Cyber Report

April – June 2021

Reichman University
International Institute for Counter-Terrorism (ICT)
With the Support of the Jusidman Foundation

Contents

Executive Summary

Throughout the period under review (April-June 2021), terror activity continued to permeate through the cyber arena. Jihadist terrorist groups continued their efforts spanning from operational to defensive and offensive actions. Terror groups have also been continuing the trend of using various social media platforms to disseminate propaganda and communicate with their audiences worldwide, often in several languages. This period saw an increase in incitement of physical lone wolf attacks through cyberspace. Throughout April – June 2021, jihadi groups launched several campaigns and continued to disseminate material through various publications, newspapers, and magazines. During this period, Irani and Shia cyber groups made efforts to remain connected with their audiences in the cyber arena by opening new channels and websites. They also carried out various hacks, stealing and publishing personal information of their targets.

In May 2021, tensions escalated between Israel and the Palestinians, culminating in Operation Guardian of the Walls. The cyber arms of terrorist groups and terrorist hacking groups joined in the conflict, spurred by the escalation of violence in tandem with OPIsrael, the annual cyber attack campaign against Israel that occurs every April. During this time, Israel saw a wave of cyber attacks from many various terrorist and hacktivist groups. These attacks are analyzed in a case study in this report.

We are observing a period of time in cyberspace where terror groups are exploiting cyberspace to the best of their abilities, such as for fundraising and propaganda, and are also actively working towards raising their cyber capabilities in order to transform their motivations into tangible attacks. This report analyzes these trends over the period of April – June 2021.

In the period reviewed in this document (April – June 2021) terror activity in cyberspace has been identified in three major aspects:

In the international arena, the global response to cyber threats included activity on the part of governments attempting to quell cyberattacks and remain up to date in their cybersecurity departments by implementing new regulations, policies, sanctions, and roadmaps to improve their cybersecurity. These actions include international cooperation to defend and act against cyber attacks. In May 2021, the United States suffered an attack on a major oil system, Colonial Pipeline. This attack comes following the SolarWinds attack, which acted as a wakeup call to the United States. The Colonial Pipeline attack had tremendous impacts and revamped discourse pertaining to cybersecurity in western countries.

Global Jihad

Operational

Use of Social Media and Comunication Platforms

During the period under review (April - June 2021), Global Jihad organizations, continued to carry out propaganda activities through different media platforms, mainly through social networks, their own websites, and communication platforms such as RockChat, Telegram, Twitter, Conversation, Element, and Chipwire.

- In April 2021, Islamic State linked **Afaq cyber defense unit** (Electronic Horizons Foundation) developed a cloud platform based on Nextcloud intended for followers to utilize to store propaganda materials. They also developed a new chat platform named S-chat on the Element matrix server to use for more secure communication. The chat consisted of multiple channels which were opened by Islamic State supporters over the course of a month until the server was shut down for unknown reasons.

  After the server was shutdown, Afaq continued to encourage Islamic State supporters to use the Element app for communication, providing options for existing servers to be used as opposed to using the default one provided by the Matrix.

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

- One of the main ways Afaq has continued to encourage followers to use Element is by publishing 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 for Element on an iPhone or iPad.

Afaq publication on different advantage and disadvantage of communication apps

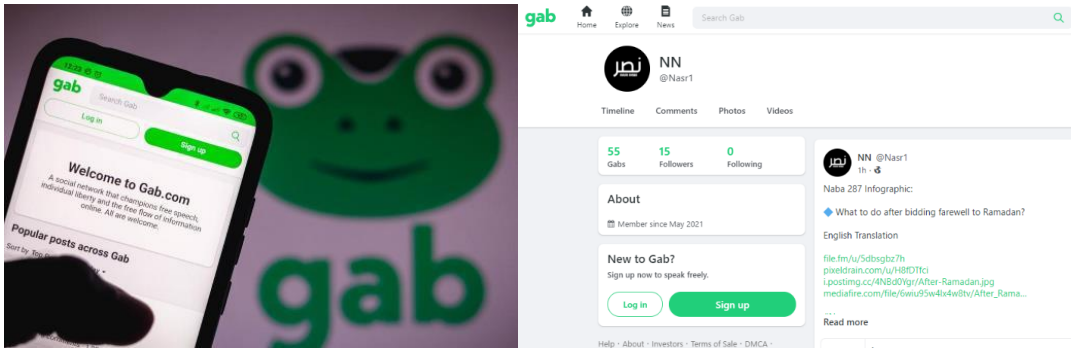
Guide how to register to Element via iPhone or iPad

Islamic State supporters continue to use a variety of communication apps and social media simultaneously including Matrix based platforms such as Element and RocketChat as well as other communication apps and social media such as Telegram, Conversation, Twitter, Instagram, and more.

Among the most common use of apps during the period under review (April-June 2021) was Telegram, with emphasis on the use of Telegram Bots. Telegram bots enable Islamic State supporters to stay up to date with current accounts and links to Islamic State platforms. Some of the Islamic State's bots published links to accounts on Telegram on a daily basis, while others published full lists of links to all Islamic State platforms (websites, other apps etc) on a weekly basis. The bots also provided daily news on Islamic State operations in the Jihadi arenas created by Amaq or Nasher news.

***Left: example of Islamic State bot that published once a week full list of Islamic State platforms; Right: example of Islamic State bot that published new IS affiliated accounts on a daily basis*.**

Islamic State supporters also attempts to use varity of communication apps that are less common among jihadists such as Gab. Accounts affiliated with Islamic State supporters on RocketChat have recommended the use of the gab communications platform. For example, the "**Nasr**" communication institution, which supports the Islamic State, published several accounts on gab.[1]



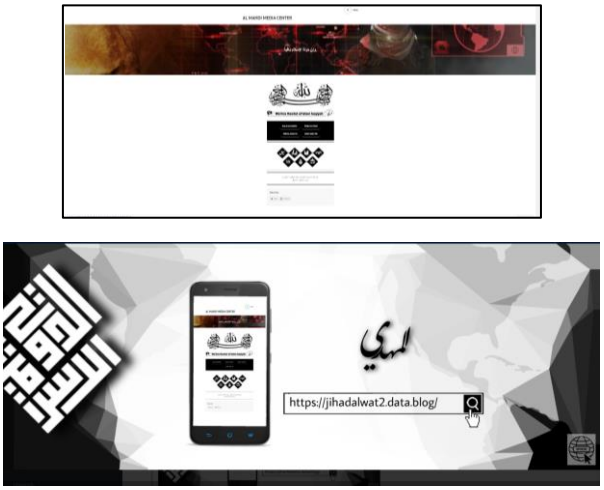
Nasr channel on gab

Islamic State supporters also continue to explore options to create their own platforms such as websites, chat rooms etc. For example, In May, **Al-Mahadi media institution** (Supporters) affiliated with the Islamic State developed a website on a WordPress platform. The website published propaganda created by the Al-Mahadi media institution. The website also provided links to external acounts of Al-Mahadi media on social media and communication apps.

Most of the websites that are operated by supporters media institution are only up and running for a short period of time before they are shut down. This is due to two main reasons:

[1] June 2021, RocketChat.

The first is that they are easily detected by security agencies, since they are operating under free servers and domain platforms. Thus they can be easily removed. The second reason is that they lack the necessary cyber defence to protect the site from cyber attacks, which are very common against the Islamic State. It should be noted that there are several websites operating efficiently by Islamic State supporters. These websites receive funding through cryptocurrncy and use these funds to pay for donains, servers and cyber protection.



The website homepage & Banner with link to the website

Propaganda

Incitement

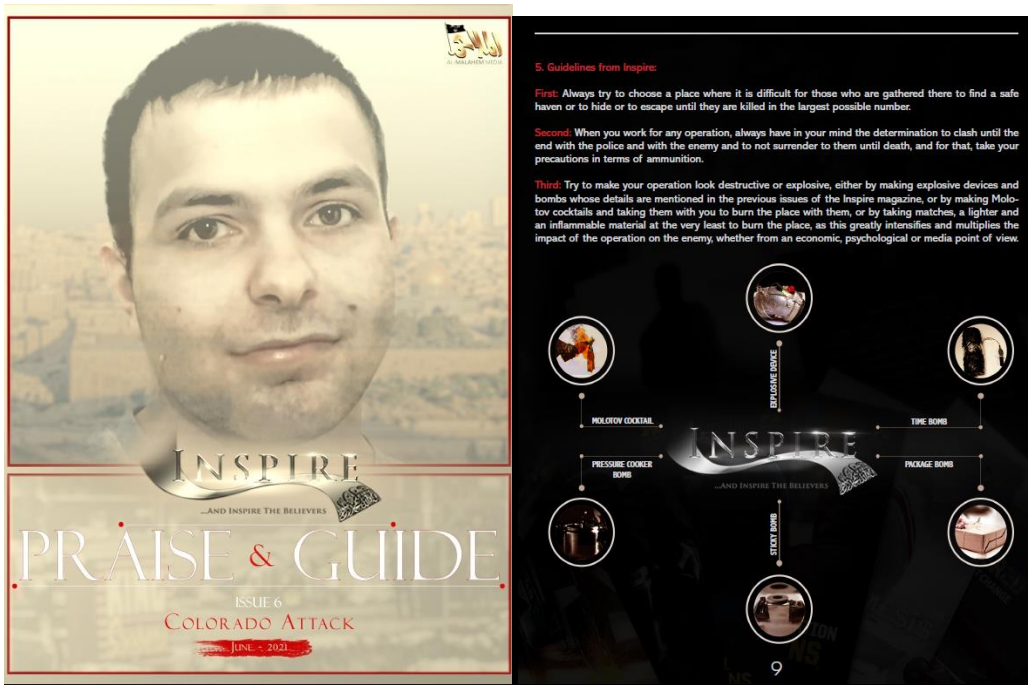
- The "**Al-Malahem Cyber Army**" group, which supports al-Qaeda in the Arabian Peninsula, has published the second edition of the Wolves of Manhattan Magazine (second edition), in which they called for violence against police in the West. For example, the group offered to pay one bitcoin, worth $60,000, to every Muslim who murders a Christian policeman in Western countries. They stated that in order to receive the cash prize, a photo of the documentation of the murder incident must be sent to a designated website called Geonews.[2]

[2] Apr 2021, Telegram.

Banner detailing cash prize - one bitcoin for anyone who kills a police officer in Western countries

- In June, 2021, **Al-Qaeda in the Arabian Peninsula (AQAP)** published a guide in Arabic, English, and French on the subject of lone wolf attacks, based on insights it gained from the March 22, 2021 terrorist attack in Colorado. The guide is the 6th part in the series of publications called "Inspire Praise & Guide". In the opening of the guide, the organization condoned the shooting attack carried out by a Muslim citizen in the United States in a supermarket in March 2021 and emphasized the importance of continuing terrorist attacks against Jews and Christians on distant enemy lands. Next, the organization described the character of the terrorist Ahmad al-Issa, along with the logic of the terrorist's decision to focus on the target of the attack, and how it was carried out. Finally, they offered some advice on how to refine the methods of operation of a single threat, such as choosing a location that would make it difficult for passers-by to hide, or how to convey a threatening message to the target audience before the attack, such as filming the attack with a head camera.[3]

[3] Jun 2021. Telegram.



Title page of the guide and a page containing tips for lone wolf attacks

- The **Al-Taqwa Media Institute**, an advocacy group that helps distribute propaganda for the Islamic Stated, launched a campaign in April 2021 calling on the Mujahideen and Muslims to break into prisons and infiltrate refugee camps in Muslim countries where Islamic State women are staying with their children, in order to free them and to restore their dignity from their captors. As part of the campaign, banners were published under the headline "Be patient with Muslim prisoners".[4]

[4] Apr 2021, Telegram.

Banners published under the headline "Be patient with Muslim prisoners"

Campaigns

- The main campaign of the Islamic State during the period under review (April – June 2021) focused on the **Jihad Media campaign**. First presented in Al-Naba magazine, the campaign highlights the importance of Jihad Media alongside the physical battlefield. The campaign also provides legitimization for the ongoing Jihad Media conducted by Islamic State supporters and calls upon them "to unite the ranks … in assisting the Islamic State" (Al-Naba). The call for unification in the Media arena was also translated into a variety of languages and published on multiple chats affiliated with the Islamic State.

In the subsequent months, official statements regarding unions between media institution operated by Islamic State supporters have been posted on different platforms such as Telegram and RocketChat.

Left: Al Naba Magazine – Editorial on Media Jihad; Right: Graphic Article on Al-Naba aimed for supporters (Al-Naba - translated by Supporters to English)

Response among Islamic State followers to the leadership Media campaign: from left to right: call for supporters to join media Jihad (translated to French); Al-Nabn main article on media jihad translated to Indonesian; Islamic State Media institutions (supporters) declare unification on Telegram.

Another example is the publication by the **Al-Taqwa Media Institute**, which published an article condemning the enemy's propaganda machine and propaganda efforts against the

organization. According to the author of the article, all attempts to break the spirit of the organization's members through Fake News and misrepresentation were doomed to failure, and the organization continues to absorb engineers and other professionals.[5]

Banner of the article

- Another main campaign which was highlighted during the period under review (April-June 2021) was the "**Economic War Campaign**". The economic war campaign was first introduced at the end of 2020 in Al-Naba magazine and since then has been published in nearly every Al-Naba edition. Attacks within the scope of the Economic War include mostly attacking gas facilities, oil, and electrical infrastructure. While this phenomenon is not new, it has gained popularity during this period of time in the Jihadi arenas and in the media platforms.

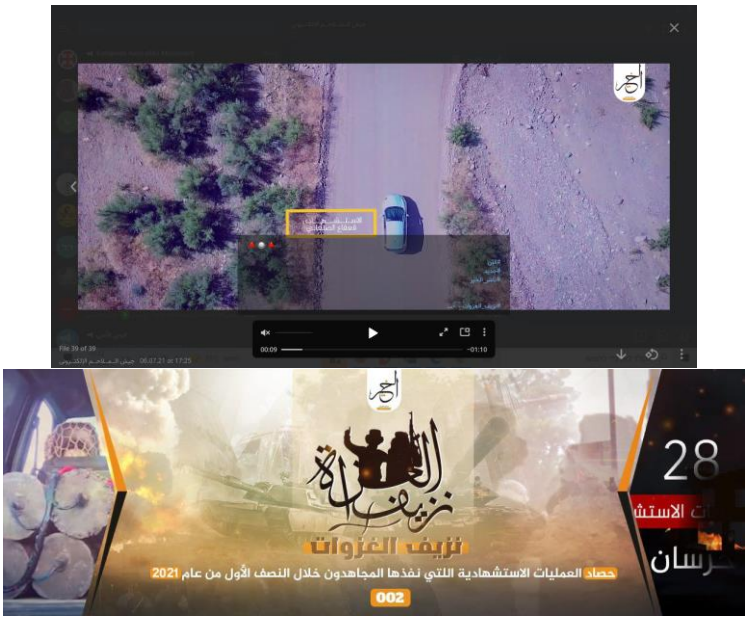
Al-Naba graphics on number of electric polls that were attacked in Iraq

Main Publications and Digital Magazines

- In June 2021, **Al-Qaeda** supporters established a new media institution named **Al-Khair**. The institution publishes high quality graphics including flyers, announcements, and videos, mainly

[5] Apr 2021, Telegram.

on Telegram. One example is a video describing the successful activities of Al-Qaeda around the world, similar to those publications that were published many times by the Islamic state supporters.



Formal Banner of the Video; Picture taken from the video

- In June, **al Malahem Cyber Army,** which is affiliated with Al-Qaeda, released the second edition of the magazine "**Wolves of Manhattan**" on Rocketchat and Telegram. Among the articles is a summary of a cryptocurrency course that al-Malahem cyber army held in December 2020- January 2021.

Cover page of Wolves of Manhattan Magazine

- In May 2021, **Arkan Media Center** which is affiliated with the Islamic State published the second edition in English of Arkan magazine on Rocketchat. The magazine includes articles such as "a guide for Muslim prisoners during the imprisonment"; an article on "who is the real enemy?" providing pictures of Putin and Trump, and an article on the "revival of the Khalifah".

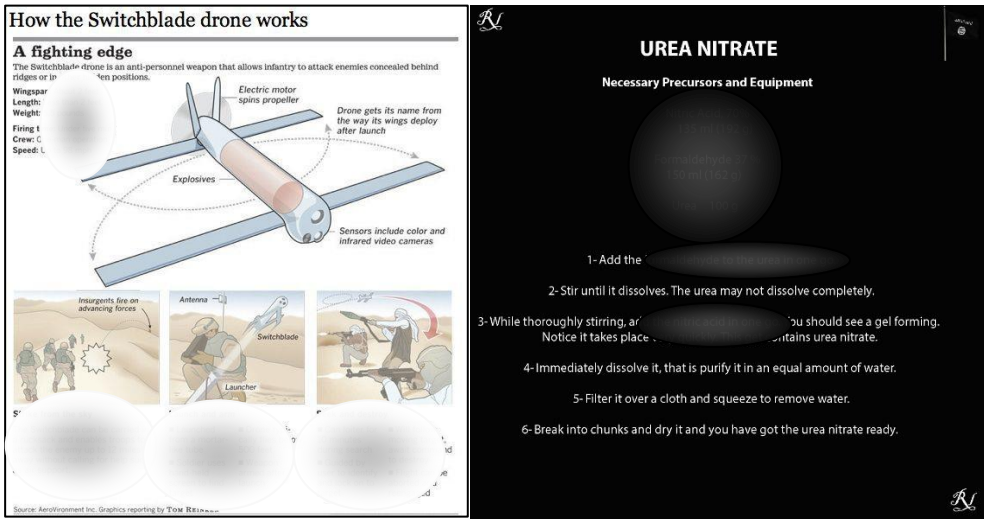
Arkan Magazine Second edition

- In June 2021, the digital English magazine affiliated with Islamic State - **Voice al Hind** – published its 17th edition on Rocketchat. The magazine included articles such as "Israel of South Asia". The article began by addressing the recent escalation between Israel and the Palestinians and noted how quickly the world lost interest in the Palestinian cause once the situation calmed down. The article goes on to discuss the Muslim situation in South Asia.

Left: cover page of the latest Voice of Hind 17; Right: article on Israel in Voice of Hind

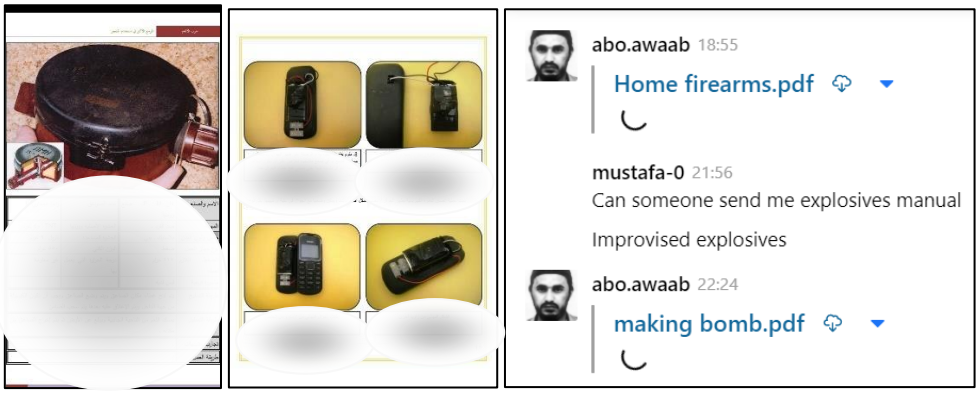
Tactical

- During the period under review (April-June 2021), users on the RocketChat platform published tactical guides such as "How the Switchblade drone works" and a guide to nitro-explosive. On the Element app a channel named *Rome Libera* a user published instruction how to make Nitro Urea and TATP.



On the right: switchblade drone; On the Left: NITRATO DI UREA

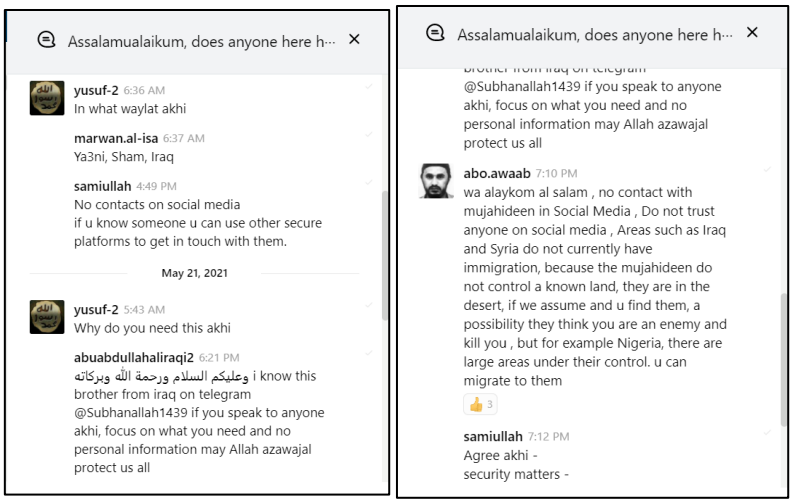
- In June, a private room on Rocketchat was opened named *Explosive science* which publishes tactical materials. Most of the publications were instructions on how to make explosives and the use of remote detonations at home.



Post on how to make explosives

Jihadi arena

- In June 2021, on Rocketchat, Islamic State supporters' discussed **arriving to Jihadi arenas**. A user advised other supporters not to contact the provinces through social media. *"If you do contact then do not give personal details... Foreign fighters who are looking for a destination, offer them Nigeria and ask them not to come to Iraq and Syria."*



Islamic State supporters discuss arriving at jihadi arenas on Rocketchat

- In June 2021, another chat on Rocketchat discussed **arriving to Jihadi arena mainly in Africa**. *"Africa is not like all other countries, not like Iraq or The Levant, and the coalition losses there will never be easy, vast areas, mountain ranges and many dense forests, it's like the Vietnam War and all the allies are threatened with drowning.* ***Immigration to it is very easy, especially since it is adjacent to Europe****...The caliphate there (Africa) is expanding so quickly"..*

Discussing arriving to Africa on Rocketchat

- **Sheikh Abu Hafs al-Maqdisi**, leader of the **Army of Ummah**, a Salafi jihadist organization supporting al-Qaeda in the Gaza Strip, issued a number of proclamations in May 2021 condemning Palestinian statements praising Iran for its contentious stance on the issue of Jerusalem and its support for the Hamas movement. He expressed that Iran is not entitled to such praise because it acts in accordance with narrow Iranian interests and exploits the Palestinian issue for its political needs. The leaflets were published against the backdrop of Operation Guardian of the Walls and the expression of sympathy by Hamas members towards Iran.[6]

Proclamation condemning Iran by Sheikh Abu Hefetz al-Maqdisi entitled "Victory is not for Iran and not for those who thank Tehran"

[6] May 2021, Telegram.

- The **Al-Raya Communications Institute**, which operates on behalf of the Army of the Ummah, a Salafi jihadist supporter of al-Qaeda in the Gaza Strip, published a banner detailing its military activities against Israel during Operation Guardian of the Walls. For example, the organization claimed to have fired 14 rockets at southern communites in Israel.[7]

A banner detailing the organization's military activities against Israel during Operation Wall Guard

- In May 2021, the **Al-Taqwa Media Institute**, which assists in advocacy for the Islamic State, published propaganda materials calling on Muslims to liberate the Al-Aqsa Mosque from Israeli control through terrorist attacks. The timing of the publication is related to the events of Operation Guardians of the Wall, during which there was an escalation between Israel and Hamas against the backdrop of the Jerusalem issue.

[7] May 2021, Telegram.

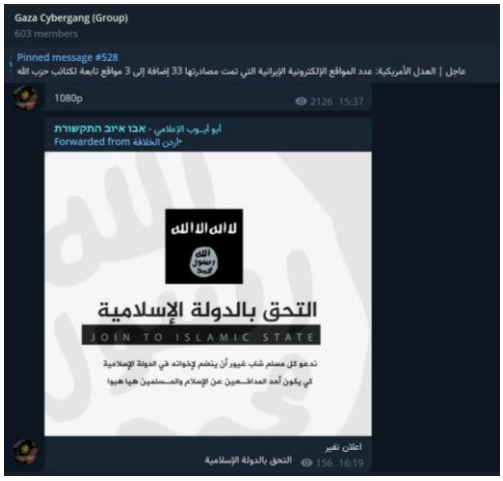
- The Al-Qaeda linked media outlet published in its official "Al-Nafir" official newspaper, as well as Al-Qaeda-affiliated Telegram channels calling on Palestinians to launch a wave of stabbing attacks against Jews and renew the knife intifada.[8]

[8] May 2021, Telegram.

Left to right: Banner of Islamic State supporters; A banner of al-Qaeda supporters and the al-Nafir coupon issued by the al-Qaeda leadership

Recruitment

- In June 2021, on the Telegram channel belonging to the Palestinian hacker group "Gaza cyber gang", a user published a call from the Islamic State under the title "Join us". This is not the first time this user has attempted to **mobilize Palestinians to act in the name of Islamic state**. He has been publishing propaganda materials in a few affiliated Palestinian Telegram channels for the past few months.



Recruitment post on Telegram: Mobilizing Palestinians.

- In May 2021, the Al-Mahadi media institution affiliated with the Islamic State published a recruitment flyer on the **Element** app, calling to "***Wake up, Muslim brother, now is the time of awakening, bring faith and courage…" "Join the Islamic State".***

Al Mahadi call for recruitment

Terrorism Financing

The practice of financing terrorism through cryptocurrency has continued throughout the period under review (April-June 2021). A new trend we have seen recently is the distancing from blatant requests for donations to specific Bitcoin addresses. The Know Your Customer (KYC) policy that ensures virtual cryptocurrency exchanges refuse any transactions from addresses that have been flagged as terrorist organizations has hindered these groups' abilities to publicize their specific addresses. Therefore, we have seen a trend in terror groups posting private contact information through which they can privately provide Bitcoin addresses to donors, as well as a transition to less detectable cryptocurrencies such as Monero.

Many terrorist groups fundraising through Bitcoin follow a technique called layering, in which they transfer bitcoin through several addresses in a very fast chain to obscure who the intended recipient is. These chains often lead to a virtual exchange, such as Binance, where it is then impossible to follow. With these tactics, terror groups that choose to use Bitcoin can still obscure their identity within the transparency of the blockchain.

During the period under review (April – June 2021), there was a spike in cryptocurrency donations to Palestinian terror organizations in response to the escalation of violence in the region during Operation Guardian of the Walls.

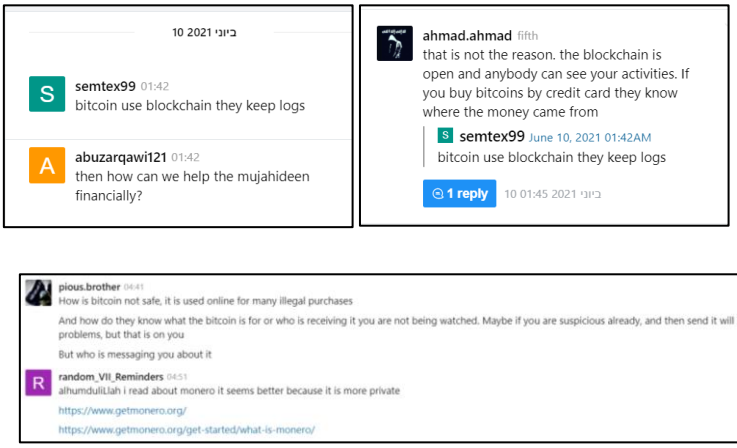
- In April 2021, Islamic State linked cyber defense unit, Afaq, issued a warning on Telegram, calling on their followers **to avoid using Bitcoin** currency because it is trackable via Blockchain and to avoid using any exchange service because "*they are cooperating with government agencies*" the announcement is part of an ongoing Islamic State campaign to avoid using Bitcoin and to use private coins such as Monero.

Warning published by Afaq against the use of Bitcoin currency

- In April 2021, Arakan magazine second edition published a call for donation using Monero coin**. The address wallet was added as well as scan code option to enable easier interface.**

The page on Arkkan magazine (second edition) calling to donate using Monero coin

- In June 2021, discussion on Rocketchat about safe ways to donate to the Islamic State revealed that supporters of the Islamic state also understand that using bitcoin is unsafe. They also discussed Monero as a more secure option.



Example of the discussion on Bitcoin and Monero on Rocketchat

- The Al-Raya Communications Institute, which operates on behalf of the **Army of Ummah**, a Salafi jihadist organization that supports al-Qaeda in the Gaza Strip, is continuing its fundraising campaign through Bitcoin. As part of the campaign, an e-wallet address, an e-mail address and a dedicated telegram account were published as contact information in order to donate.[9]

[9] May 2021, Telegram.

Banners from the Army of Ummah Organization in the Gaza Strip for the purpose of raising Bitcoin coins

In May 2021, **Army of the Ummah** received two transactions to one of their bitcoin accounts. The transaction came in response to the aforementioned funding campaign and was the first after almost a year (transactions were worth approximately $14.91 and $22.40). This group published many funding campaigns in recent years via their Telegram channel and media arm website in Hebrew.

- Sheikh 'Abd al-Razak al-Mahdi, a sheikh from Salafi Jihadi affiliated with the **Tahrir al-Sham** organization in Idlib, published the hashtag entitled "The Campaign - Let the Warrior Sitting on the Front Line Through His Hand". As part of the al-Razak campaign, he called on Muslims to donate money to the benefit of the Mujahideen fighting on the front lines. For this purpose, account numbers were provided on Telegram and WhatsApp.[10]

[10] April 2021, Telegram.

Post by Sheikh 'Abd al-Razak al-Mahdi

- In May 2021, during Operation Guardian of the Wall, Al-Qassam Brigades, the military wing of Hamas, sought donations through various communication platforms. Their fundraising method consists of providing each donor with a unique Bitcoin address for their donation. This tactic obscures the chain of transactions, as their main Bitcoin account is not widely publicized. They managed to increase donations significantly during the escalation. This fundraising campaign involved transactions from a wide variety of cryptocurrencies, including Bitcoin, Ethereum, Tether, and even dogecoin. Throughout May 2021, Hamas received over $70,000 in donations through numerous chains of transactions.

Post on Al-Qassam Brigade Telegram channel solociting donations during Operation Guardian of the Walls

- The Bitcoin and other cryptocurrency exchange office in the northern Syrian province of Idlib continues to publish details in Arabic and English about the services it provides in the field of cryptocurrencies on social media. The firm has published other online forms of payment in which it deals such as Advcash, Binance, Payeer and more. They noted that they convert Bitcoin, Tether and other currencies. The firm also offers training courses in cryptocurrency trading for a fee of $100.[11] The Bitcoin exchange office is located in Idlib, in territory controlled by Hay'at Tahrir al-Sham (HTS). HTS is the leading Jihadi organization. The slogan of the Bitcoin exchange office is “First Office in the Liberated Territories”. We therefore can deduce that terrorists involved with HTS may be likely to use this exchange office. Bitcoin exchange offices like this can be used to convert Bitcoin into Fiat currency, after which the trail cannot be traced. As long as the currency is in the blockchain it can technically be traced since the blockchain is transparent. At these locations, a terrorist group can convert their Bitcoin into useable currency that they can use to help their cause without leaving a trail.

advcash

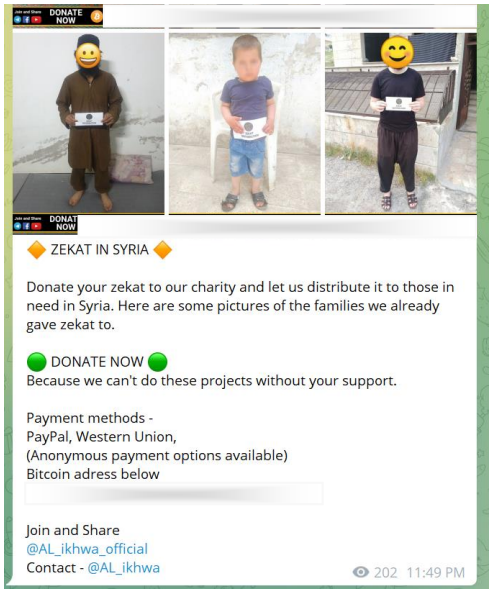
BINANCE

PAYEER®
ACCEPTED HERE!

[11] April-June 2021, Telegram.

Banners of payment methods such as Binance, advcash, and Payeer

- In the period under review (April – June 2021), Al Ikhwa, a group that has been linked to Malhama Tactical, a jihadist military company, published new Bitcoin addresses and performed several transactions.[12]



Telegram post by Al Ikhwa with Bitcoin address

The Bitcoin address posted by Al Ikhwa has six transactions that took place from the end of April 2021 through the beginning of May 2021. One transaction was received from Al Ikhwa's formerly publicized Bitcoin address which had been previously flagged by the United States Department of Justice as being involved in Terrorist financing. The received transactions end up being transferred to Binance, as is the common pattern with terrorist accounts. The account balance is currently zero. [13]

[12] April 2021, Telegram.
[13] August 2020, *United States Department of Justice*

Defense

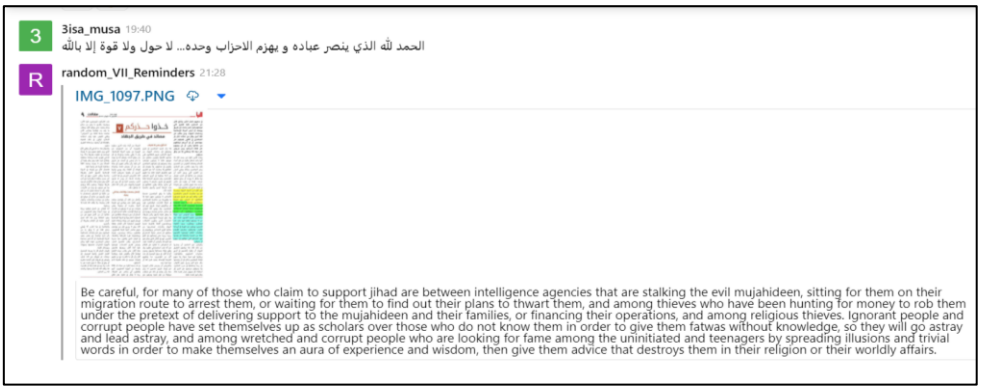
- In May 2021, **Qiman Electronic Foundation,** affiliated with the Islamic State, published an article on Rocketchat explaining how to check if data from Facebook had been leaked. According to the article *"The security breach notification website HaveIBeenPwned, has added 533 million phone numbers which were exposed in the Facebook data leak. The leak happened in 2019, but now the entire dataset has been posted on a hacking forum for free, and it is now easily available to anyone"…what can be done?, change the two-factor authentication method from text messages to other forms of verification."*

Banner of the article published by Qimam Electronic Foundation

- In June, **Al Burhan Media** (supporters of the Islamic State) published a warning on RocketChat regarding a fake account on Instagram. "*This page on Instagram is not run by us. It's a fake page. Al Burhan channel is present only on Rocketchat, Telegram and Hoop. Except these platforms, we nowhere have any channel or page untill now. We are not responsible for any content from this page on Instagram".*

The Warning as it was published on Rocketchat

- In June 2021, a discussion on Rocketchat by Islamic State supporters provided a warning to exercise caution regarding the provision of details, donations, and attempted mobilization to ISIS via the Internet. *"Be careful, for many of those who claim to support Jihad are between intelligence agencies..".*



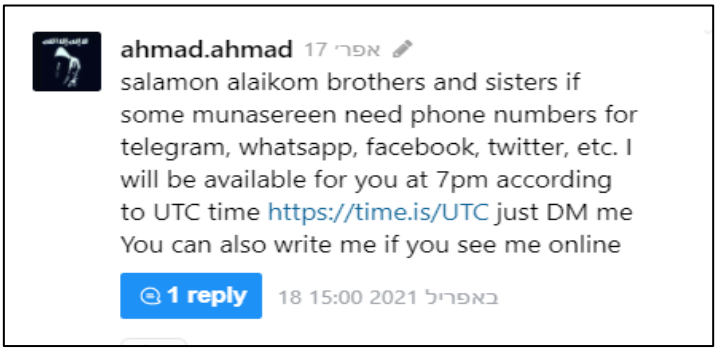
The warning post which was published on Islamic State chat – Rocketchat

- In May 2021, **the Al-Mahdi media institution**, affiliated with the Islamic State published a warning on **Element** for correct ways to use cyber-space "we urge supporters to use VPN and Tor. To pay attention to privacy leaks, use virtual numbers".

Warning published by Al-Mahadi on Element

- In June 2021, a user on Rocketchat offered Supporters on Islamic State temporary phone numbers to register anonymously for social media platforms that require a phone number to join, such as Telegram, Whatsapp, Facebook, Twitter etc. The user *Ahmad.Ahmad* is a

prominent user (might be even an admin) on RocketChat and provides supporters with technical advice.



Rocketchat: Numbers for supporters of the Islamic State

Offense

- In April, **Caliphate Cyber Shield (CCS),** allegedly carried out a cyber-attack against a port company in France. Since the collapse of the Islamic Caliphate in Iraq and Syria, there has been a significant decline in the activity of hacker groups affiliated with the Islamic State. The most prominent group operating on behalf of the Islamic State was the United Cyber Caliphate (UCC) however, since 2019 no group activity has been identified and it has apparently disbanded. Out of the UCC remains a central active hacker group Caliphate Cyber Shield. During 2019-2020 the group published only summaries of cyber-attacks that it carried out.
- In June 2021, on a Telegram channel named "**hackers of the Islamic State**" it was claimed that the hacker group "**Cyber Islamic Caliphate Army**" is launching a new offensive **cyber campaign against the *"Zionist enemy"*** *(Israel). They published that "Messages containing files with ransomware viruses will be sent to more than a thousand emails belonging to the Zionists. As soon as the file is opened, all the device data will be deleted."* It is speculated that this group is affiliated with the Islamic State organization following the group name and use of the jihad flag that characterizes the Islamic State organization. However, no further indications have been released to confirm this. In the past, a group with a similar name operated within the framework of the United Cyber Caliphate (UCC) – the offensive cyber arm of the Islamic State until 2019.

Left: Profile photo Group name about Telegram: Hackers of the Islamic Caliphate;

Right: The message as it was posted on the Telegram channel

- In April 2021, on the RocketChat platform, online discourse between Islamic State followers began to be emerge on chat rooms, discussing ways to hack security cameras, providing links to hacking tutorials and more.

On Rocketchat – chatter of Islamic State supporters on hacking a camera

- In May 2021, there was a Cyber attack on an Islamic State linked supporter's website called Elokab. The formal statement by the website admins was published on a pro-ISIS Telegram channel: *"we would like to inform you that the site has been penetrated by the enemies.."* On Rocketchat, ISIS supporters also identify suspicious activity on the Elokab website. One of the activities was offering IP log files in exchange for bitcoins. ISIS supporter published a warning on Rocketchat and encouraged users to continue to use VPN and Tor.

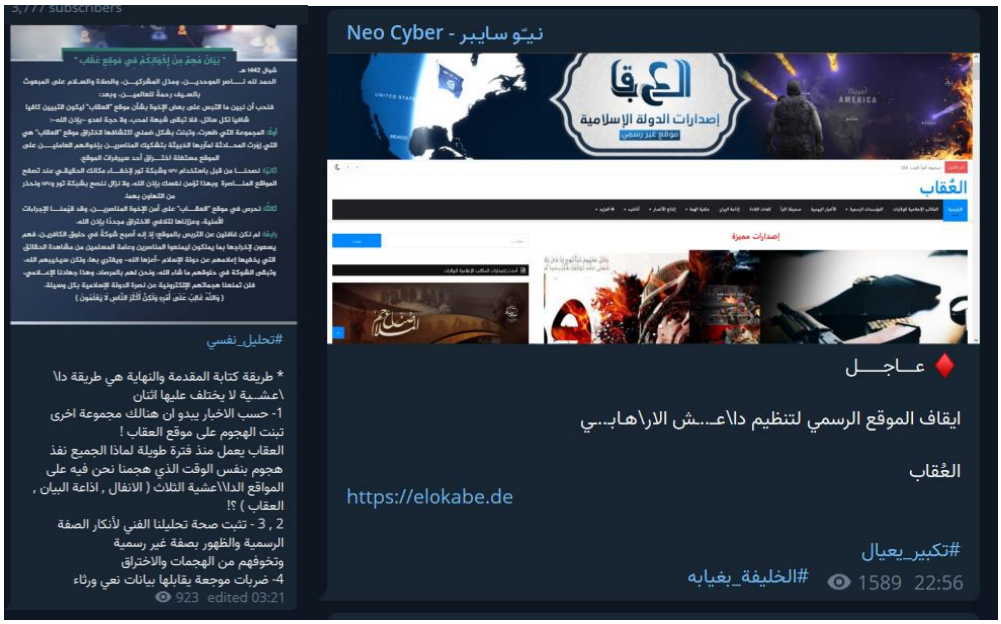
First statement published on pro-ISIS Telegram channel, announcing the Elokab website was hacked.

Picture published on Rocketchat of chat with the hacker who attacked Elokab offering to sell IP logs of the website visitors for bitcoins

- A few days later the administrators of Elokab website published statement in multiple languages stating that "*Those who carried out the cyber attack on website are a group of people whose goal was to* create *a buffer between ISIS supporters and the site's operators. They repeatedly encourage VPN use. They claim that since then activity has been done to tighten the security of the site. They claim that the administration is trying to download the site all the time but they manage to stick to it and stay here*".

Elokab administrators' official statement after the attack on the website

- Further research revealed that the attack was conducted by **a pro-Iranian Shia militia from Iraq named Neo-Cyber who is operating via the cyber space**. The claim of responsibility was published on their affiliated Telegram channel. The group also commented on the official statement by the Islamic State claiming responsibility for the attack on the Islamic State website.



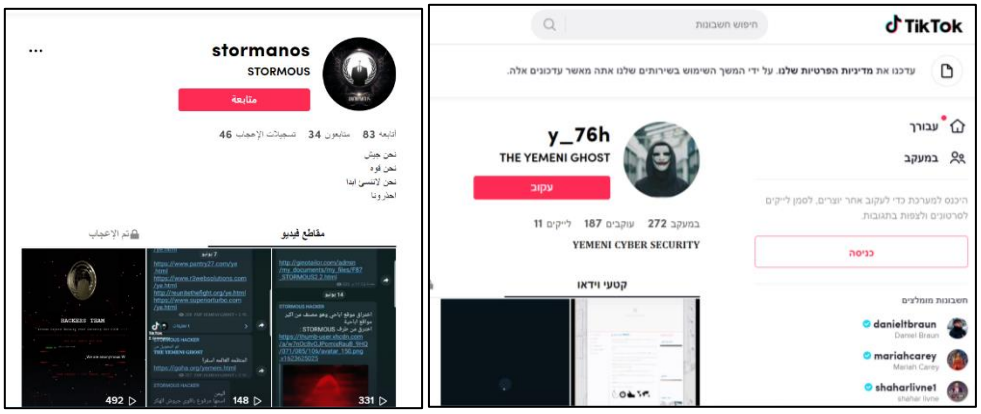
Neo Cyber claim of responsibility for attacking ISIS affiliated website (supporters of the Islamic State) Elokab.

Palestinian and pro-Palestinian Hackers

Operational

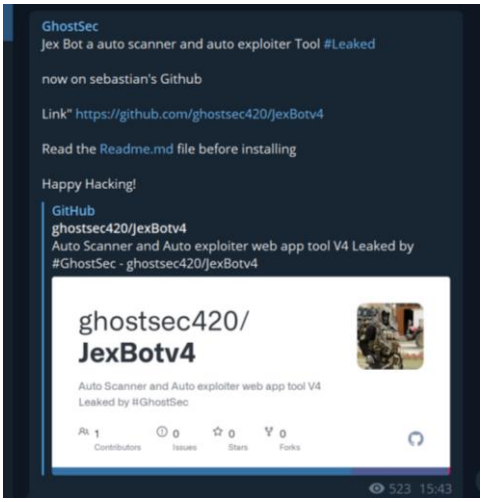
During the period under review (April-June 2021), most Hacktivists continued to use Telegram as their main communication platform. The groups have a several types of Telegram accounts – channels devoted to formal publications of hacks, a chat channel where supporters and collaborators can discuss hacking related topics among them, and in some cases, groups also use Telegram bots to maintain communication with supporters in the event that their formal account has been deleted.

Hacktivists also use Twitter and Facebook as well as running their own websites. Most recently, Hacktivists began using **TikTok** as well to present their cyber-attacks. Among these hackers are The Yemeni Ghost and Stormous Hacker group.



Accounts of Hackers groups identified on TikTok

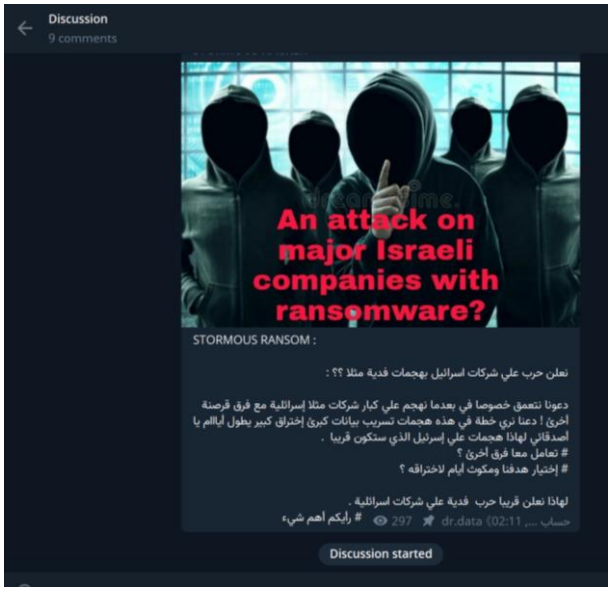
Within the above platforms, Hacktivists publish operational information including hacking tools, information on hacks they have conducted, and defense instruction. For example, In June 2021, Ghostsec hacker group published on Telegram that the group has developed a tool to help integrate intelligence gathering before carrying out hacks, such as an automated web crawler. The tool, as they claimed has been published on GITHUB.



Ghostsec publication on Telegram – new hacking tool

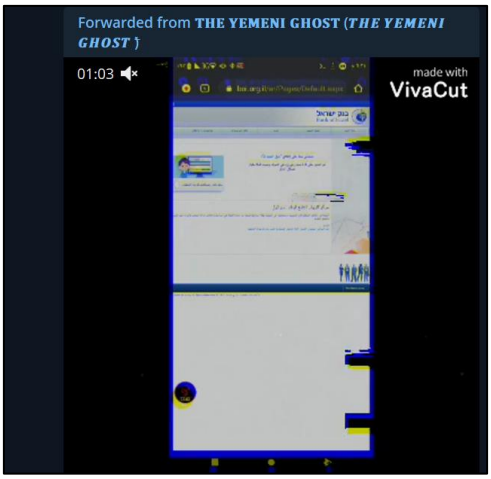
Offense

- In June 2021, the Hacker group "Stormous hackers" declared on their Telegram channel a Ransomware operation against Israeli companies. *"We Declare war on Israeli companies with ransom attacks… with other hacking teams… major data leakage, a major intrusion that takes days, my friends, for this attacks on Israel, which will be soon… a ransom war against Israeli companies.*



Stormous Hacker post on their Telegram channel declaring war against Israel

- In May 2021, the hacker group "**The Yemeni Ghost**" claimed it had hacked the Bank of Israel website *"the hacking and defacement of the fifth largest back in Israel by The Yemeni Ghost will lead to a significant decline in the Israeli economy."*



Yemini Ghost claimed they hacked the Bank of Israel website

- In June 2021, the hacker group "The Yemeni Ghost" declared that they were planning an attack on the government website of the Corporations Authority. The announcement was published on a Telegram channel associated with the group and states that the website of the Israeli Corporations Authority is "their next victim". No data has been released on the date of the attack or if it has been successful. Earlier that day, the group claimed that Israel had carried out an attack on the Al-Aqsa Mosque and that "there will be a severe response."

Picture of the government page of as it was published on the hacker group the Yemeni ghost.

- The group has also published data about websites in Israel with SQL weakness - advertising that was distributed among a number of hacker groups that work against Israel and they were invited to attack these sites.

SQL weakness in Israeli Website post

The hacker group The **Yemeni Ghost** is a group of pro-Palestinian Hacktivists from Yemen that operates against Israel and other countries in the Middle East, including Saudi Arabia. The group has three main media platforms: Telegram, which distributes publications about attacks, guides and tools in the field of hacking, and more; YouTube where it distributes assault videos; Tiktok - The group also recently opened an account in Tiktok, where it has so far distributed two attack videos.

- On June 22, 2021, a group of hackers from Malaysia named **Dragon Force** called on its partners to mark Friday 25.06.21 for a DDOS attack against websites of Israeli banks, including Bank Hapoalim, Bank Leumi, Bank Mizrahi Tefahot and the International Bank.

Left: The call as posted on the group's website; Right: The call as posted on the Telegram page

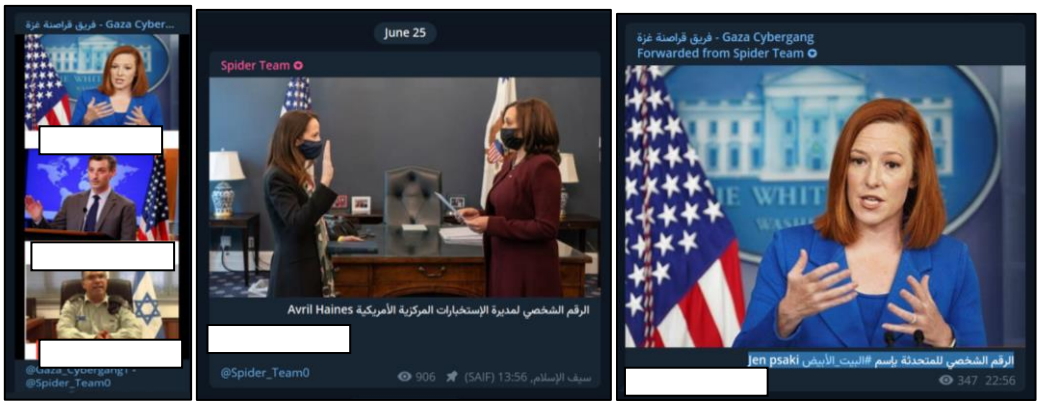
The call for a cyber attack against the websites of the leading banks in Israel is intended to encourage the participation of other hacktivists to assist in the attack efforts. For example,

Dragon Force distributed a message on Telegram: "We call on all hackers from Malaysia and Indonesia to attack."

The message on Telegram calling other groups to join

According to the publications of the Malaysian hacker group Dragon Force, several websites of banks in Israel were attacked, including Bank Leumi, Bank International, Bank Mizrahi Tefahot and the Bank of Israel, which was not planned to be a target of the attack.The group has released screenshots that allegedly show the success of the attacks against the websites mentioned above.

- In June 2021, the hacker group **Spider Team** with collaboration of the hacker group **Gaza Cyber Gang** published a post on Telegram doxing CIA Director Avril Haines, publishing her personal number, along with Jen Psaki's personal number for the White House spokeswoman and IDF spokesperson. **AnonGhost hacker** groups also doxed various people. They published on their Telegram personal information of the former Prime Minister of Israel, Benjamin Netanyahu.



Doxing

- In May 2021, a hacking group called **Hackers of Savior** emerged, and allegedly stole the personal information of millions of Israelis. Hackers of Savior is a hacking group self proclaimed

to be "doing our best to take back the occupied land of Palestine from the Zionist occupiers with help of all the freedom seekers around the world."[14]

Post by Hackers of Savior publishing the personal information of Israelis

Iranian and Shia Hacker Groups

Operational

- In April, **Neo cyber**, a pro-Iranian Shia cyber group affiliated with pro-Iranian Shia militias from Iraq, declared the opening of a new Telegram group that aims *"to be closer to our followers, to help followers with digital issues and to help us clean the web of enemies".*

[14] May 2021, Telegram.

Neo Cyber post on Telegram: the opening of a new group

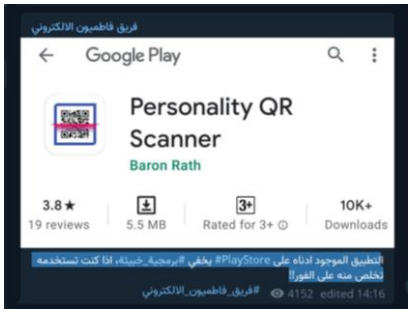
- In June 2021, the pro-Iranian hacker group **BlackShadow,** who hacked the Israeli insurance company Shirbit and K.L.S capitol, launched a new website. The website contains data linked to the aforementioned cyber-attacks, ways to contact the group, and a donation page with Bitcoin and Monero address. Further investigation did not reveal any transaction in or out the Bitcoin wallet affiliated with Blackshadow.

K.L.S sample Data on Blackshadow website

Donation page on Blackshadow website

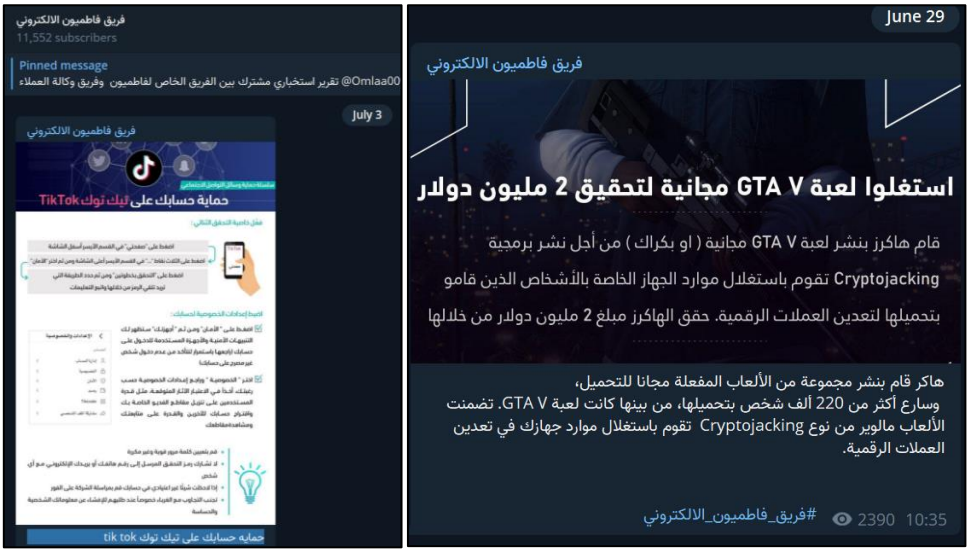
Defense

- In April 2021, a pro-Iranian Shia cyber group from Iraq named the **Fatemiyoun Electronic Team** published on their Telegram channel warnings against software that contains malware.



One example for warning of the program "QR Scanner"

- In June 2021, the **Fatemiyoun Electronic Team** published on their Telegram channel information regarding Microsoft Updates; Cyber protection warnings and a guide detailing how to protect Tiktok accounts.



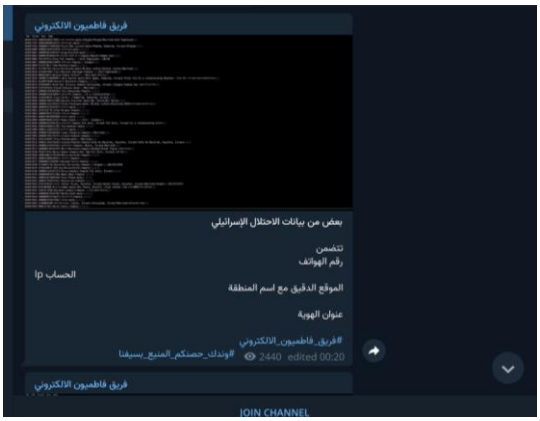
Post of Fatemiyoun Electronic Team on cyber defense

Offense

- In April, the **Fatemiyoun Electronic Team** posted on their Telegram channel that they hold information belonging to **Israeli citizens**. *"Some of the data of the Israeli occupation includes phone number, IP account, Exact location with area name, ID".* The Fatemiyoun Electronic Team posted screenshots on its Telegram account that it claimed contained data of Israeli citizens and their personal details, such as photos and a number of identity cards. According to the group, the data was obtained through a hack of Israeli accounts on Facebook. The group also posted a screenshot of the "Israel speaks Arabic" Twitter account operated by the Israeli Ministry of Foreign Affairs. According to the group, they were able to reveal the names of the operators of the aforementioned Twitter account, along with their photos and addresses. The

group claimed responsibility for hacking into other Twitter accounts, such as that of the American Arab University.[15]

A photo published by the Fatemiyoun Electronic Team in which it claimed responsibility for hacking into the Foreign Ministry's Twitter account "Israel speaks Arabic"

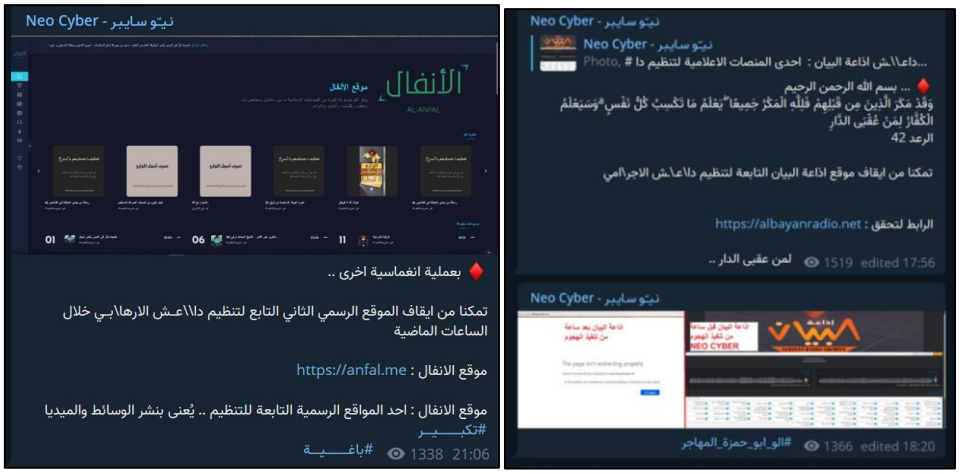


Fatemiyoun Electronic Team post on telegram: Data of Israelis' personal information

- In June 2021, a pro-Iranian Shia cyber group from Iraq named **"Neo cyber**" published on their Telegram channel a call for followers to provide them with links and bots affiliated with the Islamic State with the purpose to bring them down. "⚠ *Dear followers.. We receive ISIS*

[15] May 2021, Telegram.

websites links on bots (only websites, not channels)". In the course of this month, Neo cyber claimed to hack Islamic State social media accounts and websites. Such platforms included website such as Anfal, Elokab, Al-Byan radio.

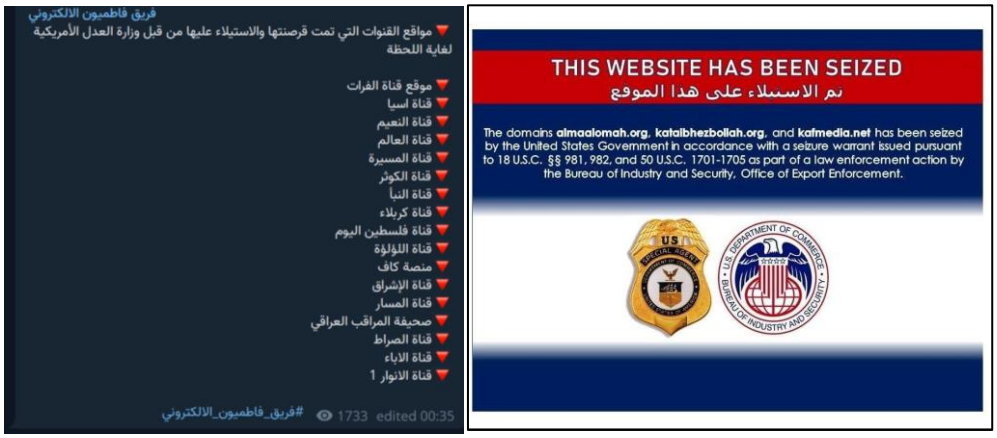


On the Left: Neo cyber claiming to hack Anfal website; On the right: Neo cyber claiming to hack Al-Bayan Radio website

- In June 2021, the US seized Iran's affiliated news websites from the Middle East which are operating based on US servers' companies. In response cyber group affiliated with pro-Iranian Shia Militia published statements on their Telegram channels:

  The cyber group **Neo Cyber** stated that *"we offer our services to host satellite TV sites affected by the American attack ,while ensuring that the site's dignity and prestige are preserved. We offer our services to host and protect the affected websites and ensure that they are not stopped by the US administration anymore. Contact us via the bot".*

  The cyber group named **Fatemiyoun Electronic Team** stated that Channels that have been closed down by the US administration can Re-open in sites or agencies with the **same name and with ease, but that it is preferable to buy a domain outside of U.S. control**. *"You can request a free domain through Fatemiyoun's online team.. as well we offer our services to host and protect websites and ensure that they are not stopped by the US administration anymore".*



Left: list of news website that were seizes by the United States; Right: the notice which was published by US on the selected websites.

Left: Al-Fatmayon statement responding the US act against pro-Iranian websites. Right: Neo cyber statement responding the US act against pro-Iranian websites.

- The seizure of websites by the US also received reactions from other Pro-Iranian militias from Iraq such as "**Katib Hizballah**", which published a few visuals with criticism towards the US. In one example it said that "*The new American deterrence equation: No to freedom of expression"* (See picture below) and in another: "*The voice of truth terrifies them*" (see picture below).

Left: The new American deterrence equation: No to freedom of expression; Right: The voice of truth terrifies them.

- **Hezbollah** leader **Hassan Nasrallah** commented on the seizure of the website as well in a speech: *"The media* sites *that were seized by the American administration had a great role in solidarity with Palestine and had a position on American hegemony and a position on sedition and takfiris- The American decision to block these sites reveals the falsehood of the allegations of the successive American administration about democracy and freedom of opinionWe express our condemnation and condemnation of the American media aggression against media outlets belonging to the culture and axis of the resistance-"*[16]
- In April 2021, the IRGC posted about an alleged cyber attack by Iranian hackers of Israeli and US doctors. The campaign was attributed to "**Charming Kitten**", an Iranian hacking group aligned with the IRGC. The group used phishing tactics in order to target the medical personnel.[17]

[16] AL-Manar
[17] https://www.proofpoint.com/us/blog/threat-insight/badblood-ta453-targets-us-and-israeli-medical-research-personnel-credential

Post on the IRGC Telegram channel about a cyberattack on U.S. and Israeli doctors

Case Study: Op-Israel 2021 – Operation Guardian of the Walls

The riots that erupted in sheikh Jarah during Ramadan 2021, coupled with other central memorial days such as Nakba Day, Iranian Jerusalem Day, and the Israeli Jerusalem Day escalated the situation between Israel and Gaza that culminated with Operation Guardian of the Walls. Cyber space users sprang to action and groups of hackers around the world announced a wide scale cyber campaign against Israel under the title OpIsrael. The attacks were launched against Israeli government and civilian targets.

OpIsrael cyber-attacks take place annually on April 7th, since 2013. The first campaign launched in tandem with the Holocaust and Valor Memorial Day (that in 2013 took place on April 7th)[18]. Anonymous who led the campaign claimed that the campaign launched due to "Israeli disregard to warnings regarding the rights of Palestinian citizens"[19].

Since 2013, annually, every April 7th sees a wave of cyber-attacks against Israel under the headline OpIsrael Birthday. The scope of the attacks varies in correlation with the security situation

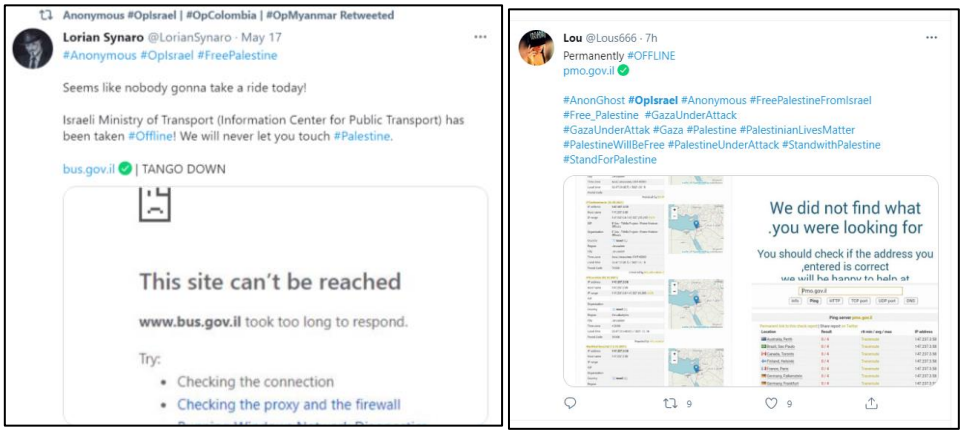
[18] Op-Israel 2017, Cyber Desk. ICT. Retrieved: file:///C:/Users/Dell/Downloads/Op_Israel%20(4).pdf
[19] Cyber-Terrorism Activities Report No. 7 December 2013 - January 2014. ICT. Retrieved: https://www.ict.org.il/UserFiles/Cyber%20Report%207.pdf

between Israel and the Palestinian. In recent years one can also observe campaigns under the headline Op-Jerusalem which is mostly identified with the Iranian Jerusalem Day.

OpIsrael 2021 was planned for its annual April 7th date however the escalation between Israel and Gaza led to wide scope and high intensity attacks that continued through May and culminated in Operation Guardian of the Walls. The cyber-attack campaign was launched by Anonymous via a clip on Twitter where they claimed: "Greetings world, we **will fully support Palestine that suffers from the Israeli attacks and its oppressive policies**…it is time to pay the price…Anonymous announces a cyber campaign against Israel and the Zionists…**we are one…in solidarity with Palestine, they need our help, you don't have to be Muslim to support them, only human…**".

The attacks during OpIsrael 2021 included website defacement, denial of service, information leaks, hacking into social media accounts of Israeli citizens, hacking into security cameras, taking over news casts, doxing, media campaigns and more. While one cannot determine the exact scope of the cyberattacks that were perpetrated, there is no doubt that the incitement and media campaigns carried out against Israel had a significant impact.

Most of the attacks associated with OpIsrael focused on defacing websites and denial of service from governmental and civilian web sites. Reviewing the list of websites posted by the hacktivists provides two major insights: **(i) the hacktivists aim at garnering media attention and reverberation of their messages by attacking high quality targets**, i.e. official Israeli government web sites. It is clear that most of the damage to these web sites was in the form of denial of service and allegedly taking them off the internet; **(ii) Posting long lists of web sites with the suffix co.il that the hacktivists claimed the hacked into point to an attempt to create a media buzz regarding the number of web sites haked into,** even though, de facto, in many cases breaking into one host server may grant access to several web sites that are hosted on it.



Examples for responsibility claiming for attacking web sites including the prime minister's (Twitter)

Defacing websites provides a platform to hacker groups to list the rationale for the attack by claiming responsibility for the attack on the defaced web site's landing page. For example, AnonGhost posted the same message in all of their attacks as follows: "we are the voice of Palestine and we will not be silent, we are the voice of forgotten groups, freedom fighters in cyber space and our main goal is the Zionists and Israel and if you ask why your web site has been broken into? It is because we want to convey our message to the world….Muslims are everywhere…remember that…. We will enter Palestine shortly".

Right: Hacker group Palestine Cyber claiming responsibility for attacking Israeli web sites;

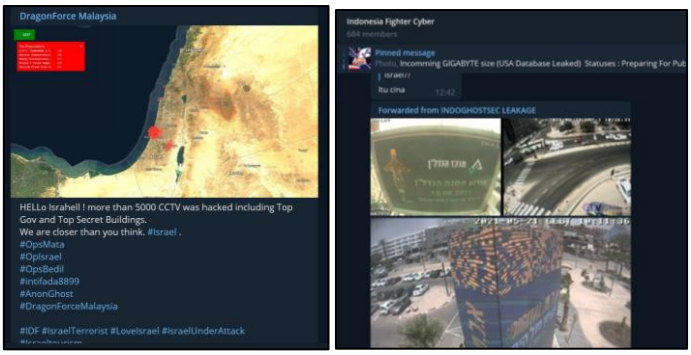
Left: AnonGhost claiming responsibility for defacing web sites

Another modus operandi providing a high-quality target for hacktivists perpetrating cyberattacks against Israel, OpIsrael 2021 included, is hacking into **Israeli news channels**, and posting Palestinian propaganda. Throughout May 2021, hacktivists claimed they broke into Israel's main news channels including channel 13 Reshet, Kan 11, the Knesset channel and posted Palestinian propaganda which later was disseminated on social media.

Examples for claims of break into Israeli new channels

Beyond flexing offensive muscles in cyberspace there has been virtually no damage to Israeli infrastructure or tactical assistance to Hamas. Per AnonGhost, the goal of their attacks was "to convey the message to the world", i.e. **the attacks against Israel are part of a perception campaign against Israel**.

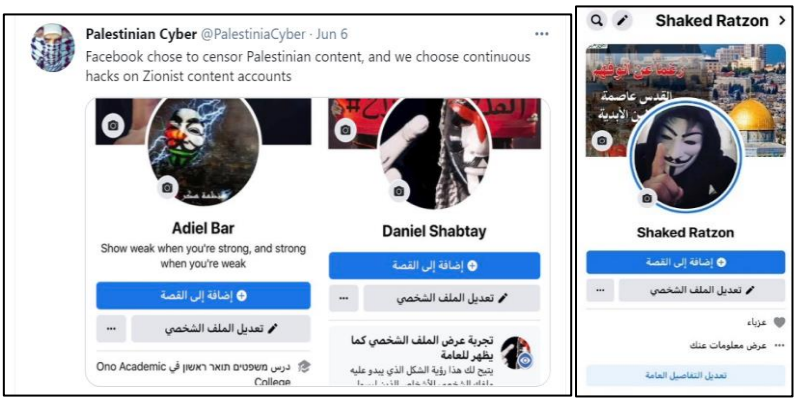
Within this framework the hackers aimed to convey to Israeli citizens that **Israel in its entirety is a Home Front and (even though they don't overtly say so) every Israeli is a target and isn't secure even in his home, whether the case is breaking into a security camera, hacking social media account, Gmail account etc.** For example, during the campaign, the Malaysian hacker group Dragon Force and AnonGhost posted on Twitter and Telegram photos of Israeli citizens in their homes. In another case the Indonesian hacker group Indonesia Fighter Cyber posted photos taken off Israeli homes' security cameras



Right: claiming responsibility for breaking into home security cameras;

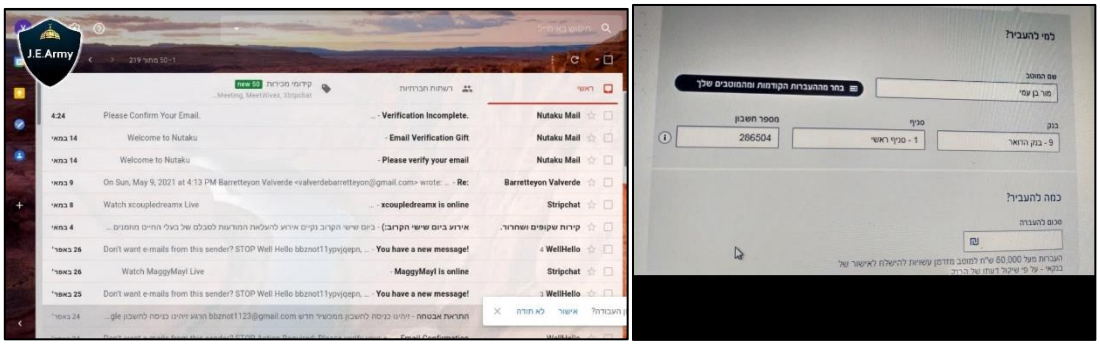
Left: photos from security cameras in commercial areas on Israel

In yet another case, Palestine Cyber claimed responsibility for a series of attacks on Facebook accounts of Israeli citizens. On their Twitter page they claimed that "Facebook chose to apply censorship to Palestinian content therefore we will keep breaking into Zionist accounts and content". In most of the breaches of Facebook accounts of Israelis Palestine Cyber replace the profile picture with a photo that is identified with Anonymous and a background of Jerusalem.



Break into Israeli citizens Facebook accounts

Palestine Cyber also claimed it attacked an Israeli citizen's bank account. In this case, this is a singular incident whose credibility has not been established. Similarly, it has been claimed that attacks were allegedly perpetrated by J.E. Army during 2020. In the wider context, **J.E. Army** claimed responsibility for breaking into email accounts of Israeli citizens.



J.E. Army claims responsibility for attacking a Gmail account; Left: a photo of an alleged Palestine Cyber attack on an Israeli bank account

Recently, doxing has been a rising trend among hacktivists. Doxing is the publication of a person's personal details, inter alia, to encourage cyber attacks against them. For example, during Operation Guardian of the Walls, doxing was performed on Israeli senior officials among them prime minister Benjamin Netanyahu whose personal details as well as his teams were posted on

Telegram and Twitter by the Indonesian Ghost Security Group. It should be noted however that the information posted was mostly already readily available to the public.

Posting prime minister Netanyahu and his team's personal details (Twitter, Telegram)

In another case, the IDF spokesperson was doxed by GhostSec. In addition to bragging about their ability to obtain information on senior Israeli officials, the hacktivists also called for cyber attacks on said officials.

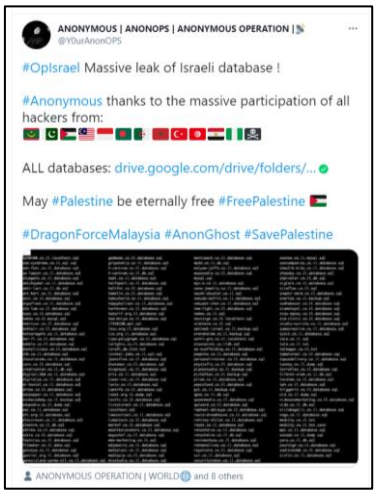
IDF's spokesperson's doxing by GhostSec

Another major effort during OpIsrael 2021 was **doxing Israeli citizens. The information leaked can be mostly found in databases breached by the hackers**. During the wave of attacks there were many such leaks, mostly information that saw light on web sites such as Pastebin or an open Google Drive folder. For example, the Malaysian group Dragon Force leaked information about Israeli citizens Facebook accounts.

Other hacktivists endeavors included "reports" to Facebook on Israeli citizens who were "active" in assisting Israeli propaganda efforts. In their "reports" they asked their supporters to complaint that the Israelis disseminated fake news. As can be seen below Dragon Force called to report an Israeli citizen that posted the banner Israel Under fire that is identified with Israeli propaganda

.

In the post announcing the end of OpIsrael 2021 on Twitter, Anonymous' operations department credited hackers from different countries and wrote that "all of Palestine shall be free". Additionally, they posted a leak to all data bases leaked during the campaign



OpIsrael 2021 ending banner

Despite announcements about the end of the campaign, some actors continued the anti-Israeli activity, mostly in the media. For example, the Muslim Cyber Army organized a Twitter Storm on June 6th, 2021, when it called on its followers to upload posts under the hashtag #FreePalestine in order to spark a discourse on the issue. Some of the supporters were diverted to landing page identified with Anonymous where they were required to copy a post and upload it with various hashtags.

Right: a call for a Twitter Storm; Left: a request to copy a post to Twitter with various hashtags

In another case, there was call to hacktivists on Telegram to post to social media a banner claiming that "Israel violated the truce" to spark a discourse on the subject.

OpIsrael 2021 was at its core a propaganda campaign against Israel aimed at assisting Hamas and the Palestinians on social media. Claiming responsibility for cyber-attacks was almost always under the OpIsrael hashtag and other Hamas identified hashtags such as #FreePalestine and #gazaunderfire. The above is also manifested in the style of the attacks and the selected targets as well as the wording of the responsibility claiming messages. The end of Operation Guardian of the Walls doesn't guarantee the end of cyber attacks on Israel, especially in light of the ongoing tensions between Israel and the Palestinians. The aforementioned groups operate in varied intensity against Israel on a day-to-day routine however it is safe to assume that a cyber campaign in the scope observed during OpIsrael 2021 will likely occur only on future OpIsrael anniversaries as well as future hostility rounds between Israel and the Palestinians.

International Response

Colonial Pipeline Attack

On May 7th, 2021, Colonial Pipeline, an oil system in the United States, suffered a ransomware attack. The attack had tremendous impact, resulting in a declaration of emergency in 17 states by the Federal Motor Carrier Safety Administration (FMCSA). The attack was the largest cyberattack in history on oil infrastructure in the United States. The hackers were identified as a hacking group called DarkSide.

- In May 2021, following the ransomware attack on the Colonial Pipeline, U.S. President Joe Biden signed an executive order with the intent to improve cybersecurity in the United States.[20]
- In May 2021, following the attack on the Colonial Pipeline, two new bills were introduced in the US. One of the bills calls for the TSA to update pipeline security guidelines within a set timeframe along with increasing congressional involvement in certain matters. The other bill is called CISA Cyber Exercise Act. This bill details the creation of a national cyber exercise program and calls for CISA to help agencies assess the state of cybersecurity of critical infrastructure within their jurisdictions.[21]
- In June 2021, following the attack on the Colonial Pipeline, the Transportation Security Administration (TSA) began working on a cybersecurity directive for pipeline companies. The directive aims to tighten and improve cybersecurity measures.[22]

Legislation, Policy, and Regulations

- In April 2021, US President Joe Biden signed an executive order aimed at improving the government's ability to evaluate and respond to cybersecurity incidents and to promote better defense methods in the cybersecurity realm. [23]
- In April 2021, legislation was introduced in the U.S. to create a program designed for civilians to help act against hackers. The The Civilian Cyber Security Reserve Act is meant to help defend critical infrastructure from various types of cyber threats. The reserve program would provide training to civilians who would then be capable and available to help the U.S. government agencies in their cybersecurity efforts. [24]
- The European Council of the EU extended the framework for sanctions against cyberattacks that threaten the European Union and its member states until May 2022. The

[20] https://www.usnews.com/news/national-news/articles/2021-05-12/biden-signs-cybersecurity-executive-order-following-colonial-pipeline-ransomware-attack

[21] https://slotkin.house.gov/media/press-releases/cyber-threats-grow-slotkin-introduces-bill-boost-preparedness-us-businesses-and

[22] https://thehill.com/policy/cybersecurity/558606-tsa-working-on-additional-pipeline-security-regulations-following

[23] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[24] https://thehill.com/policy/cybersecurity/550802-lawmakers-introduce-legislation-to-create-civilian-reserve-program-to

Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities was introduced in 2017 and it allows EU member states to take certain measures against cyberattacks, including to prevent and respond to malicious cyber activities aimed at harming EU member states.[25]

- In June 2021, U.S. lawmakers introduced several bills related to cyber security. A Senate bill, the International Cybercrime Prevention Act, increases the criminal penalties for attackers who target U.S. critical infrastructure. The House introduced a separate bill, called the Enhancing K-12 Cybersecurity Act, which provides funding to protect school district networks. An additional bill, the Data Protection Act, details the creation of a federal agency to protect Americans' private data.[26]
- In May 2021, the British government announced that they would be taking more offensive action against rogue states and ISIS terrorists. The focus is on shutting down the ability of ISIS to spread propaganda. Britain also declared £22 million ($31m) in funding to help a several African countries start joint operations against cyber crime in Africa, as an action in response to the emergence of extremists in the region.[27]

Government and Critical Infrastructure

- In June 2021, The U.S. Department of Justice increased the priority of investigations of ransomware attacks to the level of terrorist threats as a reaction to the Colonial Pipeline and other recent cyber threats.[28]
- In June 2021, CISA introduced a vulnerability disclosure program that allows hackers to report security bugs to U.S. federal agencies.[29]

---

[25] https://www.consilium.europa.eu/en/press/press-releases/2021/05/17/cyber-attacks-council-prolongs-framework-for-sanctions-for-another-year/#:~:text=The%20Council%20today%20decided%20to,year%2C%20until%2018%20May%202022.&text=Additionally%2C%20EU%20persons%20and%20entities,funds%20available%20to%20those%20listed.
[26] https://www.bankinfosecurity.com/lawmakers-unveil-cybersecurity-legislation-a-16918
[27] https://www.thenationalnews.com/world/europe/britain-to-harness-new-cyber-powers-in-pursuit-of-hostile-states-and-terrorists-1.1221731
[28] https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/?&web_view=true
[29] https://techcrunch.com/2021/06/08/cisa-launches-platform-to-let-hackers-report-security-bugs-to-us-federal-agencies/?&web_view=true

- In June 2021, several members of the North Atlantic Treaty Organization (NATO) approved a new cyber defense policy which included a decision to use Article 5 of the North Atlantic Treaty on a "case-by-case basis" involving cyberattacks on NATO members. Article 5 states that if a NATO allied nation is attacked, other members would consider it an attack against all NATO nations and will respond accordingly.[30]

Geopolitics and Terrorism

- In April 2021, the U.S. expelled 10 Russion diplomats and imposed sanctions against a number of Russian companies and individuals for hacking federal agencies and interfering in the last U.S. presidential elections.[31]
- In April 2021, Iran updated its national budget to include an extra $71.4 million for cyberspace operations, in particular of two government controlled organizations in Iran's media sector.

  The bulk of the added budget is designated for the Islamic Republic of Iran Broadcasting (IRIB) agency's "cyberspace activists" program. The rest of the additional funds were allocated to the "cyber section" of the Islamic Development Organization (IDO).[32]
- In June 2021, G7 leaders published a comunique emphasizing their commitment to combatting ransomware attacks, stressing that cyber-criminals represent an extremely significant threat. [33]
- In June 2021, the United States seized 33 websites of the Iranian Islamic Radio and Television Union (IRTVU), which has been designated as a Specially Designated National (SDN) since it is controlled by the IRGC. They also siezed three websites operated by Kata'ib Hizballah (KH), which violated U.S. sanctions.[34]

---

[30] https://thehill.com/policy/cybersecurity/558383-nato-member-states-agree-to-new-cyber-defense-policy-following?&web_view=true
[31] https://apnews.com/article/us-expel-russia-diplomats-sanctions-6a8a54c7932ee8cbe51b0ce505121995?&web_view=true
[32] https://therecord.media/iran-updates-budget-to-allocate-71-4-million-to-cyberspace-operations/?web_view=true
33 https://www.infosecurity-magazine.com/news/g7-turns-up-heat-putin-ransomware/?&web_view=true
34 https://www.justice.gov/opa/pr/united-states-seizes-websites-used-iranian-islamic-radio-and-television-union-and-kata-ib

ABOUT THE ICT

Founded in 1996, the International Institute for Counterterrorism (ICT) is one of the leading academic institutes for counterterrorism in the world, facilitating international cooperation in the global struggle against terrorism. ICT is an independent think tank providing expertise in terrorism, counterterrorism, homeland security, threat vulnerability and risk assessment, intelligence analysis and national security and defense polic

ICT is a non-profit organization located at the Interdisciplinary Center (IDC), Herzliya, Israel which relies exclusively on private donations and revenue from events, projects and programs.

ABOUT ICT CYBER-DESK

The Cyber Desk Review is a periodic report and analysis that addresses two main subjects: cyber-terrorism (offensive, defensive, and the media, and the main topics of jihadist discourse) and cyber-crime, whenever and wherever it is linked to jihad (funding, methods of attack).

The Cyber Desk Review addresses the growing significance that cyberspace plays as a battlefield in current and future conflicts, as shown in the recent increase in cyber-attacks on political targets, crucial infrastructure, and the Web sites of commercial corporations