IDC HERZLIYA

ICT International Institute for Counter-Terrorism

With the Support of the Jusidman Foundation



Cyber Report

July-December 2020

Executive Summary *3*
Global Jihad *4*
Palestinian Organizations *22*
The Jerusalem Electronic Army (J.E. Army) **22**
Hamas - Izz al-Din al-Qassam Brigades **26**
Iranian and Shia hackers' Groups *27*
"Iranian/Persian Hacker" Group (a/k/a Bax 026): **27**
Cyber-Crime and Cyber-Terrorism *30*
Shirbit Attack: BlackShadow Group: **30**
Far-right Extremism *32*
International Response *44*
Geopolitics and Terrorism **44**
Legislation, Policy, and Regulations **46**
Government and Critical Infrastructure **46**

Executive Summary

During the period of July-December 2020 and throughout 2020, terror activity in the cyber arena has advanced and developed. Terrorist groups are utilizing cyberspace to achieve numerous objectives and are actively working to increase their cyber skill level in the operational, defense and offense arena.

The global pandemic of COVID-19 has exacerbated the presence of terrorism in cyberspace and allowed for greater opportunities for terrorist groups to commit cybercrimes and reach impressionable potential recruits. One of the main trends during the year of 2020 is the emergence of a motivated community of **Far-Right extremists** with mostly operational activity on the dark web (i.e. propaganda, recruitment etc.). These groups are attempting to shift from cyber space to physical activity but have not yet brought this intention to fruition. As long as this intention exists within these groups, we must not dismiss them as a potential threat. Throughout the period under review (July-December 2020), far right groups focused on US Elections, COVID-19 anti-vaccination campaigns, and mobilization to conduct lone wolf attacks.

During 2020, **Global Jihadists groups** continued to exploit cyberspace to the best of their abilities, such as for fundraising, propaganda, recruitment, and cyber defense. They are also actively working towards raising their cyber offence capabilities in order to transform their motivations into tangible cyber-attacks. Throughout the period under review (July-December 2020), ISIS and Al-Qaeda launched a campaign to recruit new hackers. They have also increased their use of cryptocurrency with an emphasis on using less detectible coins such as Monero. There has also been an increase of jihadi activity of social media, especially in the Idlib region.

While Global Jihadi groups are still on the run for Cyber offence capabilities**, Iranian hackers** have launched cyber war against Israel, USA and Western interests. Among them are a series of attacks against Israeli targets throughout 2020. Throughout the period under review (July-December 2020), a network of Iranian hackers with links to Hezbollah have been detected and traced on social network. The network claimed to have conducted cyber-attacks against Israel and US targets.

Palestinian hackers also stood out during 2020 claiming responsibility for attacks against Israelis critical infrastructure, communications sector, and Israeli citizens. Throughout the period under review (July-December 2020), the hacker group Jerusalem Electronic Army

(from Gaza) have claimed to carry out numerous cyber-attacks against Israeli targets, mainly defacement of websites.

The following report analyzes these trends over the period of July-December 2020.

Global Jihad

Operational

Terrorist organizations continue to use the Internet for a wide range of functions, including propaganda, recruitment, financing, and providing guides and tutorials. They do so through various media platforms, distributing their messages and guidance. Recent trends observed include a focus on encouraging potential recruits to study subjects related to computer science and hacking. Additionally, terrorist fundraising through cryptocurrency has become more difficult to trace as we have observed more precautions being taken by the terrorist groups in this regard.

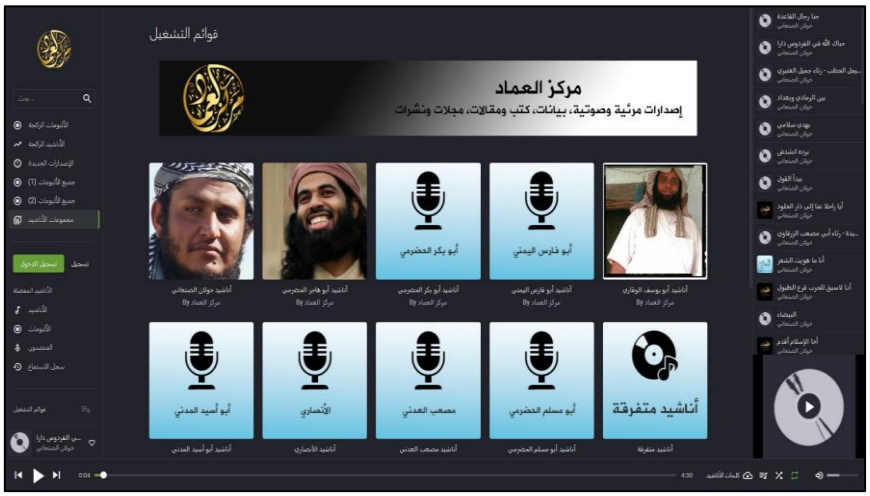
Propaganda

During the period of July-December 2020, ISIS and Al-Qaeda continued to carry out propaganda activities using different media platforms such as, Websites, RockChat, Telegram, Hoop, Twitter, Chipwire, forums, Threema and most recently Element.

There are many advantages to using the above platforms, such as allowing the jihadists to communicate through public channels as well as through private channels. Some of the platforms are encrypted, thus allowing administrators to choose who can view the published content. They have also been attempting to design a self-created platform.

- For example, in July 2020, Al-Imaad Communication Institute, which provides information for the benefit of al-Qaeda, has launched a website distributing propaganda materials such as videos, audio clips, articles, songs and more.[1]

[1] July 2020. https://emaad.net/VUVLT (The site is no longer active)



The "Al-Imaad" Website

- In another case, Thabath news agency, which reviews news related to the activities of al-Qaeda affiliates in the various jihadist arenas, has announced the launch of a special application for cell phones. According to the agency, the idea behind the launch was to completely disengage from social media networks, especially Telegram. This is due to the large scale of removal of its accounts and channels. According to the agency, the new application will be able to provide cell phones with news flashes and data about the scope of activity of the jihad operatives on a regular basis and without fear of the removal of accounts by the regulators.[2]

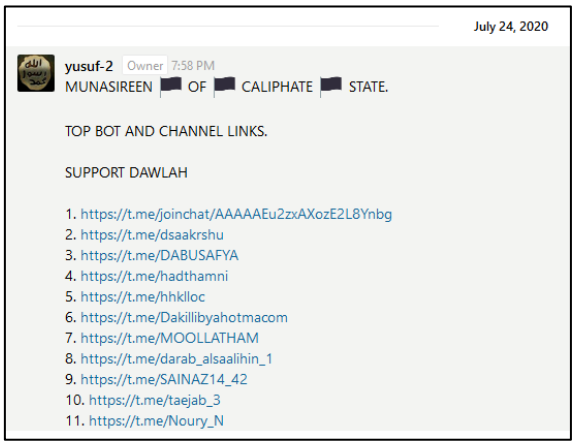


Announcement of the launch of an application for telephones called "Thabat Agency"

To gain greater media exposure, Jihadists continue to publish propaganda on various media platforms simultaneously. They are also known to publish updates of external links of their main media.

[2] September , Telegram

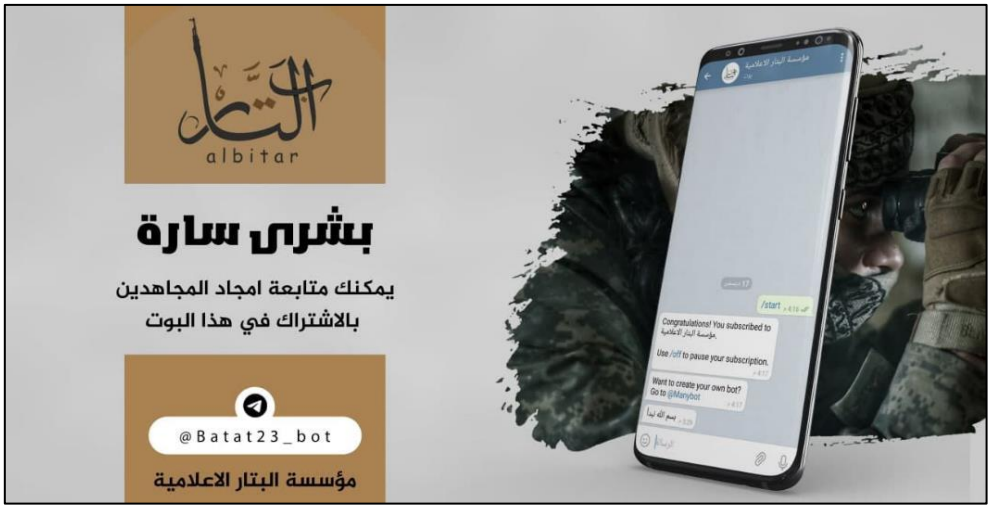
- For example, on July 24th, 2020, a participant on one of the ISIS channels in RocketChat published a list of bots on Telegram in order to distribute the organization's propaganda materials to a large number of users.[3]



List of bot channels on the Telegram for the distribution of ISIS propaganda materials

The use of bots on Telegram has become a powerful tool for the ISIS media department. The bot allows admins to update followers on new chat rooms, links to websites and contact information. Al-Qaeda has begun using bots as well.

- On December 2020, Al-Batar Communications Institution, which provides information to al-Qaeda, announced the launch of a bot on the Telegram through which it will be possible to be receive updates on news related to jihad operatives in the various jihadist arenas.[4]



Al-Batar Communications Institution: the launch of a bot

[3] 24.7.20. RocketChat.
[4] Dec 2020. Telegram.

There is also a constant attempt to optimize the use of social media and communication platforms that will serve the propaganda efforts best. This is a concern not just for the leadership but also a main discussion seen among supporters.

- For example, in July 2020 a participant in the jihadist forum, Shumukh Al-Islam, which is affiliated with ISIS, asked the forum members to make suggestions that could help improve the Mujahideen's propoganda system. The suggestions included methods of concealment when surfing the Internet, establishing additional fictitious social media accounts, establishment of a designated group that will be responsible for implementing transcripts in videos, and use of platforms for secure storage of files such as Sia Skynet and IPFs.[5]

The main use of social media and communication platforms is first a foremost to distribute propaganda aimed for followers, potential recruits and mostly the "Enemy". Both ISIS and al-Qaeda invest in content production and graphic design to emphasize the "message".

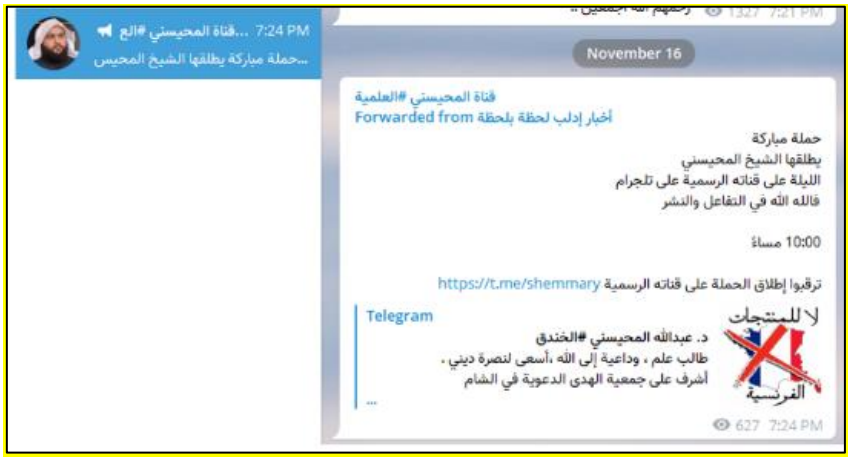
- For example, during the months of July-December, the Taqwa Communications Institute, which provides information to the Islamic State, published numerous banners and articles praising the continuation of the jihadist war against the enemies of Islam, led by Western countries and the United States. In August, the institute published banners emphasizing the importance of waging a war of attrition against Iraqi security forces as a result.

[5] 21.7.20. https://alshumukh.net/forum/%D9%82%D8%B3%D9%85-%D8%A7%D9%84%D9%85%D9%86%D8%AA%D8%AF%D9%8A%D8%A7%D8%AA-%D8%A7%D9%84%D8%B9%D8%A7%D9%85%D8%A9/%D9%85%D9%86%D8%AA%D8%AF%D9%89-%D8%A7%D9%84%D8%A3%D8%AE%D8%A8%D8%A7%D8%B1-%D9%88%D9%82%D8%B6%D8%A7%D9%8A%D8%A7-%D8%A7%D9%84%D8%A3%D9%85%D8%A9/3568740-%D9%86%D8%B1%D9%8A%D8%AF-%D9%85%D9%86-%D8%A7%D9%84%D8%AC%D9%85%D9%8A%D8%B9-%D8%A3%D9%81%D9%83%D8%A7%D8%B1-%D9%88-%D8%A7%D9%82%D8%AA%D8%B1%D8%A7%D8%AD%D8%A7%D8%AA-%D9%84%D8%AA%D8%B7%D9%88%D9%8A%D8%B1-%D8%A7%D9%84%D8%A7%D8%B9%D9%84%D8%A7%D9%85-%D8%A7%D9%84%D9%85%D9%86%D8%A7%D8%B5%D8%B1



From right to left: a call to continue the war of attrition against enemy forces; Marking the anniversary of the September 11, 2001 attacks; Threat to assassinate Emanuel Macron, President of France, against the background of the cartoon affair that made fun of the Prophet Muhammad

- In November 2020, Sheikh Abdullah al-Mahseini, a prominent jihadist Sheikh in the Idlib region in northern Syria, has launched a campaign on social media to boycott French products. The boycott is in response to the publication of cartoons featuring the Prophet Muhammad, which is considered forbidden and offensive.[6]



Sheikh Abdullah al-Mahseini campaign on Telegram

The use of communication platforms also enables jihadists groups control over populations. This was prominent under the Islamic State Caliphate rule and is now being implemented in Idlib region, Syria under Hay'at Tahrir al-Sham (HTS). HTS is the leading Jihadi organization in Idlib and controls most of the territory. They have established governmental institutions such as the police force.

[6] Nov 2020. Telegram.

- For example, in July 2020, the Hay'at Tahrir al-Sham (HTS) organization in the northern Syrian province of Idlib has issued a proclamation on behalf of the general management of the checkpoints regarding the allocation of a communication channel with the citizens through which they can contact the relevant authorities and complain about any problem or robbery using a specific telegram or Whatsapp account.[7]



Proclamation by Hay'at Tahrir al-Sham (HTS)

Recruitment

During the period of July – December 2020 there has been an increase in publications to recruit hackers to the ranks of the global jihad.

- For example, The Taqwa Communications Institute, which assists in advocacy for the Islamic State, has issued several leaflets calling on its supporters to study hacking in order to set up armies of hackers who will attack the West through cyberspace in a way that will economically exhaust the "Crusader enemy".[8]

[7] Dec 2020. Telegram.
[8] 27.12.2020. RocketChat.



A proclamation calling on Muslims to set up armies of hackers

to operate in cyberspace against the West

- In another case, the group “Al-Malaham Electronic Army”, which assists in advocating for al-Qaeda, published a magazine in November called "The Lone Wolves of Manhattan". The magazine included an article which dealt with the need to focus on courses on hacking. It is written that an army of hackers must be created that will be able to utilize cyberspace to break into critical infrastructure and destroy it, such as hacking into economic centers or control towers at airports in order to lead to plane crashes and more.



Article on hacking from "The Lone Wolves of Manhattan" magazine

- The “Lone Wolves of Manhattan” was published in Arabic and focused on encouraging Muslims living in the West to carry out individual attacks against government affiliated targets and civilian targets. For example, articles have been published about how to make bombs and manufacture weapons through the purchase of certain materials that are available on the market. One article encouraged Western Muslims who are sick with COVID-19 to enter crowded places and police stations to infect people with the Coronavirus. An article dealt with the need to focus on courses on hacking. It is written that an army of hackers must be created that will be able to utilize cyberspace to break into critical infrastructure and destroy it, such as breaking into economic centers or control towers at airports in order to lead to plane crashes and more. In December 2020, the guide was also published in English.[9]

[9] Nov-Dec 2020. Telegram.



Left to Right: Manhattan's Lone Wolves Guide Cover Page; Instructions for creating a bomb

Terrorism Fundraising

The practice of financing terrorism through the Internet during the period under review was mainly through groups which identify with ISIS and al-Qaeda or local Jihadists groups in Syria. It should be noted **the increasing funding difficulties of ISIS, which runs a survival campaign in Syria and Iraq, and the dwindling of its financial resources.** Therefore, it can be assumed that the efforts to raise funds through internet platforms will be magnified.

Terrorist groups seem to be aiming for a shift of their main funding method to be over the internet and through cryptocurrencies. They have published instructions and guidance on how to donate through these methods and have been applying effort to execute this shift.

It can be observed that terrorist groups are becoming more cautious in their efforts to raise money through cryptocurrencies. For example, many groups no longer publicize their cryptocurrency accounts and instead provide contact information publicly for anyone who is interested in donating in order to retrieve the account numbers privately. Additionally, they have been using different tactics to ensure their accounts do not get flagged by those regulating cryptocurrency. They have also been seeking cryptocurrencies that are less easily detectable such as Monero over Bitcoin.

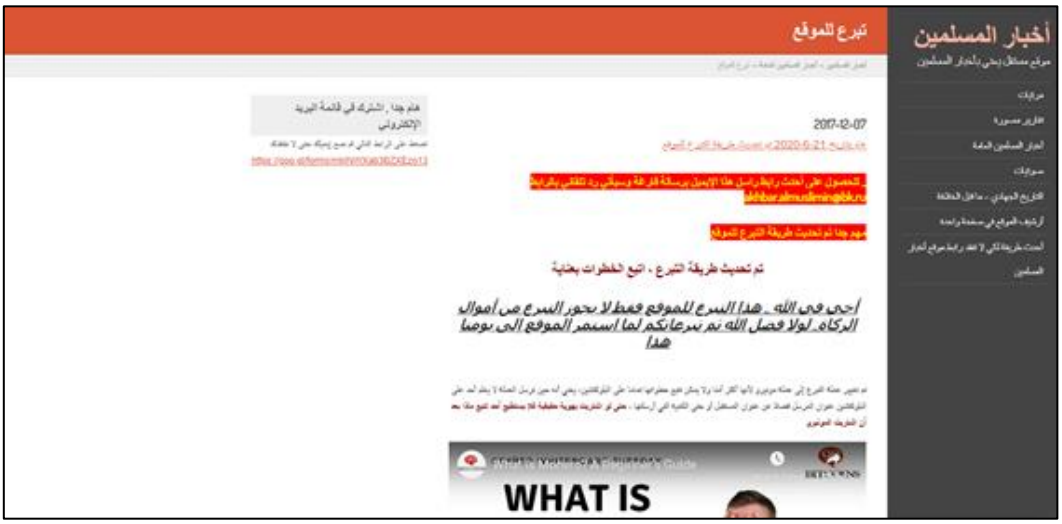
- In July, The al-Imaad Communications Institute, which assists in advocacy for the benefit of al-Qaeda, with an emphasis on hymns published by the organization's branches over the years, wrote a post on Telegram calling on the organization's supporters to donate bitcoin toward the continued operation of the website.[10] They did not provide a wallet or website through which to send the donation.



The Al-Imaad Communications Institute call for Bitcoin donation

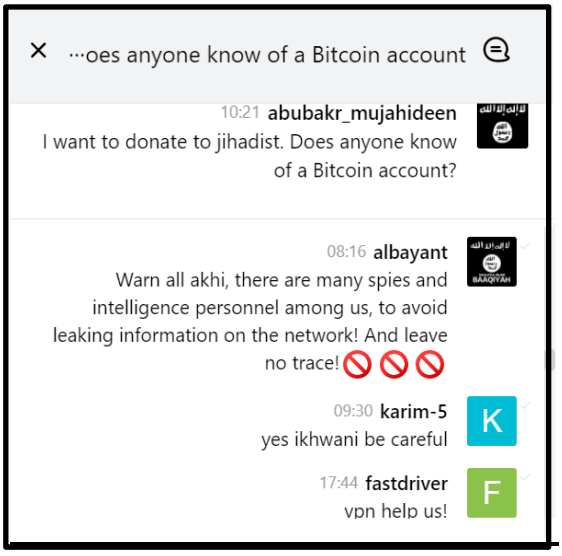
- The ISIS linked website "Muslim News" changed its donation method from Bitcoin to Monero currency during July 2020. They claim that the transition is due to the fact that Bitcoin can be traced more easily while Monero currency is much safer from detection. Within that scope, they provide a guide to instruct their supporters on Monero and how to make donations with Monero. They provided an email address through which they could be contacted by potential supporters and donors. [11]

[10] 11.7.2020. Telegram.
[11] Muslim News Website



Donation page on Muslim News website

- In December 2020, in a RocketChat room named "baqiya" (linked to the Islamic State), a user asked to receive details on how to donate to Jihad using Bitcoin. In response, he was warned by other users that intelligence personnel are viewing the chat room and therefore he should avoid leaking information. They also advised him to use secure connections such as VPN. The same user also asked for information on "Tech Heaven" chat room (Rocket Chat) and received similar replies, excepting one user who advised him to send money to sisters in camps Al Holl and camp Roj, in Syria. [12]



Attempt to donate to Jihad using Bitcoin on Rocket Chat

[12] Rocket Chat

During July-December 2020 there was an increase in the use of cryptocurrency in Syria mainly in the Idlib area under the territories of HTS:

- Jihad operatives in the northern Syrian province of Idlib have posted a Telegram channel dedicated to Bitcoin. For example, the founders of the account noted that Bitcoin can yield great profits in a short period of time and hence it can help the jihad activists in Idlib. The Telegram channel publishes analyses of fluctuations in Bitcoin currency and explanations of how it can be traded online.[13]
- In another case in August, Jihad operatives in Idlib in northern Syria ran a fundraising campaign for women and their families in Syrian refugee camps. According to the organizers of the campaign entitled "Release the Prisoners", the nation of Islam and jihad operatives must work to free Muslim women from prisons and donate money to Muslim women in distress in the refugee camps.[14]
- An office for the conversion of bitcoin and other cryptocurrencies in the northern Syrian province of Idlib has published an advertisement on social media about the services it provides in the field of cryptocurrencies. The firm also posted photos about its whereabouts and details about the cryptocurrencies in which it trades.[15] The Bitcoin exchange office is located in Idlib, in territory controlled by the HTS and its slogan 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.



The cryptocurrency trading business in Idlib

[13] Jul-Dec 2020, Telegram.
[14] Aug 2020. Telegram.
[15] Jul-Aug 2020. Telegram.



Advertisement for the Bitcoin Exchange office with slogan "First Office in the Liberated Areas"

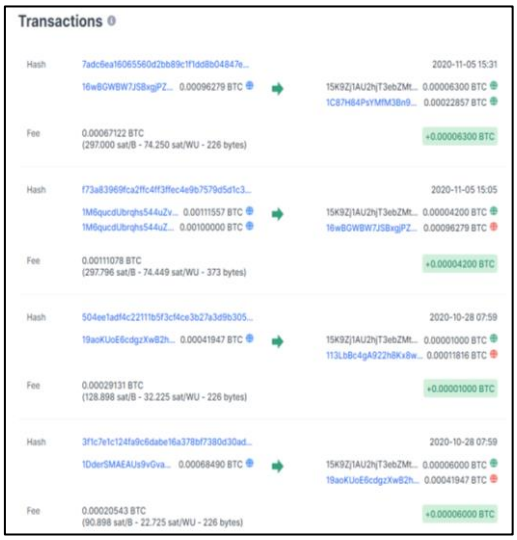
- In November, Sheikh Abdullah al-Mahseini, a prominent jihadist Sheikh in the northern Syrian province of Idlib, launched a fundraising campaign called "Warm Them." According to al-Mahseini, the campaign is intended to raise funds for the purchase of heating products for Muslims living in refugee camps affected by the recent rains. According to al-Mahseini, donors in Idlib province are supposed to donate in person, and donors outside of Syria should contact them through WhatsApp and Telegram in order to donate.[16]



Fundraising campaign "Warm Them" by Sheikh Abdullah al-Mahseini Al Sadaqah

[16] Nov 2020. Telegram.

- Al Sadaqah, a Syrian organization that operates social media accounts on multiple platforms which seek to finance terrorism via BTC solicitations, has reemerged in October and November 2020 after a two year hiatus for their publicized Bitcoin address. Between October - November 2020, there were 15 transactions, all incoming.[17] They described themselves as “an independent charity organization that is benefiting and providing the Mujahidin in Syria with weapons, financial aid and other projects relating to the jihad. "You can donate safely and securely with Bitcoin".[18]



Incoming transactions in October – November 2020 to Al-Sadaqah’s Bitcoin account



Al Sadaqah organization request for donations through Bitcoin

[17] Blockchain.info
[18] Telegram

Guides and Tutorials

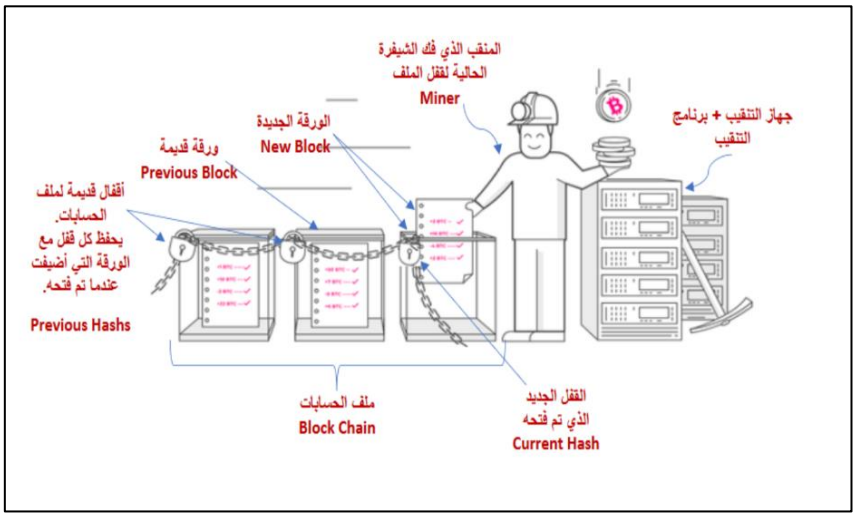
- The group “Al-Malaham Electronic Army”, which assists in advocacy for al-Qaeda, has announced the launch of a course on using Bitcoin currency. According to them, this is "the first course of its kind in the world of jihadist electronic armies [...]". The group clarified that registration for the course could be done through its RocketChat account.[19]

- The course, which consisted of five lessons, was published on the Al-Malaham Electronic Army website. The first lesson on cryptocurrency covered the history and basic definition of concepts in cryptocurrency. The second lesson covered technical ways to operate an electronic wallet and security measures that need to be taken. The third lesson covered the method of mining. The fourth lesson provided with a more in-depth theoretical knowledge on mining, methods, and devices. The fifth lesson covered more practical aspects of cryptocurrency of providing concrete examples of miming and using calculators.[20]



Announcement on the launch of an online course on cryptocurrencies on RocketChat

[19] 10.12.2020. RocketChat.
[20] Al- Malahim Website



Picture from the third lesson on mining

Defense

Terrorist organizations are aware of the unceasing defensive efforts of security agencies and the activities of the major players on the internet in general, and in the social media in particular, to remove Jihadist content from their platforms.

Terrorist organizations, therefore, continue to pursue a "cyberspace safe haven", where they can communicate and publish without being detected. To achieve this goal, leading entities linked to Global Jihad and other actors (Shia, Palestinians, etc.), took the initiative to distribute guidelines and instructions to their followers on how to avoid detection online. The guidelines discussed preferred more secure communication apps, guides on safe online surfing via computers or phones (i.e. the use of VPN, Tor etc.), and warnings regarding security vulnerabilities in apps and social media.

Jihadists organizations

During the months of July-December, the Afaq Electronic Horizons Foundation, which is affiliated with the Islamic State and is responsible for the distribution of Cyber Security related Materials, published several updates about cyber in Arabic and English:

- Videos about how to install and use various applications such as the encrypted messaging application Element.[21]

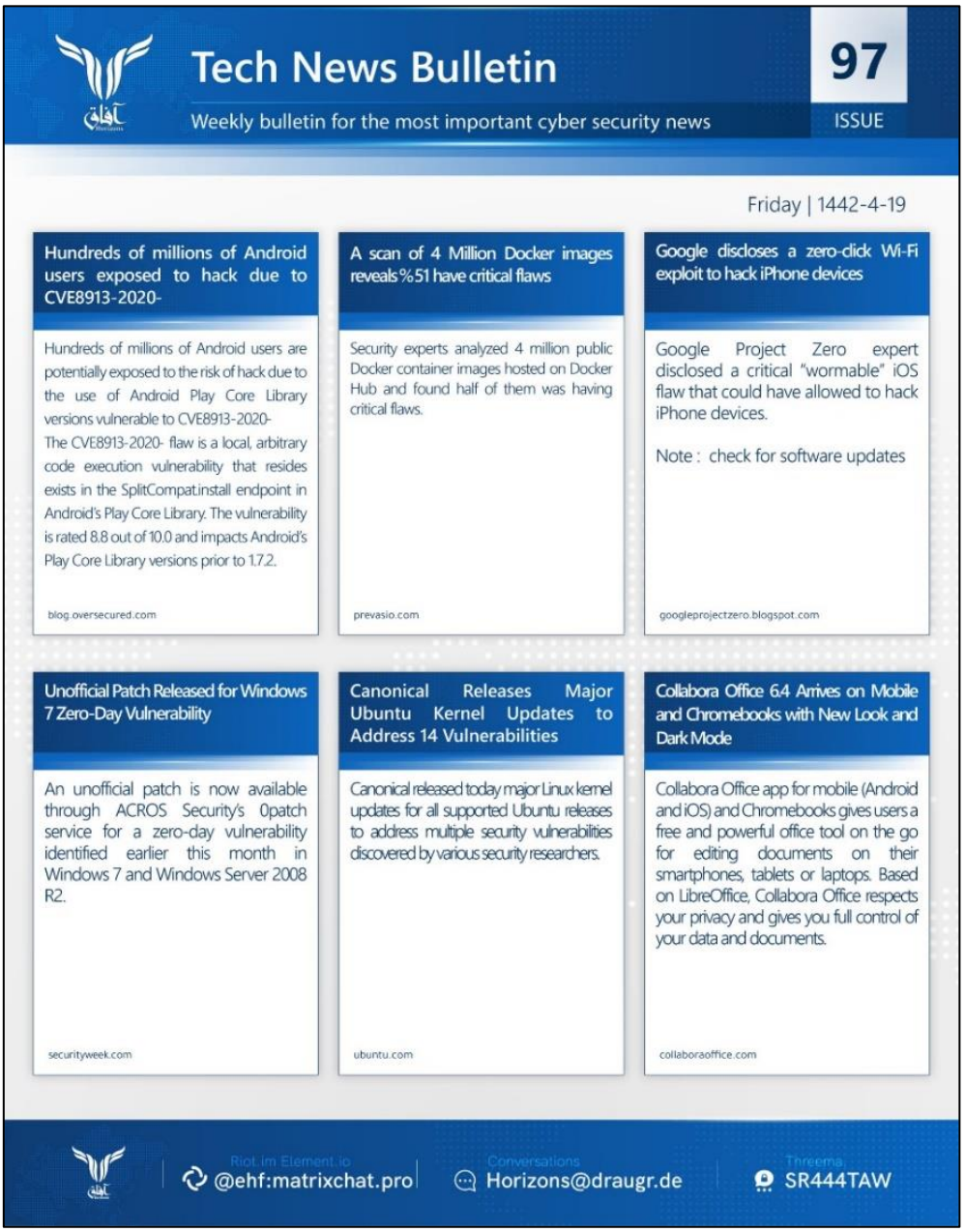


Guide for registration to Element

- In December, Afaq published a tech news bulletin detailing various vulnerabilities such as exposure to hacking due to CVE-8913-2020, which is a vulnerability in the Android Play Core Library. Other vulnerabilities they noted were a zero-click WiFi exploit to hack iPhones, and a zero-day vulnerability discovered in Windows 7, for which an unofficial patch was released.[22]

[21] .10.2020. Afaq Website

[22] 4.12.2020. https://e-horizons.io/tnb97/



Tech news bulletin

- In December, 2020 Afaq (Electronic Horizons foundation), published a manual titled: ***How to Protect Your Data on Android Phones***?[23] The manual focuses on cases in which a person might be arrested by authorities and they will have access to that person smartphone. Therefore, Afaq suggests downloading the app "Locker" to protect Android phones. *"if someone gets your phone's password, and is able to unlock the phone, he can recover files deleted from the phone……Locker app is open source and free on the F-droid store, and it activates a system feature that allows phones to be erased after entering a wrong password for a number of attempts"*

[23] Afaq Website



How to protect your data on Android Phones

- In December 2020, on RocketChat room "techhaven" which is linked to the Islamic State, a few users indicated that the communication app "Discord" is suspending users and advised not to use it.[24]



Discord App Logo

Offense

During the period of July-December 2020, Jihadists groups focused mostly on recruitment of hackers as seen above. However, no significant cyber-attacks were carried out.

Palestinian Organizations

The Jerusalem Electronic Army (J.E. Army)

[24] Rocketchat

J.E. Army are group of hackers from Gaza with links to Hamas that cooperate with other hackers' groups around the world. During 2015-2017 the “army” carried out a limited number of attacks against Israeli targets however the majority of its activity is attributed to 2020 when it launched a media covered cyberattacks on Israeli targets. An analysis of the activity includes three major areas of operation. First**, offensive**- cyberattacks. Second**, operations-** propaganda, recruitment, and finance. Third**, defense**, dissemination of information on information security and preservation of user anonymity.

During the period of July-December 2020, J.E. Army activity included:

Operational

The Propaganda disseminated by J.E. Army focuses on content identified with the Palestinian resistance and Propaganda aimed at Israel. During the period of July-December 2020 the group published numerus graphics presenting their support in "the Palestinian Couse" as seen below.

.



Propaganda on social media[25]

[25] https://twitter.com/JEArmy0

Defense

The **Jerusalem Electronic Army**, published on their website and social media information, articles and warnings related to online security:

- J.E. Army issued a warning against using TikTok software, claiming that it is used to spy on cell phone users.
- In December, 2020 J.E. Army issued a **warning related to Facebook pages** - According to the publication**,** the Israel intelligence services, through pages on social media, ask citizens in the Gaza Strip to photograph specific places and streets on their mobile phones, and send them through these pages in exchange for rewards in various forms.
- In December, 2020 J.E. Army published an article on their website titled **"Five reasons make you the ideal target for cyberattacks".** According to the publication, most of the attacks target small companies and private individuals. This is for five main reasons:
    - Overconfidence in the protection software that comes with the device (they advise to install firewall, anti-virus and use VPN)
    - Weak passwords
    - Ignoring updates
    - Opening random links
    - Using public open network Wi-Fi



Warning Related to Facebook pages

Offense

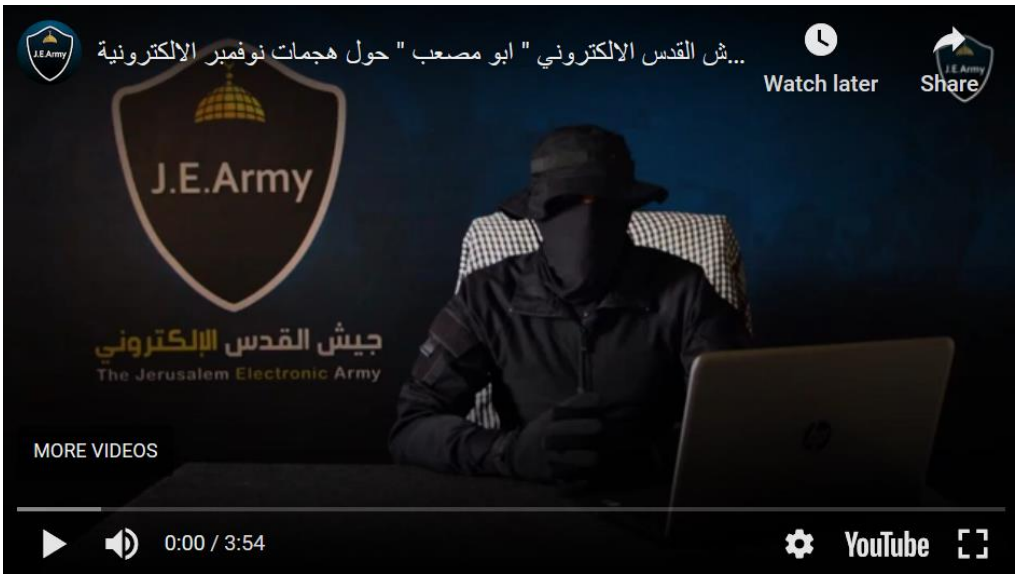
- J.E. Army claimed responsibility for alleged cyberattacks on Israeli websites and servers that caused the disconnection of the Internet at many Israeli companies and residences. In addition, the hacker group claimed that during July 2020 it managed to infiltrate hundreds of Israeli cameras.
- J.E. Army claimed responsibility in December 2020 for an alleged attack on Israeli servers and theft of a database containing Israeli telephone numbers. According to the group, its members sent 10,000 Israeli cell phone numbers warning messages in the Hebrew language, such as: "Red Alert" [this is the national code in Israel to warn of incoming rockets], "Power outage!", and "Israeli enemy, we will meet on the battlefield".



Post by J.E. Army claiming responsibility for an attack targeting Israeli servers

- J.E. Army claimed of responsibility for an alleged burglary of Israeli bank and business accounts and theft of funds that will be used for the benefit of the resistance organizations in Gaza.
- A video released on November 10, 2020 regarding an extensive cyberattack that they allegedly carried out against Israeli servers and websites during the month of November. A spokesman for the hacker group referred to the targets attacked as follows:
  - Attack on an Israeli cellular company (Cellcom)
  - Sending text messages to the cell phones of a thousand Zionist settlers demanding that they leave the lands.

- Hacking into 20,000 routers in different areas.
- Hacking into the Israeli cyber unit in Jericho and stealing all the data.
- Breaking into Israeli television Channel 12 and disrupting its broadcasts, which coincided with the anniversary of Baha Abu al-'Ataa (commander of the northern brigade in the military wing of the Palestinian Islamic Jihad terrorist organization that was assassinated by Israel).
- Activation of siren alarms in Haifa and Beit Shemesh hotels.
- Break-in and takeover of the solar energy system in the Kiryat Malachi hotels.
- A cyber-attack against Cellcom network link towers in the city of Tel Aviv and complete takeover of the server for three consecutive days.



The spokesman of J.E. claim to attack Israeli Targets in a video

Hamas - Izz al-Din al-Qassam Brigades

- In July 2020, the Izz al-Din al-Qassam Brigades, the military arm of the Hamas movement, issued a proclamation calling on Muslims to donate through Bitcoin. According to the organization, financial support for jihad operatives is considered a key commandment in Islam and that donors will be rewarded with entry into heaven in the afterlife. The organization has published WhatsApp telegram addresses dedicated to make donations.

- In October 2020, the Izz al-Din al-Qassam Brigades again called on their followers to donate Bitcoin through a designated email address under the "Support the Resistance" campaign.[26]



Proclamation by* Izz al-Din al-Qassam Brigades *asking for donations

Iranian and Shia hackers' Groups

"Iranian/Persian Hacker" Group (a/k/a Bax 026):

- On September 16th and 17th the US Department of Justice indicted a total of five Iranian hackers for various charges including identity theft and hacking with the intention of stealing sensitive governmental data. At least three of the hackers were linked to the Islamic Revolutionary Guard Corps (IRGC), which the US has designated as foreign terrorist organization.[27]
- An Iranian hacker linked to the IRGC dubbed "Mamad Warning" who is an active member of the hacking group Bax 026 of Iran, was observed to be actively hacking websites throughout this time, although he was not one of the hackers indicted by the US Department of Justice. [28]

[26] Jul 2020. Telegram.
[27] https://www.justice.gov/opa/pr/state-sponsored-iranian-hackers-indicted-computer-intrusions-us-satellite-companies
[28] https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-theft-campaign-targeting-computer-systems-united-states

- On September 16th 2020, Mamad Warning posted the image of the FBI wanted page for Behzad Mohammadzadeh (a/k/a "Mrb3hz4d"), one of the hackers indicted by the US Department of Justice, with the caption: *"Following the pursuit of Behzad Mohammadzadeh, a colleague and teammate, we announce that we stand behind our ideals, Whatever happens to us or the members of the team or any other Iranian hacker, we will continue stronger than before. A heavy answer is waiting for you, dear Americans, there are many of us in our channel"*[29]



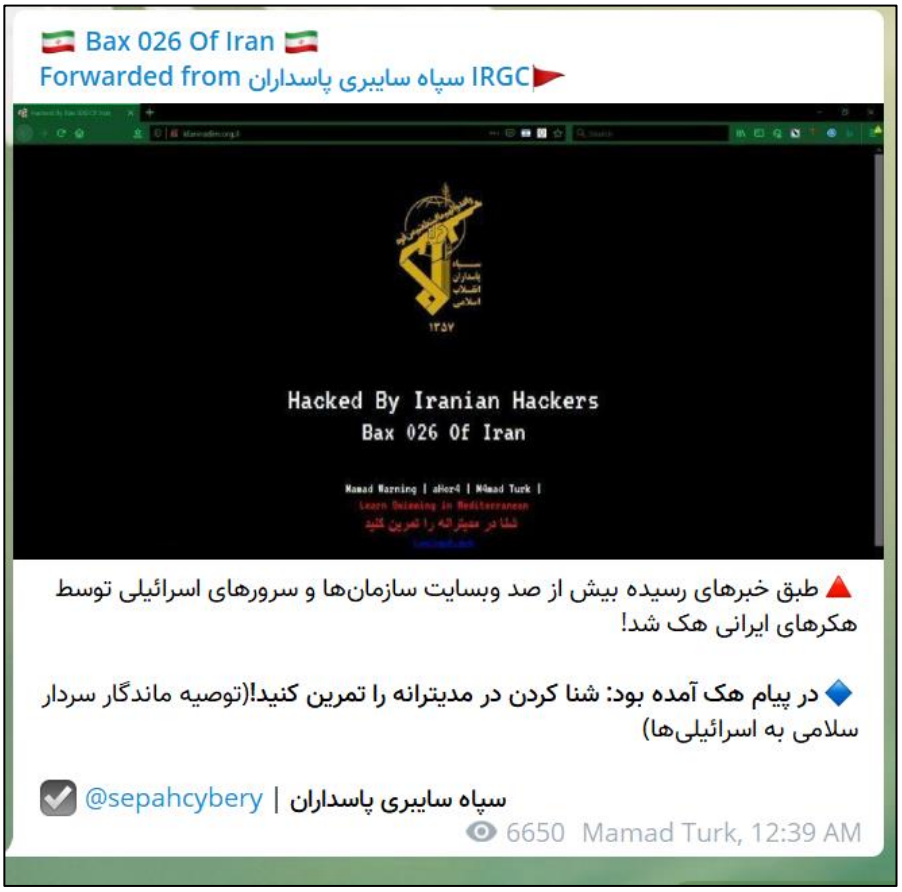
Post by Bax 026 of Iran Telegram Channel

- Mamad Warning claims to have hacked into websites of University of Washington, Substance Abuse and Mental Health Services Administration, Carnegie Mellon University, Saudi Arabia Institute for Diplomatic Studies, three US government sites,

[29] Sept 2020. Telegram.

Wyoming State Department of Criminal Investigation throughout the months of September and October 2020. He also posted pictures of personal information he gained from some of his hacks, such as drivers licenses and insurance papers.[30]

- Bax 026 may be linked to the IRGC. On July 15th 2020, the IRGC posted an image of an Israeli website (kfarvradim.co.il) that Bax 026 had hacked.[31]



Post by the IRGC on Telegram

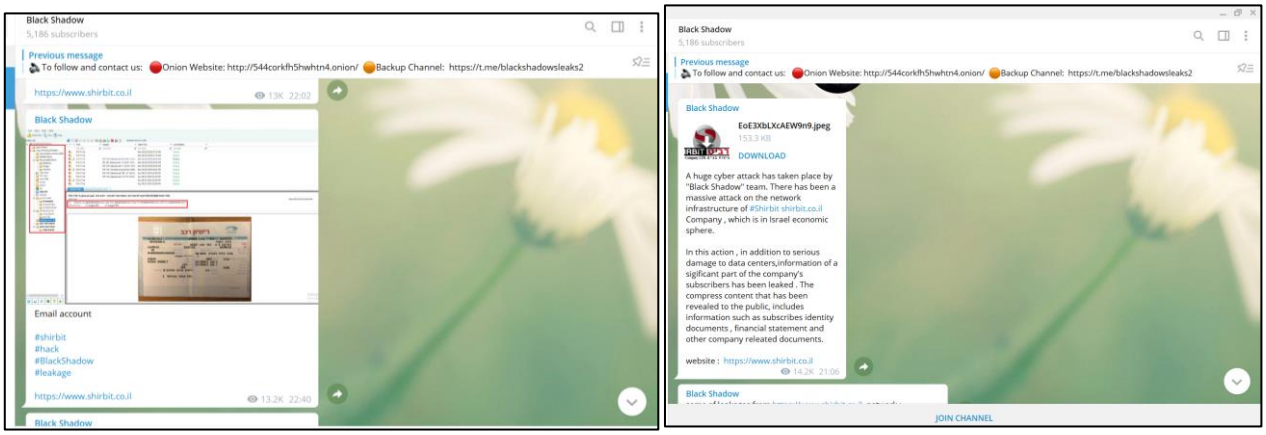
[30] Sept-Nov 2020. Telegram.
[31] Jul 2020. Telegram.

Cyber-Crime and Cyber-Terrorism

Recent years have seen an increasing number of cyber-attacks against political targets, critical infrastructure, and the websites of commercial corporations. These attacks, which receive increasing amounts of international attention, are perpetrated by states (which do not claim responsibility for them), groups of hackers (such as Anonymous), organized crime and lone hackers. We believe that terrorist organizations are working in close collaboration with organized crime to learn from their attempts [at cyber-crime] and may even be hiring their services. In light of this, it is important to examine and analyze cyber-crimes attributed to criminal organizations, as well as new development trends and patterns.

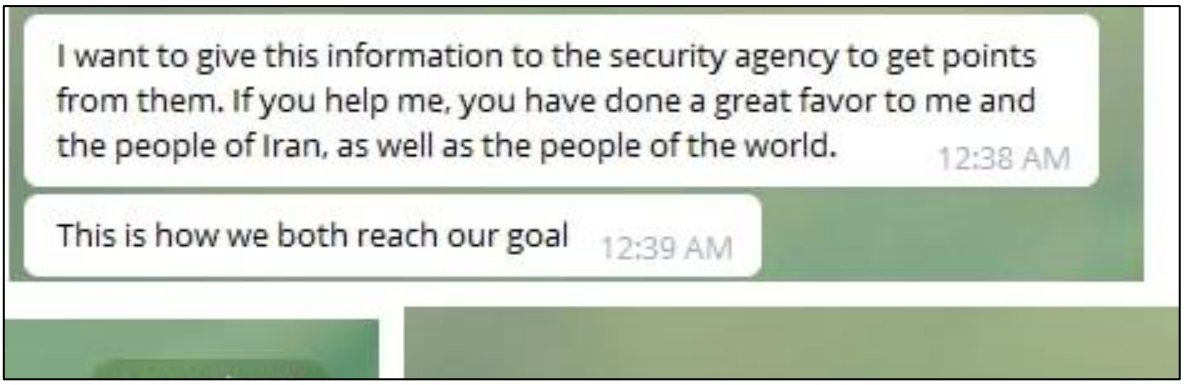
Shirbit Attack: BlackShadow Group:

On November 30th, 2020 the Telegram channel under the name "BlackShadow" (@Blackshadowleaks) published a statement claiming to attack Israel's insurance company Shirbit. On December 1, 2020 Israel Cyber authority confirmed the attack. *"There has been a massive attack on the network infrastructure of #Shirbit shirbit.co.il Company, which is in Israel economic sphere. In this action, in addition to serious damage to data centers, information of a significant part of the company's subscribers has been leaked. The compress content that has been revealed to the public, includes information such as subscribes identity documents, financial statement and other company related documents."*



Black Shadow statement on Telegram channel ; Personal information for sale on Black Shadow Telegram channel

The same Telegram channel named BlackShadow (@Blackshadowleaks) published the sale of the Shirbit data package, including some examples of photos of private I. D's, emails, driving license, passports etc. They also published the Black Shadow link to its Onion website. One of the potential customers included the #Iranian intelligence.



Black Shadow corresponding with a potential buyer form Iran



Onion Website of Black Shadow with links to Telegram

Far-right Extremism

In recent years, and especially lately due to the COVID-19 pandemic, there has been an increase in far-right activity online. One of the major manifestations of this process relates to the transition from using more limited “soft violence” to more comprehensive “hard violence” demonstrated by lone wolf attacks resulting in mass casualties.[32] The internet is one of the major platforms contributing to success of this phenomenon and it serves as a major operative tool.

Far-right organizations are active in cyberspace and are using essentially similar methods to the Global Jihadist organizations (operational, defense, offense). While there are significant differences, the far-right movement overlaps with the Jihadi movement in certain areas. For example, far right groups have been utilizing cyberspace to disseminate propaganda, recruit new members and to encourage lone wolf attacks. Additionally, far right extremist groups seem to be learning from the tactics used by Jihadi groups.

Throughout the period under review (July – December 2020), the Far-Right extremist groups have continued to be active in cyberspace. They have used various platforms to disseminate propaganda, advertise their ideologies, and encourage physical violence. Certain events have exacerbated the Far-Right presence in cyberspace and warrant deeper analysis, such as the United States Presidential elections and the CoVid-19 pandemic. This section will evaluate these and other trends such as doxing.

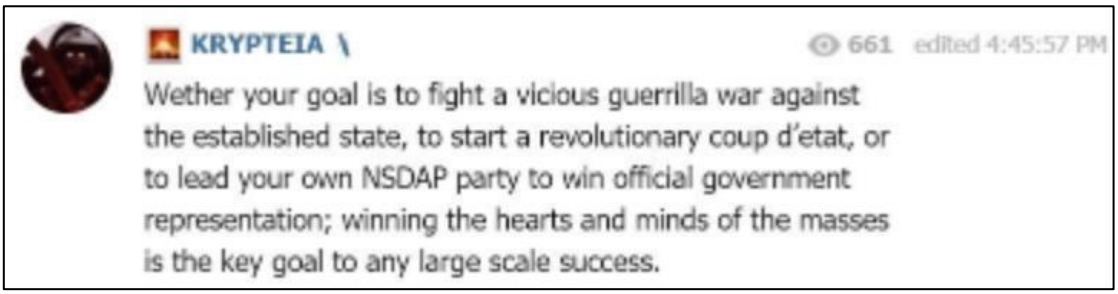
Operational

Propaganda

- On December 13th, 2020, the Telegram channel KRYPTEIA shared a post about the importance of garnering support for their movement. The post argued that if the NSDAP (Nazi Party) is going to be successful at overthrowing the existing regime, they need to develop popular support by winning the "hearts and minds" of the

32 https://www.ict.org.il/Article/2643/The_Far_Right_Ideology_Modus_Operandi_and_Development_Trends#gsc.tab=0

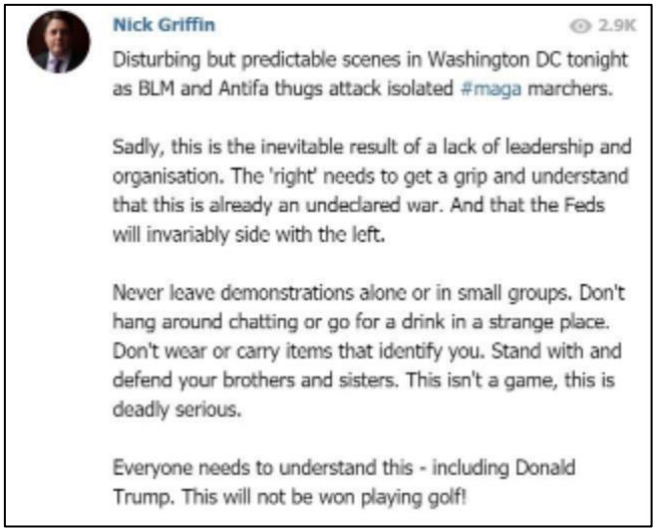
general population. The account also specifically mentioned guerilla warfare. This portrays a new trend in which far-right activists are beginning to liken themselves to guerrilla fighters.



Telegram post by KRYPTEIA

Propaganda: United States Presidential Elections

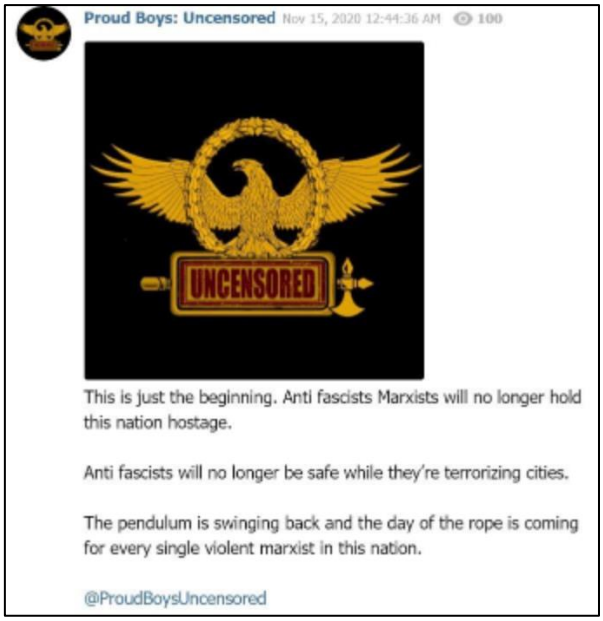
- British politician Nick Griffin posted a response to the alleged violence between Antifa/BLM activitist and Trump supporters during the "Stop the Steal" political march in Washington, DC on November 14th, 2020. Nick Griffin argued that this conflict between the political left and right is an *"undeclared war"* and that the political right needs to begin defending themselves. He further argued that *"the Feds will invariably side with the left."*



Post by Nick Griffin

- On November 15th 2020, the Proud Boys Telegram channel posted against anti-fascists, implying they will pay for violence with violence and stating that anti-fascists

"will no longer be safe when they're terrorizing cities", referring to the protests held in November.



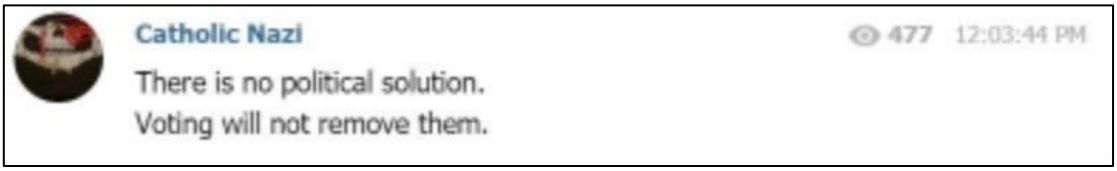
Telegram post on the Proud Boys channel

- On November 17th, 2020, the B R E A D P I L L E D Telegram channel posted a response to a tweet stating that more people were moving towards accelareationist ideology because their preferred political candidate (Donald Trump) lost the election. The post challenged the claim, stating that those alluded to by the aforementioned tweet were simply *"waking up to the truth".* The post went on to describe elections as *"fake and gay"* and that is why so many individuals are embracing accelerationism and extremism. They also suggested that *"the system"* (referring to voting and current status quo government) is corrupt and must be destroyed. The post concluded with the statement *"Voting will not remove them."*



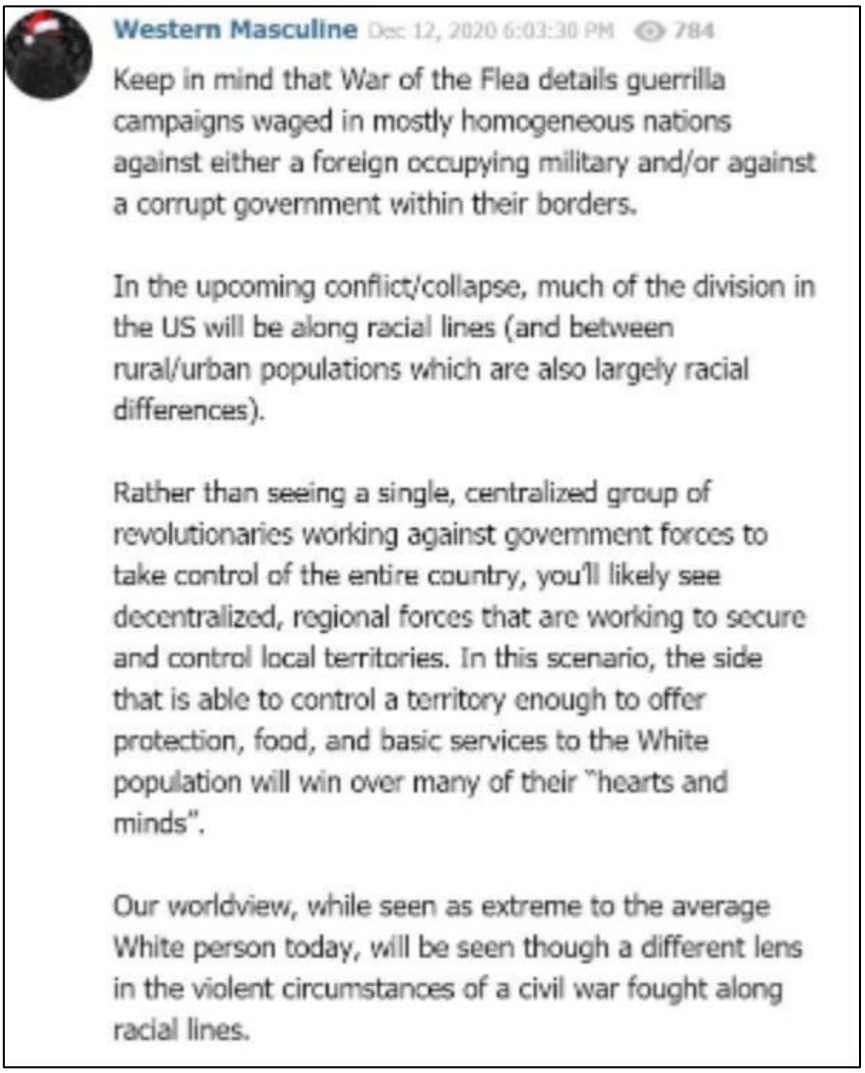
Post by B R E A D P I L L E D Telegram channel

- On December 11th 2020, the Telegram channel Catholic Nazi posted a short text stating: *"There is no political solution. Voting will not remove them."* This rhetoric has been very common in the far-right online ecosystem for during United States Presidential elections. It seems to insinuate that violence is necessary to remove the in-coming administration.



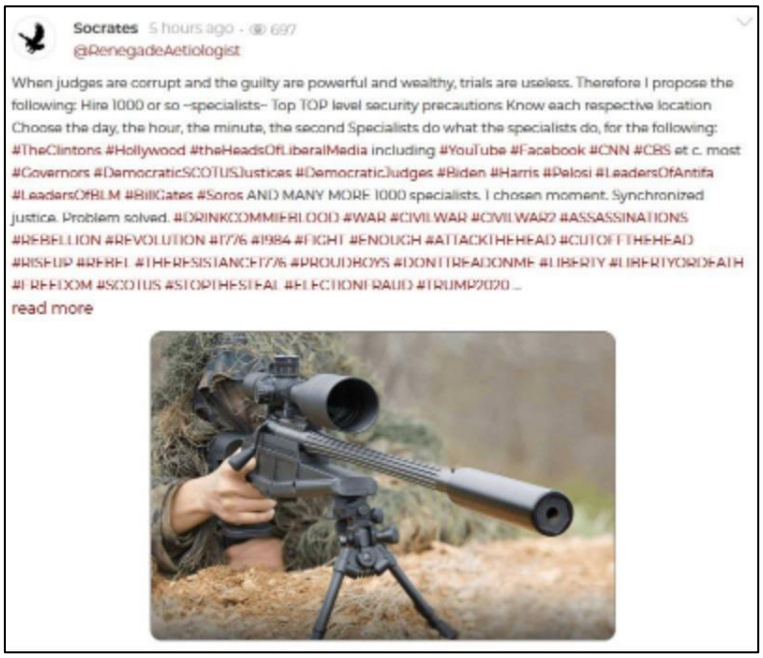
Post by Catholic Nazi Telegram channel

- On December 12th, 2020 the Telegram channel Western Masculine discussed the inevitability of an upcoming conflict as a result of the most recent elections. The user argues that the conflict will be small insurgent groups combatting what they view as an occupying force. The user suggests that to be successful these individual insurgent or militia movements will need to gain popular support by offering *"protection, food, and basic services."*



Post by Western Masculine Telegram channel

- On December 13th 2020, a Parler user, dubbed Socrates, shared a post on their Parler homepage. The user expressed anger about the current administration and the fraudulent elections. “Socrates” suggested hiring 1000 "specialists." They then suggested that at a chosen time, these specialists should target liberal leaders such as the Clinton family, leaders of media companies, Joe Biden, Kamala Harris, Nancy Pelosi, Bill Gates, George Soros, and other prominent figures. This post had an image of an individual holding a rifle attached.



Parler post by "Socrates"

Propaganda: COVID-19

- On November 10th 2020, a user posted that they may have contracted COVID-19. They state that they are currently planning to become a "super spreader" and are looking for advice. The author of post further explained their current plan: to attend exams on Wednesday and Friday (infect at least 4 people at each exam, who will then infect their families), go to a "gay bar" attempting to infect 10-20 people by going on to the dance floor, and drive 10-20 minutes to an "ethnic church" to avoid going to the "mostly white church" that is nearest.



Post by a user intending to transmit COVID-19 to members of an "ethnic church"

- On December 17th, 2020, the Telegram channel HateLab shared a post in response to the Daily Beast article discussing the use of anti-vaccine sentiment amongst the far-right and extremist community on Telegram. The user stated that they will continue to spread information to oppose the vaccine. The post suggests that they believe it is linked to the "Great Reset" conspiracy theory.


HateLab

Again they missed the mark, brother. (What can really be expected from the kike media though).

Dear, Daily Beast

We are without a doubt opposed to the vaccine for our people, and we will continue to tell everyone, that will listen, to be Defiant in the face of the TYRANNICAL Pharmaceutical Industrial Complex.

Your system is over-reaching and we're not the ones causing it. You are. It is you, the cheerleaders(media) and the sycophantic system-cult of lemmings that lap up your bullshit, that are enabling and propping up this tyrannical agenda.

We aren't able to force the system to engage hard power mechanism to force the public into taking a brand new research chemical vaccine, but they will engage those mechanisms when large sections of the public refuse to comply.

We Will Not Comply.
And many others will not comply either.

When a state-structure starts going down the path of open tyranny (Hard Power) it causes a violent backlash, we aren't causing this, it is just how systems work. Governments engage in tyrannical and arbitrary laws, and a subsection of the public starts to fight back.

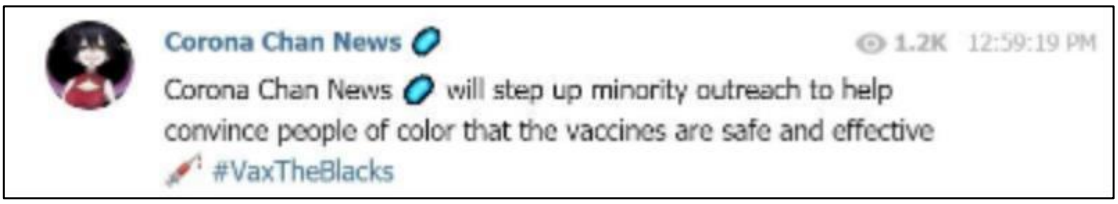
So, you can cheer on the great reset, you can cheerlead for the MRNA vaccine causing massive health problem all you want, you can lie to your readers and hold that guilt against yourself forever, you can even continue to label us as "the problem", but in reality the system itself is broken and we didn't cause it.

We're just the most apparent proof.

Happy Holidays, go fuck yourself.
HH

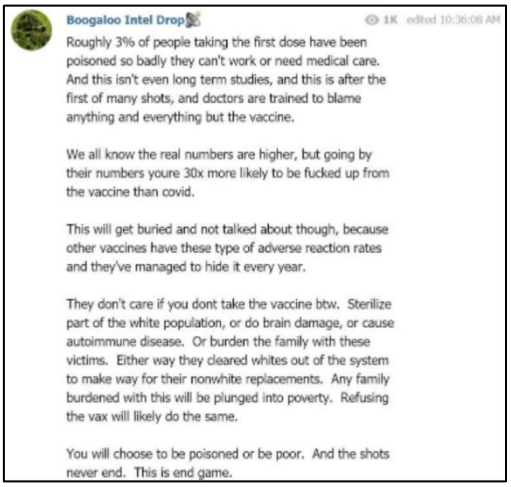
Post by HateLab Telegram channel

- On December 18th, 2020, the Corona Chan News Telegram channel shared a post advocating for people of color to take the COVID-19 vaccine. The post concluded with the hashtag #VaxTheBlacks. The hashtag #VaxTheBlacks has appeared on numerous white-nationalist and white-supremacist channels this week. Although the groups believe the vaccine is either toxic or causes harm to those vaccinated. As a result, it appears that these channels support vaccinating people of color because of their belief in the dangers of the vaccine combined with their racist ideologies.



Post by Corona Chan News Telegram channel

- On December 19th, 2020, the Boogaloo Intel Drop Telegram channel shared a post suggesting that the COVID-19 vaccine is a part of the "Great Replacement" conspiracy theory. The post suggests that the vaccine is substantially worse that contracting COVID-19, and that it is meant to target the white population .



Post by the Boogaloo Intel Drop Telegram channel

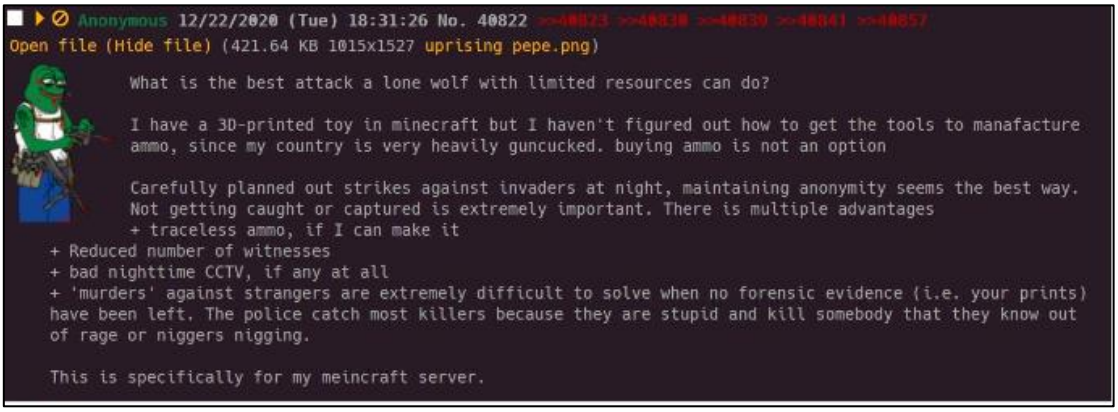
Offense

Recent trends in cyber offense focuses on online mobilization to conduct lone wolve attacks. The issue most discussed in this context, addressed the type of weapon to be used in an attack. Within this scope, the 3D printer has become a vital tool, mainly in Europe, where weapons are less accessible.

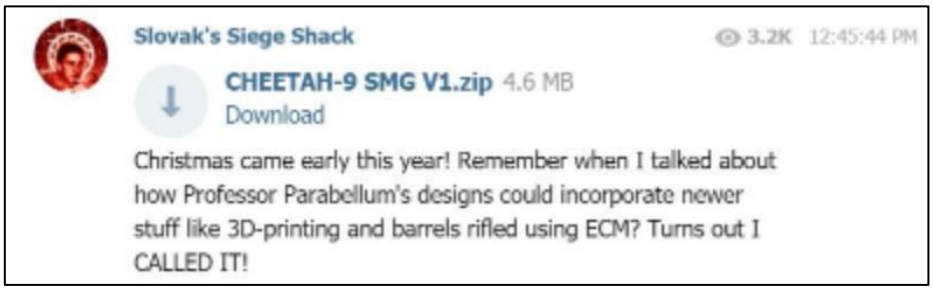
- In December 2020, anonymous users on an imageboard asked for suggestions for **planning an individual initiative ("lone wolf") attack somewhere in Europe**. The post states that the user has access to a 3D printed "toy" (gun) but does not have access to ammunition. They request suggestions for how to acquire or produce ammunition as it is not readily available to them. Additionally, they explain that they

plan to target a random individual, in an area with reduced CCTV status and few witnesses. The original user asked for suggestions on how to perpetrate such an attack.

- In December 2020, two Telegram channels, Slovak's Siege Shack and FEDPOST posted zip files containing 3D printer parts for an improvised firearm. The user has posted similar content in the past and suggested that members download and utilize the files.



Anonymous post regarding "lone wolf" attack

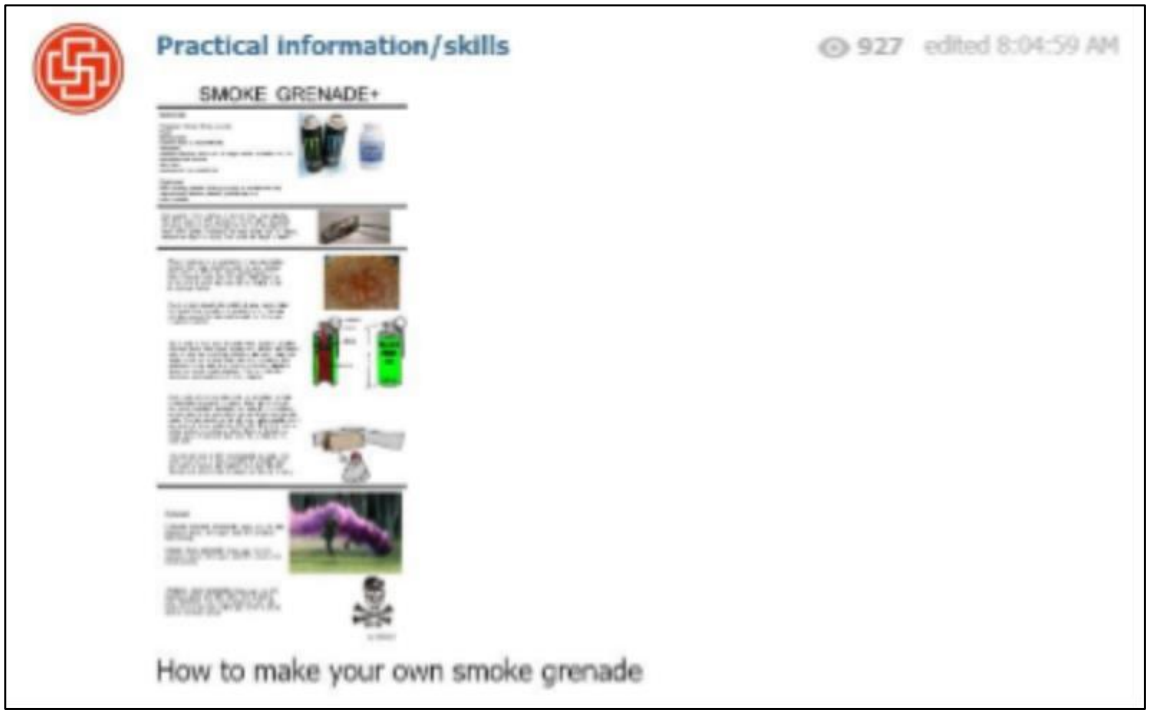


Post by Slovack's Siege Shack Telegram channel

- On December 13th 2020, a Telegram user posted an image file with instructions on how to create homemade smoke grenades using improvised items. The image also explains how to add additives to make the smoke poisonous.



Telegram post with instructions on how to create homemade smoke grenades



Post on how to make a smoke grenade

Another key trend in far-right offense, is the continued effort to encourage kinetic attacks through cyber means. Yet their capabilities have not yet flourished and as of today they mainly focus on Doxxing.

- On Novemebr 10th 2020, a user dubbed SoL posted on the darkweb that he/she as well as others had been collecting information on individuals engaging with Antifa (anti-fascist movement) social media content in the Portland, Oregon area. SoL stated that he/she had indentified many individuals to investigate for their connections to Antifa. SoL shared that more information would be released slowly and over an

indeterminate period of time so that "opsec" (operation security) could be maintained. Finally, SoL suggested that members reading the post should continue to do individual research on the individuals identified . Responders to the post began to release names, and work places of individuals that SoL had suggested in the initial post . Within two hours of being posted, the moderators of the 4Chan site removed the thread.


[–] ▸ **apping Portland Antifa social networks** **Anonymous** 11/11/20 (Wed) 04:45:41 ID: 94a3a8 No.179576 [Watch Thread] [Show All Posts]

This information was dropped on cukpol, so I can't answer any questions about it's origin. It spawned digging threads that were uncovering a lot of good information very rapidly. Mods over there started pruning the digging threads, and its impossible to continue the research. Hopefully we can get started again before the leads go cold and the enemy erases their tracks. SoL (op of first thread) said:

>For the last two months, we've been wardriving around antifa rioters, letting them associate with mobile honeypots to access internet, so we could look at their traffic. The results were extremely interesting. We were able to map roughly 8632 individuals engaged at all levels of antifa activity, from rioting and planning, to handling funds for riot gear and legal fees. These networks were used to make social network maps, with k=3 to identify those individuals with the densest inter-connectivity within the broader network. These represent the most socially connected individuals in Portland's antifa community; this indicates who is most valuable to investigate. At first we limited this to the Portland area, but then we noticed that the connections were national, and international. We will be leaking this information periodically. Make sure to use whatever leads we leak to dig. Antifa included members of city and state government, including the city council, prosecutor, and mayor's office. It helps us maintain opsec to release this piecemeal, and ask you to further contextualize it through your own analysis. We're giving you enough to find valuable connections. We will leave hints, the rest is up to you.

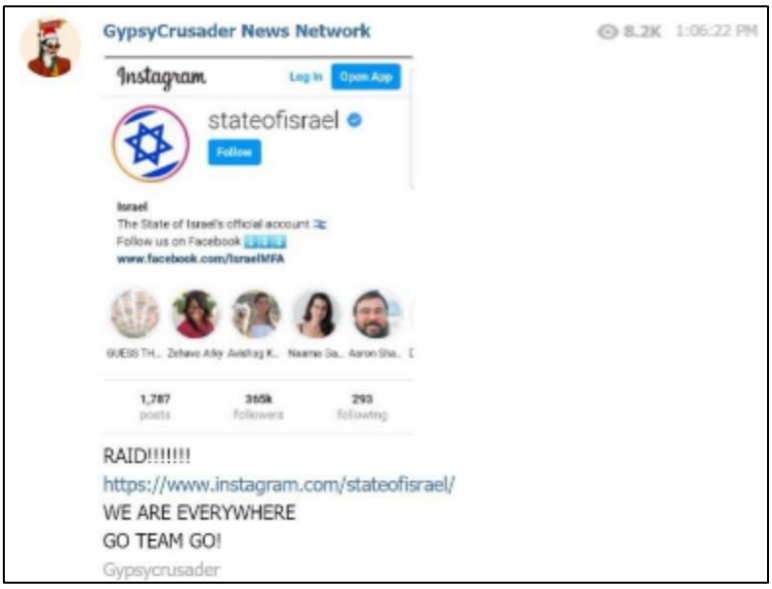
>Archived threads:

https://archive.4plebs.org/pol/thread/289740587
https://archive.4plebs.org/pol/thread/289714307/
https://archive.4plebs.org/pol/thread/289688413/
https://archive.4plebs.org/pol/thread/289671994/
https://archive.4plebs.org/pol/thread/289539968/

Current active threads (not pruned yet but soon):
https://boards.4chan.org/pol/thread/289754598
https://boards.4chan.org/pol/thread/289753283

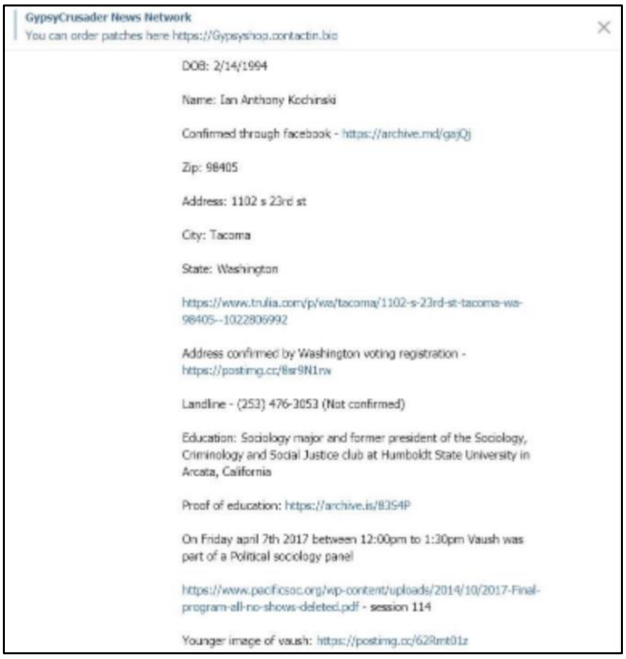
Post by user "SoL"

- On November 11th, 2020, an anonymous user posted on 8Kun (after the original threads were taken down from 4Chan) a database of individuals from the Portland area who had allegedly engaged with Antifa content on social media networks. In follow up posts, an anonymous user encouraged users to continue researching the individuals to identify their places of work and residence. This post also contained archived copies of the removed threads from 4Chan.
- On December 7th 2020, the Telegram channel GypsyCrusader posted personal information of an individual including legal name, date of birth, social media account(s), home address, and home phone number. GypsyCrusader chose to Dox this individual because they engaged in sociological work that was counter to the ideology of the far-right and white nationalist movement.
- On December 7th, 2020, GypsyCrusader News Network instigated a "raid" on the Instagram profile of "dannycullum0" under the program "Project Mayhem." This user did not explain why a "raid" targeting this individual was necessary. The user later posted evidence of the "raid" from individuals involved with "Project Mayhem."



Post by GypsyCrusader Telegram channel

- On December 11th 2020, the Telegram channel GypsyCrusader News Network instigated a "raid" on the official Instagram profile for the State of Israel. The user later posted evidence of the "raid" from individuals involved with "Project Mayhem."

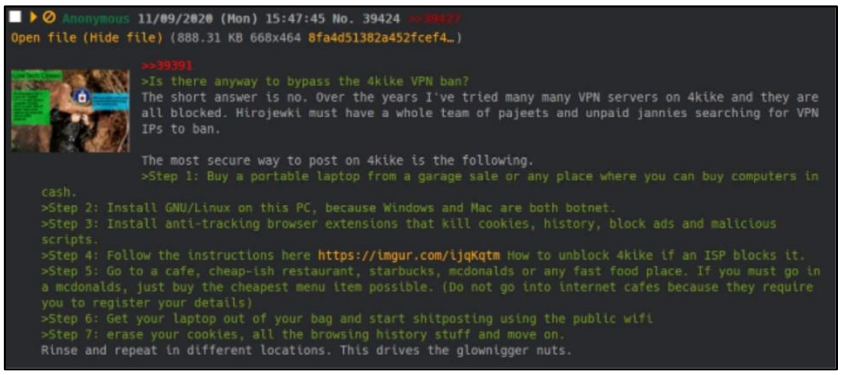


Post by GypsyCrusader Telegram channel

Defense

- On November 9th 2020, a user responded to a question from a fellow user asking: *"Is there anyway to bypass the 4kike VPN ban? Posting the most radical messages*

possible now there would be the most effective place to do so, but it seems to be quite heavily locked down." The author responded with a post explaining how to avoid detection by utilizing technical ("anti-tracking browser extensions") and physical methods (going to a public WiFi location to post materials & utilizing a computer purchased with cash). The author explains that "this drives glowniggers nuts." "Glowniggers" seems to be a pejorative word utilized by members of the site to reference those attempting to gather intelligence about a particular individual or group based on their activity on the site.



Post on the dark web asking how to bypass the 4kike VPN ban

International Response

Geopolitics and Terrorism

- 92 domains used to disseminate propaganda and fake news by Iran's Islamic Revolutionary Guard Corps (IRGC) have been seized by US law enforcement. The Department of Justice (DoJ) claimed that the IRGC used the domains to "unlawfully engage in a global disinformation campaign."[33]
- The US Department of Justice seized $2 million worth of cryptocurrency from terror groups in the Middle East. This is the United States' largest seizure of funds related to cryptocurrency supporting terror financing. The funds were seized from ISIS, al Qaeda and the al Qassam Brigades, the military wing of Hamas. It is predicted that the assets would have been used by the groups to buy weapons and train potential attackers.

[33] October 2020, United States Department of Justice

The report detailed three terror finance campaigns, all of which relied on sophisticated cyber-tools, including the solicitation of cryptocurrency donations from around the world. The action demonstrates how different terrorist groups have similarly adapted their terror finance activities to the cyber age.

Each group used cryptocurrency and social media to garner attention and raise funds for their terror campaigns. The fundraising campaigns utilized several methods, with some groups soliciting contributions explicitly to support the Mujahideen and Jihad, while other groups posed as charity organizations and asking for donations to help their charitable cause, such as providing food to hungry children in Syria. Still others scammed contributors by taking advantage of the global pandemic and claiming to be a reputable company selling personal protective equipment.

The US listed over one hundred Bitcoin addresses linked to designated terror groups. The transactions made to and from these addresses can be traced through the blockchain, which is transparent. It is clear that these organizations used several methods to remain undetected, such as layering, a method where several new Bitcoin addresses are created and the transaction is passed through them before reaching the designated address. Many of the transactions go through the red-flagged addresses and eventually reach the virtual exchange, Binance, where the chain is lost.[34]

- For the first time, Canada has named state-sponsored programs in China, Russia, Iran and North Korea as major cybercrime threats. They have expressed concern that foreign actors could try to disrupt power supplies. The Communications Security Establishment (CSE) signals intelligence agency said the aforementioned programs posed a significant strategic threat to Canada.[36]
- The FBI and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) issued a joint statement that Iranian hackers had successfully accessed voter data.[38]

[34] August 2020, United States Justice Department

[36] November 2020, Reuters

[38] December 2020, CISA

Legislation, Policy, and Regulations

- A new Office of Joint Cyber Planning proposed in an amendment to the 2021 United States defense policy bill aims to help government and private actors respond more quickly to cyberattacks launched from Russia, China, and elsewhere.[39]
- The Australian Department of Home Affairs proposed national security laws in a consultation paper aimed at industry, academia and state and territory governments. The proposed laws will grant federal government agencies the power to "take direct action" against cyber-attacks and obtain information from critical infrastructure entities if it is deemed to be in the national interest. The reforms outlined in the paper would include a number of additional sectors to the definition of critical infrastructure: banking, finance, communications, data, the Cloud, defense industry, education, research, innovation, energy, food, grocery, health, space, transport and water.[41]

Government and Critical Infrastructure

- The US Senate voted in favor of banning TikTok on government employees' cell phones. Government officials have cited the collection of immense amounts of personal data through the popular app as reason for this ban.[42]
- The Israeli Water Authority confirmed that previous cyberattacks were continuing. The attacks were aimed at agricultural water pumps in northern Israel. [43] The cyber threat actor, was believed to be working for the Iranian government recently launched another round of attacks on Israel's water sector. Israeli authorities confirmed in late April 2020 that hackers had targeted industrial control systems (ICS) at several water and wastewater facilities across the country. People familiar with the attacks said at

[39] July 2020, Potomacofficersclub

[41] August 2020, The Mandarin

[42] August 2020, Security Week

[43] July 2020, Hamodia

the time that the attackers had targeted programmable logic controllers (PLCs) and they knew how to target such devices.

- Gen Sir Patrick Sanders, the UK's strategic command chief, announced that that the UK has implemented an advanced offensive cyberwar capability that could potentially "degrade, disrupt and destroy" the critical infrastructure of its adversaries.[45]

[45] October 2020, Security Affairs

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 policy.

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