

Cyber Terrorism and Radical Islamist Organizations

An Operational Outlook on Terrorist Cyber Operations

By Jeremy Makowski
Cyber Crime and Terrorism Intelligence Expert

November 2022

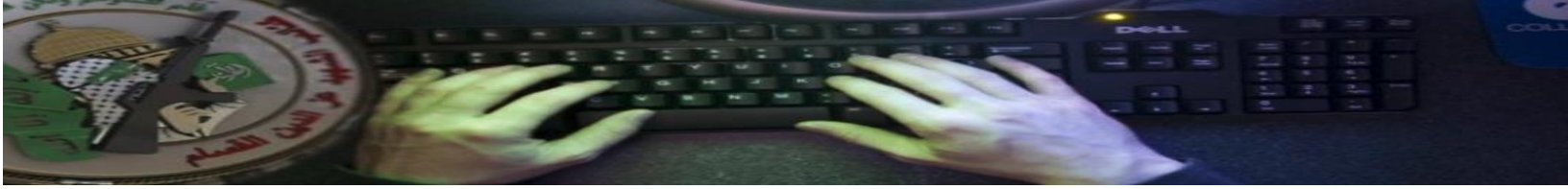


Table of Contents

1. Introduction 3

2. Cyber Terrorism and Radical Islamist Organizations 4

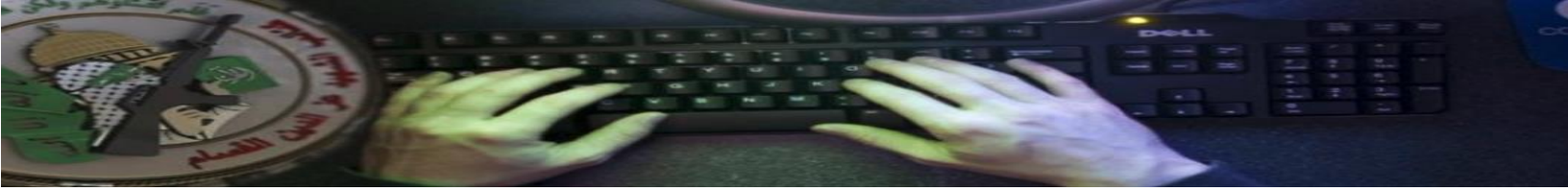
3. Use of Cyberspace by Radical Islamist Organizations 5
   - 3.1. Social Networks 5
   - 3.2. Encrypted Messaging Applications 8
   - 3.3. Darknet 11

4. Cyber Capabilities of Radical Islamist Organizations 12
   - 4.1. Hamas 12
   - 4.2. Hezbollah 19
   - 4.3. Islamic State 21
   - 4.4. Al-Qaeda 26

5. Conclusion 29

6. About The Author 30

7. References 31



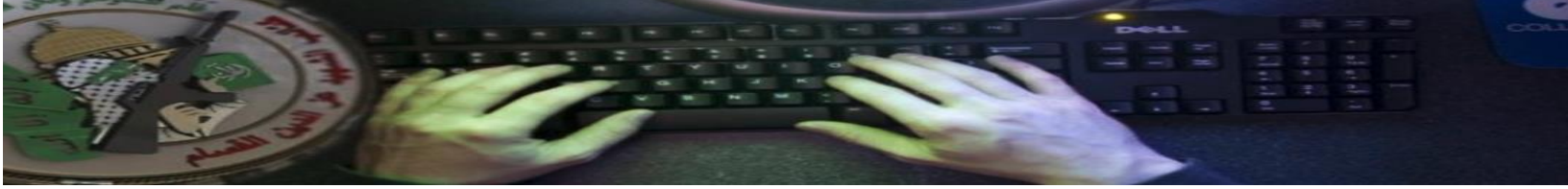
1. Introduction

Cyberterrorism can be defined as the use of technology and computer means to terrorize a civilian population, influence government policy, or target critical state infrastructure for religious or ideological purposes. The nation of cyberterrorism began being talked about in the 1990s, then emerged in the 2000s and really started to have a significant impact in the 2010s.
Cyberterrorism is a phenomenon that must be differentiated from hacktivism and cyberwarfare. Like other cyber threats, cyber terrorism has gained prominence due to the increasing expansion of cyberspace and technological development. Terrorist organizations play on the growing dependence of states on computer systems and communication networks to manage their critical infrastructures. They, therefore, adapt their modus operandi by using new technologies and personalized tools to carry out their subversive activities. For some, cyberterrorism is seen as an extension of traditional terrorism; for others, it is a phenomenon.

For many terrorist organizations, cyberterrorism is an attractive option for various reasons. First, operating in cyberspace is relatively cheaper than working in the real world. Although this is a general statement since we have observed isolated terrorists claiming to be supporters of the Islamic State and committing physical terrorist attacks with minimal financial means. On the other hand, carrying out an attack that would significantly affect a state requires substantial funds. Cyberterrorism also offers the possibility of operating remotely and more anonymously than traditional terrorist methods, notably through encryption systems and false identities. Finally, cyberterrorism makes it possible to reach a tremendously larger number of targets, such as national critical infrastructures, government facilities, administrations, public services, and also private companies. Today, terrorist organizations use cyberspace for the following purposes:

- Propaganda
- Psychological Warfare
- Recruitment
- Training
- Fundraising
- Information Collection
- Secured Communications
- Cyberattacks (DDoS, Malware, Defacement, Data Leak)



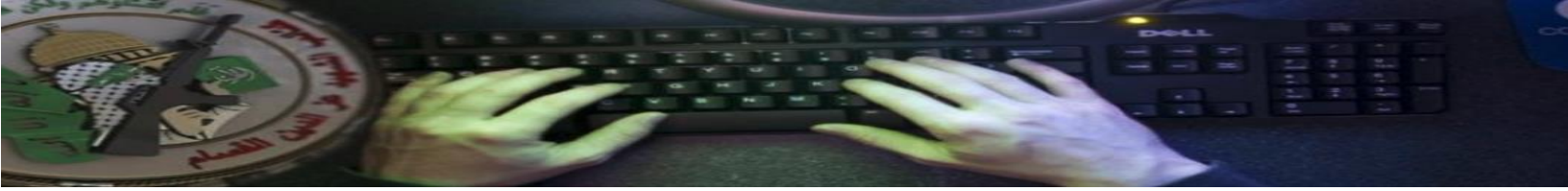


Unlike criminal organizations that exploit cyberspace for financial gains, terrorist organizations abuse it primarily to harm states and propagate their extreme religious, political, or ideological vision. However, like criminal organizations, they quickly realized the potential of cyberspace and its tools. Thus, for more than ten years already, many terrorist organizations have created cyber units within their organizational structure by training their members in new technologies or by recruiting professional hackers.

2. Cyber Terrorism and Radical Islamist Organizations

The development of the Internet and social networks enabled activists with technical skills to launch cybercampaigns for religious or political purposes. This phenomenon began with the emergence of the most well-known hacktivist movement, Anonymous, and then inspired other groups, especially those supporting religious causes (particularly Muslims). As it evolved, cyberspace became an essential source of information for many Muslims worldwide despite many things Islam can define as “unethical.” The use of cyberspace, particularly social networks in the Islamic world, became a real frenzy during the Arab Spring in 2011. Social networks significantly impacted the political events that followed, allowing revolutionaries to exchange, communicate, be informed, and communicate to the world the evolution of the "revolutions" in progress. Social networks have thus become a weapon symbolizing a new form of freedom guiding people.

But the Arab Spring has also led to civil wars and sometimes to radicalization. Many terrorist organizations have been able to take advantage of the development of cyberspace and its means to expand, diversify and connect with their target. Cyber jihad is the continuation of traditional jihad in the virtual world. Some organizations, like the Islamic State (ISIS), have weaponized it as a communication weapon by using cyber jihad to promote themselves and expand their reach. The development of these cyber capabilities has depended on several factors, including the organization's willingness to develop this area of expertise, its ability to train and recruit hackers, and its financial capacity. According to the 2022 ranking established by Forbes magazine, the five richest terrorist organizations are the Taliban, Ansar Allah, Hezbollah, Al-Qaeda, and Hamas (Figure 1). Due to their financial resources, these groups also have the largest potential to expand their cyber capabilities.





Rating	Organization	Annual Revenues (Estimated $US Millions)	Areas of activity	Primary sources of income
1	Taliban	2,500	Afghanistan and Pakistan	Taxes and fees, drug trafficking and mining
2	Ansar Allah (The Houthi Rebels)	2,000	Yemen	Taxes from companies and corporations, illegal oil trade
3	Hezbollah	1,200	Lebanon and Syria	Aid funds from Iran, drug trafficking
4	Al Qaeda and its affiliates	600	Global	Taxes, illegal trade (drug, arms & human trafficking)
5	Hamas	500	Gaza Strip and the West Bank	Taxes and fees, Aid funds from Iran
6	Kurdistan Workers' Party (PKK)	250	Turkey, Iraq and Syria	Illegal trade (drug, arms & human trafficking)
7	ISIS and its affiliates	150	Global	Taxes, kidnapping and ransom illegal trade (oil & Antiquities trafficking)
8	Real IRA	70	UK and Ireland	Illegal tobacco trade
9	Kata'ib Hizballah	50	Iraq and Syria	Aid funds from Iran
10	Palestinian Islamic Jihad	35	Gaza Strip and the West Bank	Aid funds from Iran

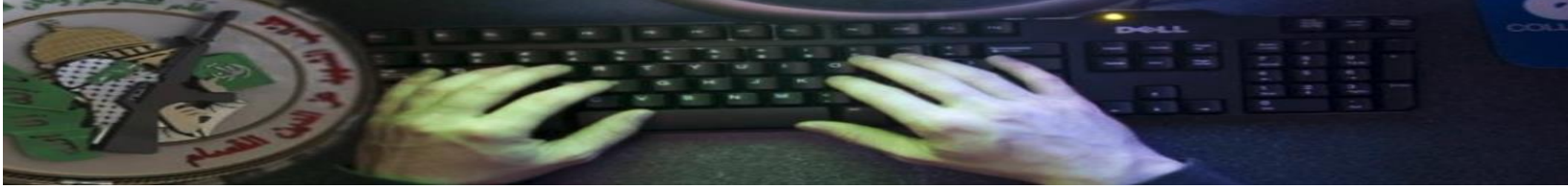
Figure 1 – 2022 Forbes ranking of the richest terrorist organizations (Source: Forbes)

3. Use of Cyberspace by Radical Islamist Organizations

Terrorist organizations have figured out how to better exploit the different layers of cyberspace to carry out their recruitment, propaganda, and intelligence-gathering activities. Broadly speaking, the use of cyberspace by terrorist groups can be divided into three categories social networks, encrypted messaging applications, and the darknet.

3.1. Social Networks

Social networks are the platforms with the highest number of active users worldwide. They are hosted on servers connected to the Internet and are accessible with traditional search engines. Over the past ten years, social networks have widely multiplied, and today, beyond Facebook and Twitter, there is an abundance of social networks specific to fields of activity and in many languages. For terrorist organizations, social networks provide a powerful means of expression and communication, allowing them to carry out propaganda operations and claim their responsibility for terrorist attacks (Figure 2).



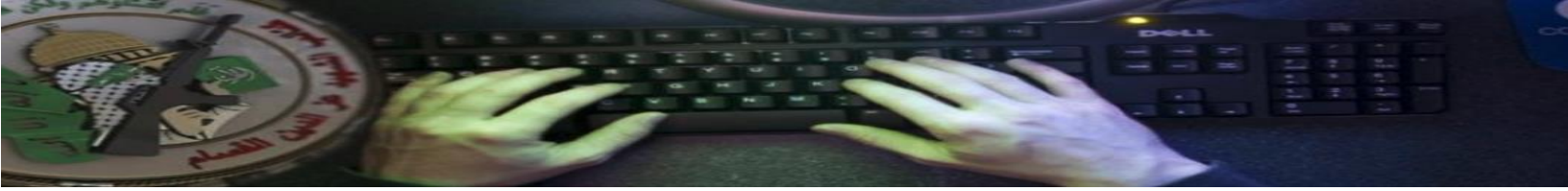
In large parts of Middle East countries, the most popular and widely used social networks are Facebook, WhatsApp, and Instagram. Many Islamist terrorist organizations maintain social pages on these platforms, which enable them to reach as many people as possible. They usually create public or private groups to share information about their ideology and communicate their actions. The use of social networks by terrorist groups has become commonplace for several years now, with some organizations having community managers to manage them daily. (Figures 3, 4).



Figure 2 - An Instagram post by Hamas' military wing claiming responsibility for an attack against Israel



Figure 3 – The Facebook page of the Jerusalem Electronic Army



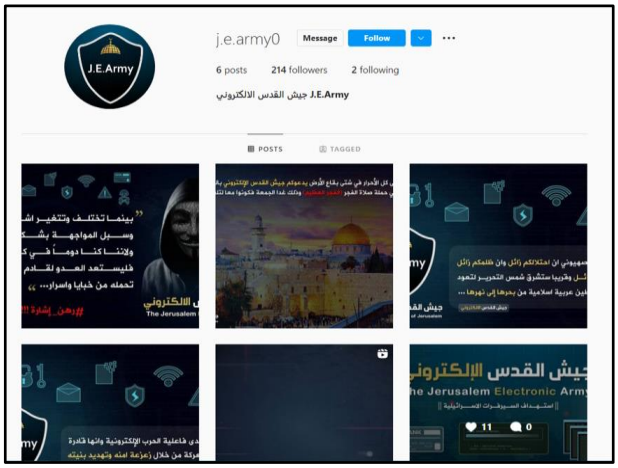


Figure 4 - The Instagram page of the Jerusalem Electronic Army

Social networks are a virtual playground for terrorist organizations. Some of them, like Hamas, regularly exploit Facebook to launch cyberattacks against Israeli soldiers. One of their primary modus operandi for gathering intelligence on military operations is to create fake social network profiles of attractive young women (Figure 5) and send private messages to Israeli soldiers. Once the dialogue is established and they have gained the soldiers' trust, the terrorists convince them to click on a link that infects their victims' smartphones with a Trojan to gather information on geolocation, SMS, email messages, and phone conversations. This is one of many examples of the relatively easy effort to exploit the human factor to implement a cyber intelligence strategy while relying on the naivety of the targets.

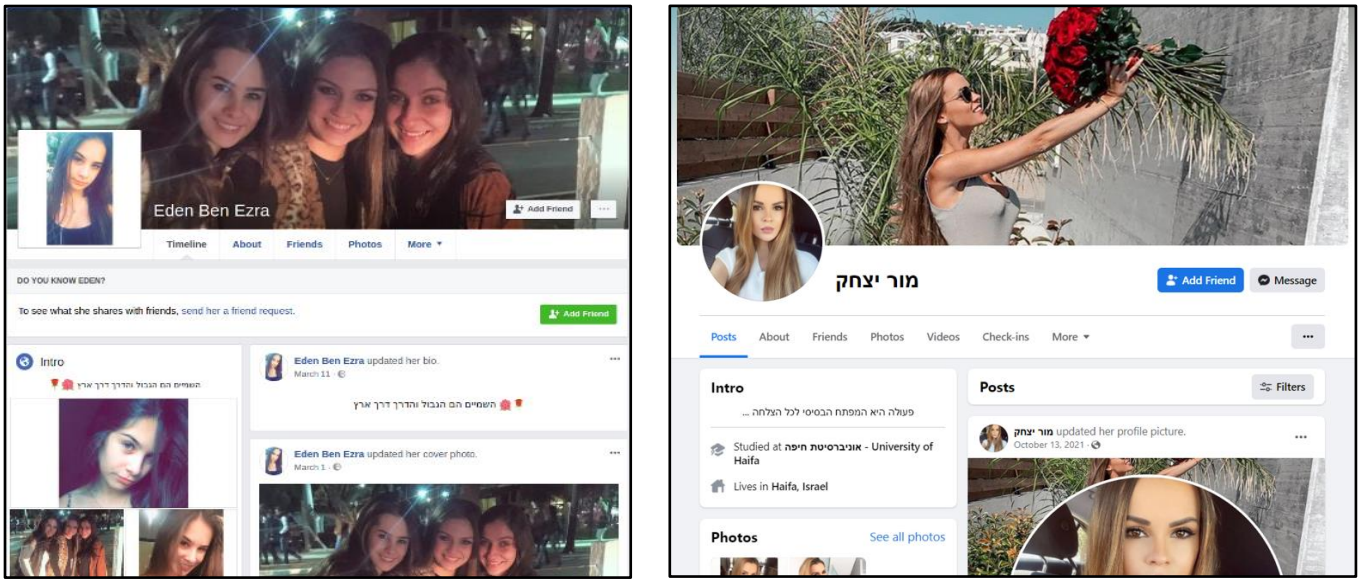
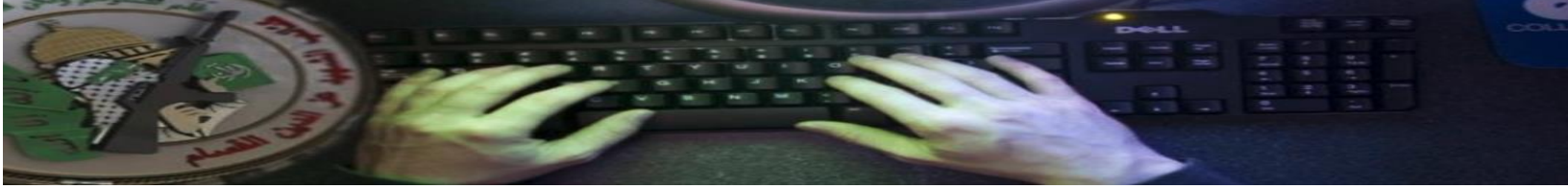


Figure 5 - Hamas' fake Facebook profiles created for luring Israeli soldiers



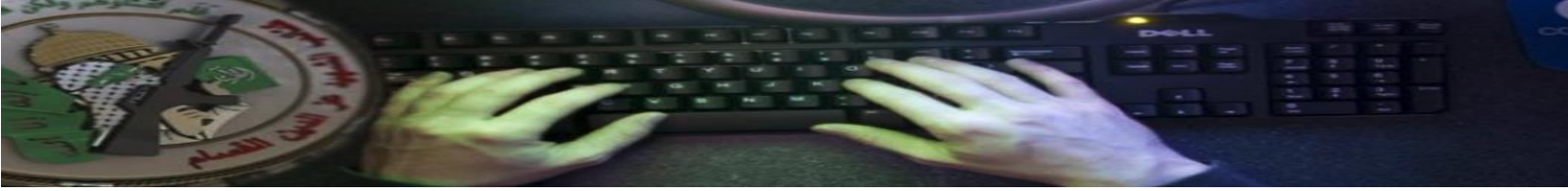
3.2. Encrypted Messaging Applications

With the proliferation of data collection operations by governments and some private companies, operational security became one of the top priorities of terrorist organizations to avoid intelligence surveillance. Over the years, encryption systems have been increasingly used in different appliances, such as smartphones, computers, or hard drives, and in instant messaging apps (Figure 6). However, as encryption technology helps protect so-called sensitive and classified data, it is also a formidable weapon in the hands of terrorists, who have used it to secure their communications and shared information. In addition, the emergence of several end-to-end encrypted messaging apps, publicly available on the iTunes Store and Google Play, has provided terrorist organizations with a stealthy method to recruit people and plan their operations. From Al-Qaeda to ISIS, Hamas, or Hezbollah, all use encrypted messaging apps.



Figure 6 – Logos of the most popular encrypted messaging applications used by terrorist organizations

WhatsApp was one of the first encrypted instant messengers used by terrorist organizations and opened the door to other more secure applications. However, WhatsApp exposes the phone numbers of people using the application and thus does not provide complete anonymity (Figure 7).



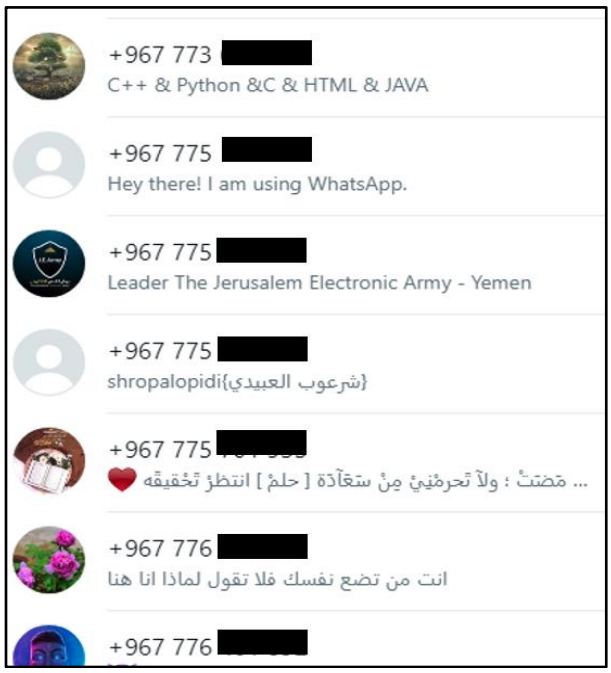


Figure 7 - A WhatsApp group of the Jerusalem Electronic Army

Today, many other applications are more secure than WhatsApp, such as Telegram. Since its development, the application has been used by many users worldwide, including members and supporters of terrorist organizations like Hezbollah (Figure 8). One of the particularities of Telegram which has attracted these groups is end-to-end encryption and Phone number anonymity. Terrorist groups using Telegram generally use a phone number linked to a prepaid SIM card purchased in a country where the request for identification is not mandatory.

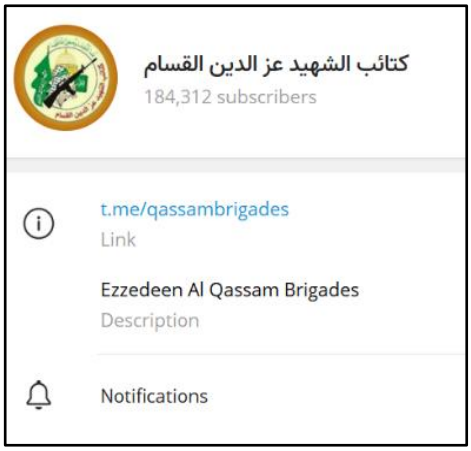
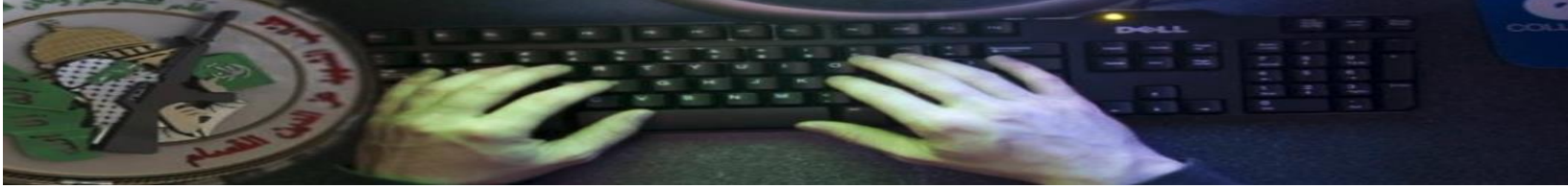


Figure 8 - The Ezzedeen Al Qassam Brigades' Telegram Channel



However, Telegram is not the only encrypted instant messaging application used by these groups. In 2018-2019, the Islamic State and Al-Qaeda started using the RocketChat application (Figure 9). Moreover, according to an investigation by the Indian National Investigation Agency (NIA), terrorist organizations in India and abroad use the application Threema to communicate with their counterparts worldwide without being traced. In Pakistan, terrorists appear to be using another application developed by a Turkish company to communicate among themselves and with potential recruits in the Kashmir Valley.

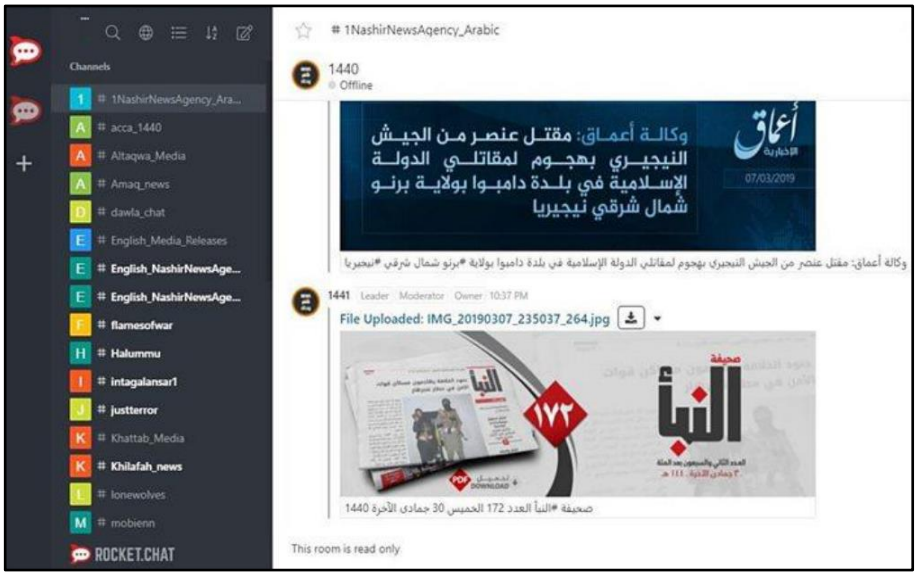
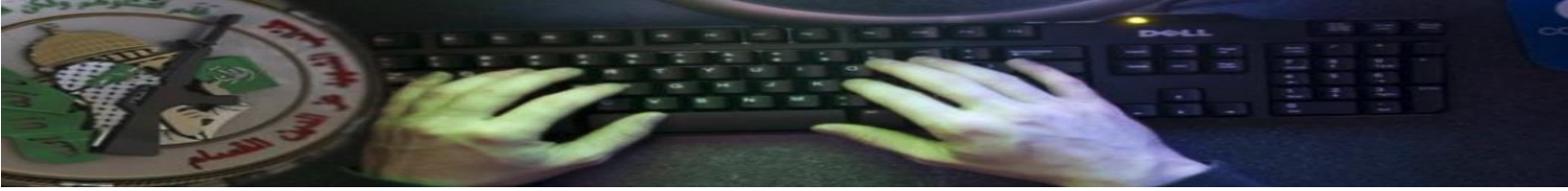


Figure 9 - The Nashir News Agency broadcasting Islamic State propaganda on RocketChat

In 2021, the Islamic State affiliate group, Electronic Horizon Foundation, AKA Afaq, published a table comparing different encrypted messaging applications features (Figure 10).



Figure 10 - Afaq table comparing different encrypted messaging applications features



3.3. Darknet

The Darknet, and especially The Onion Router network (TOR), has for several years been an excellent tool for terrorists to communicate and broadcast their ideology in a secure way. The network's architecture and the robustness of its mixed symmetric and asymmetric cryptography system make it a powerful means of protection and anonymity. The Islamic State uses the Darknet primarily to deliver the organization's official announcements and religious content, relying on the secure hosting provided by the TOR network. The exploitation of the darknet by jihadists is generally seen as a primary means of disseminating propaganda, even though this propaganda has been shared more widely through social media and encrypted messaging applications (Figures 11, 12).

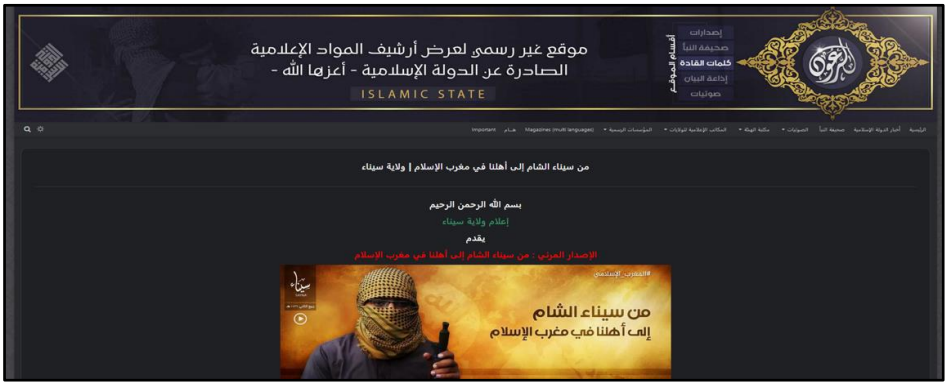
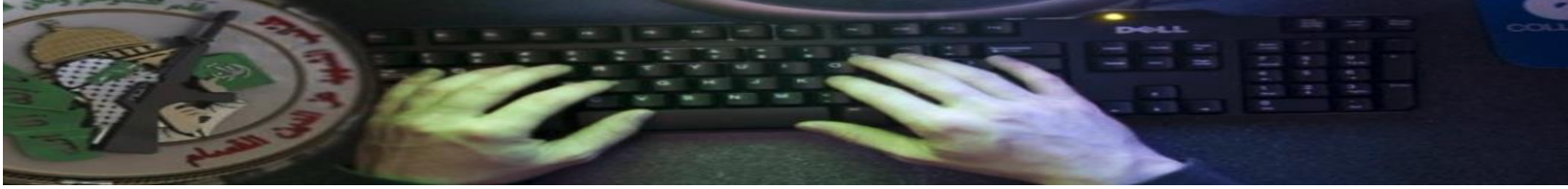


Figure 11 - A hosted TOR website broadcasting ISIS announcements and ideology (Source: dark web)



Figure 12 - A hosted TOR website broadcasting ISIS announcements and ideology (Source: dark web)



4. Cyber Capabilities of Radical Islamist Organizations

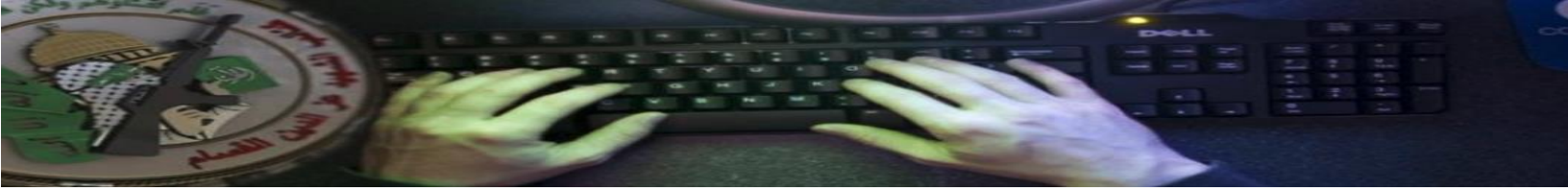
With the emergence of new technologies, terrorist groups have adapted and succeeded in developing their cyber capabilities, especially offensive ones. Islamist groups, such as Hamas or the Islamic State, managed to conduct cyber operations and created cyber branches within their organizations. From a cyber point of view, terrorist operations can be divided into three categories: defensive, operational, and intelligence.

- **Defensive**: refers to operational security measures, including communication and hosting encryption and information security advice given to supporters and affiliates.
- **Operational**: refers to online operations, including propaganda, recruitment, and attack planification.
- **Intelligence**: refers to information collection activities performed using malicious tools.

4.1. Hamas

For over a decade, Hamas has engaged in offensive cyber operations against Israel, sometimes the United States, and specific Palestinian targets. Their cyber operations are mainly focused on espionage and information. Hamas uses its intelligence branch to provide its leaders with information to make strategic decisions in the political and military fields. The intelligence branch of Hamas comprises members of the al-Majd security force belonging to the larger Izz al-Din al-Qassam Brigades, which is the military wing of Hamas.

Cyber espionage campaigns operated by Hamas increased over the past decade with some evolution in the modus operandi which became more sophisticated over time. In 2013, the tactic used by the organization focused on a broad approach by sending general emails with malicious attachments to many targets in the hope that some of them fall into the trap. Later, Hamas changed its attack mode by using links to infect its targets. On the other hand, social engineering is also a technique used by Hamas to target Israeli soldiers through Facebook to infect their smartphones with malware. While most of Hamas's cyber operations focus on intelligence gathering, another part is aimed at hacking data, exposing it, and using it for psychological manipulation. The organization claims several hacks, including Cellcom,
Egged. and IAI. In addition, DDoS-type attacks for nuisance and Defacement for propaganda are also part of the cyber operations carried out by Hamas.



- In 2012, Hamas claimed responsibility for a cyberattack on the Israeli army's website, including that of the IDF Spokesman's Homefront Command.

- In 2013, Palestinian hackers claiming to be from the Hamas' armed wing Izz ad-Din al-Qassam launched a distributed denial-of-service (DDOS) cyberattack against the website of American Express.

- In 2014, Hamas claimed responsibility for hacking into the classified IDF network and released several videos taken earlier in the year of Israel's Operation Protective Edge in the Gaza Strip.

- In 2018, Hamas launched a cyber operation using fake Facebook profiles of attractive women to contact Israeli soldiers and take control of their computers and smartphones. They also exploited WhatsApp by impersonating Israeli soldiers and sending messages to army personnel to gain access to confidential information. According to the threat intelligence company ClearSky, Hamas members attempted to infect the smartphones of Israeli citizens with malware by using an application that imitated the "Red Alert" application, which provides real-time alerts of missile launches at Israel. According to Clearsky, Hamas planted a download link for the malicious app in fake Facebook and Twitter profiles. Once downloaded, the malicious program enables full access to the mobile device for monitoring purposes.

- In 2019, the Israeli army bombed one of Hamas' buildings, serving as its cyber base (Figure 13). While this attack partly affected the organization's cyber capabilities, Hamas has not stopped its cyber operations.

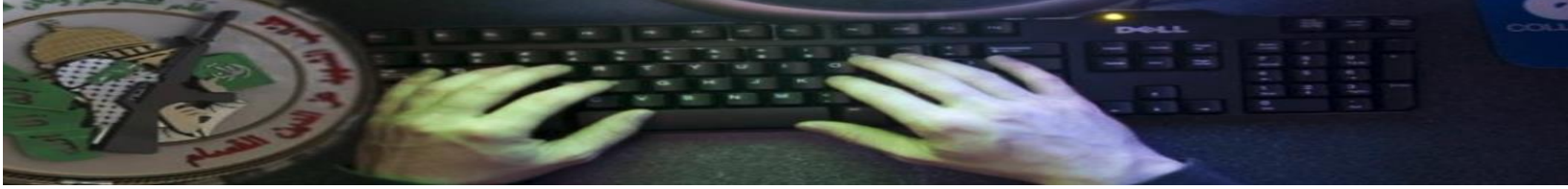


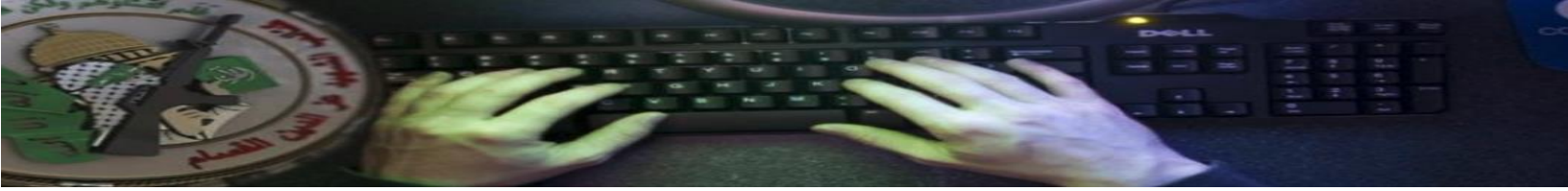


Figure 13 - One of the Hamas' cyber command buildings destroyed by the IDF in 2019

- In 2020, Hackers affiliated with Hamas exploited Facebook, Dropbox, and Google Drive to spread spyware that aimed to target Arab leaders and states, using lures mentioning Israeli Prime Minister Benjamin Netanyahu and the Saudi Arabian Crown Prince, Mohammed bin Salman (MBS).

- In 2021, the Hamas-affiliated group Molerats claimed to be a part of the Gaza Hackers Team and took part in cyberattacks using malware and targeting Middle Eastern entities, including governments, think tanks on foreign policy, and a state-affiliated airline.

- In 2022, according to research performed by the cybersecurity firm Cybereason, a Hamas-linked attack group, APT-C-23 (AKA Arid Viper, Desert Falcons), was involved in a sophisticated intelligence-gathering campaign targeting senior Israeli officials. Beyond social engineering using fake Facebook accounts, the group managed to introduce new malware, including a fake messaging app known as VolatileVenom, a downloader known as Barbie Downloader, and theBarbWire Backdoor (Figure 14).



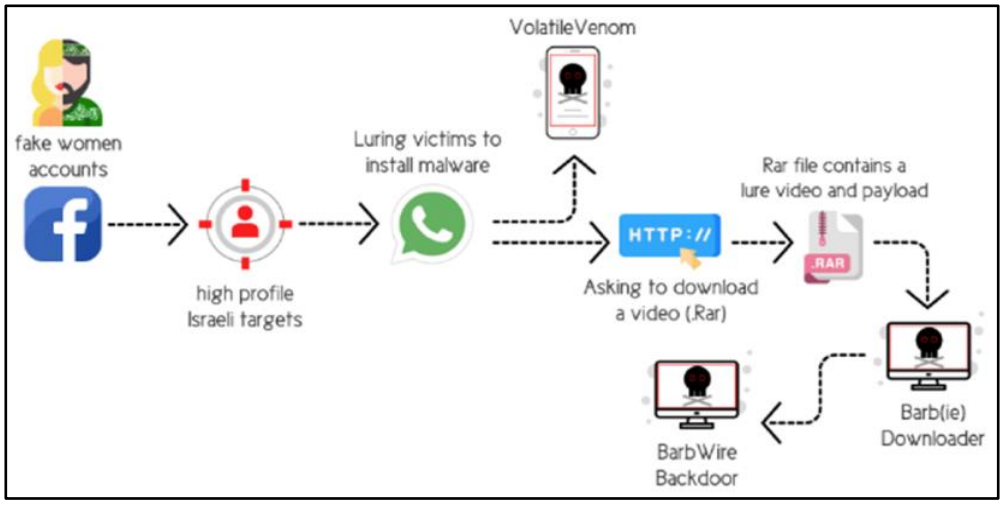


Figure 14 - Hamas Volatile Venom malware infection method (Source: Cybereason)

- In 2022, Hamas officially revealed in a video that it had been operating a cyber unit for eight years with multiple cyberattacks against Israel (Figure 15, 16). Hamas claimed the team was established in October 2014 by Juma al-Tahla, the former head of Hamas' cyber command, whom the IDF had killed during the 2021 Gaza conflict.



Figure 15 - A Hamas cyber fighter from their official Video

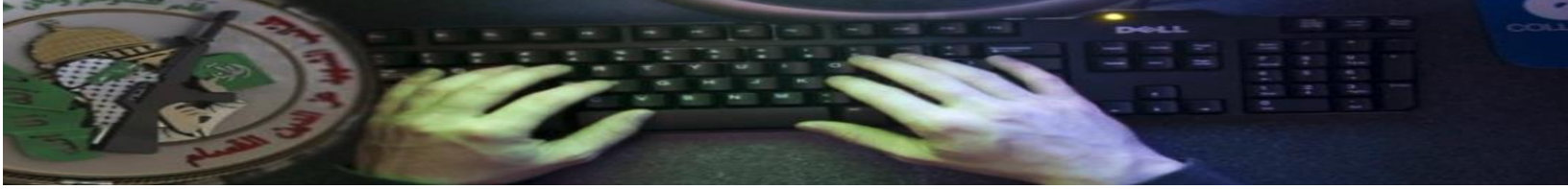




Figure 16 - Hamas' alleged cyber operations list

Apart from its cyber fighters, the organization can also rely on affiliates such as the Jerusalem Electronic Army, which has also launched offensive cyber operations, particularly against Israel, as well as Gaza Hacker Team or Gaza Cybergang, which often targets Israel (Figure 17, 18).

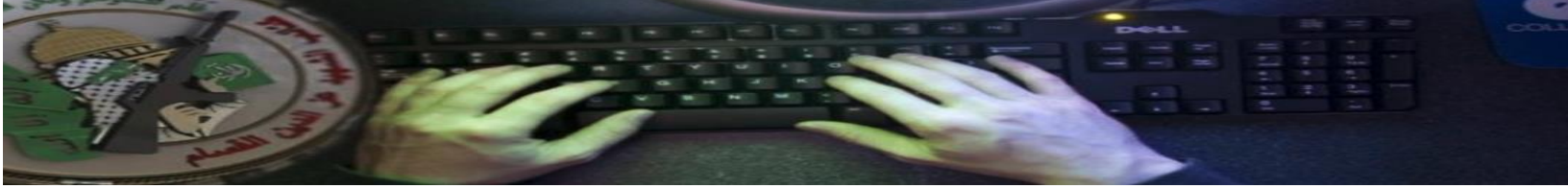


Figure 17 - Hackers from the Jerusalem Electronic Army (Source: Telegram)



Figure 18 - Facebook page of the Gaza Hacker Team

Decades ago, terrorist financing relied on traditional methods until terrorist groups began to use cryptocurrencies to send and receive funds anonymously and securely. Hamas and its affiliates have practiced using cryptocurrencies for some time with a Bitcoin fundraising campaign on their website. They allow their supporters to donate anonymously and securely via a unique Bitcoin address automatically generated for each donor. Once received, funds are often transferred from wallet to wallet to hide the source and path of payment. The funds are then withdrawn using mediators with money (money mules). For those who prefer to make a more traditional donation, Hamas also provides an email address to contact someone for a gift. (Figures 19, 20). For a few years, Bitcoin transactions have been traceable thanks to Blockchain analysis OSINT collection systems such as Chainalysis or Elliptic. Some terrorist organizations have understood this and have decided to change tactics. In 2021 a particular change has taken place in the use of cryptocurrencies with greater interest on the part of terrorists in the cryptocurrency Monero, which is not at all traceable to the detriment of Bitcoin, even if the latter is still well used.



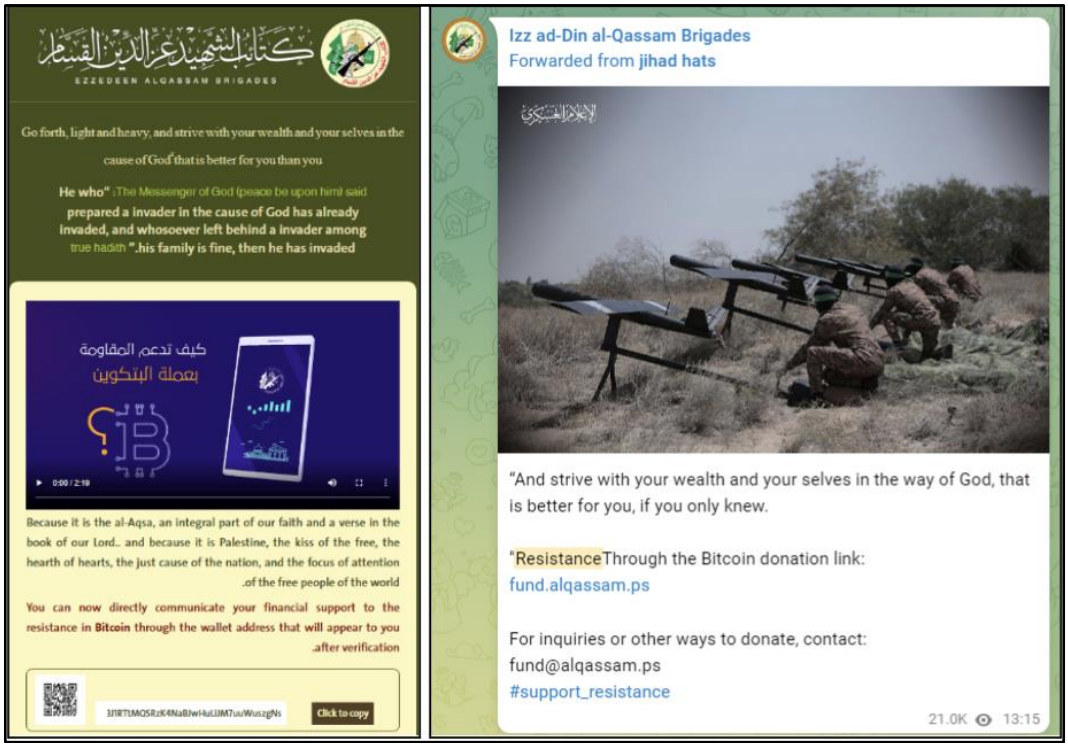
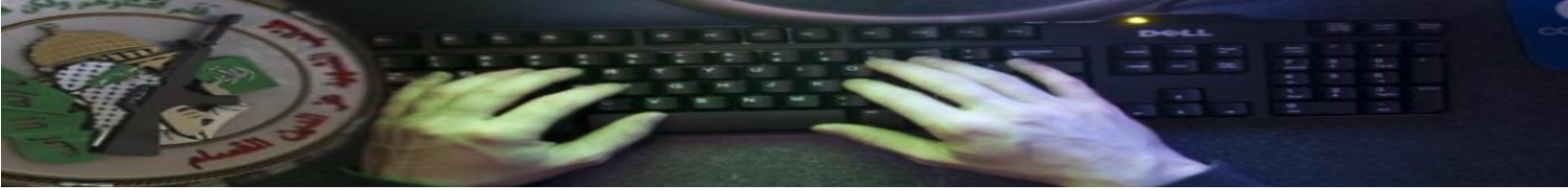


Figure 19 - Messages on the Hamas website and Telegram for people who want to financially support them by sending Bitcoin or contacting them by email



Figure 20 - A post from the Jerusalem Electronic Amy on Telegram with a Bitcoin address for donations (Source: Telegram)



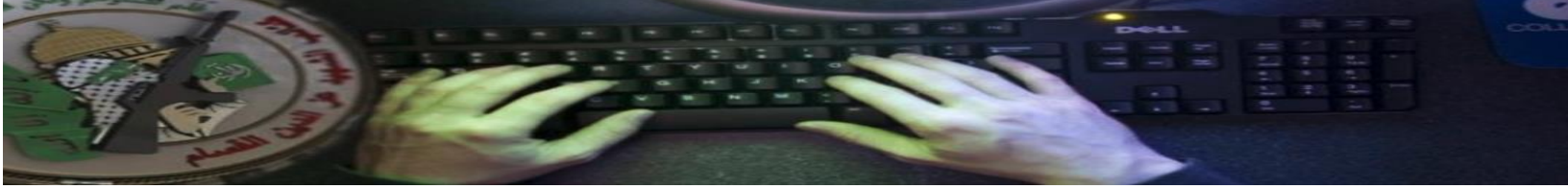
Hamas developed relatively good cyber capabilities over the past ten years. Despite poor electricity stability and modest infrastructures in the Gaza Strip and even though the terrorist organization is not equipped with significant technological power and sophisticated tools, it should not be underestimated. Their cyber operations can be classified as medium level because their impact is still low compared to an Advanced Persistent Threat (APT) group, which would have more financial and technical resources. Currently, the organization's cyber operations are insufficient to cause significant harm to state entities. However, the organization could embark on more complex cyber operations with external financial support. Indeed, Hamas maintains close relations with Turkey, Iran, and Qatar. Hamas will continue to develop cybernetic offensive capabilities, which, if supported financially and technologically by a third state, could have more significant consequences than at present.

4.2. Hezbollah

Since the Second Lebanon War in 2006, Hezbollah has developed cyber capabilities and has performed several cyber operations. Although the organization and its affiliates have been active in cyberspace since the 2000s, these cyber operations have intensified over the past five years. Hezbollah enjoys significant financial and technological support from Iran, which has allowed it to grow faster. Since the large-scale cyberattack against one of its nuclear power plants by the Stuxnet virus in 2010, the Iranian government has invested heavily in developing defensive but offensive cyber capabilities. Beyond elevating its cyber capabilities to the level of major developed nations, this investment has also enabled Iran to help Hezbollah develop its cyber cadre. At the same time, it allows Iran to increase its number of cyber fighters outside Iranian territory and expand its reach.



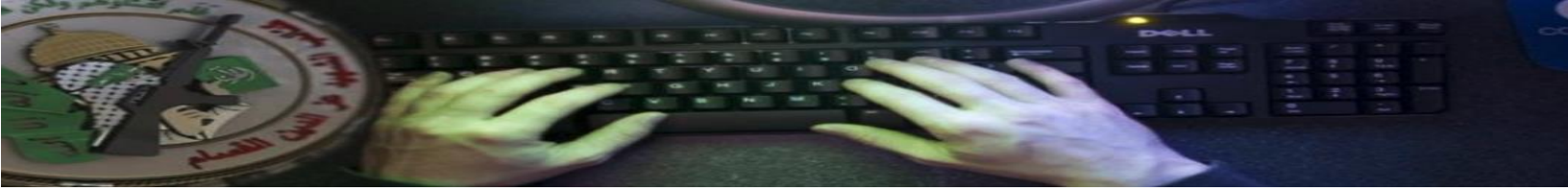
A few years ago, the Iranian Revolutionary Guard Corps' Quds Force set up a new cyber warfare unit for Hezbollah. This new cyber unit is based on the cooperation of members of Hezbollah and the Iranian intelligence services and includes seasoned hackers and other contractors specializing in various fields of cyber. The team was created to carry out cyberattacks and intelligence-gathering operations using different capabilities to target cell phones, intercept Wi-Fi signals, collect information on social networks, and infiltrate government networks. Apart from preeminent targets, such as Israel or the United States, this cyber unit attacks various targets, including Lebanese businesses and government organizations. These cyberattacks allow the organization to collect confidential information that Hezbollah uses to control Lebanese public opinion and track down its opponents.



The unit also targets various Arab and Western countries for the same reason. As mentioned earlier, Hezbollah has been involved in cyberattacks for over 20 years. The following events are their main feats of arms:

- In 2006, Hezbollah was implicated in cyberattacks against websites in several countries that supported Israel during the Second Lebanon War between Israel and Hezbollah. The group hijacked corporate communications portals, cable companies, and web hosting servers in the United States to spread propaganda.
- In 2013, during the war in Syria, Hezbollah developed a technique for securing communications by designing a system that would allow its fighters to use radios without fear of interception by external parties.
- In 2015, Hezbollah hackers, using the name Lebanese Cedar, carried out a cyber espionage campaign using malware to access public and private organizations associated with Israel's defense sector.
- In 2017, like Hamas, Hezbollah exploited social networks by creating fake profiles of attractive women to trick targets into clicking on links that downloaded malware.
- In 2020, according to a Daily Telegraph report, Hezbollah trained thousands of social media activists to help spread fake accounts, creating electronic armies across the Middle East.

According to a report issued by the cyber intelligence company CleakSky in 2021, since 2020, the Hezbollah-affiliated hacking group, Lebanese Cedar (AKAVolatile Cedar), has compromised approximately 250 servers in multiple countries for intelligence collection (Figure 21). According to the report, most of these companies belonged to the telecommunications sector in the following countries: Europe, Egypt, Israel, Jordan, the United Kingdom, and the United States.



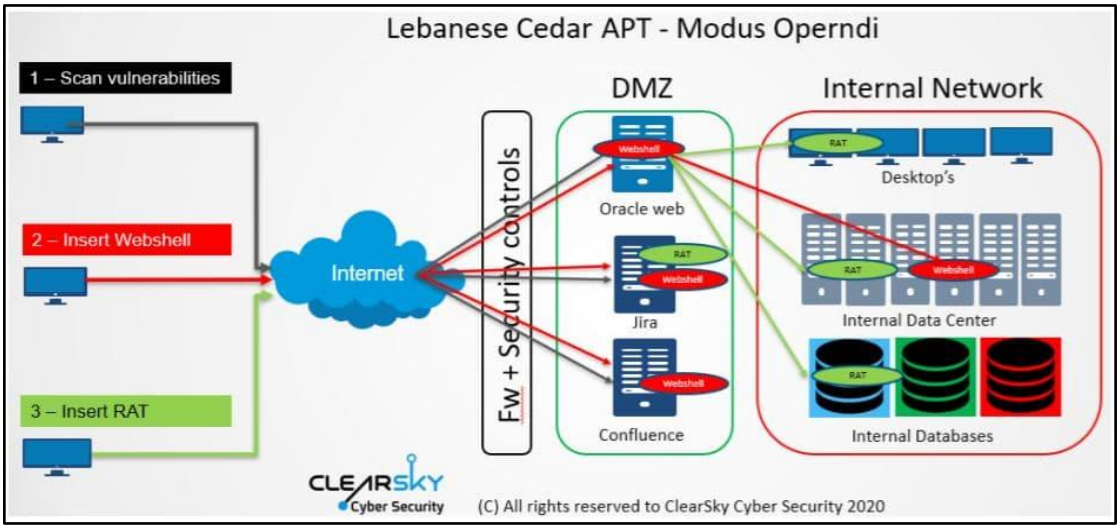
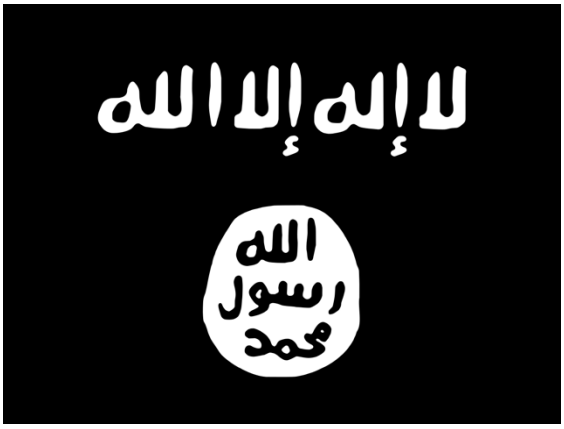


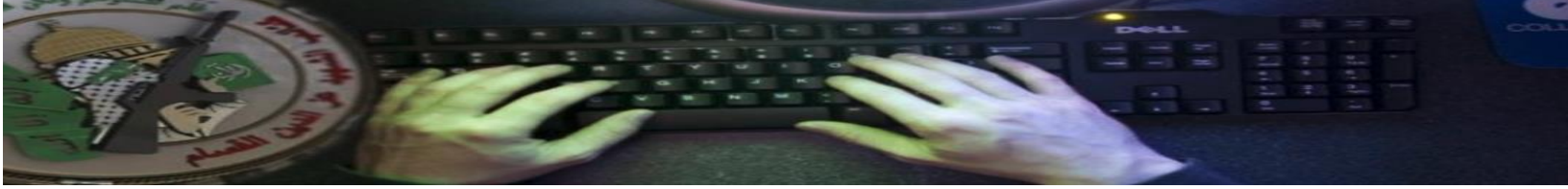
Figure 21 - Hezbollah Lebanese Cedar APT Modus Operandi (Source: ClearSky)

Hezbollah has relatively good capabilities and has conducted medium-level cyberattacks so far. However, the organization is primarily supported by Iran, which could lead it to carry out much more sophisticated and damaging cyber operations. Suppose Iran decides to initiate a full-scale cyberattack against a cooperative state through Hezbollah. In that case, it will provide the terrorist organization with significant technological and financial means to launch the operation, further increasing cyber security—the capacity of Hezbollah. State-backed terrorist groups like Hezbollah are much more likely to launch significant cyberattacks one day because their resources are far greater than other terrorist groups. Without Iranian help, Hezbollah would probably not have the same financial and technological resources.

4.3. Islamic State

The Islamic State (ISIS) terrorist organization was created in 1999 and has had a global impact since 2014. The organization only started to exploit cyberspace for operational purposes in 2015 with several cyber operations against American websites under the aegis of the Cyber Caliphate Army. Since 2015, several cyberattacks have been launched by the Islamic State hacking group Cyber Caliphate Army and other affiliates, such as Sons Caliphate Army and Kalashnikov TN. Among these attacks, the following were the most significant:





- In 2016, the Caliphate Cyber Army launched a cyberattack on Solar UK. The website was modified and displayed the ISIS logo with a message stating, “Fear us.” We are the Islamic Cyber Army.” The same year, the Islamic State hacked 20 Australian websites in a coordinated attack on Australian businesses.
- In 2017, the Islamic State released online a kill list of 8,786 people.
- In 2019, an Islamic State-affiliated hacking group hijacked 150 targeted Twitter handles using an unknown vulnerability.
- In February 2022, the Islamic State posted a guide called "Drone Survival Guide" on RocketChat, which provided technical information on different types of drones and tips for defending against them (Figures 22, 23)

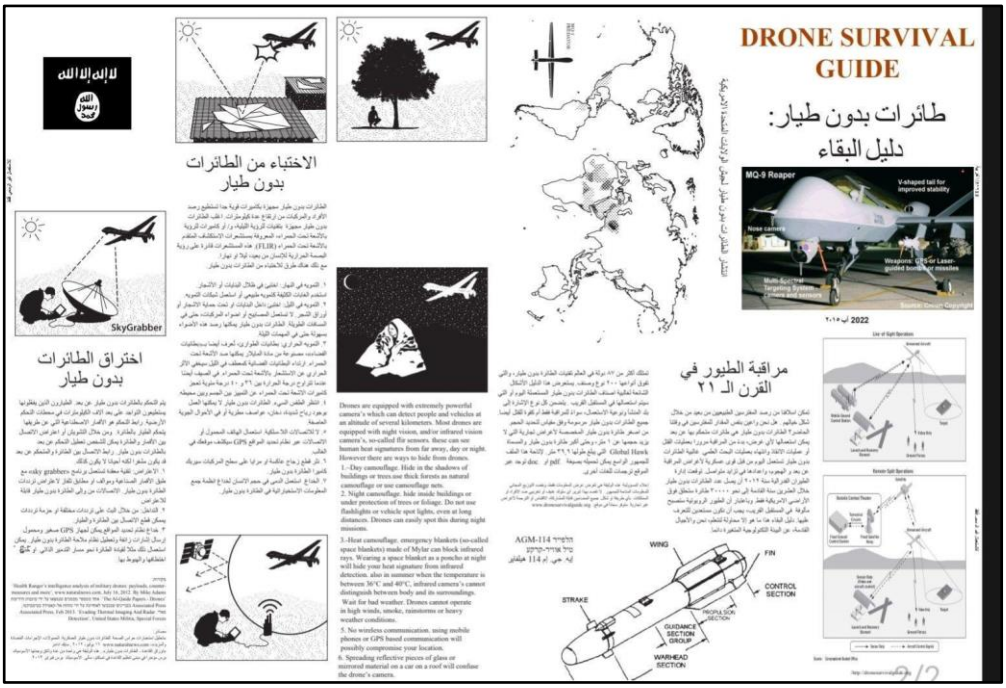
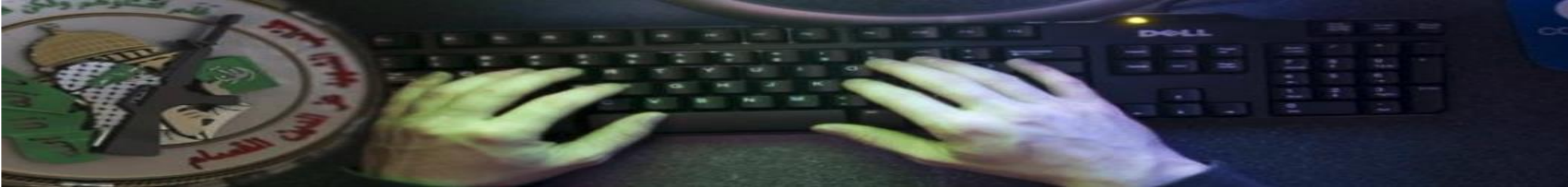


Figure 22 - A survival guide created by the ISIS group teaches how to protect against drones on RocketChat (Source: dark web)



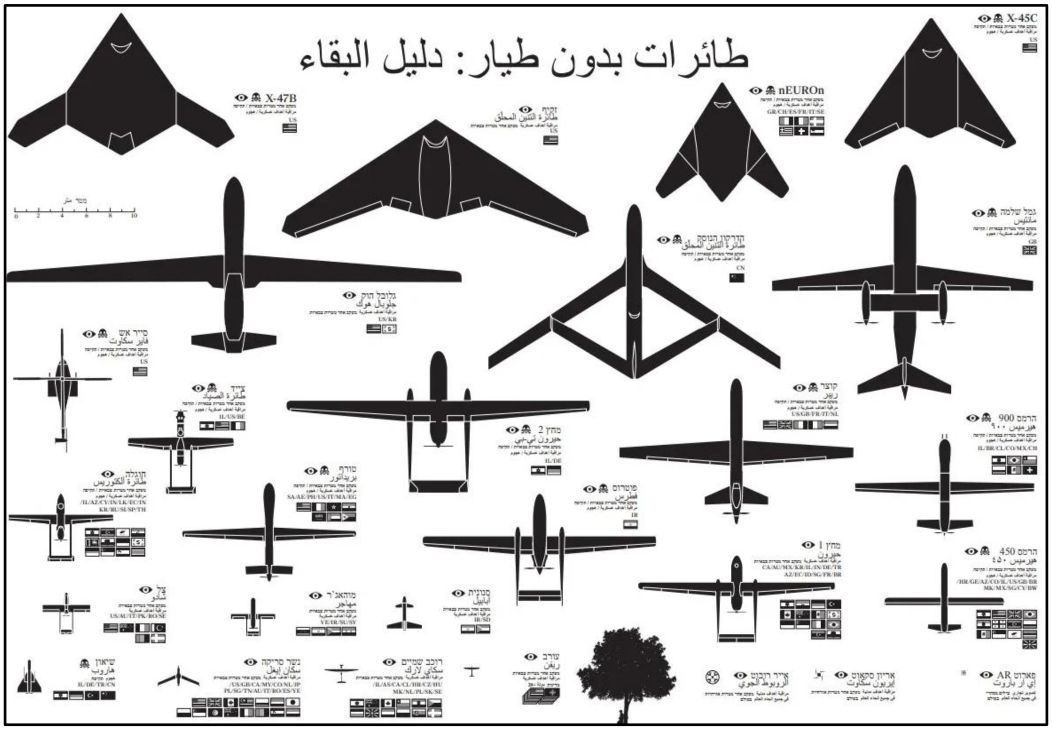


Figure 23 - A survival guide created by the ISIS group teaches how to protect against drones on RocketChat (Source: dark web)

Although the terrorist organization has carried out a few cyberattacks, it has mainly used cyberspace for propaganda, recruitment, and communication purposes. It used various platforms, like Facebook, Twitter, and WhatsApp, to communicate with recruits and spread its propaganda. In 2015, the terrorist group even released a list of applications with a ranking of recommended private messaging. ISIS considered Telegram a secure and reliable communication application and they encouraged their supporters to use Telegram to discuss sensitive issues such as travel to Islamic State-controlled territory. The Islamic State has also created multiple public channels on Telegram to deliver news updates and propaganda messages through its news agency Amaq Agency. On the defensive side, the Islamic State published a manual in 2015 on how to avoid intelligence surveillance and what to do to stay safe and anonymous online. Furthermore, the Electronic Horizon foundation Afaq, established in 2016 and aligns with the ideology of ISIS, published a magazine a few years to raise awareness among ISIS supporters and media activists about operational security (Figure 24).

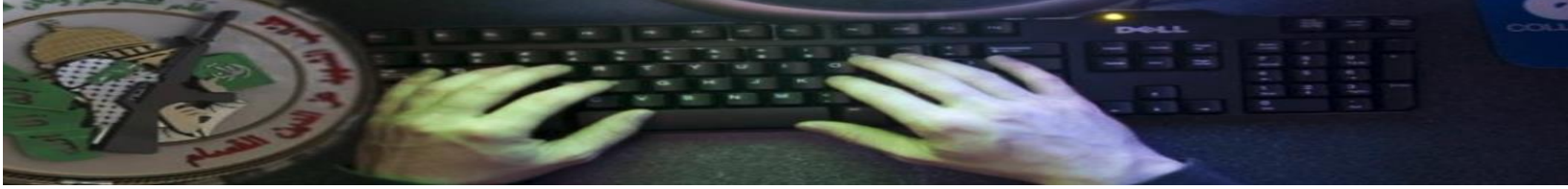




Figure 24 - Magazine from Afaq, which aims at raising security awareness among ISIS supporters (source: JihadoScope)

In 2019, the territorial defeat of the Islamic State represented the beginning of the end for the organization. Nevertheless, the Islamic State still has many supporters seeking to promote the organization's ideology. In 2021, the Islamic State released a video to encourage hacking and, at the same time, to try and recruit hackers but without any official group name. These calls for the recruitment of hackers did not have the expected effect or results. However, as of 2022, the organization still has multiple supporters that are active on several Telegram channels or underground websites, promote the Islamic State ideology, and discuss the organization's activities (Figures 25, 26, and 27).

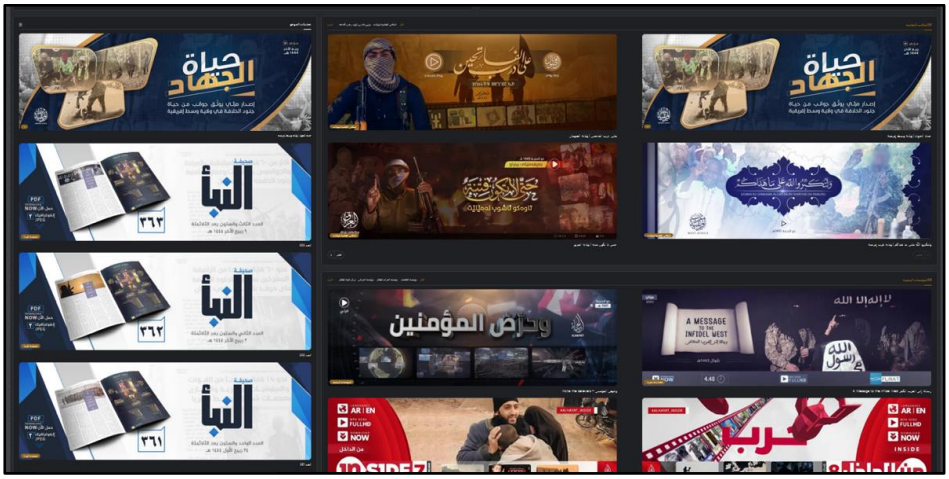


Figure 25 - Some ISIS publications on an active darknet website in 2022 (Source: dark web)

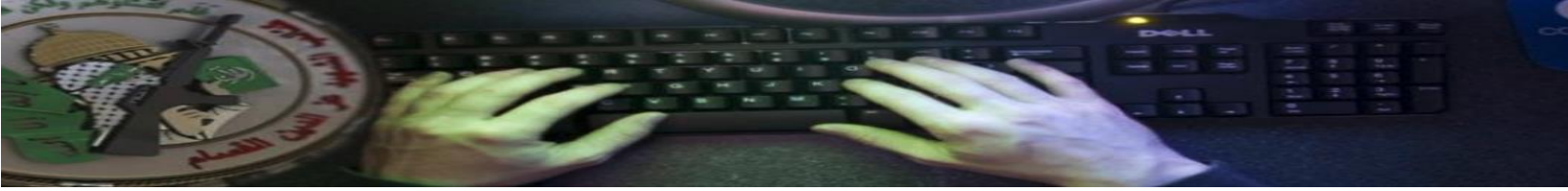
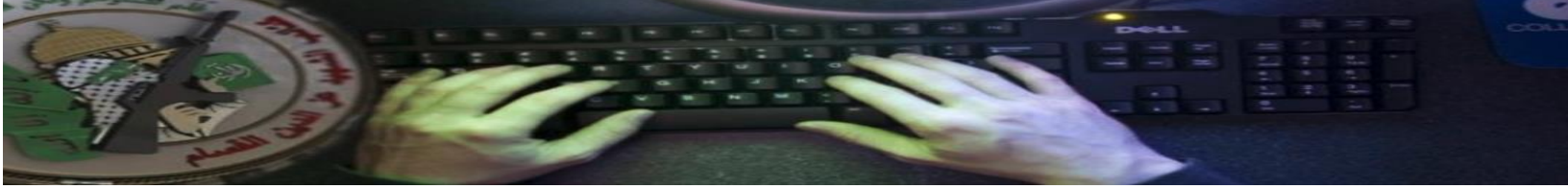




Figure 26 - Some ISIS Telegram channels still active in 2022



Figure 27 - An Islamic State-linked propaganda broadcaster announced the merger of three media units (Source: Telegram)



Based on their previous cyberattacks and online activities, the Islamic State does not appear to pose a significant threat to international security in terms of cyberattacks. The group never had solid cyber capabilities and has mainly exploited cyberspace to recruit and communicate their activities. Today, the Islamic State's offensive cyber capabilities are almost non-existent and therefore do not pose a severe threat. What is left of the cyber activity of the organization is more concerned with continuing to propagate its ideology using social media, messaging applications, and the darknet, rather than seeking to develop offensive cyber capabilities.

4.4. Al-Qaeda

Al-Qaeda is probably one of the most prominent terrorist organizations in the world and has influenced several other movements. The organization had been known before the 2000s as the origin of several terrorist attacks. The organization gained wide prominence with the September 11 attacks on the United States. In this large-scale attack, Al-Qaeda showed the world that with few means, it could carry out large-scale attacks with significant human, political and strategic impacts.



Al-Qaeda has been using cyberspace since the end of 1990. For the organization, using the Internet is an inexpensive and anonymous way to broadcast its message and ideology. With cyberspace, Al-Qaeda has also managed to circumvent traditional sources of information with numerous websites and forums. The organization has given impetus and had a substantial impact on the global cyber jihad. Al-Qaeda and its affiliates have developed cyber jihad considerably and are primarily active in cyberspace for propaganda and communication purposes. In 2015, Al-Qaeda Electronic announced its formation as a new branch of Al-Qaeda to be engaged in cyber warfare (Figure 28). However, the organization has never been involved in severe or successful cyberattacks. Most cyberattacks launched by the Al-Qaeda Electronic branch have consisted of website defacements against relatively low-value targets. The group has also occasionally launched DDoS attacks.

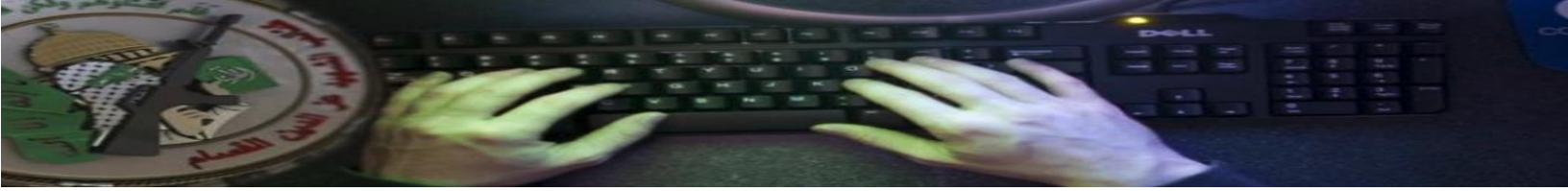




Figure 28 - Symbol of the Al-Qaeda Electronic Army

Like the Islamic State, Al-Qaeda primarily uses cyberspace to plan its operations, communicate its activities, and broadcast its jihad ideology. On the defensive side and to secure communications between members, Al-Qaeda has been using and developing encrypted messaging systems since 2007. According to deep research by the company Recorded Future in 2013, the Al-Fajr Technical Committee, a mainstream Al-Qaeda organization, created an encryption software program (Figure 29). Later its members used more commercial applications, such as Telegram or Rocketreach, to broadcast their messages and communicate. In 2020 Al-Qaeda supporter group, Jaish al-Malahem al-Electronic, posted on Telegram a magazine with advice on various things, from online safety to carrying out different attacks (Figure 30).



Figure 29 – Encrypted messaging software developed by Al-Fajr (Source: Recorded Future)

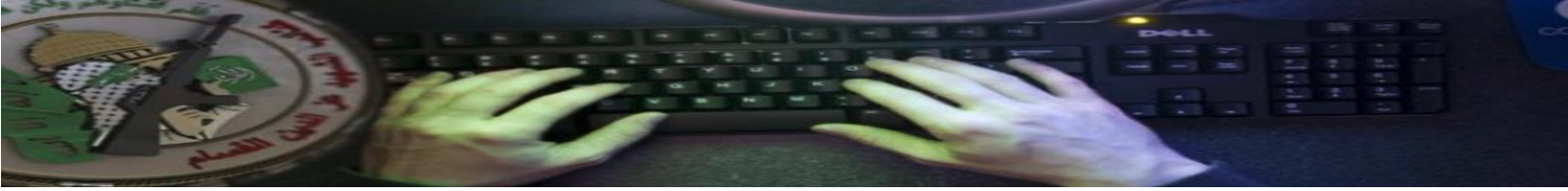


Figure 30 – A magazine with different advices, from online safety to carrying out different attacks on Telegram

In 2021, the pro-Al-Qaeda group Jaish al-Malahem published a message claiming to recruit different people for propaganda and hackers (Figure 31).



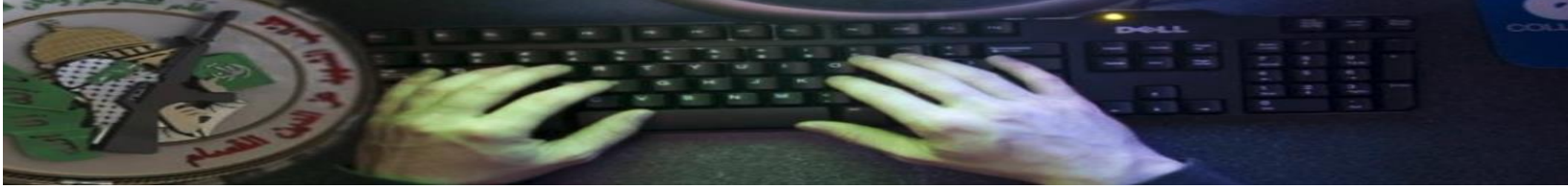
Figure 31 - Message from the Jaish al-Malahem group claiming to recruit different people, including hackers (Source: CTI-ME)



In terms of traditional terrorism, Al-Qaeda had a powerful impact on the world through its attacks and activities. It has influenced the security policy of many countries and led to many changes in security procedures. On the cybernetic level, although the organization has contributed to the expansion of cyber jihad like the Islamic State, it has not impacted cyberattacks against the countries' critical infrastructures. Despite some members and affiliates, who use their hacking skills to perform cyber activities, the significant lack of technological resources and actual cyber structure means that Al-Qaeda does not represent a real cyber danger to the security of states.

5. Conclusion

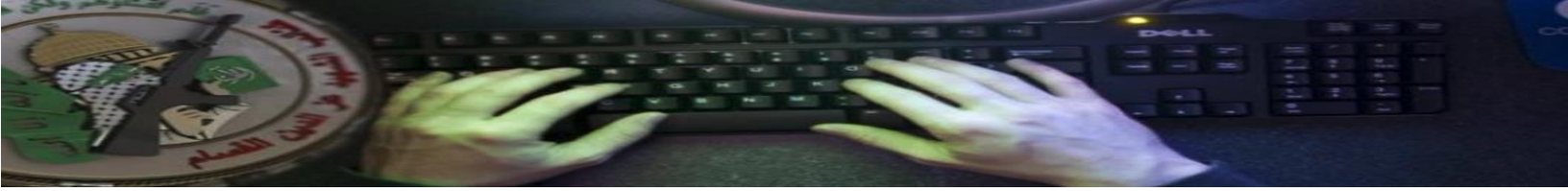
Radical Islamist cyberterrorism can be seen as a threat to states' national security. However, its impact is much lower than cybercrime of ransomware groups and banking malware, and cyber warfare by state-sponsored APT groups that conduct cyber espionage campaigns or target critical infrastructures. While some terrorist groups have developed cyber branches responsible for operations in cyberspace, their activities do not yet have sufficient impact to endanger the security of states. It is true that where some groups like Al-Qaeda and the Islamic State use cyberspace mainly as a communication and propaganda tool for cyber jihad, other groups like Hamas or Hezbollah are more active in offensive cyber operations. However, as mentioned above, these cyberattacks are still far below what states or state-sponsored groups can carry out. Cyberterrorism could significantly impact national security if nation sponsors terrorist groups to increase their cyber capabilities. Indeed, an act of cyberterrorism that would have a substantial effect on the safety of a state, such as an attack on a nuclear power plant, an airliner, or the electrical system, would require many resources in terms of intelligence, technology, and funding that a terrorist group alone would not have without the help of a supporting nation. Today, radical cyberterrorism represents more of a danger in terms of propaganda than cyberattacks. The real threat for a state comes from cybercrime, which generates an underground economy with billions of dollars yearly. Moreover, in a context where states increasingly use cyber weapons, the real danger will come from states’ cyber armies engaging in offensive cyber operations or state-sponsored APT groups.



6. About The Author



I am a cyber intelligence expert who has worked in various environments over the past ten years, including academia, high-tech, military, and law enforcement. My field of expertise is cyber intelligence, including strategy, collection, research, and analysis, and the lead of Cyber HUMINT operations on criminal and terrorist activities within cyberspace. I have trained many civilian analysts and Military and Law Enforcement officers on the Deep & Dark Web environments, Cyber intelligence collection, and Cyber HUMINT operations.



7. References

1. International Institute for Counter-Terrorism (ICT) Cyber Desk
   https://ict.org.il/desks/cyber-desk/
2. Middle East Media Research Institute
   https://www.memri.org/
3. The Meir Amit Intelligence and Counter Terrorism Information Center
   https://www.terrorism-info.org.il/en/
4. Lebanese Cedar' APT, ClearSky Cyber Security, 2021
   https://www.clearskysec.com/cedar/
5. Hamas's Facebook catfish operation on Israeli officials - report, Jerusalem Post, 2022
   https://www.jpost.com/arab-israeli-conflict/article-703451
6. Jerusalem Electronic Army JEArmy.
   https://twitter.com/JEArmy001
7. Terror groups in Pakistan switch to new messaging apps amid privacy debate, Business Standard, 2021.
   https://www.business-standard.com/article/current-affairs/terror-groups-in-pakistan-switch-to-new-messaging-apps-amid-privacy-debate-121012400363_1.html
8. How Terrorists Use Encryption, ROBERT GRAHAM, 2016.
   https://ctc.usma.edu/how-terrorists-use-encryption/
9. Forbes Israel Special Report: The World's Richest Terrorist Organizations, 2022
   https://forbes.co.il/e/the-worlds-richest-terrorist-organizations/
10. Israel Neutralizes Cyber Attack by Blowing Up A Building With Hackers, The Hacker News, 2019.
    https://thehackernews.com/2019/05/israel-hamas-hacker-airstrikes.html
11. The cyber strategy and operations of Hamas: Green flags and green hats, Simon Handler, 2022
    https://www.atlanticcouncil.org/in-depth-research-reports/report/the-cyber-strategy-and-operations-of-hamas-green-flags-and-green-hats/
12. Site Intelligence Group. https://ent.siteintelgroup.com/
13. Israel Defense Forces, Hamas' online Terrorism
    https://www.idf.il/en/mini-sites/hamas/hamas-online-terrorism/