



# Trends in Cyber - Terrorism 2021

ICT CYBER DESK



**Reichman  
University**

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

**January 2022**

## About International Institute for Counter-Terrorism (ICT)

---

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

## About ICT Cyber Desk

---

The Cyber Desk addresses the growing use terrorist's organization online. Quarterly reports are published on ICT website and include recent information on terrorists' organizations and hacker groups use of the operational arena, the defensive arena and the offensive areas.

### Cyber Desk Team

**Dr. Eitan Azani**, Director of Research & Head of the Cyber Desk, ICT

**Dr. Michael Barak**, Head of Jihadi Websites Monitoring Desk and Palestinian Desk, ICT.

**Dr. Liram Koblentz-Stenzler**, Head of the Global Far-Right Extremist Desk, ICT.

**Ms. Yehudit Shuter**, Researcher in the Cyber Desk, ICT.

**Ms. Daniel Habermeld**, OSINT & Counter-Terrorism Analyst, ICT.

## Table of Content

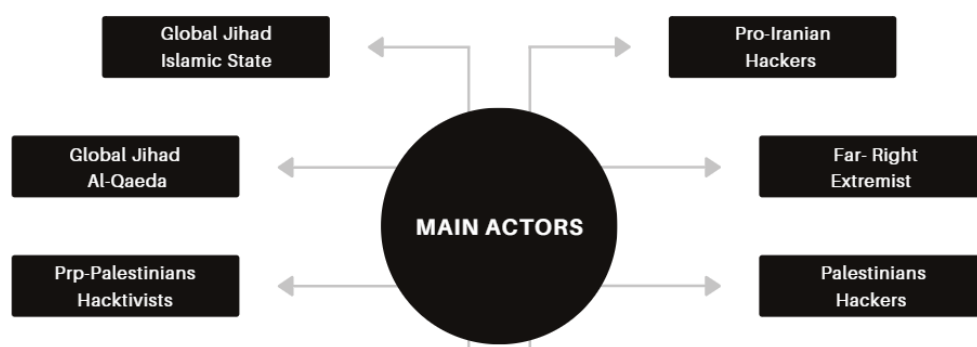
<b>General Overlook</b> .....	4
<b>Global Jihad in Cyber Space</b> .....	7
Trends in the Operational Arena .....	7
<i>Use of Platforms</i> .....	7
<i>Propaganda, Recruitment and Fundraising</i> .....	9
Trends in the Cyber Defensive Arena .....	16
Trends in the Cyber Offensive Arena .....	18
<b>Pro-Iranian Hackers</b> .....	21
Trends in the Operational Arena .....	21
Trends in the Defensive Arena .....	23
Trends in the in the Offensive Arena .....	24
<b>Palestinians Hackers and Pro-Palestinians Hacktivists</b> .....	26
Trends in the Operational Arena .....	26
Trends in the Defensive Arena .....	28
Trends in the Offensive Arena.....	29
<b>Far-Right Extremism in the Cyber Space</b> .....	31
Trends in the Operational Arena .....	32
<i>Use of Platforms</i> .....	32
<i>Propaganda, Recruitment and Fundraising</i> .....	32
Trends in the Defensive Arena .....	35
Trends in the Offensive Arena.....	37
<b>Outlook 2022</b> .....	38

## General Overview

Cyberspace has become one of the main arenas for state warfare. It is also **largely used by non-state actors or state sponsored actors, including criminal networks and terrorist organizations**. In recent years, their operations in Cyber Space have become a real challenge for global security.

**Throughout 2021 terrorist actors continued to operate in cyberspace in three main arenas – operational, defense, and offense. The operational arena** serves as the main arena used by terrorist organizations in cyberspace including the use of communication platforms, propaganda, recruitment, training, intelligence gathering, information sharing and financing. **The defensive arena** is designed to protect the anonymity of users and information security and to offer followers tips and warnings on cyber security. **The offensive arena** includes cyber-attacks, doxing, hacking tutorials, and hacking discourse.

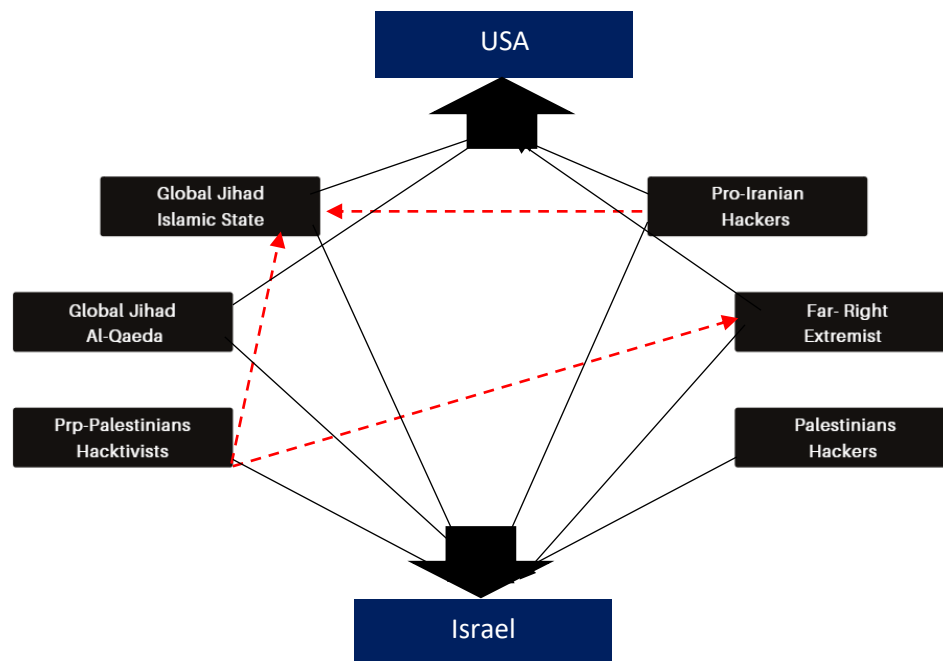
The main actors presented in the following report are: Global Jihadi organizations; Pro-Iranian hacker groups; Palestinian hackers and pro-Palestinian Hacktivists; and Far- Right Extremism.



**Main Actors monitored in Cyber Space**

Throughout 2021, we have seen complex developing relationships between the above-mentioned actors in cyberspace, such as: rivalry of pro-Iranian hackers against the Islamic State organization; and rivalry of Hacktivists against Far-Right extremist and Global Jihadi organizations. Even though these groups have attacked one another, they also have common enemies in the West, such as Israel and the US. A visual

depicting the rivalry and common enemy relationships can be observed in the graphic below.



**Main actors' rivalry map & common enemy**

Analysis of the main actors during 2021, showed an increase in activities in the offensive cyber arena, mainly by the pro-Iranian and pro-Palestinian hackers. In the cyber operational arena there was an increase of use by Global Jihadi organizations and Far-Right extremists. **Within this scope, there are common trends:**

### ***The Economic war Campaign***

Throughout 2021, terrorists **increased their operations against economic targets under the agenda of the Economic War, both in the physical arena as well as in cyberspace.** Within the physical arena, the Islamic State organization expanded their operation targeting electricity infrastructure, gas, oil facilities, and agricultural fields. The operation was also highlighted in an extensive online campaign documenting the attacks around the world.

In cyberspace we have observed an increase in attacking targets that symbolize or cause economic damage. Such examples can be viewed in cyber-attacks on Israeli banks system by pro-Palestinian hacktivists or conducting ransomware attacks against Western private sector companies by pro-Iranian hackers.

### ***Terrorism – Crime Nexus: Data Leaks***

Over the course of the year, it became clearer that terrorist actors also utilize the information they have gained from data breaches attacks for financial gain. This type of attack has two outcomes. First, it may paralyze systems or cause reliability problem for the target. Second, the hackers may profit from the attack by selling the information in hacking forums or criminal networks on the Dark web. Even if the information is not sold, the hackers might publish the information on their media channels exposing personal details or confidential information.

### ***Fundraising via Cryptocurrency Goes Darker***

Terrorists have been using cryptocurrency to raise and transfer funds for a few years now. Although they initially believed that their actions in the crypto world were private, counter-terrorism efforts and new regulation have proven them otherwise. During the past year, **terrorist organizations and hackers showed less use of Bitcoin and found sanctuary in private coins such as Monero**. They have also taken caution and ceased displaying crypto addresses publicly. The address is only provided through private online chats, allowing them to selectively choose to whom they send the information.

***The following report will present the main trends seen in 2021 with each of the main actors – their activities in the operational, defensive, and offensive arenas.***

## Global Jihad in Cyber Space

During 2021, Global Jihadi organizations **continued to exploit cyberspace to the best of their abilities and to carry out their media Jihad Strategy** (fundraising, propaganda, recruitment, cyber-attacks etc.). Although many elements are operating to disable their online capabilities, Global Jihadi organizations **continue to survive and expand in the cyberspace, including in cyber offensive arena.**

The main organizations monitored by the ICT are the Islamic State and Al-Qaeda. Both organizations have formal and informal units working online. One of the main trends seen throughout the past year, is the **decentralization in Islamic State media operations, providing informal media institutions with greater legitimization.** Following the success of the Islamic State, **Al-Qaeda has also increased the number of its formal and informal media institutions.**

### Trends in the Operational Arena

#### *Use of Platforms*

Throughout 2021, the Islamic State and al-Qaeda made use of different online platforms with emphasis on communication platforms such as Telegram and Rocketchat (and Chirpwire, used mainly by Al-Qaeda). Furthermore, Global Jihadi organizations continued to use social media platforms as well, mainly Twitter and Instagram. Within this scope, there was an **increase in the use of Telegram Bots.** Global Jihadi organizations use Bots to expand their reach, challenge security measures and to provide varies information such as propaganda, news, links to other platforms and channels on Telegram.

Since the beginning of the year, Afaq (Electronic Horizons Foundation), which supports the Islamic State has been encouraging the use of a safer communication platform such as **Element**, *"depending on any platform like Telegram, Twitter and Facebook as primary platform is a bad choice."* In April 2021, Afaq developed a cloud platform based on Nextcloud intended for followers to utilize as a place to store propaganda

materials. They **also developed a new chat server** named S-chat on the Element platform 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 and was again opened in July under the Coffespot server.

Another **prominent trend is the attempt by Islamic State supporters to use a variety of new communication apps**. For example, accounts affiliated with Islamic State supporters on RocketChat have recommended the use of the GAB communications platform. Meanwhile, another user suggested the use of TamTam communication app and invited followers to join his channel on the app. The main agenda in using new apps is to find platforms that rarely have deletion campaigns and are less visible to security agencies.

Al-Qaeda and the Islamic State **also continue to explore options to create their own websites**. In 2021, the Islamic State opened various new websites, mostly managed by supporters. Some of the **websites also have an onion dark web address** due to ongoing cyber-attacks against them. Al-Qaeda supporters have also shared varies links to new websites, mainly based in Southeast Asia. In September, supporters of Al-Qaeda also opened a new central website named *sadaislam*, where they publish videos, general information and propaganda.



Al-Qaeda Sadaislam website

**Global jihad organizations also continue to create their own apps.** In July, NadayeHaq media which supports the Islamic State organization, published a new app that aims to provide Urdu language news about the Islamic State activities. The application runs on Android and can be downloaded via an APK file. In November, Annajiyah Media Center, an Islamic State supporter's media foundation, based in Indonesia, also published a link to download their new app. Al-Qaeda, Thabat News Agency, which disseminates news related to the activities of al-Qaeda affiliates in the various jihadist arenas, launched an app for mobile phones in July 2021.



**Banner of NadayeHaq's new App**

Al-Qaeda and the Islamic State have shown capabilities in creating safe havens online in order to avoid de-platforming campaigns by **creating independent websites, servers, and apps and maintaining them online.**

### *Propaganda, Recruitment, and Fundraising*

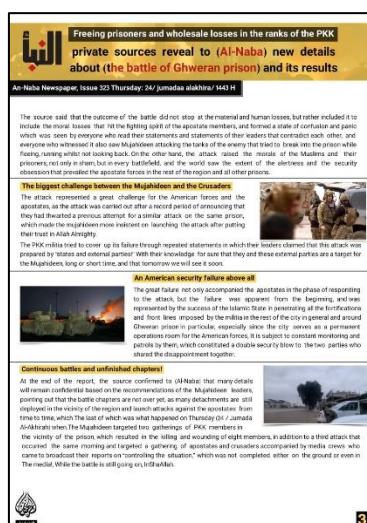
Throughout 2021, Global Jihadi organizations continued to disseminate propaganda online. For example, the Islamic State published various campaigns on their formal weekly online magazine - Al-Naba. One of the main campaigns focused on releasing prisoners under the title "We have not forgotten you." Following the announcements,

pro-Islamic State media outlets launched an extensive campaign on social media about the importance of releasing Muslim prisoners and Muslim women prisoners from enemy prisons such as Iraq, Syria, and other areas.



## Message from the Islamic State leadership in Al-Naba Weekly and Voice of Hind monthly in the Indian province on the importance of releasing Muslim prisoners from prisons under the headline "We have not forgotten you"

The campaign was proven effective also in the operational arena with the Islamic State battle of Ghwayran prison as the main highlight. The operation aimed at releasing prisoned members of the organization was successful, however for a limited time until many were captured or killed by Kurdish forces.



## Information on the battle of Ghwayran prison - published in Al-Naba magazine and translated to English

The second campaign was the "Economic War", which was first introduced at the end of 2020 in Al-Naba magazine. Operations within the scope of the Economic War included mostly attacking gas facilities, oil, and electrical infrastructure. While this phenomenon is not new, it has gained popularity in the Jihadi arenas and on the media platforms. Both campaigns, releasing prisoners and the Economic War, remain active in 2022.



#### Islamic State - Economic War Campaign

In May, a new campaign was launched in Al-Naba – "The Media War", that highlights the importance of Media Jihad alongside the physical battlefield. The campaign also provides legitimization for the ongoing Media Jihad 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, statements regarding unions between media institutions operated by Islamic State supporters have been posted on different platforms such as Telegram and RocketChat.



#### Islamic State - Media War Campaign

Another prominent media campaign was launched by Islamic State supporters towards the end of the year, under the title "Lone Wolf Incitement". The campaign encouraged lone wolf attacks in the West, mainly during the December holidays. Although this campaign was first introduced by Islamic State supporters, it received formal reference in Al-Naba in January 2022.



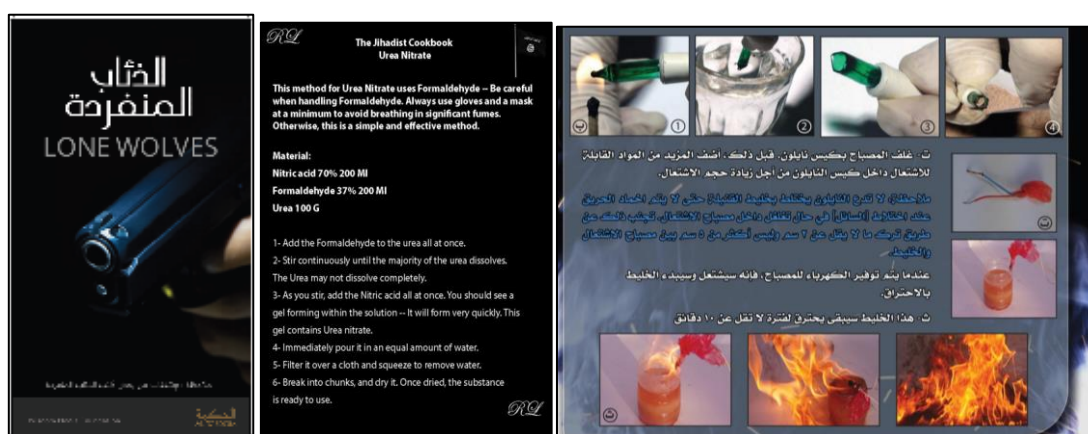
Islamic State supporters Incitement campaign

Al-Qaeda also published incitement campaign for lone wolf attacks throughout the year. The "Al-Malahem Cyber Army" group, which supports al-Qaeda in the Arabian Peninsula, published the second edition of the Wolves of Manhattan Magazine in which they called for **violence against police in the West**. In the magazine, the group offered to pay one Bitcoin, worth \$60,000, to every Muslim who murders a Christian policeman in Western countries.



Al-Malahem Cyber Army offers Bitcoin for lone wolf attacker

During the period under review, The Islamic State and Al-Qaeda published guides on how to conduct lone wolf attacks in the west, as well as tutorials on how to build weapons, detonators, and more from easily accessible materials. For example, 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. In another example, an Islamic State user on Rocketchat, published a guide to nitro-explosive and instruction how to create TATP.



From left to right: A short article advising Muslims living in the West to carry out attacks on Western targets; Jihadi cookbooks published by IS supporters online

**Recruitment efforts were also prominent during 2021.** For example, Al-Qaeda and the Islamic State published calls to join the **operation zone** in the India-Kashmir arena. Furthermore, **recruitment for media work** was also conducted mainly by the organizations' supporters, calling upon experts in graphics, social media managers, and bot engineers to join their ranks. **Recruitment for online media jihad by the Islamic State supporters' media institutions was also accompanied by advertising courses** such as beginners on the basics of design on Android devices and editing courses.

**The practice of financing terrorism through cryptocurrency has continued throughout 2021.** In January, the Islamic State organization ceased using many of its linked Bitcoin addresses and began using Monero private coin. The change came due to their understanding that Bitcoin is not untraceable. Afaq (Electronic Horizons Foundation), which supports the Islamic State, joined the organizational effort and published warnings and articles for followers and members, encouraging them to use

Monero. The trend gained popularity and throughout the year, funding campaigns used mainly Monero coin. This was observed through Arakan magazine funding efforts (Arakan is an unofficial foundation that supports the Islamic State), as well as on Islamic State websites, dedicating pages for soliciting donations.



Left: Afaq warning against using Bitcoin; Right: Arakan foundation funding campaign

Bitcoin continues to be used by Jihadists mainly in the territories under the control of terrorist organizations. For example, in Gaza, the Army of Ummah, a Salafi jihadist organization that supports al-Qaeda has been soliciting donations through online campaigns via Bitcoin throughout 2021.

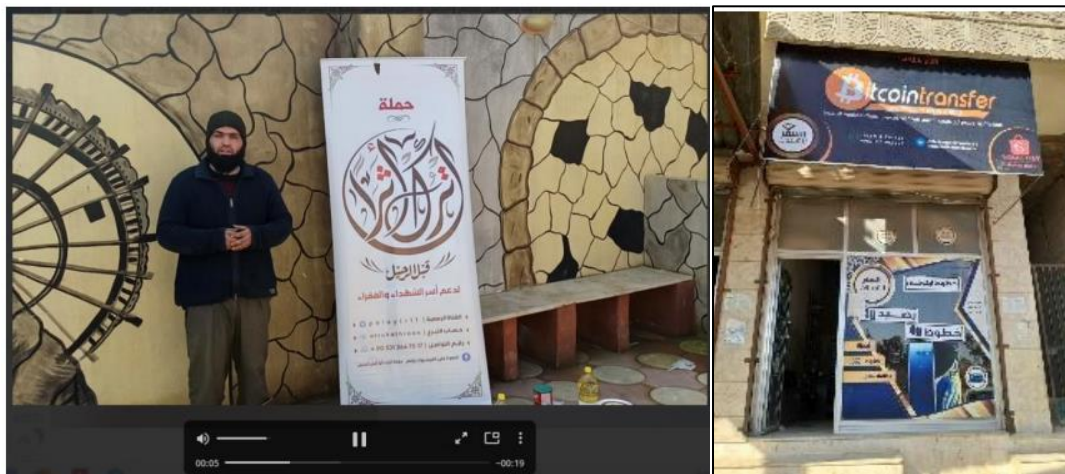


Online campaign of the Army of Ummah soliciting donation via Bitcoin

Hamas, which controls the Gaza strip territory, also uses Bitcoin and other cryptocurrencies for fundraising. In May, **donations spiked during Operation Guardian of the Walls**. In July 2021, the National Bureau for Counter Terror Financing of Israel (NBCTF) issued an order of seizure on multiple cryptocurrency accounts linked

to Hamas. Since then, some of the addresses decreased activities or ceased to be active.

Another prominent territory under Jihadist control is Idlib in Syria, which is dominated by Hay'at Tahrir al-Sham. Funding campaigns in this region are usually published in an attempt to raise funds by linking jihadists' charities. For example, In January-March 2021, jihadist activists in Idlib ran a financing campaign "to support the families of the martyrs and the poor" through the use of Bitcoin currency. Within this scope, there is also a crypto exchange office in Idlib which enable Jihadists in the region to exchange money without western regulations.



**Left: jihadist activists in Idlib ran a financing campaign; Right: Bitcoin exchange office in Idlib**

## Trends in the Defensive Cyber Arena

During 2021, Global Jihadi organizations continued to publish cyber security guidance. The main Islamic State security publications were issued by Afaq (Electronic Horizons Foundation) and al-Qiman Electronic Foundation. The foundations published guides, tips, and articles on technology, internet, funding etc. They have also published warnings against using apps and have recommended others. For example, announcement by Afaq in Arabic and English, warning against using the Hoopoe app while encouraging supporters to use Element. In another example, al-Qiman Electronic Foundation offered methods to check if your data on Facebook has been leaked.



Left: Al-Qimam user the check Facebook leaks; Right: Afaq warning against the use of Hoopoe app

A prominent trend during the year, was the **opening of new chat rooms on cyber security**. For example, on Chirpwire, Al-Qaeda opened a new chat named "The security workshop for Mujahideen", which gained popularity and currently also holds a closed Telegram channel. This trend is also visible on Islamic State platforms. One example is the new chat room named "Ansar Electronic Security" that was opened on Rocketchat. Within these chat rooms, articles on cyber security are published. The chat rooms also enable users to communicate their questions and remarks.



**Left: The security workshop of Mujahideen; Right: Ansar Electronic Security**

Throughout 2021, the Islamic State organization was subjected to a hacker's attack on their websites. The main attack was in May 2021 by Neo Cyber group, a pro-Iranian Shia hacker group from Iraq. The attack conducted on Islamic State linked supporters' website called Elokab. The attackers also **offered to sell the IP logs of the website users in exchange for Bitcoin**. The effect of the attack brought upon more caution in the use of websites and the Internet in general, including increased use of VPN and Tor. In August, Afaq (Electronic Horizons Foundation), which supports the Islamic State organization also issued an article titled "Security Threats: Website Hacking and the Way to Confront". The article explains the threat of hacking and why does penetration occur and how to face the threat of hacking.

In September 2021, Telegram users linked to the Islamic State and Al-Qaeda **experienced a deplatforming campaign**. In the aftermath of the campaign, there was extensive discussion on how to overcome these type of campaigns. Tips were given on how to use Telegram more safely. Other solutions were offered by users, such as to buy numbers or to use disposable numbers.

## Trends in the Offensive Cyber Arena

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.

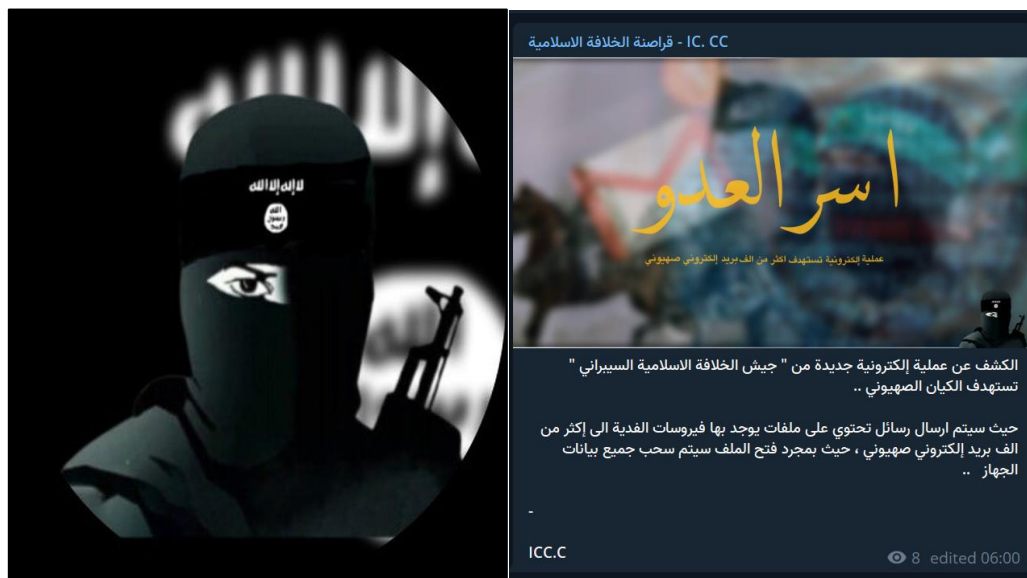
From the UCC remains a central active hacker group called Caliphate Cyber Shield (CCS). During 2019-2020 the group published activity summaries of cyber-attacks that it had carried out. In April 2021, the CCS allegedly carried out a cyber-attack against a port company website in France. However, since then, no information has been published about their activities. It should be considered that the formal list of the attacks of 2021 may be published in a summary in the first months of 2022.



Up: CCS allegedly carried out a cyber-attack against a port company in France; Left: Summary of the CCS activity during 2020; Right: Summary of the CCS activity during 2019;

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's 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.



**Cyber Islamic Caliphate Army threat to Israel**

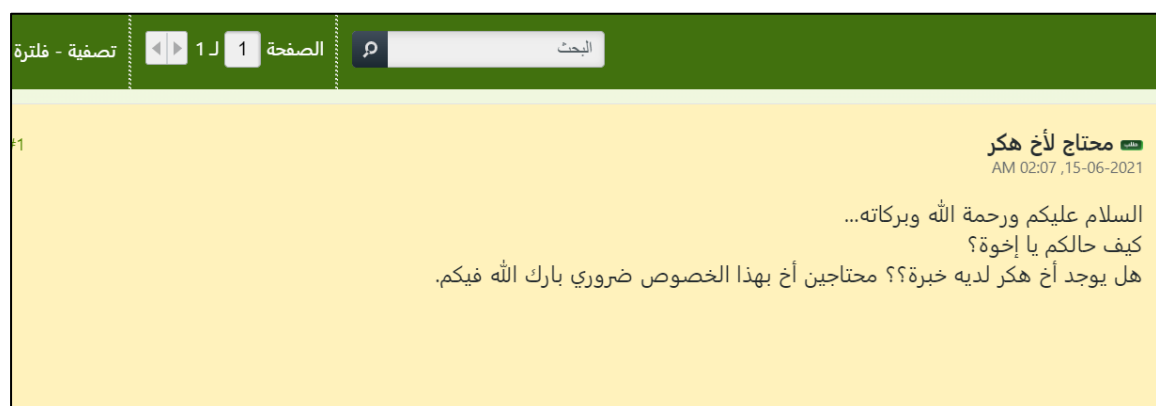
Although fewer cyber-attacks occurred by Global Jihadi hackers, there was an **attempt to re-create capabilities**. During 2021 both Al-Qaeda and the Islamic State published a call to **recruit hackers to join their online efforts**. Calls for hackers were published on social networks alongside other tech positions such as platform managers, bot engineers, and more. For example, al Malahem Cyber Army, which supports Al-Qaeda published a call for social media experts and hackers. In another case, Islamic State supporter's media foundation called for the recruitment of hackers to join their ranks.

The Islamic State also published a propaganda video documenting hacking into social media accounts in Iraq. The publication was most likely to promote recruitment of hackers, as no official hacker group was mentioned in the video.



Left: IS Recruiting Hackers on telegram Right: IS propaganda video documenting hacking

**Another prominent trend observed was the publication of hacking tutorials and discussions on hacking.** On the RocketChat platform, online discourse between Islamic State followers began to emerge on chat rooms, discussing ways to hack security cameras, providing links to hacking tutorials and more. In another example, Telegram account affiliated with the Islamic State has published a beginner's guide to hacking in the English language. In July, a user on Shumukh al-Islam forum (linked to the Islamic State) asked to consult a "hacker brother". Another user responded and asked him to contact him via ProtonMail.



Print screen from Shumukh al-Islam Forum – Brother hacker

## Pro-Iranian Hackers

During 2021 there was an **increase in cyber-attack operations conducted by pro-Iranian hacker groups**, primarily due to the wave of cyber operations by pro-Iranians Shia militias from Iraq. These groups are believed to be supported by the Iranian. Furthermore, in some cases, groups present state level capabilities that may indicate a deeper involvement in guidance and funding from Iran.

Pro-Iranian hackers and Iran share common enemies, hence many of the cyber-attacks conducted by these groups are against the West, mainly the US and Israel; Sunni governments such as Saudi Arabia; as well as the Kurds. Their operations are also conducted against the Islamic State media platforms.

Among the Pro-Iranian hackers are groups which identify with local conflicts/Iranian proxies, such as pro-Iranian Shia militias from Iraq that include Fatemiyoun Electronic Team and Neo Cyber; pro-Houthi actors from Yemen that include Yemeni Cyber Army; and Pro-Hezbollah Hacker groups that include Lebanese Cedar. There are also hacker groups which directly identify with Iran that includes, Charming Kitten, Bax 026 of Iran, Hackers of Savior and more. During 2021, new hacker groups linked to Iran appeared active against Israel, such as Black Shadow which conducted ransomware attacks, Moses Staff and Sharp Boys.

## Trends in the Operational Arena

Throughout 2021, pro-Iranian hackers **continued to use mainly Telegram, Instagram, Twitter, and Dark web websites to distribute propaganda and to publish their cyber-attacks**. Some of the groups also have YouTube channels and Tiktok accounts. Furthermore, pro-Iranian hackers continued to use symbols and pictures to indicate their affiliations with Iran and its proxies.



Left: Fatemiyoun Electronic team on Telegram; Bax 026 of Iran defacement announcement which include Qassem Sulimani's picture

One of the most prominent operational trends, is the emphasis these groups place on their followers. For example, Shia hacker groups from Iraq, the Fatemiyoun Electronic team and Neo Cyber opened Telegram channels for their supporters to discuss recent attacks and to provide them with security tips. *"To be closer to our followers, to help followers with digital issues and to help us clean the web of enemies"*. They also offered their followers to contact them via a dedicated bot. In some cases, the hacker groups also utilized followers for Intel. Such was the case for the Neo Cyber group that requested their supporters to find links to Islamic State social media platforms.

Most of the groups also publish propaganda aimed at their enemies. Propaganda threats aimed at Israel, for instance, were published in Hebrew.



Left: Moses Staff affiliation with Iran and a threat to Israel; Right: Neo Cyber threat to Israel written in Hebrew.

In the fundraising realm, most of the pro-Iranian hacker groups had no funding campaigns as we estimate most of them receive funding directly from Iran. However, at the end of 2020 and during 2021 a new set of pro-Iranian hacker groups appeared to be operating against Israel, conducting ransomware attacks on Israeli companies, and demanding Bitcoin in exchange for leaked information. Amongst these groups is Black Shadow, whose link to Iran was identified and published by the Israeli press. The group also opened a donation campaign on their Darkweb website and Telegram channels, soliciting funding via Bitcoin and Monero.



### Donation Page on Black Shadow website and Telegram

## Trends in the Defensive Arena

In the defensive arena, **pro-Iranian hacker groups continued to provide cyber security tips to their followers on their Telegram channels**. This may include, for example, warning against using apps or security tips on how to use the apps safely.

In June 2021, US seized Iran's affiliated news websites from the Middle East which are operating based on US servers' companies. **In response, cyber groups affiliated with the pro-Iranian Shia militias from Iraq, offered to host and protect Iran's affiliated websites and published recommendations for domains outside of the US.** The event highlighted the unified hand of Iranian proxies.



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

## Trends in the in the Offensive Arena

In the offensive arena, pro-Iranian hacker groups present different level of capabilities (Some with higher capabilities that may indicate Iranian involvement) and yet, **most of the attacks during 2021 continue to be DDOS and defacement of websites**. Such examples include defacement of US universities by Bax 026 of Iran; and DDOS attacks against Islamic State linked websites by the Neo Cyber group.

There was also a **rise in the defacement of social media accounts**. During the year the Fatemiyoun Electronic team claimed to deface linked account of the Islamic State on Instagram. In another case, Charming Kitten claimed to hack twitter accounts of Israeli and US doctors.



Left: Attack on Islamic State website by Neo Cyber; Right: attack on Islamic State Instagram accounts by the Fatemiyoun Electronic team.

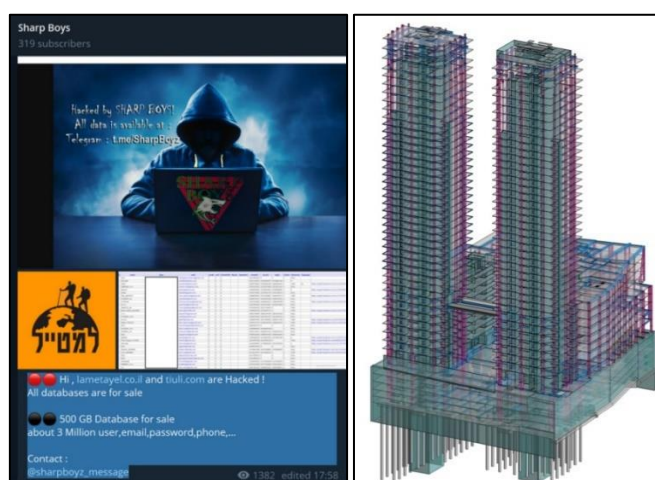
Another prominent type of cyber-attack that occurred during 2021 **was data leaks**. For instance, Neo Cyber hacked the Aramco in Saudi Arabia and leaked data, including information on refineries, contracts, maps, employee and customer data and more. In another example, The Fatemiyoun Electronic Team claimed responsibility for a breach of the database of KBR, a US based security company. Other database leaks comprised of Israeli citizens personal information as well as information on member of the Islamic State in Iraq.



Left: Information on Member of the Islamic State in Iraq; Right: The Aramco attack

At the end of 2020 and continuing through 2021, new pro-Iranian hacker groups began conducting ransomware attacks. **Most of the ransomware attacks were directed towards Israel and consisted of hacking to Israeli companies and websites.**

Among the main attacks were the Black Shadow cyber-attack on K.L.S. capitol, and on CyberServe. The latter provided them with sensitive information on users of the Atraf dating website, but users of Kavim, and more. After most of the attacks, the Ransomware groups demanded to be paid via cryptocurrency and when rejected, they published samples of the information online. Following the Black Shadow attacks, Moses Staff and Sharp Boys conducted similar types of attacks on finance and engineering companies in Israel and other popular websites such as "Lametayel". **Apart from the publications of the cyber-attacks, these groups also utilize the attack for propaganda against Israel, highlighting their terrorist agenda.**



Left: Sharp Boys attack on Lametayel website; Right: Data leak from of construction company.

## Palestinians Hackers and Pro-Palestinians Hacktivists

During 2021, there was an increase in cyber-attack operations conducted by **Palestinian hackers and pro-Palestinians hacktivist groups**. The attacks spiked during April-May 2021 during the annual **Op-Israel Anniversary and Operation Guardian of the Walls**. And again, in December 2021, after Bedouin riots broke out in southern Israel.

The main Palestinian hacker groups that operated during 2021 are Hamas cyber unit, Jerusalem Electronic Army (J.E. Army), Anonymous Palestine, Gaza Spider Gang, and Cyber Palestinian. **Although these groups play a key role, it is the hacktivist groups which support the Palestinians resistance that conduct most of the cyber-attacks** against Israel. Throughout 2021, the most active Pro-Palestinians hacktivists included, Stormous Hacker, Anonymous, Spider Team, Anonymous Islam, Yemen Ghost, Ghost Sec, Anon Ghost, Dragon Force Malaysia and many more.

Hacktivists distinguish themselves from hackers because they believe their actions may help raise awareness to human rights issues. As such, the groups mentioned above take part in other cyber operations in the world under their belief of human rights violations (such as Op-Colombia, Op-ISIS and more). While they believe to be operating "for the greater good", these actors don't necessarily verify facts or understand local conflicts. They are also subjected to online propaganda and often facilitate it by **conducting criminal and terrorist acts such as cyber-attacks and the distribution of fake news**.

### Trends in the Operational Arena

In the operational arena **Palestinian hackers and pro-Palestinian hacktivist groups continued to use Telegram as their main communication platform**. They also used Twitter and Facebook as well as running their own websites. **Most recently, they began using TikTok to present their cyber-attack videos**.

One of the main commonalities for all groups is the publication of their attacks on **social networks**. During Op-Israel 2021, for example, publications were coordinated in a similar way by using the same headlines and hashtags. In this way, they were able to facilitate negative discourse on social media against Israel.

The aforementioned groups **also continued to take part in Palestinian propaganda online, which includes distribution of fake news and threats to Israel**. For instance, analysis of Anonymous Palestine hacker group social media accounts during 2021 presented propaganda that identifies with Hamas. In another case, at the end of Op-Israel 2021, there were calls among the Hacktivist groups to create a "Twitter storm" under the hashtag #FreePalestine to stimulate discussion on the subject.



Left: Anonymous Palestine – Hamas propaganda; Right: fake news distributed by hacktivists during Op-Israel 2021

In other cases, Palestinian hackers and pro-Palestinian hacktivists groups **attempt to incite and encourage hackers to participate in attacks against Israel**. Throughout 2021, we observed publications of videos calling for attacks on Israel in cyberspace by Dragon Force Malaysia under the title "This is a call for all Hackers". **They also released a target list of Israeli banks and called other hackers to attack simultaneously.**



Left: Call by Malaysia Dragon force; Right: Call by Anonymous

## Trends in the Defensive Arena

Palestinian hackers and pro-Palestinian hacktivists **continued to share articles on cyber security and warnings on their websites and social networks and publish it on their media platforms.**



**Jerusalem Electronic Army warning on Telegram: Be careful not to log into your secret accounts from public networks and devices.**

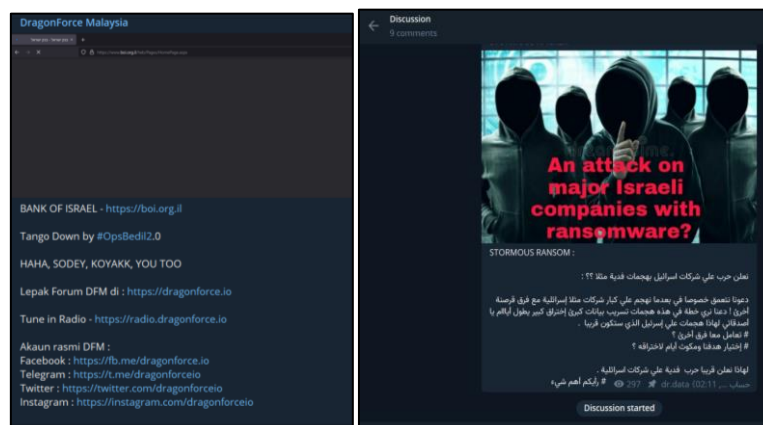
Another main trend was issuing **links to professional hacking tutorials and courses.** Many of the groups share the same links to professional Telegram channels and blogs which specialize in hacking.



**Left: Telegram post advertising a hacking course; Right: Telegram post advertising hacking courses**

In 2021, most of the cyber-attacks by Palestinian hackers and pro-Palestinian hacktivists against Israel consisted of defacement of websites, denial of service DDOS, data leakage, hacking into the social networks of Israeli citizens' accounts, hacking into cameras, taking over news broadcasts (two attacks during operation Guardian of the Walls), doxing of senior officials of the Israeli IDF and government, activities on social media and more.

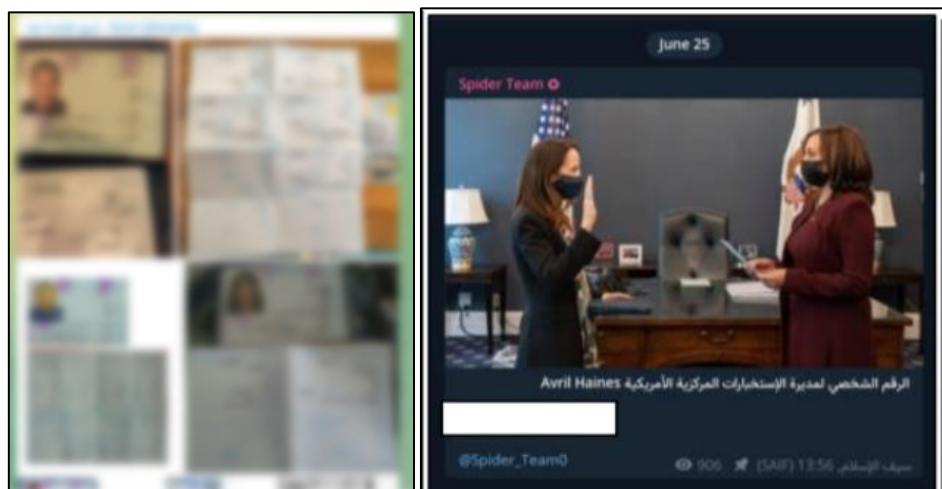
One of the ongoing trends among pro-Palestinian hacktivist viewed during the year, is the **economic damage these groups are attempting to cause Israel** by choosing targets such as Israeli bank systems and conducting ransomware attacks on Israeli hospitals and companies.



**Left: Cyber-attack on the Bank of Israel website, organized by Dragon force Malaysia; Right: Stormous Hacker ransomware claimed of attack (Telegram)**

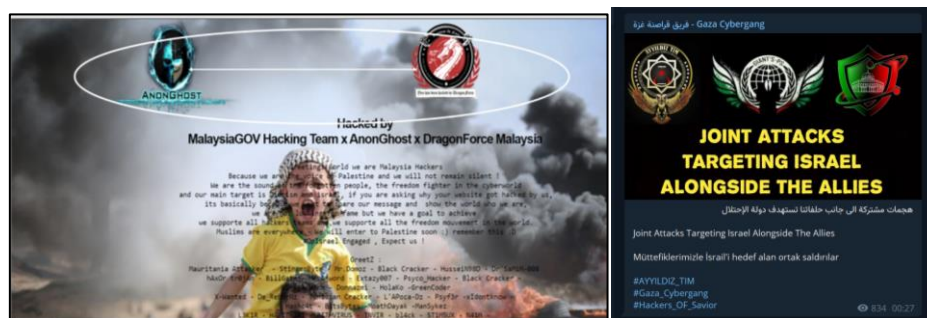
29

simultaneously by different groups, hence it is unclear which of the hacktivists conducted the cyber-attack. Most of the information consisted of ID cards, passports, driving licenses, and more. The same trend occurred with **doxing**, as it appeared **simultaneously on many of the groups'** media platforms. For example, in September, Gaza Cyber Gang released the data of Israeli citizens on their Telegram channel, although no responsibility for an attack was declared. In June, Spider-Team published doxing of CIA Director Avril Haines. (The publication was also present in many similar groups).



Left: Data leak of Israeli citizens ID Right: Doxing of CIA Director Avril Haines

Another key trend is the **cooperation amongst hacktivist groups in cyber-attacks against Israel** as seen in the backdrop of campaigns such as Op-Israel (some of them cooperate on a regular basis). Information regarding such cooperation is being posted either on the hacktivists' online platforms or defaced websites as seen in the pictures below.



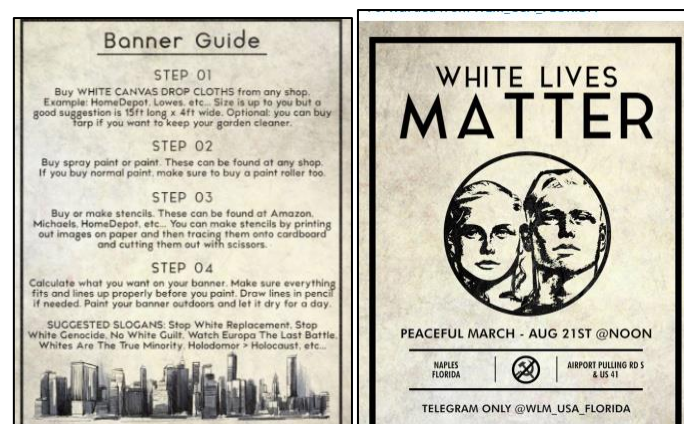
Examples of taking joint responsibility following a cyber attack on Israeli targets during OpIsrael 2021

## Far-Right Extremism in the Cyber Space

Throughout 2021, there was a **significant rise in far-right extremist activity around the world and in cyberspace**. One of the most pivotal events was the January 6<sup>th</sup> (2021) riots, where American far-right extremists stormed the US capitol. The violent event brought public awareness to the growing threat of far-right radicalization in the US and around the world.

The growing wave of far-right extremism online was highlighted throughout 2021 mainly by white supremacist organizations, conspiracy theorists, and anti-government organizations. Such organizations include Proud Boys, Oath Keepers, Qanon, Atomwaffen Division along with many others. While organizational activity is prominent among far-right online activities, nonaffiliated individuals are also visible and active on their discussion forums and communication platforms.

One of the key trends seen in 2021 within the far-right extremist strategy was **"localization", encouraging "cell" type of organizational structure**. At the same time, their strategy also focused on **"globalization" of online operations** via media platforms, focusing on cells' connections and the creation of grand movements. **The online arena continues to play an important role in facilitating the activities of these groups, organizations, and movements**, mainly by maintaining international connection via the cyber arena along with assisting in conducting mass events around the world such as the "White Live Matter" protest movement.



A post that teaches how to make posters with slogans of white supremacy

## Trends in the Operational Arena

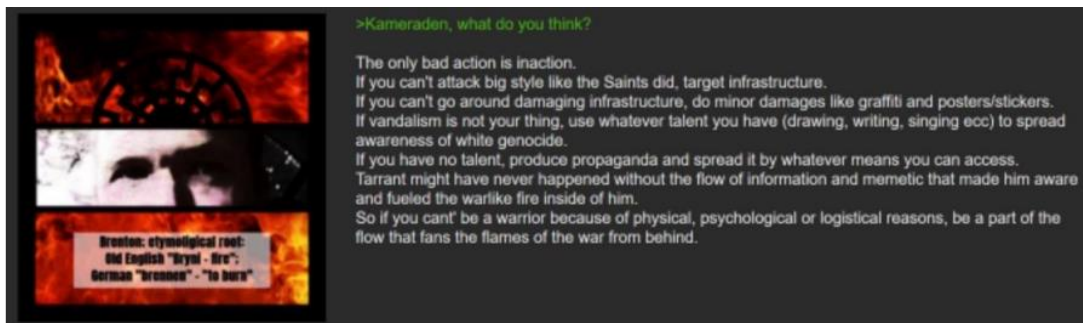
### *Use of Platforms*

In the operational arena, **far-right members continue to use** Telegram, Parler, Gab and Darknet imageboards as their main communication platforms. In July, a **new pro-Trump social media platform named Gettr** was established, aimed towards far-right members, and another one has been **announced to go live in the upcoming months** by Donald Trump, under the name Social Truth. A number of the far-right organizations also use Odyssey for video streaming as well as **websites** where they distribute propaganda and raise funds. While most propaganda distribution takes place in the aforementioned platforms, we have also witnessed an **increase in the use of video games as a platform to radicalize young crowds**.

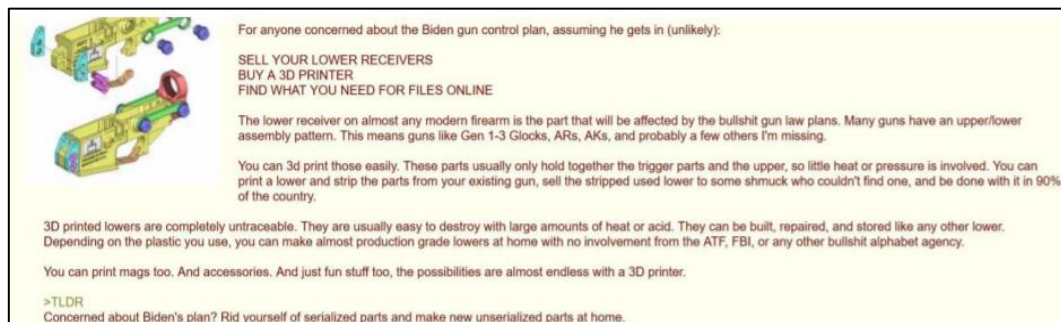
**The January 6<sup>th</sup> capitol riots and arrests in the aftermath of the event had a substantial effect on how far-right use online media platforms.** As such, many of their activities became more covert, **hiding in online safe havens in the deep web and dark web**. The change was also **demonstrated in the rhetoric used by these groups**, which became more coded and secretive.

### *Propaganda, Recruitment and Fundraising*

Far-right members continue to distribute propaganda, recruit, and fundraise for their cause. **Radicalization and incitement throughout the year focused on "taking action" and encouraging lone wolf attacks.** Targets were mentioned from the political sphere, security forces, far left wing Antifa, immigrants and supporters of the COVID19 vaccines. Inciters also published information **on how to conduct lone wolf attacks** using creative methods, such as **3d printers, as an ideal way to obtain arms**.

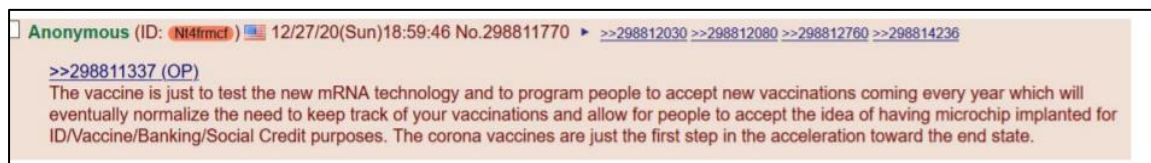


Encouragement of attack - post by a user on an imageboard on Darknet



Post advocating for the use of and providing instructions for construction of 3D printed weapon parts (4Chan, 29 November 2020)<sup>1</sup>

A prominent propaganda campaign during 2021, focused on spreading anti-vaccine rhetoric, publishing fake news and conducting mass protests around the world. These campaigns promoted accelerationism and conspiracies while inciting against the government and pro-vaccination figures.<sup>2</sup>



Post discussing how the COVID-19 vaccine is being used to condition the population to accept microchip implants (4Chan, 27 December 2020)<sup>3</sup>

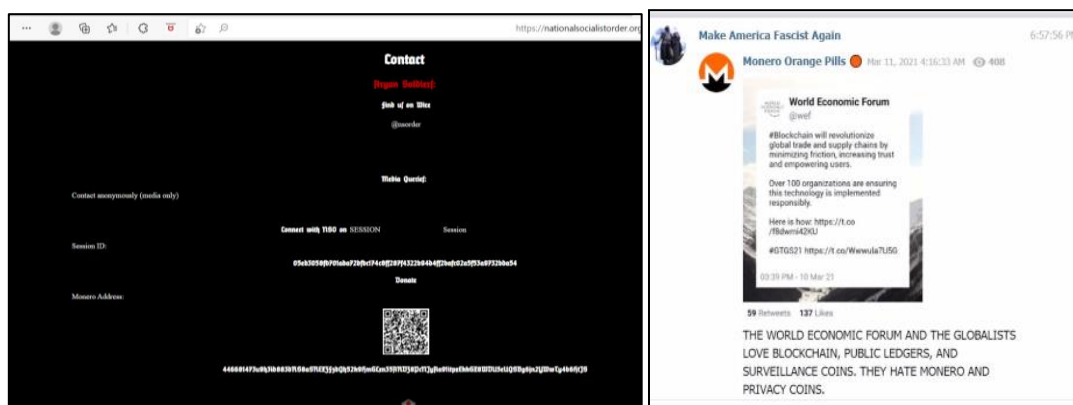
<sup>1</sup> Dr. Liram Koblenz-Stenzler, Alexander Pack (July, 2021) "Locked and Loaded: American Far-Right's Growing Interest in Homemade Firearms". <https://www.ict.org.il/images/Locked%20and%20Loaded1.pdf>

<sup>2</sup> Dr. Liram Koblenz-Stenzler, Alexander Pack "Infected by Hate: Far-Right Attempts to Leverage Anti-Vaccine Sentiment". <https://www.ict.org.il/images/Infected%20by%20Hate%20-02-03-2021.pdf>

<sup>3</sup> Dr. Liram Koblenz-Stenzler, Alexander Pack "Infected by Hate: Far-Right Attempts to Leverage Anti-Vaccine Sentiment". <https://www.ict.org.il/images/Infected%20by%20Hate%20-02-03-2021.pdf>

**Recruitment focused on calling to join or create local cells.** Among the attempts to recruit newcomers was **the trend of using "softer" rhetoric.** Such examples may be found in white supremacy groups that highlighted defense of the white race rhetoric rather than hate and racial rhetoric. Another "softer" way to recruit members seen during the year, is the use of **community type of activities to encourage people to arrive and later join,** such as meetings in gyms or for activities such as hiking.

**Fundraising** included the use of **cryptocurrency to solicit funds for jailed members' trials, training, preparation and more.** Most of the fundraising campaign via cryptocurrency were made **via Monero private coin. However, in some cases campaigns were made via Bitcoin.** Towards the end of the year, the Trump crypto coin was launched, gaining popularity with far-right members. Other prominent fundraising methods included **sale of merchandise and crowdfunding.**



**Left: National Socialist Order donation page on their website via Monero; Right: discussion on Monero benefits by Far-Right**

## Trends in the Defensive Arena

Throughout 2021 and following the January 6<sup>th</sup> riots at the US capitol, far-right extremists have been attempting to make their activity in cyberspace more secure and difficult to track.

Counter-terrorism efforts in the physical and online realm were not the only threat to far-right cyberspace activity. **Cyber-attacks by hacktivists and de-platforming campaigns** also played a key role in the far-right migration to more covert safe havens. Examples include the **cyber-attack on the Gab app exposing users, personal chats, and group discussions**. An additional example is the hacking into the **Epic web hosting company**, which was home to far-right platforms such as 8chan, the Oath Keepers website, and many more. Hacktivists also track and collect intelligence on far-right online platforms and provide information on their Telegram channels.

far-right organizations began warning and advising their members to proceed with caution in online forums. The suggestions included restricting any incriminating statements or conversations to private, preferably in person meetings and decrease information sharing via cyberspace.

**Another recommendation given by some of these groups was to “harden” their online profiles.** This entails limiting any personal information that could link the account to the person behind the account. Specific instructions ranged from updating privacy settings on social media platforms to suggesting members register for accounts through untraceable phone numbers. For example, In July, a post was distributed on a Telegram channel of white supremacy activists dedicated to the issue of information security. Among them was a guide that teaches how to avoid cell phone tracking. In September, a list of platforms that allow better encryption than Telegram was also distributed.

### Privacy & Security Goys

**Privacy & Security Goys**

Just in: Since 2016, jewish spyware targeted over 50,000 iPhones ... Unless you want Moshe Shekelstein tapping your phone, listening in on your conversations, and downloading pictures of your wife (meant for your eyes only), consider hardening your phones.


Enhanced privacy doesn't have to be exclusively for your boog phone after all!

<https://t.me/PrivSecGoy/355>  
<https://t.me/PrivSecGoy/201>

### Telegram

**Privacy & Security Goys**

Today I'm releasing a brief guide showing the steps involved in modifying a device to prevent spying via mic, camera, and light sensors. The steps in the guide will differ slightly from device to d...



**mod-phone.pdf**

23.5 MB

DOWNLOAD

10.6K 00:20

Leave a comment

As we continue to live under increasingly dystopian regimes, the need for secure communications is more vital than ever. Telegram has been a great resource and platform for disseminating information and content to racially conscious dissidents, but it certainly isn't perfect either.

Some [research](#) was done into which digital communication protocols are most ideal for our purposes. The top picks are as follows and are in no particular order:

- XMPP
- NextCloud
- Jami
- Briar
- Tox
- Kontalk
- Delta Chat
- Bitmessage
- Ricochet
- Status
- Scuttlebot

Session has not had an E2E audit completed yet, but not a bad choice

ō

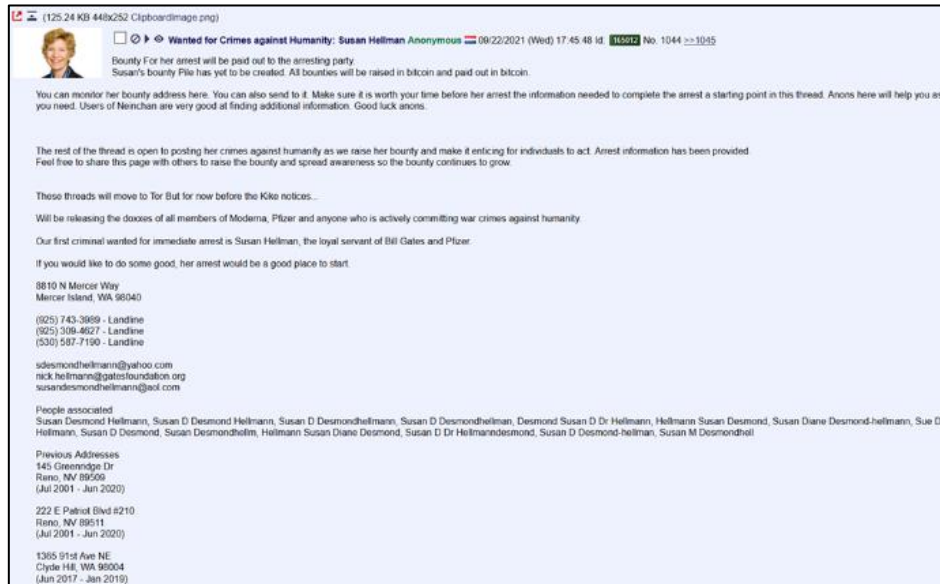
[Protocol for Synchronous Conferencing \(PSYC\)](#)

Matrix is *not* recommended, and not just because it's [jewish](#).

Left: better encryption than Telegram platforms; Right: guide that teaches how to avoid cell phone tracking.

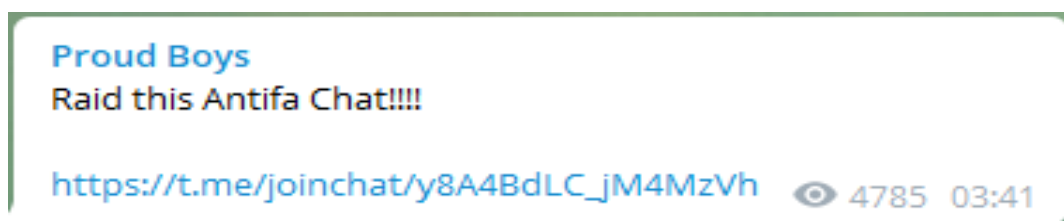
## Trends in the Offensive Arena

In the offensive arena, the main operation of far-right extremists continues to be **doxing**. In September, far right extremists took doxing to another level when they offered Bitcoin to those who would take action in attacking the specified targets.



Explanation of the target for DOXXING and the awarding of the "prize"

Another key tactic used in the offensive arena are **calls to corrupt the social networks**. The main target was of far-left activists such as Antifa under the title "**Raid Antifa chat**".



Call to raid Antifa chat on different Far right Telegram channels

## Summary and Outlook 2022

Terrorist groups continued to **seek safe haven in the deep web and dark web** as ongoing online counter-terrorism operations, de-platforming campaigns, and further planned regulation will most likely continue to develop and increase. They also analyze and adjust quickly to changes in the cyberspace; therefore, we will most likely observe **creative techniques to use even popular social media and communication apps**.

Global Jihadi groups which **focused on developing independent platforms** (apps, servers on matrix and websites), will most likely continue to **explore further possibilities**. Certainly, this will inquire them to enhance their recruiting campaigns, in search for professional staff to enable such actions.

**Recruiting efforts for hackers as seen by the Islamic State throughout 2021, will most likely remain a key mission during the next year.** While their cyber offence operational capabilities decreased since the collapse of the caliphate, the organizations have shown indication for **slowly organizing a new cyber offensive wing**.

In the funding efforts, Global Jihadi organizations were successful in understanding how to overcome cryptocurrency regulation and counter-operation by **changing the use of Bitcoin to less detectable private coin such as Monero**. This trend was also prominent with hacker groups and Far-right organizations online and most likely will play a key trend during 2022.

Terrorist organizations from a spectrum of ideologies continue to present lone wolf attacks as their preferred strategy in recent the year. This trend will most likely also continue during the year 2022, and may potentially escalate as online incitement might translate to physical acts of terrorism.