Kenza BERRADA B00527477

Marie BOUDIER B00595883

ESSEC BUSINESS SCHOOL
SEM IDS: Applied Cybersecurity

Can ISIS's cyber-strategy really be thwarted?

Introduction

Google stated in February 2016 that more than 50,000 people search for the phrase "Join ISIS" each month. This fact illustrated the latest trend in today's world terrorism, which is the heavy use of social media and cyber capabilities to assert their domination. The Islamic State of Iraq and Syria (ISIS) is by far one of the most advanced terrorist organizations in terms of their social media capabilities. It is no coincidence ISIS is so successful on the virtual landscape. The group benefits from an extremely elaborate media and public relations strategy. Indeed, Al Hayat Media Center, their own media hub, produces, distributes and manages all their virtual content. With a designated press officer and their own designed mobile application, ISIS takes advantage of a true branding and marketing strategy, as if it were a regular business.

ISIS's cyber-strategy will be studied first, looking how it uses the Internet for their personal agenda, such as recruitment, propaganda, internal communication, fundraising, and cyber-attacks. Then, focus will be on the possibility to block the Internet, and how diverse stakeholders like the US or private companies plan on controlling the terrorist organization and thwart their online presence.

ISIS's Cyber-strategy

Propaganda

ISIS spreads its ideology on the Internet mainly through Twitter accounts. Members tweet proselytism messages regarding their faith, hate against Western countries and non-Muslims, and the necessity to attack and conquer. Most of the tweets, coming from various accounts claiming to belong to ISIS, include very specific information and live updates, aiming to give credibility about the group's progress. Updates include the number of bombings, deaths toll, illustrated by several pictures highlighting their military strength, as well as threats and pictures of hostages.[1] Messages and videos are shared through specific hashtags all over social media platforms. These platforms, especially YouTube and Twitter, are paramount for the group, which often initiates global online campaigns and calls for support from Muslims all around the world. One example is the campaign from June 2014, where supports were asked to share messages, photos and videos of them pledging allegiance to IS and waving the flag, through a hashtag in Arabic which translated to #TheFridayofsupportingISIS. As part of ISIS's strategy to spread their word to as many as possible, the group mixes their violent hashtags such as "StevensheadinObamashands" with other topics related to popular teenage culture (such as hashtags mentioning One Direction or , as the Dailymail explains[2].

ISIS came up with an elaborated application called the Dawn of Glad Tidings. The free app automatically posts pre-approved tweets by ISIS social media managers, to the accounts of subscribers. Since the messages are centralized and sent simultaneously, it allows ISIS an important online reach and to keep users up-to-date on the latest news.

[1] http://www.bbc.com/news/world-middle-east-27912569
[2] http://www.dailymail.co.uk/news/article-2734534/ISIS-use-US-journalist-hostage-focus-latest-terror-campaign-social-media-hijacking-discussions-using-StevensHeadInObamasHands-hashtag.html

In 2014, Mujatweets shared on YouTube and Twitter eight high definition videos, showing the lifestyle of ISIS members, whether they are grown adults or children. These videos, carefully elaborated and edited, even adding slow-motion for dramatization, are intended to convince as many and spread the Islamic State vision. They, as opposed to the violent and barbaric ones – notably of beheadings, threats and violence- transmitted by Western media, deliver a positive message. As part of their communication strategy, these short propaganda clips show the lifestyle of the mujahedeen, all smiles and helping out the population, handing candies to small children. The goal is to show the Caliphate as a refuge for all oppressed Muslims in the world, and emphasize its international outlook, thanks to the many testimonies of members explaining why they left their family in Europe to join the cause. All the means of marketing communication are used to portray the Islamic State as an attractive opportunity for every potential recruit. These videos have since then been removed from YouTube and other social media; however the impact they had on outsiders and supporters cannot be underestimated.

Other videos are regularly being released and have not yet been removed. A few days after the attacks in Brussels in March 2016, Al-Battar Media Foundation, a pro-ISIS media group, released another video featuring Donald Trump and using his anti-Muslim speech following the attack, to portray the USA as a racist and xenophobic nation. The popular website Al-Rahma (directly accessible on http://alrahma.tv) has its own TV channel and covers various subjects on radical Islam and distorted Quranic teachings. One video for example explains why music is "haram" (prohibited) and should be forbidden[3] . Websites conveying a radical view of Islam are available to all and referenced on any search engine. It then does not require any effort from an individual to look into propaganda material on the web, hence the dangers of such a proliferation of hateful content on the Internet.

One does not need to be a legitimate funded website such as Al-Rahma TV or ISIS's media team to produce propaganda videos. A multitude of videos produced by amateurs are widely available for free on YouTube. With the simple combination of "Allah + music" in the search bar, close to one million videos are suggested, ranging from basic inoffensive songs praising God to more threatening ones such as "Soldiers of Allah- Nasheed", on the first page of the results. Another one titled "Why did Allah forbid music" explains in sixteen minutes the supposed reasons for forbidding music and accounts for more than 28,000 views since 2014[4].

Recruitment

ISIS's main stake is to recruit members in order to continue their military progress. To attract members from Europe or America (known as "outsiders"), they bet on social media. Being extremely savvy to market their ideas and spread their message, they attract members to join them in Syria through videos, tweets, Facebook posts. Their strategy is particularly effective for young targets adept of Internet and social media[5].Recruiters are based on the battlefronts in Syria, but also in other Middle Eastern countries, Europe, Canada, the United States, and United Kingdom.

[3] https://www.youtube.com/watch?v=FGoriapzFrE ("Music is haram", subtitled in French)
[4] https://www.youtube.com/watch?v=-uyFWfRuMVA
[5] https://securityintelligence.com/funding-terrorists-the-rise-of-isis/

The particularity of the organization relies on its unprecedented number of female and children recruits. Women are recruited through effective social media campaigns promising them a devout jihadist husband, a life of devotion to God and happiness in the Islamic States of Syria and Iraq. Due to the Islamic Law prohibiting them from mixing the two genders together, women cannot fight at the frontlines. Therefore they gladly endorse a vital support role in areas such as medical care, food preparation, or as comfort women, and many intend to spread the message to attract other fellow females. How exactly are these women targeted and recruited online?

In 2014, more than 30 women from the Netherlands were said to have flown to Syria to in their jihadist husbands or with the intention of marrying one, according to the International Centre of the Study of Radicalization[6]. Many examples involve young women, as young as 16 years old, leaving the United Kingdom, France, Canada or Norway in the hope of joining Syria. How were these women drawn to ISIS in the first place? ISIS leverages its strategy on attracting Western women – or muhajirah (female immigrant) - so as to expand internationally. The messages sent on social media are carefully tailored to appeal to that particular group. Many Tumblr pages and Twitter accounts held by female members helped foster a sense community of among the followers. Some talked about their journey to Syria and gave advice to future recruits on what to bring. Since then, most of these pages have been taken down. One Twitter personality, going with the name of Khadijah Dare, a female UK immigrant to Syria, living with her Swedish jihadist husband cheered on Twitter as the video of the beheading of hostage James Foley was released. Her messages were retweeted hundreds of times.

Some younger women were tricked into joining ISIS without their knowing. Through Facebook, they conversed with a young man who lured them into providing humanitarian aid for the civil war in Syria. They ended up serving as “comfort women” for the jihadists. Other are even approached on Muslim dating websites, being promised a house, servants, and jewelry, if the joined their future husband in Raqqa.

There have been an increasing number of children enrolled into ISIS with their parents’ blessings. As of February 2016, 88 children were said to have been eulogized by ISIS in the last thirteen months, most of whom coming from Syria and Iraq. According to reports, there would be over 1500 child fighters, more than previously seen in any other terrorist organization[7]. The happy children fighters portrayed in the propaganda videos work as mean to convince parents to let them join ISIS and die for the cause.

What makes it so difficult to control the expansion of this propaganda is that all the material is freely available online, without even having to search in the Deep or Dark Web. As an anonymous official in Jordan said, “What makes ISIS so dangerous is that if you were trying to join the organization tomorrow, and weren’t sure where to start, Google would have most of your answers”. Authorities could shut down every mosque, or arrest every person supporting ISIS, a young man would still find

[6] http://www.icct.nl/download/file/ICCT-Bakker-de-Leede-European-Female-Jihadists-In-Syria-Exploring-An-Under-Researched-Topic-April2015(1).pdf
[7] http://edition.cnn.com/2016/02/19/middleeast/isis-child-soldiers/

recruitment videos portraying soldiers with guns, tweets praising the organization, and Telegram and Whatsapp to communicate with anyone[8].

Internal communication within the group

In addition to recruitment and propaganda, and almost most importantly, ISIS uses the Internet as a mean for internal communication. Consequently, one serious challenge they faces while having such an important online presence is the threat of being intercepted and localized by intelligence agencies and government authorities.

ISIS has been known using the Telegram application, founded by Russian Pavel Durov. Unlike WhatsApp, Kik, Facebook or Twitter, Telegram strives to guarantee privacy to its users. Law enforcement agencies cannot track individuals or demand that material inciting terror be taken down[9]. By reading the features on the official website Telegram.org, the app seems to answer all the criteria for ISIS's communication needs. Indeed, it allows you – to name the most useful for a large terrorist organization- "Connect from most remote locations", "Coordinate groups of up to 5000 members", "Send documents of any type", and more notably "Encrypt personal and business secrets", "Destruct your messages with a timer" while keeping the messages "safe from hacker attacks". [10] To this day, Telegram has more than 100,000 active users. The question remains to know how many of them belong to ISIS. Not only can users benefit from encrypted communication, a relatively new feature allows them to create "channels" through which they share images and videos to anonymous subscribers. ISIS created a channel gathering more than 10,000 subscribers with propaganda materials in English, French, Arabic and German, and plans for attacks. Telegram's CEO eventually decided to block all ISIS related channels.

They are prone to being tracked rather than if they used more traditional means communication and stayed off the Internet and ISIS is aware of this risk. However, as Abu Jihad, an active ISIS member has declared, "There are rumors that our forums are infected. But it is impossible for us to stay of the Internet".[11]

Since Internet communication at the heart of their internal communication and as a mean to spread their and attacks, any flaw in their strategy would be detrimental to their progress. It is therefore paramount for them to make sure to cover their traces. Many guides are available in French, English, German or Spanish, explaining how to use a secure connection. The online magazine Dar Al-Islam, written in French and published by ISIS's media center Al-Hayat, is retrievable solely by typing the keyword in any search engine. In the 9th edition released at the beginning of the year, the magazine issued a 16-pages section dedicated to online security. Chapter 1, "Introduction to communication securitization" is a step-by-step guide to secure web-surfing, and starts by introducing Tor[12]. After explaining that Tor can conceal your IP address, the reader is then warned not to send any personal

[8] https://www.buzzfeed.com/sheerafrenkel/everything-you-ever-wanted-to-know-about-how-isis-uses-the-i?utm_term=.wyQgO6L4N#.ct6wQ8MWv

[9] https://www.washingtonpost.com/world/national-security/islamist-militants-turn-to-less-governed-social-media-platform/2015/10/29/265dbaea-7e53-11e5-beba-927fd8634498_story.html

[10] https://telegram.org/

[11] https://www.buzzfeed.com/sheerafrenkel/everything-you-ever-wanted-to-know-about-how-isis-uses-the-i?utm_term=.wyQgO6L4N#.ct6wQ8MWv

[12] https://azelin.files.wordpress.com/2016/04/dacc84r-al-islacc84m-magazine-9.pdf (starting from p.38)

file through the software: “Can the NSA break the code? The answer is probably yes. Therefore you should never send anything on Tor that is personal, sensitive, or which you wouldn’t want the content to be intercepted”. The next section covers the HTTPS “Hidden service”, followed by the SSL Certificate. Chapter 2 covers PGP and Linux Tails OS, and the user is again reminded the DO’s and DON’Ts to keep his online anonymity. In this chapter, the application Telegram is mentioned. Using the example of Abu Bakr and Umar, the concept of PGP encryption is explained in a very clear and simple manner. Although the example seems very nicely written and didactic, the fact that such a magazine and instructions are available to anyone online is extremely worrying.

From Virtual Box, the installation of Linux Tail, to XMPP, Jabber, OTR, each concept is explained in precise details, yet the step-by-step illustrated guide makes it very easily understandable for anyone with a computer, wishing to take all precautions online. There is even a lexicon defining each term aforementioned.

Once again, this rigor and precautions show ISIS is organized on the cyber-landscape. However, if some government authorities believe encryption won’t necessarily make them untraceable by governments, other intelligence agencies state that they failed to identify signs of the attacks because ISIS was using the “dark web” to communicate. ISIS uses another encryption program as well, TruCrypt, as Reda Hame, a Parisian IT specialist planning to join ISIS told. Some doubts still remain whether ISIS really used encrypted communicated to plan the Paris attacks. Indeed, “When an encrypted email is sent, it still appears in inboxes and sent folders, it is just that the text is garbled.”[13] Cybersecurity experts have found none of these traces of emails. The Grugq, an Information security officer, believes ISIS does not use encryption but rather traditional unsophisticated methods (burner phone, SMS), summarized for each attack since May 2014 on his blog[14].

Fundraising

ISIS leverages on social media to fuel their fundraising endeavor. David Cohen, from the U.S. Treasury Department explains in a video how the terrorist organization receives donations through social media platforms. Despite the U.S’s efforts to cut ISIS’s access to revenue, the latter have the ability to collect funds and move them across countries. Indeed, there has been a shift from a person-to-person fundraising to social media as way to raise funds, bundle those funds and move them out of the Gulf to Iraq and Syria.[15].

Cyber-attacks

To this day, no major cyber-attacks have been claimed by ISIS. Only “petty” cyber-crimes with little impact would be coming from the organization. A group of hackers supporting ISIS, acting under the name “United Cyber Caliphate”, would be responsible for cyber-attacks. So far, the attacks have been limited to hacking and defacement of government websites and social media accounts.

[13] https://www.buzzfeed.com/sheerafrenkel/everything-you-ever-wanted-to-know-about-how-isis-uses-the-i?utm_term=.wyQgO6L4N#.ct6wQ8MWv
[14] https://medium.com/@thegrugq/just-the-facts-isis-encryption-c70f258c0f7#.wac7iy5li
[15] http://www.dailymail.co.uk/video/news/video-1130325/ISIS-fundraising-social-media.html

The Islamic State uses the cyber landscape to their profit. It is a place for cyber recruits, whether they have extensive IT knowledge or not. Indeed, the Deep&Dark Web is full of forums teaching basic technical and hacking abilities, where beginners can improve their skills, communicate with other members, and review manuals.

Laith Alkhouri, from the intelligence firm Flashpoint,explains that the attacks remain "relatively novice-level", "opportunistic, such as exploiting vulnerabilities to compromise websites and launching DDoS attacks"[16]. Pro-ISIS supporters are likely to use open source hacking tools (BeEF, evercookies, Newscaster) combined with custom malware[17]. Flashpoint reassures that ISIS does not represent a big threat for the Internet for the moment, notably not the Internet of Things nor governments. Indeed, if in 2014 the story of the Cyber Caliphate hacking the Twitter account of U.S. Central Command (CENTCOM) made a buzz, Alkhouri puts things in perspective: they obtained the credentials to a Twitter account, not classified information[18]. This "attack" was therefore rather trivial, and if we were to assess it using the rick assessment model (score = identification x estimation x probability), the risk would have been low: easily identifiable, low impact, and high probability. As a matter of fact, anyone could have performed the hacking, since it's a rather easy operation and tutorials are available online. The Cyber-Caliphate actually attacks "soft targets" such as small businesses with poor data security, whose impact is negligible. They have failed to take down big businesses such as Google, Facebook or Twitter, despite what they claim.

Since the Cyber Caliphate is "under-sophisticated" and "under-funded" according to Alkhouri, the Internet of Things seems safe for the time being. However, the day they will be able to send a driverless car instead of a suicide bomber will be a game-changer in the cyber-war. With a growing number of cyber-attacks and hackers, more sophisticated each time; ISIS's cyber capabilities are improving and should not be underestimated. The role of each authority now is to be proactive, as opposed to waiting for a more serious attack, and identify the vulnerabilities ISIS previously exploited. For instance, many hacked websites shared a common vulnerability (an outdated PHP script).

Shutting down the internet

In December 2015, in another one of his much publicized announcements, Donald Trump, the Republican runner for presidency in the United States expressed his wish to « shut down the internet ». Because ISIS has been so active on the web, for recruitment purposes, propaganda and terrorism, Donald Trump has urged the government to work closely with internet companies to stop the Islamic Organization. It would consistent in blocking internet access in parts of the world where ISIS is operating or where the US is at war. But is it really possible with today's technology to simply block access to internet? Wouldn't it result in more bad than good to do so?

[16] http://www.securityweek.com/isis-cyber-capabilities-weak-poorly-organized-report
[17] http://www.securityweek.com/attackers-increasingly-abuse-open-source-security-tools
[18] http://readwrite.com/2016/05/10/isis-hack-internet-things-iot-dt4/?utm_source=feedly&utm_medium=webfeeds

There are obvious technical obstacles in trying to deny access to internet. First of all, no one actually controls the internet, it is not owned by anyone. By its definition, internet is just a global network of networks that are owned by different countries, institutions and persons. It is just not possible for the US to prevent ISIS from getting on the internet in the US. The internet was designed to be redundant, that means that even if parts of it – a number of networks – are prevented from working, it is possible to find access to internet using other networks.

Governments and businesses have repeatedly tried to block access to some parts of the internet. One can remember during the Arab Spring in 2011, the attempt of the Egyptian government to shut down access to social media in order to prevent any information from leaking on the internet. One can also remember that these efforts were in vain and users found a way to circumvent the blocking.

Maybe the most famous example of internet censorship is the one taking place in China: some of the methods used include IP blocking, DNS poisoning, URL and packet filtering. But even in this case where a government takes very organized action in order to prevent access to some sites and increase the surveillance of the network, some people can still use secure VPN or SSH connection methods to computers outside mainland China to have access to blocked websites. Ai Weiwei, the famous artist and activist famously proclaimed: "leaders must understand it's not possible for them to control the Internet unless they shut it off". In the same way totalitarian governments cannot stop citizens from accessing internet, the US cannot prevent US citizens who are curious about ISIS to go to the websites they want.

Let alone the fact that the internet is rapidly changing and extremists are quickly moving between networks and countries. Moreover, the US doesn't have the ability to shut down the internet in countries they don't control. They could do so with military operations but even this possibility has its own technical complexities.

The US Cyber war strategy

However, given the danger of letting extremists freely enroll citizens in violent operations and the critical nature of the subject, action has to be taken. So what are the remaining options in the hands of the US government to fight ISIS' activity on the web?

In April 2016, the US acknowledged they are currently conducting cyber operations to fight ISIS. *"This was a historic moment," Peter Singer,* a cyber-security specialist told the Financial Times. *"We're not only using the capability but we are owning up to using it."* He also says it is the *"normalization of cyber warfare"*[19].

By using their extended use of the internet against them, the military are taking a different approach of the problem. The goal of the Cyber unit in charge of the operations is to disrupt their command, conduct and communication. But what is cyber warfare exactly? How does the Obama administration intend to use it against ISIS and how effective could it be?

[19] http://www.ft.com/cms/s/0/5b35eed8-00c4-11e6-99cb-83242733f755.html#axzz4D4disHk4

According to Richard Clarke, a former presidential advisor and counter-terrorism expert, in his book Cyber War: The next threat to national security and what to do about it, cyber warfare is defined as *"actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption"*[20]. But it also includes businesses, institutions and terrorists. Cyber warfare can be of two types: sabotage or espionage. Sabotage includes attacking power infrastructures, transportation, communications and equipment in order to prevent normal operations from taking place whereas espionage is the act of gathering intelligence and classified information by infiltrating the system of the enemy[21].

So how exactly is the US Cyber command fighting the Islamic State online? Cyber command is a division of the military that is only six years old and it has historically aimed its cyber weapons to Iran, Russia, China and North Korea. In its fight against ISIS, the US has planned different types of attacks:

Military hackers have been infiltrating the computers and other devices of ISIS members and placed viruses and malwares in order to be able to mine the machines and find useful information such as locations, names and hints to decipher the organization's next move and the plans they have designed. And some US officials are already reporting some successful operations. They say these attacks have led to the identification of key members and figures of ISIS, something Obama has confirmed at Langley, the CIA's HQ. These figures include Sulayman Dawud al-Bakar, responsible for the organization's chemical weapons program and Haji Iman, the second most prominent leader of the group[22].

The second key strategy of cyber command is to disrupt communications. The method used is similar to jamming but goes beyond it. This way, ISIS' networks are over solicited and do not work normally, which in turn prevents the organization from conducting its operations like it wishes to. It targets the organization's ability to attract new recruits, send orders and keep control of the situation.

Another goal of this strategy is to make ISIS members paranoid. The US military are said to be studying the online habits and methods of key leaders in order to imitate them and send wrong information to ISIS members, attracting them in places they can be captured. This is something cyber command could do on Telegram, the famous social network ISIS has been using because of its encryption feature. And by making encrypted channels unsafe, the US is pushing the Islamic State to use other channels of communications that they can easily monitor. Also, potential recruits are scared that they might be watched on Telegram and caught before joining ISIS.

One of the problems is, as soon as Cyber Command shifts from a passive posture of surveillance to an active attack, they lose a source of intelligence[23], as fighters stop using the watched channel as soon as an attack is identified. But finding the right balance between the need to collect information and the importance of disrupting operations is an issue as old as war strategy.

[20] https://www.amazon.com/Cyber-War-Threat-National-Security/dp/0061962244
[21] https://www.techopedia.com/definition/13600/cyberwarfare
[22] http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html
[23] http://www.thedailybeast.com/articles/2016/04/17/u-s-ratchets-up-cyber-attacks-on-isis.html

In order to take the group by surprise, Cyber Command did not share more information about the methods and strategies used against ISIS. It is also not apparent yet whether the operations have been successful and how effective they will be in the future to stop ISIS from running their cyber operations. When it launched cyber operations in Iraq in 2008, the US had deployed troops on the ground and armies of hackers and analysts. At that time, they would systematically mine the computer of every leader they would capture to generate intelligence and order new raids but it is not the case today. We also don't know much about ISIS ability to defend and attack back US infrastructures. If ISIS has been recruiting hackers as talented as the designers and video makers for their online communications; they might have the power to answer the attacks. Some analysts only see in this sudden outing about Cyber Command's operations a public relations campaign to justify the existence of the unit.

Silicon Valley's role

Even though Silicon Valley cannot shut down the internet like Donald Trump would imagine it, there are other ways tech companies act to slow ISIS' propaganda and operations online. Indeed, top US officials travelled to Silicon Valley days after the Paris attacks in order to meet with the companies' top executives and find ways to collaborate in the fight against terrorism. Technology companies meeting with US officials included Apple, Facebook, Google, Twitter, Microsoft, Linkedin and YouTube.

In the government's ideal world, companies would do most of the work. Tech companies already gather and process tons of data and are able with very precise algorithms to analyze user behavior. This would allow them, according to the government, to identify behavior that is prone to violence or accounts that have links to the Islamic State. For example, one of the features of Facebook consists in identifying suicidal behavior thanks to a "flagging" system where anyone can report accounts that are at risk of committing suicide. The government has been asking Facebook to use this kind of technologies to signal suspicious accounts to the authorities. But tech firms have been reluctant to fully collaborate. One of the reasons is guaranteeing user's privacy. The government is basically asking Facebook to predict a violent behavior and act on that prediction. The Apple vs FBI case is another illustration of the dilemma where security comes at the cost of privacy.

However, tech companies have also taken action on their own. They started developing and effectively using technologies that can detect hateful, violent and illegal content, take it down and prevent similar content from popping up again on their websites. These technologies are similar to the tools they have been using to remove child pornography for example. In the same spirit, Facebook, Microsoft, Google and Twitter agreed in March 2016 to an EU regulation that requires them to take down hateful speech from their platforms within 24 hours[24]. But once again, there is a fine line between censorship and policing illegal content. The four companies reassured their users that they will find the necessary balance and that their platforms will continue to guarantee free speech[25]. Google announced last February it planned on changing what comes up when people type search for ISIS related queries in their engine[26]. Now, non-governmental organization will be able to

[24] http://www.theverge.com/2016/5/31/11817540/facebook-twitter-google-microsoft-hate-speech-europe
[25] http://www.vanityfair.com/news/2016/06/google-and-facebook-quietly-escalate-their-cyber-war-on-isis
[26] http://www.mirror.co.uk/tech/google-fighting-isis-changing-what-7331274

advertise for free counter extremist content. This means that anyone typing an ISIS related search will be possibly targeted by an anti-radicalization ad, and hopefully, that person will click on the link.

As great purpose comes with responsibility, communication platforms should be required to police the content uploaded by users. Especially given the number of people that can be reached on such platforms and the availability of the network everywhere. ISIS understood it and made it a weapon.

Anonymous' own war against ISIS

Independently from government and business, the Anonymous organization has decided to wage a war against ISIS. Mirroring the lone wolf terrorism witnessed in the last years, Anonymous are urging independent hackers to join their force against ISIS. They have even published a guide to teach step by step the most amateur internet user how to help in the online fight against the Islamic State. The goal of Anonymous is to expose information of ISIS members online and go after their most vital infrastructures, like payment processing tools for example and the forums where they gather and send orders. Anonymous have shown their strength in the past when, for example, they complicated access to the phone system in Ferguson after Michael Brown's shooting last year. In our case, it has already taken down thousands of twitter accounts related to ISIS and targeted websites connected with terrorism[27]. Anonymous' action might not suffice but it sure is a force to be reckoned with.

Conclusion

Never in the history of terrorism had an organization appeared as web-savvy as the Islamic State. The extensive use of the internet allows ISIS to conduct its most vital operations. It can easily spread its hateful and violent messages to every corner of the world, reach vulnerable young people and lure them into joining the force, send orders and raise funds. All of it without much sophistication, only using available tools such as Telegram or the Deep&Dark net. Confronted to the issue, the US government, Silicon Valley's top executives or the hackers organization Anonymous have each taken action to fight the terrorist organization's sprawl on the internet. There is no evidence for the moment proving the effectiveness of their initiatives as ISIS continues to recruit, plan attacks and does not show any sign of weakness.

[27] http://fortune.com/2015/11/16/anonymous-cyber-war-isis/

Reference list (in order of appearance)

- Irshaid, F.(2016). *BBC News*. Retrieved 1 July, 2016, from http://www.bbc.com/news/world-middle-east-27912569
- Bloom. C. (2014). *Mail Online*. Retrieved 1 July, 2016, from http://www.dailymail.co.uk/news/article-2734534/ISIS-use-US-journalist-hostage-focus-latest-terror-campaign-social-media-hijacking-discussions-using-StevensHeadInObamasHands-hashtag.html
- Satti charles, B. (2014). *Security Intelligence*. Retrieved 1 July, 2016, from https://securityintelligence.com/funding-terrorists-the-rise-of-isis/
- Baker, Leede. (2016). *Icctnl*. Retrieved 1 July, 2016, from http://www.icct.nl/download/file/ICCT-Bakker-de-Leede-European-Female-Jihadists-In-Syria-Exploring-An-Under-Researched-Topic-April2015(1).pdf
- Mclaughlin, E. (2016). *CNN*. Retrieved 1 July, 2016, from http://edition.cnn.com/2016/02/19/middleeast/isis-child-soldiers/
- Frenkel. S. (2016). *BuzzFeed*. Retrieved 1 July, 2016, from https://www.buzzfeed.com/sheerafrenkel/everything-you-ever-wanted-to-know-about-how-isis-uses-the-i?utm_term=.wyQgO6L4N
- Miller, G. (2016). *Washington Post*. Retrieved 1 July, 2016, from https://www.washingtonpost.com/world/national-security/islamist-militants-turn-to-less-governed-social-media-platform/2015/10/29/265dbaea-7e53-11e5-beba-927fd8634498_story.html
- The grugq. (2016). *Medium*. Retrieved 1 July, 2016, from https://medium.com/@thegrugq/just-the-facts-isis-encryption-c70f258c0f7
- Dailymailcouk. (2016). *Mail Online*. Retrieved 1 July, 2016, from http://www.dailymail.co.uk/video/news/video-1130325/ISIS-fundraising-social-media.html
- Lennon. (2016). *Security Week*. Retrieved 1 July, 2016, from http://www.securityweek.com/isis-cyber-capabilities-weak-poorly-organized-report
- Kovacs. E.(2016). *Securityweekcom*. Retrieved 1 July, 2016, from http://www.securityweek.com/attackers-increasingly-abuse-open-source-security-tools
- Curwin. T.(2016). *Readwritecom*. Retrieved 1 July, 2016, from http://readwrite.com/2016/05/10/isis-hack-internet-things-iot-dt4/?utm_source=feedly
- Khalaf, R.(2016). *Financial Times*. Retrieved 1 July, 2016, from http://www.ft.com/cms/s/0/5b35eed8-00c4-11e6-99cb-83242733f755.html
- Clarke, R.A & Knake, R. (2012). *Cyber War: The Next Threat to National Security and What to Do About It*. : Ecco.

- Techopediacom. (2016). *Techopediacom*. Retrieved 1 July, 2016, from https://www.techopedia.com/definition/13600/cyberwarfare
- Sanger. D.(2016). *Nytimescom*. Retrieved 1 July, 2016, from http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html
- Thedailybeastcom. (2016). *The Daily Beast*. Retrieved 1 July, 2016, from http://www.thedailybeast.com/articles/2016/04/17/u-s-ratchets-up-cyber-attacks-on-isis.html
- Toor,A. (2016). *The Verge*. Retrieved 1 July, 2016, from http://www.theverge.com/2016/5/31/11817540/facebook-twitter-google-microsoft-hate-speech-europe
- Kosoff, A.(2016). *The Hive*, Google and Facebook quietly escalate their cyber-war on ISIS. Retrieved 1 July, 2016, from http://www.vanityfair.com/news/2016/06/google-and-facebook-quietly-escalate-their-cyber-war-on-isis
- Parsons, J.(2016). *Mirror, Google is fighting ISIS by changing what happens when you Google 'ISIS'*. Retrieved 1 July, 2016, from http://www.mirror.co.uk/tech/google-fighting-isis-changing-what-7331274
- Reisinger, D. (2015). *Fortunecom*. Retrieved 1 July, 2016, from http://fortune.com/2015/11/16/anonymous-cyber-war-isis/