebook, Google, Microsoft and Twitter), Europol, the EU Counter Terrorism

Co-ordinator and the European Parliament. The internet industry can play an important role, thus making the establishment of a public-private partnership a fundamental element to better detect and address harmful material online.

In the same day, the French Prime Minister together with the Minister of the Digital Affairs, the Minister of the Interior and the Minister of Justice met with the representatives of Facebook, Twitter, Google, Apple and Microsoft.

Many young Mélodies could be dissuaded from joining the IS also through concrete actions of *"**counter-narratives**",* implying the dissemination of effective discourse to counter terrorist propaganda. That's something the Parliament asked for within the resolution, together with the full engagement of **all the internet users**, by enabling them to flag illegal content and report it to the competent authorities, and the set up of **special units within Member States** concerned with the detection and removal of such content.

The MEPs expressed major concerns about the rise of **encryption technology** and the use that terrorist groups make of it, and they warmly welcomed the creation of the **EU Internet Referral Unit (IRU)** by Europol. Launched in July on the basis of the mandate given by the European Council to Europol in March, IRU's main aim is to reduce the level and the impact of the extremist propaganda on the web. This, by identifying and referring relevant online content and by supporting Member States with operational and strategic analysis.

An other central aspect of this strategy, endorsed at the european level, envisages a crackdown on **virtual currencies** and **anonymous payments made online**. In the Conclusions of the JHA Council meeting of November 20th, the Justice and Home affairs ministers invited the Commission to present new proposals in order to strengthen the controls on non-banking payments as electronic and anonymous payments and virtual currencies such as BitCoins.

All the measures contained in the Parliament resolution and the calls made by the Council don not have legal value. Not yet. It is in the hands of the Commission now to make new proposals and to lead the building of new legal instruments. On the operational plan everything remains in the hands of Member States, national authorities and some EU agencies. However, next to them, someone else has endorsed an active role in this war. A real war is going on also in the dark corners of the internet.

It's more than one year that the hacker community has undertaken online attacks against the Islamic State in both social networks, websites, and in the deep web. The war scenario gets more complicated : non-state and illegitimate actors are actively on the side of National entities in an online war campaign.

Anonymous has set up the so called #OpParis campaign in the aftermath of Paris attacks : a strengthened and focused action that complements the activities already undertaken against the IS. *"More than* ***20.000 Twitter accounts*** *belonging to ISIS were just* ***taken down*** *by Anonymous ... ISIS we will hunt you, take down your sites, accounts, emails and expose you. From now on, no safe place for you online. You will be treated like a virus and we're the cure ... ISIS it is too late to expect us",* the group reported in a video published on November 18th.

Besides social media takeovers and the diffusion of instructions on how to report ISIS terrorist accounts, Anonymous is using also **DDoS** (Distributed Denial of Service) **attacks** to shut down IS websites, including those used to spread propaganda and fundraising sites, usually set up in the dark corners of the web.

Anyone can be Anonymous. It is necessary only to have a computer and an internet connection. That's all. Anonymous has no leader. It is like a *"flock of birds"* traveling in the same direction. *"At any given moment, more birds could join, leave, peel off in another direction entirely".* The open and free nature of Anonymous is one of its main strong points. However it is also at the basis of the criticism that many address to the group's action against the IS. The lack of leadership, coordination and the disjointed approach of Anonymous, indeed, make its actions confused. Sometimes, innocent targets are being caught up.

Michael Smith, counter-terrorism advisor to members of the U.S. Congress and co-founder of Kronos Advisory, insisted on the fact that the lack of coordination among Anonymous members *"can actually serve as a form of interference* [with the work of the competent authorities]*, which ultimately benefits the enemy".*

A sort of "**web coalition**" has raised against the common enemy : Anonymous, indeed, is not the only actor. More recently, a new group has emerged, distancing itself from Anonymous. It has specialized in counter-terrorism actions. It is the "**Ghost Security Group**" (GhostSec). The core number of its operatives stands at 14.

The group works in close collaboration with other networks of data collectors : **Controlling Section**, whose main aim is to expose ISIS and Al-Qaida members on Twitter ; **Katiba des Narvalos**, a French intelligence group created as a response to the Charlie Hebdo attacks in Paris, holding access to information channels and providing analysis regarding current trends in the ongoing fight against terrorism ; **Peshmerga Cyber Terrorism Unit**, a group of elite soldiers affiliated and serving with the Peshmerga military in Iraq, relaying real time information from the actual conflict zones and providing valuable data on enemy communications and troop movements.

GhostSec identifies and **tracks online communications platforms** used by terrorist groups and **disrupts their means of communications**. It infiltrates jihadi forums and uncovers locations and IP adresses of cyber-jihadists, thus expanding its range of action also to **espionage and intelligence gathering**, both surface web and deep web.

Differently from Anonymous operational approach, GhostSec established **ties with U. S. government authorities** in order to furnish them information that may be shared with other governments. Michael Smith is one of its intermediary.

According to him, the information that was passed to the U.S. Federal Bureau of Investigation had a critical role in allowing the disruption of a jihadist cell in Tunisia, whose militants were planning a new "Sousse beach massacre".

The group claims its contribution to the arrest of many extremists and to the prevention of attacks also in NYC and Saudi Arabia. *"To date we have been able to terminate over* ***110,000*** *extremist* ***social media accounts****,* ***149*** *Islamic State* ***websites*** *and over* ***6,000*** *extremist* ***videos*** *however we do not eliminate enemy web assets that have significant intelligence value"* said DigitaShadow, the one who oversaw the creation of Ghost Security Group, in an interview released to the *International Business Time.*

In a video published on its web page, the Ghost Security Group announced the birth of a **new breed of counterterrorism** : *"We fight an invisible war in which you can not see inside the wires … For every life that extremism claims only serves to strengthen our determination and resolve. We are the ghosts that they have created".*

This digital war, involving many different actors will not be the final solution against the Islamic State. It will not free Syrian people. It will not defeat the enemy. Not by itself. However, the ongoing conflict, is being fight on numerous grounds and the cyberspace is officially one of those. Its importance has reshaped State actions, it has promote and re-launched the debates on the freedom of speech and the use of encryption technologies. Actually, it seems that it is also having an impact on the light under which the hacking community is seen.

Imagine that your Facebook account was violated. Imagine that a "geek" wearing a hoodie would have access to your data, to your activities, to your communications and could monitor everything about you. Imagine that one day he decides to take down your personal profile and he does it. Imagine now, that the same happens to the Facebook, Twitter or any other virtual account of a jihadist who makes propaganda and recruits people. Easily, the illegal nature of the actions undertaken by the "geek" would slides to the background.

Paola Tavola

For further infrmation :

International Business Times, How Anonymous' #OpParis campaign may actually be helping Isis
http://www.ibtimes.co.uk/how-anonymous-opparis-campaign-may-actually-be-helping-isis-1530023

Il Fatto Quotidiano : Terrorismo, la cyber guerra dell'Isis : account fantasma per comunicare su Twitter
http://www.ilfattoquotidiano.it/2015/11/25/terrorismo-la-cyber-guerra-dellisis-account-fantasma-per-comunicare-su-twitter/2249269/

Remarks of Commissioner Dimitris Avramopoulos at the Press Conference on the Preparation of the 20 November Justice and home Affairs Council and the Firearms Package
http://europa.eu/rapid/press-release_SPEECH-15-6125_en.htm?locale=FR

Envoyé spécial. Comment les jihadistes communiquent-ils entre eux ?
http://www.francetvinfo.fr/replay-magazine/france-2/envoye-special/video-envoye-special-comment-les-djihadistes-communiquent-ils-entre-eux_1204377.html

NBCnews, ISIS Has Help Desk for Terrorist Staffed Around the Clock
http://www.nbcnews.com/storyline/paris-terror-attacks/isis-has-help-desk-terrorists-staffed-around-clock-n464391

European Parliament resolution of 25 November 2015 on the prevention of radicalisation and recruitment of European citizens by terrorist organisations
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0410+0+DOC+XML+V0//EN

Europol's Internet Referral Unit to combat terrorist and violent extremist propaganda
https://www.europol.europa.eu/content/europol's-internet-referral-unit-combat-terrorist-and-violent-extremist-propaganda

Conseil "Justice et Affaires intérieures", 20/11/2015
http://www.consilium.europa.eu/fr/meetings/jha/2015/11/20/

Anonymous - Operation Paris Continues #OpParis
https://www.youtube.com/watch?v=ZfyVVLGWivo

Anonymous vs the Islamic State
http://foreignpolicy.com/2015/11/13/anonymous-hackers-islamic-state-isis-chan-online-war/

Ghost Security Group
http://ghostsecuritygroup.com

Le groupe « hacktiviste » Ghost Security "devient"Ghost Security GroupTM" Des changements pour intégrer le cercle du contre-terrorisme professionnel
https://ia601506.us.archive.org/6/items/GhostSecurityGroupPressReleaseFrench/Ghost%20Security%20Group%20Press%20Release%20%5BFrench%5D.pdf

(Credit Image www.businessinsider.com)