The end of Islamic State's Cyber Security unit Afaq?

Dr. Eitan Azani, Ms. Daniel Haberfeld

Reichman University
International Institute for Counter-Terrorism
With the Support of the Jusid man Foundation

July, 2022

About International Institute for Counter-Terrorism (ICT)

The International Institute for Counter-Terrorism (ICT) is one of the leading academic institutes for counter-terrorism in the world, facilitating international cooperation in the global struggle against terrorism. As a non-partisan think tank, ICT provides expertise in terrorism, counter-terrorism, homeland security, threat vulnerability, risk assessment, intelligence analysis, national security and defense policy. To promote this goal, ICT accepts article submissions from acknowledged scholars, practitioners, and experts in the field for publication on its website and social media pages.

About ICT Cyber Desk

ICT's Cyber Desk addresses the growing use of terrorist organizations online. Quarterly reports are published on ICT website and include recent information on terrorist organizations' use of the operational arena, the defensive arena and the offensive arena. The operational arena serves as the main arena used by terrorist organizations in cyberspace including communication platforms, propaganda, recruitment, training, intelligence gathering, information sharing and fundraising. The defensive arena is designed to protect user anonymity and information security and to offer tips and warnings on cyber security. The offensive arena includes cyber-attacks, hacking tutorials, and hacking discourse.

Introduction

In March 2022, the Islamic State's online chat platform underwent a cyberattack on its most encrypted server on Element. The server, which was powered by "Electronic Horizon foundation" (Afaq) a cyber defense unit that supports the Islamic State, enabled supporters of the organization to publish propaganda and chat virtually without any restriction .

The Islamic State continues to experience cyberattacks on its online platforms, including DDoS attacks on its websites and social media accounts defacement. The most prominent actors operating against the organization are **Anonymous hacktivists and pro-Iranian Shiite hacker groups**. The first anonymous campaign called Op-ISIS was launched in 2014, then again in 2016 and 2020. While cyber-attacks by pro-Iranian Shia hackers from Iraq are carried out at least once a month. Most of them are defacement attacks of Islamic State social media accounts and websites. This is in addition to the ongoing efforts by security forces to address the presence of terrorists online.

The uniqueness of the recent cyber-attack on Islamic State's Element server does not lie in shutting down of the chat platform, but rather, it was the publication made by the unknown attacker that followed said attack that played an important part as it **exposed Afaq as a fraudulent foundation and caused a trust crisis among Islamic State supporters. The following article will describe Afaq's role in Islamic State's cyber defense arena over the years; the recent cyber-attack on the foundation; and the implications of the attack**.

Profile: Electronic Horizon foundation (Afaq)

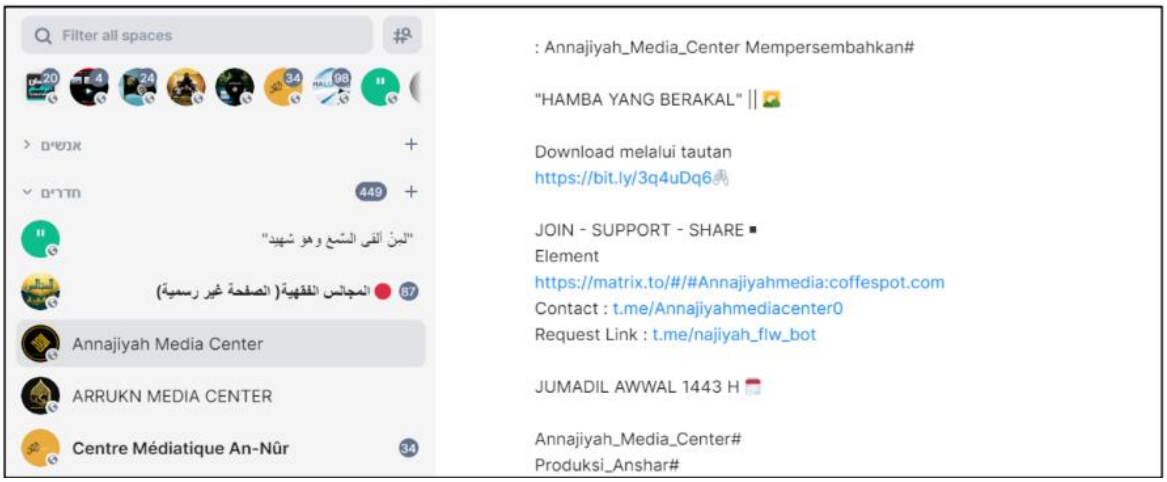
It is estimated that Electronic Horizon foundation (Afaq) was first established around 2016 and aligned itself with the Islamic State Caliphate. From the very beginning, the foundation has endeavored to provide online users with tools to prevent surveillance and secure Internet browsing (by computer or mobile phone). As such, they published on their online platforms' tips on cyber security, warnings against the use of certain apps, websites, and fake social media accounts. The foundation also provided courses and articles on cyber security, sharing general information on trends and cyber-attacks, recommending communication apps, and establishing dedicated cloud and chat platforms to be used by online followers of the Islamic State.

Among the Key trends Afaq has led during the years of operation are (1) **educating followers to remain anonymous online by using Tor, VPN and other tools to avoid being detected.** (2) **Shifting to more secure encrypted platforms** such as the move to Telegram and Element. (3) **Shifting to private cryptocurrency** such as Monero and warnings against the use of Bitcoin.

One of the latest key operations carried out by Afaq began in April 2021. Then, the foundation developed a cloud-based platform based on Nextcloud, designed for followers to store propaganda materials.

A frame from a video Afaq published explaining how to enter the new chat as well as the cloud platform

That month, they also developed a **new chat platform named S-chat on the Element matrix server for more secure communication**. While the S-chat server was shut down after a month due to an unknown reason, another chat server (named *Coffespot*) was opened shortly after in July 2021 and operated until the recent cyber-attack in March 2022. The server provided access to chat rooms that were directly and exclusively connected to Islamic State supporters.



Screenshot from the Coffespot server on Element

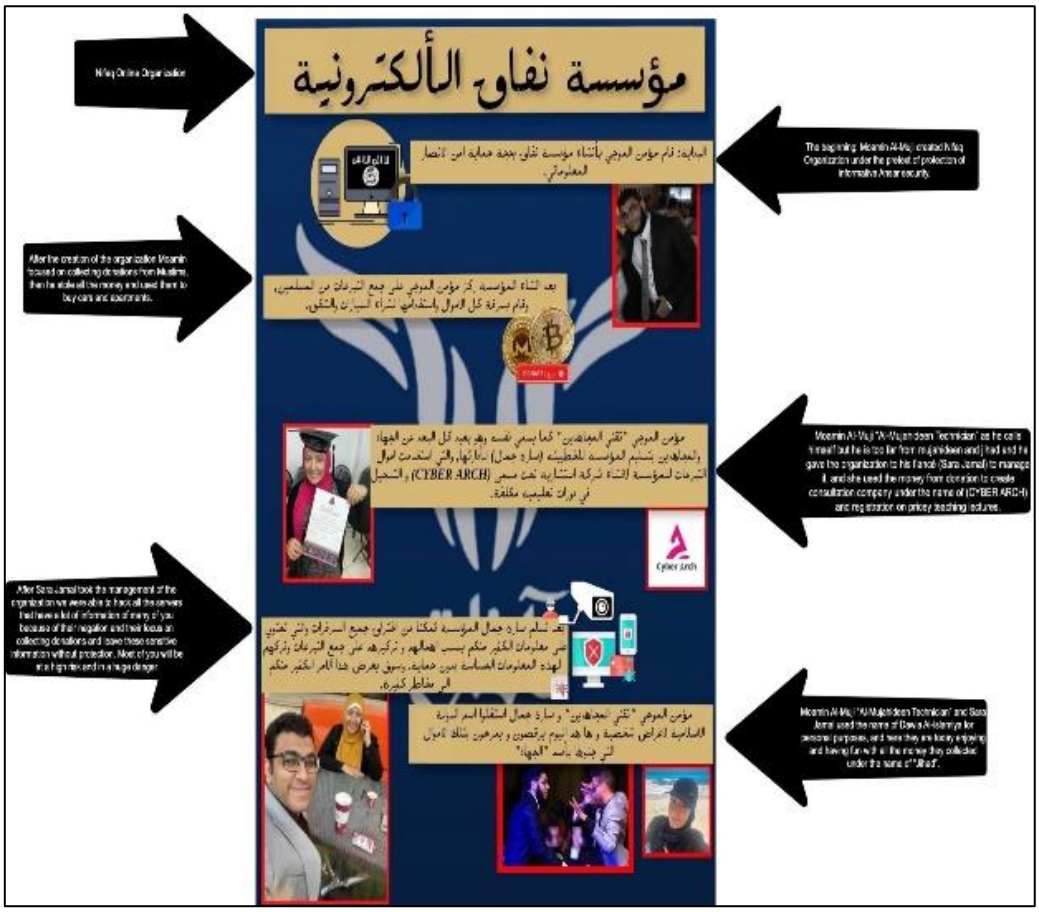
The new server on Element correlated with Afaq continuous encouragement to use Element App. A key example is the publication of the advantages and disadvantages of other apps compared to Element. Among those apps are Telegram, Signal, and WhatsApp. They also provided instructions on how to register to Element on an iPhone, iPad or a computer.

Afaq publication on various advantage and disadvantage of communication apps

According to ICT cyber desk, Afaq used multiple accounts on social media over the years as well as a website in order to publish cyber-defense materials. They also maintained ties with two other technical groups that supporters of the Islamic State: Bank al-Ansar, which focused on follower's use of social media and the Technical Support for the Electronic Afaq Institution.

The cyber-attack on Afaq and its implications

In the aftermath of the cyber-attack on Islamic State's Element chat server, the unknown hacker published Afaq's mangers' personal information, describing the foundation as a scam. According to the publication, **Afaq operators have been soliciting donations from Islamic State's supporters for years and using the money to their own benefits (such as to purchase cars and real estate and opening their own cyber security company). The information was distributed in a poster and published on Islamic State Rocketchat and other online platforms.**



Poster on Afaq mangers' real identity that was distributed on IS media platforms

The attack on Afaq caused a direct decrease in confidence among supporters who relied on the foundation for guidance. *"In truth the ikhwan need clarity. Horizons* (i.e., Afaq) *has completely disappeared, and the brothers need guidance".*[1]

It also carried more weight due to Afaq' active role in the **cyber warfare** that groups waged against the Islamic State. Such example was highlighted after the peak of cyber-attacks against Islamic State platforms during May 2021. In August that year, Electronic Horizons Foundation (Afaq) published an article titled "**Security Threats: Website Hacking and the Way to Confront".** The article explains the threat of hacking and why infiltration occurs, highlighting for supporters that "*We are in a media war, and the security threats will not stop, but your security awareness is the way to confront";* **Islamic State supporters also believed that Afaq played a key role in protecting the organization in the above cyber war as one follower described** "*Afaq had become a thorn in the enemy's path because the supporters were becoming rightly security conscious and by following their in depth step by step guide for the Munasir (Islamic State supporters), the Munasirin were protecting themselves against the enemy in the Cyber War".*[2]

At this point it is not clear if Afaq will continue operating. In their first statement released shortly after the attack, they claimed that the information released was fake. *"Some mercenaries are trying to hack the accounts of Afaq Foundation on the Element platform; They spread lies and false and misleading statements aimed at discrediting the institution."* De facto however, as a result of the attack, the foundation

[1] Supporter of the Islamic state on Rocketchat platform.
[2] Supporter post on IS Rocketchat

shut down its website and stopped publishing content on its media platforms. Most recently, Afaq also **published a poster claiming that all of the above are rumors and that they would continue to operate**.

Yet, further research conducted by one of Islamic State's supporters seemed to have provided evidence of Afaq's fraud. *"Brothers, I tried to research to see if the allegations made were true, and I found a company called Cyber Arch (the company which allegedly was open with money donating to IS) that deleted its Twitter account shortly after publishing the article about prospects, so why would this company do this if it was not true? The graphics and flyers they put up were also very similar to those of Afaq".*

Left: notification on Afaq's website that all are rumors; Right: IS supporter providing more information on the company that was allegedly with IS money

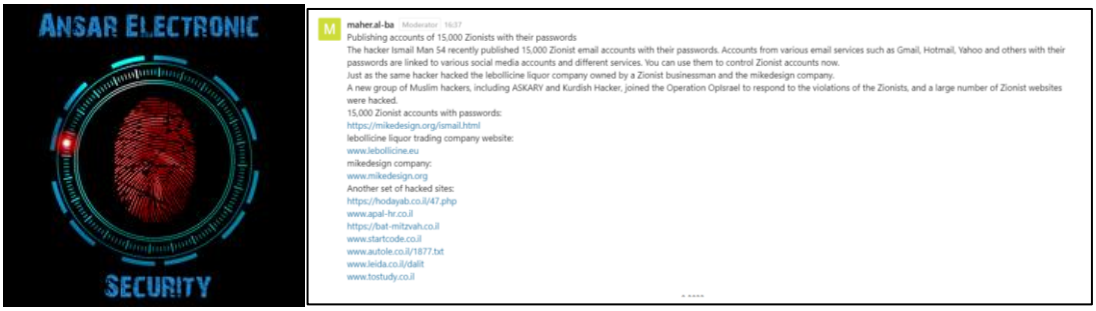
In recent months, Afaq's website ceased to operate, and they have been reluctant to publish any cyber security content. According to a user on Rocketchat *Techeaven*, Islamic State largest chat server, any accounts who publish under the Afaq name are fake and have malicious intent.

The Day after Afaq

The absence of Afaq since the March attack has enabled other foundations to become more prominent. Such is the case of al-Qiam Electronic Foundation (Qef), a lesser-known cyber unit which supports the Islamic state. Al-Qiam resumed operations only a few months ago after a long break. Their main publications at this point focus on short articles that provide tips for online use, cyber security and general trends in the cyber world. They have only recently begun publishing lessons on how to program and code websites. However, it's yet **unclear if they possess the same capabilities as Afaq, mainly in programing and providing Islamic State followers with closed secure platforms.**

Banner of al-Qiam electronic foundation article

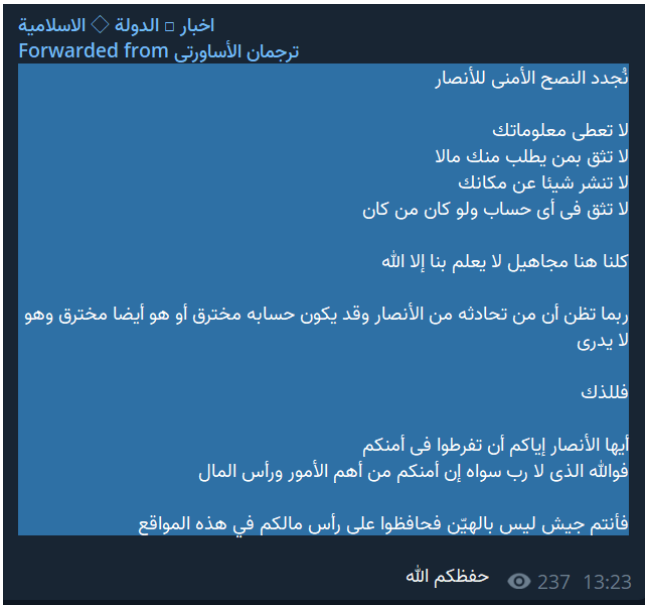
Other actors on Islamic State online platforms are taking the initiative to share cyber security tips, tracking innovation and events of cyber-attacks. **Among the prominent chat rooms are "Ansar electronic Security" and " Security Awareness".** In these chat rooms supporters discuss tips on how to remain safe in cyber space. In some cases, they are also given updates on recent trends in the cyber world including information on hacks, links to hacking tutorials and more.



Left: Ansar Electronic Security chat room on Rocketchat; Right: an example of a publication on Security awareness chat room.

The trust crisis among IS supporters

In the broader context, the reaction to the cyber-attack on Afaq might only be a symptom of a trust crisis within the IS supporters' community. The understanding that money contributed to the organizational efforts was de facto used for personal benefit only increased the mistrust online supporters have in donating via cryptocurrency to supporter's media institution. Apart from donated money, the trust crisis is also visible on chat platforms whose traffic used to mostly be chatter. The latter has been declining and been replaced with propaganda. The above correlates with instructions given to supporters that includes: *"Do not give out your information, don't trust someone who asks you for money, don't post anything about your location. Do not trust any account, even whoever it is .Perhaps you think that whoever you are talking to is from the Ansar, and his account may be hacked, or he is also hacked, and he does not know."*



Warning issued to IS online supporters

There are also voices within the Islamic State supporters' community that call upon followers to be patient and wait until more information will be released, hoping that the cyber-attack and published information is only psychological warfare against the organization. *"It's a pure preplanned and organized cyber-attack on Afaq/Horizons. Trying to make the story believable and making disputes and breaking the trusts of the supporters".*

Only time will tell how or if Afaq will reconnect with Islamic State supporters. At this point, the only known fact is that other initiatives are attempting to enter the vacuum created in the past few months.