Physical Threats in Online Worlds – Technology, Internet and Cyber under Terror Organization Services; a Test Case of "The Islamic State"

Tal PAVEL, Ph.D

Expert on Middle East and Global Internet and Cyber Threats
Editor in Chief Middleeasternet.com
tal@middleeasternet.com

Terror and internet, on the surface those are two different worlds of content:

Terror is the implication of violence, or threatening to implement it, against civilians in the name of achieving political aims. First and foremost, granted the civilians are considered the "underbelly" of society and means of heightened pressure on the government so they change their policy and actions according to the terror organization's will.

Due to its nature, terror action is discrete, mostly departmentalized, hierarchical, and defies the existing order and asks to change it. Today, most terror actions committed by Islamic organizations whose aim is to enforce with violation and force of arm the Islamic religion, values and culture on the rest of the countries in the world and emphasizing the western countries and as revenge on the physical action of those countries in various places around the world and their attitude towards Muslims viewing these organizations. This is done in contrast with values, culture, tradition, governmental orders, freedom and democracy.

On the other hand, the technology, internet and cellular in most cases are the product of the west, including hardware, software, computer games, apps, browsers, coding software, operating systems, giant companies and other technological solutions.

And yet, despite this striking contrast, Islamic terror organizations make use of all of technology's wonders and the heights of western innovation, using these tools to fight the west and its culture, which they are trying to tattoo. Meaning the Islamic terror organizations today fight the west, its culture and its values using its own tools.

Physical terror action includes several stages which, together, comprise a whole life cycle which includes, among others: spreading the ideology and the message; recruiting supporters, activists, and money; communication between the supporters and the organization, and communication between the activists before and during the execution of terror actions; gathering intelligence before committing the terror action; operational guidance for activists; executing the terror action; and finally documenting

the action and publishing it using different media in order to achieve the fear effect, the terror the action was intended for.

Today, using various technological developments, which are available to anyone, the terror organization can execute most of these stages using online means. The terror action itself is conducted in a physical space, yet almost all of the preparation stages can be conducted in the online and technological space, in order to create a physical terror action, which in turn is documented by various technological means, is published in the online and cellular arena and distributed by social networks and various media apps. Thus the life cycle of a physical terror act is closed, which began in the online space, was executed physically and came to completion in documenting the action back in the online world.

The online connection serves the "Islamic State" organization in creating communication in different ways, on vast platforms, in front of target audiences and in many languages. Social networks serve the organization and its supporters as a stage to distribute their aims, to the media, to document terror events they committed, and actually, for anything.

The "Islamic State" organization operates a **news agency** called Amaq, which publishes a lot of information, high in quality and frequency, about the actions in the areas of the "Islamic State" and the battles [1]. This is done among others by using tags on Twitter such as *#amaqagency [2]*, *#amaqnews* [3]. Among the information published by it there can be found videos that show terror actions in real time which were committed by their activists around the world including the Philippines [4], the Parliament invasion in Iran [5], and streaming updates [6] about what is going on all the while taking responsibility for the event [7], as well as for terrorist attacks. Such as those which were committed in Tunisia [8], Paris [9], London [10], Afghanistan [11], Orlando [12] and other places around the world [13]. Alongside terrorist attack documentation [14], which the organization has committed, and hostages it's caught [15], and even documenting water shortage for the citizens of the city of Raqqa in Syria after the American aerial attack which damaged the water systems [16].

In addition, the news agency published many **infographs** in different languages, which summarize in a visual way the terror actions its people are committing [17], including the battles on the city of Mosul [18].

Moreover, the organization has launched several **apps**, in order to spread news on its activity in the fields under his control [19] and the news agency's in order to spread its word in cellular means as well [20], also there are apps for communication between its activists [21].

Another use in the cellular world is not only creating apps, but also using existing ones for the benefit of the organization publications. The app **Telegram**, for the relative secrecy it provides and the capability of creating information distribution channels (Channels), became a favorite among the organization, as well as many other organizations and companies that participate in the war in Iraq and Syria [22]. It has come to a claim that it has published in December 2016, according to which the usage of this app by the "Islamic State" is more common than the social network Twitter [23]. Moreover, the organization uses other communication apps, some in a targeting way, in example Zello [24], which enables turning the cellular phone device into a Walkie Talkie, through which voice messages of its activists were spread [25].

Another area is the **social networks**, where, along with the active use in various networks, there is an attempt of the organization to create a social network alike Facebook [26], as well as a Facebook page named Islamic State Scholars, as a framework where Muslim religious people expressed their support of the organization and a stage for internet users to pose them with religious questions (the page is inactive to date) [27]. Meanwhile, the social networks serve as a stage not only for spreading the organization's messages, but also for using different tags where warnings to the USA against their military involvement in Iraq (جمعة_تحذير_الشعب_الأمريكي) are published during the year 2014 [28] and against the west as a whole [29]. Beside it being a common viral stage for creating **online psychological warfare**, the ability to create in online means that is now called Fake News, a false, alternative reality, which no longer exists in the physical one. In creating this alternative reality with online means and spreading it around the online world, the organization wants to magnify its activity and the fear effect, to assimilate it and horrify even more. The most obvious example for that is the story of the execution of Jordanian pilot Lieutenant Muath Safi Yousef Al-Kasasbeh [30], whose plane was shot down on the 24th of December, 2014 by the organization's men while participating in an attack on his viewpoints in Syria. During his capture, the "Islamic State" published an interview with him in issue number 6 of the organization's magazine, Dabiq (pages 34-37) [31]. In January 2015 a well-edited, high quality video was published, which documents for 22 minutes the pilot's execution in cremation while being inside a cage [32]. Yet a blogger named Thomas Wictor published in the beginning of February a detailed analysis where he claims that this video is nothing but a fake (a claim which was published simultaneously by the hacker organization "The Electronic Syrian Army") [33]. The pilot was indeed executed, yet by being shot in the head after carrying out his captors' instructions and making various movements, which imitate being burned in a cage. The blogger's claim was that the video was edited in a professional way and that the fire was nothing but computerized effects and weren't real [34]. Those were created to maximize the horror and fear effect and to assimilate the event in the collective memory. And on the other hand, to ensure, horrifically, that the desired movements were achieved while maintaining repetition until his captors have achieved the desired final product.

Another reason for executing an online psychological warfare by the organization, is not only to magnify its activity and the fear factor, but to attribute horrific actions to its enemies and presenting them as barbarians. An example for this is the Twitter announcement which was published in the beginning of January 2014 in which a photograph of skulls claiming that these were found by the organization's warriors after seizing an airport from Shi'ite warriors. In reality, it turns out that the photograph was taken from a Muslim cemetery in Jaffa [35].

Another online activity arena for spreading the organization's word, its Mishna and activity are **online magazines,** which are published by it from time to time in high quality and in different languages. Magazines in English include *Dabiq [36]*, which is published from time to time since July 2014, and *Rumiyah* [37], which is published monthly from September 2016. It appears that this magazine replaced several others that were active beforehand, including *Dar al-Islam [38]*, which was published in French from the end of December 2014, *Konstantiniyye* in Turkish [39], which was published from June 2015, and a Russian magazine named Istok [40].

Alongside publishing the organization's messages and communication with its supporters, modern technology serves the terror organizations with creating **operational communication** among its activists. Both by posing various operational alerts and messages in porn websites and electronic dealing [41], and even claiming to use gaming platforms such as PS4 for planning and coordinating physical terrorist attacks [42]. The arena of **computer games** serves the organization not only for communication, but also for boosting the warriors' moral and training in warfare tactics. For this purpose, it has launched back in September 2014 a game named "Sound of Swords" (صليل الصوارم) [43].

The organization uses various new technological means including **multirotor drone** for documenting suicide operations [44], and for executing terrorist attacks by dropping bombs from the drone above the target [45], alongside publications, which summarize the results of those drone bombings [46].

Another technological mean is the virtual coin, **Bitcoin**, which was charged a few times because it serves the organization's activists in events and different places around the world [47].

Simultaneously, the organization is trying to keep its security and its people's security and therefore it is **publishing various guidelines** and instructions for careful online behavior in order to avoid the NSA's eyes and not enclose their location [48], all the while using various **coding software**, most of which comprise a compilation of existing Arab software, for protection of the communication and security of its activists [49].

On the other hand, the organization acts to **recruit activists** using various technological means including sending alerts via Viber [50], but not just activists, but also active hackers. In the end of January 2016, it was published that responsible bodies recognized with "Islamic State" are ready to pay Indian hackers a sum of up to 10,000 dollars for a successful attack on the local government websites and achieving access to sensitive documents and stealing them [51]. This happened after the fact that am o nth earlier it was reported that the Indian government intends to create a war room in order to protect the social networks 24 hours a day as a part of its war against the online activity of the "Islamic State" in Indian languages and other Asian languages, aside from Hindi and English [52].

Hackers who recognize themselves with the activity of the "Islamic State" committed over the past years online actions, which do not constitute a real cybernetic attack with physical, tangible damage. These were mainly **hacks into different websites** around the world and defacing them [53], alongside **hacking accounts** in the social networks where contents supporting the organization was posted. In addition, its activists dealt with **information leaks**. Mainly personal information of bodies in the USA [54], for example the leak in March 2015 of information of about a hundred pilots of the US army [55], and publishing information and pictures of the air force bases of the US in Saudi Arabia [56]. In September 2016 a citizen of Kosovo, a minor named Ardit Ferizi, was sentenced to 20 years [57] in jail after confessing to hacking in June 2015 to the computer systems and transferring the information of 1,351 US government and army personnel [58] to Junaid Hussain [59], who was nicknamed Abu Hussain al-Britani, an organization member of the "Islamic State". He published the information on August 11th, 2015, and was eliminated by an American USAV in Raqqa two weeks afterwards. Moreover, halfway through March 2016 "Caliphate Cyber Army", which is recognized

with the "Islamic State", published the information of 36 police officers of the Minnesota Police Department.

Indeed, there are various attempts in fighting this branched online activity of the "Islamic State".

The USA and the UAE created a center named Sawab [60], for **online warfare [61]** against the extreme contents the organization is spreading. This was created, on the one hand, to show other moderate sides of the Islam religion, and on the other, to display the horrors of the organization and the price the victims, as well as the activists and their families, must pay, and this is done by creating campaigns and tags in English [62] and Arabic [63] in the social networks.

Provided the online activity of the organization is expressed in the various social networks, these are uniting to minimize the organization and its activists' online presence. At the end of April 2015 Twitter announced that it has blocked accounts related to the "Islamic State" [64] and in February it posted on its official blog that during the second half of 2015 it blocked above 125,000 accounts, which support terror actions, most of them related to the "Islamic State' [65]. Against this action messages were posted on behalf of the organization containing threats on the lives of the founders of Facebook and Twitter [66].

Does a repetitive shutting-down of social network accounts indeed assist in preventing the terrorist organizations' online activity? A study published in February 2016 determines that such a move indeed has the capability of restricting the online activity in the English language of the organization's supporters [67]. Whereas a study published roughly a year earlier analyzed the activity of the supporters of the organization on Twitter in characteristics of geographical location, the language the users write in, the number of accounts closed and the scope of their popularity. The research determines that closing the accounts can create new threats, including increasing the radicalization of the supporters of the organization in the social networks [68].

In March 2017, however, news alerts were posted, according to which, Twitter has blocked above 636,000 accounts connected with terror actions since the beginning of August 2015, when only the in second half of 2016 it blocked about 377,000 such accounts [69].

Another way is not only blocking specific accounts in social networks, but often blocking access completely to these networks. Halfway through 2014, it was reported that Iraq has blocked access to Google, YouTube and Facebook in an attempt to prevent spreading the "Islamic State" propaganda inside Iraq [70]. This is done alongside publications of the coalition of countries fighting the "Islamic State" which call users **to report messages that support the organization** in the various social networks [71], and a similar calling from the government of France [72]. Also, infographs that depict the horrors of the organization, the damages it made and its enormous financial profits [73], which sometimes are based on infographs that the organization has published [74].

Yet, the activity against this propaganda is also in the physical plane, for example **arrests** of those suspected in involvement with the organization's activity or eve in publishing online contents that support terror. At the end of February 2015 a young Kurdish man was sentenced in Vienna to six months in prison on probation for being accuses of publishing propaganda in favor of the organization on Facebook [75], and pictures from its activities. In Spain in October 2016 two Moroccan youngsters were arrested for publishing online contents supporting terror and promoting the

organization's activity [76]. Another way of stopping the organization's activists is, in example, the Russian software, which is used to detect and capture recruiters on behalf of the "Islamic State" in the various social networks. The experts search in various posts in the social networks for signs that indicate recruitment, and then address the user in a covert way and with technological means in order to expose and arrest him [77].

Another way is the combination of technological means and public activity, for example the **Hackathon**, which lasted a few days, which took place in many cities around the world including Australia, as part of a national local program for extreme online warfare, while calling Australian youngsters to suggest online solutions for dealing with the organization's online propaganda [78].

The religious bodies in some of the countries also rallied to warn against the organization's propaganda implications; in example, the high religion authority in Egypt forbade in March 2015 women from marrying activists of the "Islamic State" via the internet. This was a reaction to messages the organization posted in the social networks where there was a call for marriage via video chats [79].

Even the activist phenomenon "**Anonymous**" is acting against the "Islamic State" organization, by conducting an online hunt [80], which includes various operations and tags in the different social networks, including OpNo2ISIS [81] , OpISIS [82], OpFuckISIS [83], OpIceISIS [84]; publishing guidelines which hold guidelines for online warfare against the organization, hacking and detecting its activity in social networks and an explanation on how to report this online activity, creating an online form for reporting the Twitter accounts recognized with the organization [85]; publishing addresses of Twitter accounts associated with it [86]; and spreading videos that call for online warfare against the organization [87]. This goes along with activity of hackers who hacked in March 2017 to the news agency of the "Islamic State" and used it as a base for spreading malware [88].

The organization "Islamic State" acts in modern means to enforce religion, culture and values which root back more than a thousand years, on the western world, not only through physical terror actions and military occupations, but also using various technological means to accomplish all the stages of executing physical terror activity. Beginning with spreading the message and ideological ideas and ending with documenting the physical terror activity itself with online means and spreading it using the various platforms around the world; both to encourage the organization's supporters and to spread fear and terror among its enemies.

Therefore, the challenge the organization poses is on various planes, including: the military, ideological, and technological. Even if the technological level and the cybernetic threat its activists pose is low right now and is not posing a threat for actual cybernetic damage, dealing with its activity needs to be in all planes, including the technological, internet and cellular.

Granted the supporters and activists of the organization are youngsters who grew up in an internet, online and cellular environment, when most of them even came from the western countries, from an environment saturated in technology and internet, then these various means are available to the organization's activists and supporters and constitute a natural environment in the entire scope of its activity. Mainly in an organization which has support among many countries, resulting in a phenomenon where these don't have to physical be in the war zones, but can stay in their place, be active as "lone wolves" both as active terrorists and active in the online and cybernetic arena.

Section III - Cyber-Attacks Evolution and Cybercrime Trends

Thus, dealing with its technological and online activity needs to be in different plains, varying, in various means by individuals, organizations and countries. Autonomously and coordinated as one. Yet because of the nature of the "Islamic State" organization and the nature of its activity around the world, it is important to know that technology alone cannot provide an encompassing solution to the challenge this organization is posing. The technology provides one layer of cultural, religious, social, financial, intelligence, and military coping. As complex as the organization, its messages and activity are, so will be the coping, which is not far from being over in the technological and internet planes.

REFERENCES

[1].   https://twitter.com/arabcrunch/status/712233227939872768
[2].   https://twitter.com/search?q=amaqagency&src=typd
[3].   https://twitter.com/hashtag/amaqnews?src=hash
[4].   https://twitter.com/Terror_Monitor/status/874460306365308928
[5].   https://twitter.com/ShamiRebel/status/872399146656903170
[6].   https://twitter.com/ShamiRebel/status/872391403967586304
[7].   https://twitter.com/HTiflati/status/872388912504819712
[8].   https://twitter.com/MouradTeyeb/status/871125540278763520
[9].   https://twitter.com/cheechny/status/855205910297419783,
        https://twitter.com/SigfridSoria/status/855184863284125696
[10].   https://twitter.com/LondonLovesProp/status/844889575810125824,
        https://twitter.com/ezzsaid/status/844887108691091458
[11].   https://twitter.com/Terror_Monitor/status/839470489009430529
[12].   https://twitter.com/merriemarie/status/742079303580405761
[13].   https://twitter.com/MiaMBloom/status/837031136052318217
[14].   https://twitter.com/Terror_Monitor/status/876669140609753088,
        https://twitter.com/TheDaneChris/status/842180027584286720
[15].   https://twitter.com/Terror_Monitor/status/840885544443768832,
        https://twitter.com/Terror_Monitor/status/826621262784925697,
        https://twitter.com/Terror_Monitor/status/824944728567226369
[16].   https://twitter.com/iWXt5rOlTFLIqcx/status/877231177706459137
[17].   https://twitter.com/CyranAli/status/870833655668588544,
        https://twitter.com/elcaos/status/864234097455095808,
        https://twitter.com/ToreRHamming/status/852409573189332992,
        https://twitter.com/Caliphate_Crush/status/852231059890556928,
        https://twitter.com/Terror_Monitor/status/850169585152139264,
        https://twitter.com/BrahimCherIshaq/status/805988904298049536,
        https://twitter.com/TRACterrorism/status/845569782699184128,
        https://pbs.twimg.com/media/CkaYnAJWkAA7ViT.jpg,
        https://twitter.com/HTiflati/status/828719449448517632
[18].   https://twitter.com/iBRABO_com/status/825353431313444864,
        https://twitter.com/global_awar/status/822873696427708416
[19].   https://goo.gl/yvWWyZ
[20].   http://www.gadgetsnow.com/apps/ISIS-launches-app-to-spread-terror-
        agenda/articleshow/50150930.cms

[21]. http://securityaffairs.co/wordpress/42581/intelligence/isis-mobile-app.html, https://goo.gl/zXkEij

[22]. http://blog.godreports.com/2017/05/isis-uses-telegram-app-to-foment-terror, https://isis.liveuamap.com/en/2017/15-may-isis-have-significantly-increased-social-media-activity

[23]. http://securityaffairs.co/wordpress/54787/terrorism/telegram-isis.html

[24]. https://zello.com

[25]. https://www.voanews.com/a/is-uses-broadcast-app-to-spread-militant-message/2683632.html, https://learningenglish.voanews.com/a/islamic-state-group-using-us-based-app/2688114.html, https://zello.com/shared/rXgT, https://zello.com/shared/hCdW

[26]. https://goo.gl/cqYzFq

[27]. https://goo.gl/mLLd31

[28]. https://goo.gl/qJWAQy

[29]. https://twitter.com/alamrikiya_001/status/597441432333492224

[30]. https://en.wikipedia.org/wiki/Muath_Al-Kasasbeh

[31]. https://clarionproject.org/docs/isis-isil-islamic-state-magazine-issue-6-al-qaeda-of-waziristan.pdf

[32]. http://archives.bluenationreview.com/isis-continues-streak-savagery-burns-jordanian-pilot-alive

[33]. https://twitter.com/Official_SEA16/status/562757674417520640

[34]. http://www.thomaswictor.com/the-jordanian-pilot-was-not-burned-alive

[35]. https://twitter.com/2awsy/status/479740129591197696

[36]. https://clarionproject.org/islamic-state-isis-isil-propaganda-magazine-dabiq-50, https://en.wikipedia.org/wiki/Dabiq_(magazine)

[37]. https://en.wikipedia.org/wiki/Rumiyah_(magazine)

[38]. https://en.wikipedia.org/wiki/Dar_al-Islam_(magazine)

[39]. https://en.wikipedia.org/wiki/Konstantiniyye_(magazine), http://www.hurriyetdailynews.com/isils-magazine-slams-erdogan-turkey-for-first-time.aspx?pageID=238&nID=85754&NewsCatID=338

[40]. https://en.wikipedia.org/wiki/Istok_(magazine)

[41]. http://www.dailymail.co.uk/news/article-2974639/Terrorists-leaving-secret-messages-websites-like-ebay-Reddit-communicate-plan-future-attacks.html

[42]. https://www.forbes.com/sites/insertcoin/2015/11/14/why-the-paris-isis-terrorists-used-ps4-to-plan-attacks/#2519b7dd7055

[43]. http://www.elfagr.org/693221#

[44]. https://twitter.com/Terror_Monitor/status/876254431175598080

[45]. https://twitter.com/Terror_Monitor/status/875210517249277952, https://twitter.com/tanvirarain/status/828843858448543744

[46]. https://pbs.twimg.com/media/C4As-YCWMAAD3di.jpg

[47]. https://securityintelligence.com/isis-are-they-using-bitcoins-to-fund-criminal-activities, https://www.wired.com/2017/03/anarchist-bitcoin-coder-found-fighting-isis-syria, https://nextshark.com/indonesian-isis-militant-used-paypal-bitcoin-fund-terrorists, http://uk.businessinsider.com/report-bitcoin-anarchist-amir-taaki-investigated-fighting-isis-syria-2017-3, http://www.foxnews.com/tech/2015/11/25/isis-parks-its-cash-in-bitcoin-experts-say.html, http://www.newsbtc.com/2016/11/30/indonesian-investigator-claims-bitcoin-funding-isis-operations,

http://www.wienerzeitung.at/_em_daten/_wzo/2016/01/25/160125_1356_europol
_dokument_aenderungen_in_der_verfahrensweise_mit_is_terroranschlaegen_pdf
_englisch.pdf, https://www.cryptocoinsnews.com/ghostsec-isis-bitcoin-wallet-
worth-3-million,

[48]. http://www.ibtimes.co.in/isis-releases-training-guide-how-tweet-safely-without-
giving-out-your-location-nsa-611734, https://alkhilafaharidat.wordpress.com

[49]. http://grugq.github.io/blog/2014/08/09/jihadist-fan-crypto

[50]. http://www.yourmiddleeast.com/culture/this-photo-could-show-how-is-tries-to-
recruit-our-tehranbased-writer-through-viber-from-eu-countries_27622

[51]. http://securityaffairs.co/wordpress/44019/hacking/isis-infiltrating-indian-hacking-
community.html

[52]. http://indiatoday.intoday.in/story/government-plans-social-media-scanning-
centre-to-take-on-isis/1/554878.html

[53]. http://www.independent.co.uk/news/world/europe/french-tv-network-tv5monde-
hijacked-by-isis-hackers-in-unprecedented-attack-that-revealed-personal-
10164285.html, https://www.rt.com/news/248073-islamic-state-hackers-french-tv,
http://www.telegraph.co.uk/news/worldnews/asia/malaysia/11368991/Malaysia-
Airlines-website-hacked-by-Cyber-Caliphate.html,
https://www.hackread.com/isis-hackers-euro-atlantic-integration-nato-sit,
http://oregonfaithreport.com/2015/03/isis-hacking-christian-website,
https://www.hackread.com/pro-isis-hackers-us-dept-of-energy

[54]. https://techcrunch.com/2015/01/12/cyber-caliphate

[55]. https://goo.gl/RNi4yZ

[56]. https://justpaste.it/itmx

[57]. https://www.justice.gov/usao-edva/pr/isil-linked-hacker-sentenced-20-years-
prison

[58]. https://goo.gl/1Fk5KG

[59]. https://en.wikipedia.org/wiki/Junaid_Hussain

[60]. https://twitter.com/sawabcenter

[61]. http://www.thenational.ae/uae/government/sawab-centre-warns-youth-about-
joining-isil

[62]. https://twitter.com/hashtag/DeludedFollowers?src=hash

[63]. https://goo.gl/9uK5ht

[64]. https://twitter.com/zaidbenjamin/status/593809974981165056

[65]. https://blog.twitter.com/official/en_us/a/2016/combating-violent-extremism.html

[66]. http://www.vocativ.com/289402/isis-threatens-mark-zuckerberg-and-jack-dorsey/

[67]. https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/Berger_Occasional%20
Paper.pdf

[68]. https://www.brookings.edu/wp-
content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf

[69]. http://www.khaleejtimes.com/technology/twitter-blocks-600000-terror-related-
accounts-in-18-months

[70]. http://www.ibtimes.co.uk/iraq-crisis-twitter-google-youtube-facebook-blocked-
by-government-stop-isis-plotting-1452567, https://goo.gl/kPbHbg

[71]. http://theglobalcoalition.org/en/takedaeshdown-2

[72]. https://pbs.twimg.com/media/DCD19f7U0AAcdg4.jpg

[73]. https://twitter.com/TruthAboutISIS/status/864164754360807424,
https://pbs.twimg.com/media/C-WN4PVXcAAZx73.jpg:large,
https://twitter.com/TruthAboutISIS/status/847893765440143360

[74]. https://twitter.com/kuba_dyrda/status/839151697167597568,
https://twitter.com/TruthAboutISIS/status/839165764456308736

[75]. https://www.thelocal.at/20150226/six-months-for-isis-facebook-postings

[76]. https://www.moroccoworldnews.com/2016/10/198614/two-moroccans-arrested-spain-advocacy-terrorism-internet/

[77]. https://sputniknews.com/world/201510131028439751-russia-computer-program-isil-recruitment/

[78]. http://www.abc.net.au/news/2015-09-03/talkaboutit-myhack-youths-fight-back-against-islamic-state/6743870

[79]. https://sputniknews.com/world/201503051019088590

[80]. http://archives.bluenationreview.com/hacker-group-anonymous-isis-will-hunt,
http://securityaffairs.co/wordpress/33288/hacking/anonymous-launches-opisis.html

[81]. https://twitter.com/search?q=OpNo2ISIS,
https://www.facebook.com/hashtag/opno2isis

[82]. https://twitter.com/hashtag/OpISIS?src=hash

[83]. https://twitter.com/hashtag/OpFuckISIS?src=hash

[84]. https://twitter.com/hashtag/OpIceISIS?src=hash

[85]. https://fossbytes.com/anonymous-publishes-three-guides-to-teach-you-how-to-hack-and-fight-isis

[86]. https://pastebin.com/zZffB762, https://pastebin.com/d8ND4rvV,
https://ghostbin.com/paste/nfvej, https://pastebin.com/nuCYVgty

[87]. https://www.youtube.com/watch?v=Cy9blSPn8nw&feature=youtu.be,
https://www.youtube.com/watch?v=_kJtvFUMELM&feature=youtu.be,
https://www.youtube.com/watch?v=BPE_sRhZp6M&feature=youtu.be,
https://www.youtube.com/watch?v=b7Svk1xIWw0&feature=youtu.be

[88]. http://www.securityweek.com/pro-isis-amaq-news-site-hacked-serve-malware