IDC HERZLIYA

ICT International Institute for Counter-Terrorism

With the Support of the Jusidman Foundation

Cyber Updates

April - June 2020

Executive Summary

The potential of cyberspace was identified by terror organizations over a decade ago. However, in recent years there is a significant uptick in the use of the internet and the sophistication of such use. Where initially terror organizations utilized static websites, then later incorporated basic interactive elements, and today, through social media and various applications, these organization are active online and offer fully interactive experiences for their users. ISIS is considered a trail blazer as far as online innovation is concerned.

The traditional hierarchal structure typical of terror organizations has been undergoing dynamic changes in recent years, including changes to command and control structures. Thus, next to the hierarchal organizational structure in territories controlled by the terror organizations, one can observe the formation of an online arena in area not under the physical control of the terror organization. Such online structure is made possible due to increasing use of the internet and its accessibility worldwide.

In the period reviewed in this document (April-June 2020) terror activity in cyberspace has been identified in three major aspects:

Operational – Jihadi organizations continue to use cyberspace to recruit operatives (there is an expansion of jihadi propaganda activity to multiple social media platform, due to the removal of some 2,000 ISIS supporting Telegram channels in November 2019) and raise funds (increased use of jihadi activity of social media, especially in the Idlib region).

Defense – No major development has been identified as far as the online defense strategies of jihadi organizations and they keep disseminating content on security, encryption, privacy and anonymity, and instructions for safe use of mobile devices.

Offense – terror organizations continue their efforts to improve their offensive capabilities, especially in relation to hacking social media accounts, defacing websites and planting malware. It seems that al-Qaeda in the Arabian Peninsula wishes to motivate Muslims to put an effort towards cyber-attacks against the west.

Far-right – in recent years, and especially lately due to the COVID-19 pandemic one can observe increasing far-right activity online. One of the major manifestations of this process relates to the transition from using “soft violence” to “hard violence”. The internet is one of the major platforms contributing to success of this phenomenon and it serves, like with the jihadi organizations, as a major operative tool.

Far-right organizations are active in cyberspace and are making essentially the same use of it as the jihadi terrorist organizations (operational, defense, offense). Therefore, this report will expand and present the prominent trends and uses made by far-right organizations in cyberspace.

In the period reviewed in this document (April-June 2020) far-right activity in cyberspace has been identified in three major aspects:

Operational – Far-right organizations keep using cyberspace to disseminate propaganda, radicalization, recruitment, and inspiration if lone wolf attacks.

Defense – In the period reviewed one observed far-right organizations disseminating content on security, encryption, privacy and anonymity, warnings of imposters and instructions for safe use of mobile devices.

Offense – in the period reviewed we observed a trend of encouragement of kinetic attacks as well as cyber ones, yet their capabilities have not yet matured and they are still low, especially in relation hacking social media accounts (i.e. Doxxing) and Zoombombing to threaten and intimidate organizations, prayer centers and minority schools.

In the space of global response to cyber threats we see activity on the part of governments attempting to quell cyberattacks and remain up to date in their cybersecurity departments by implementing new regulations and policies and by responding swiftly and effectively to cyberattacks.

Jihad

Operational

Terrorist organizations continue to use the Internet for a wide range of uses, including a continued process of professionalization, and an emphasis on using various social networks as a platform for distributing messages and guidance to various sites.

Jihadist Propoganda

During the period under review, jihadist organizations continued to carry out propaganda activities with familiar features to the past.

- **The Invasion Brigade**, a group that supports the Islamic State, conducted an awareness social media campaign in March-June 2020 for the benefit of the Islamic State. As part of the campaign, they posted dozens of Twitter accounts of major American and British media outlets and called for them to plant messages and propaganda materials of the organization that they coordinated through their telegram account. The propaganda materials were originally published in Arabic with English and Turkish translations.[1]

Logo of the Invasion Brigade

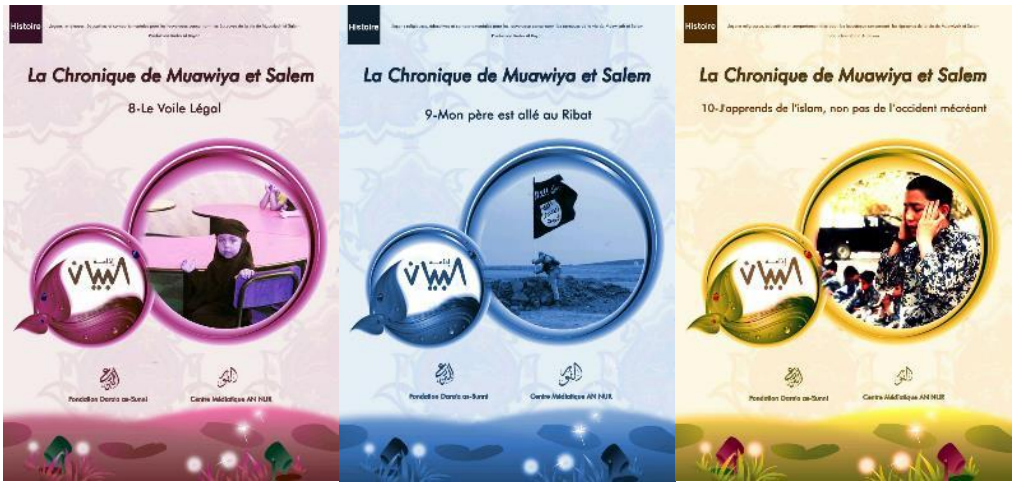
- At the end of June 2020, several telegram channels of the **Nasr communications group** were removed. The group assists in the distribution of Islamic State propaganda materials in French, English, Turkish, and Indonesian.

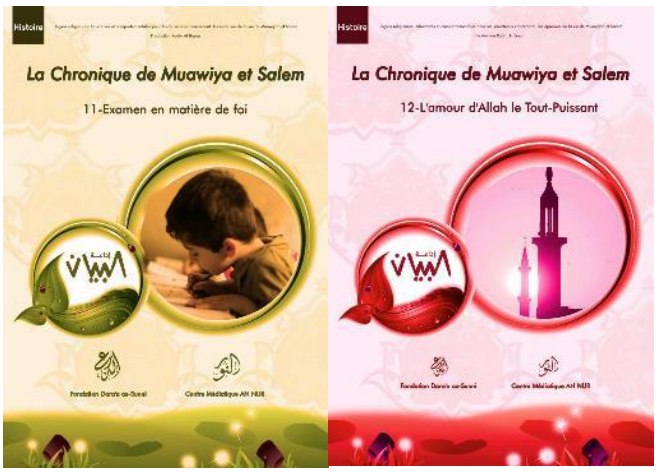
  Before it was removed, the Nasr group's French telegram channel published a series of interviews with children whose parents served in the Islamic State on the importance of fulfilling the jihadist agenda against the enemy, the importance of observing the principles of Islam, learning and more.

[1] Apr-Jun 2020 Telegram.

The series was edited in French by Fondation Dara'a as-Sunni and Centre Mediatique An-Nur, two ISIS-supporting media outlets.[2]

Logo of the Nasr Communication Group





A series of publications in French that studies the lives of the children of ISIS operatives

- The ISIS-affiliated forum, **Shumukh al-Islam**, has published links to a series of daily reports detailing the organization's activities in the various jihadist arenas. The sites to which the links lead are https://archive.fo .[3]

[2] Apr-Jun 2020 Telegram.

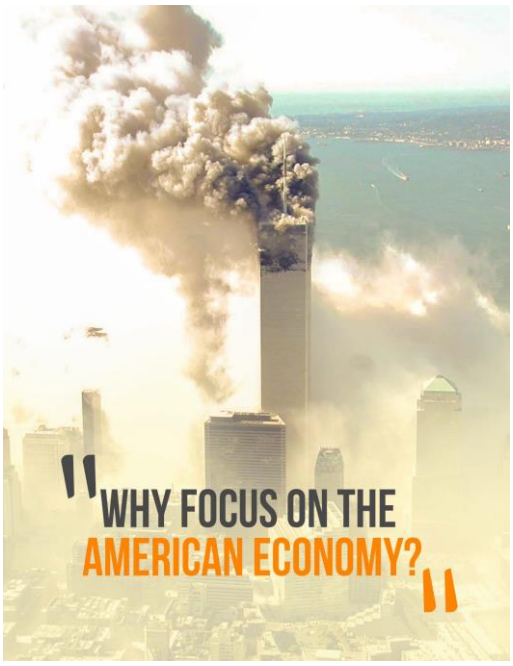
[3] Apr-Jun 2020. https://alshumukh.net/forum/

Banner of one of ISIS daily updates on its activities

- In June 2020, al-Qaeda's leadership published a second issue of **One Ummah** magazine, originally published in Arabic at the end of December 2019. One article discussed the importance of the attack on the US economy, including undermining its power and undermining its efforts to fight jihadists. Regarding leadership, the internet is constantly expanding and thanks to Amazon's programs it is set to expand to remote areas where there was previously no connection to the internet. In light of this, the leadership called specifically for young Muslims to focus on the field of computer science in their studies, in order to develop cybernetic capabilities that would allow them to launch electronic attacks or electronic jihad against the enemies of Islam. They advised young people about to start their studies in higher education institutions to enroll in computer science courses and to set up hacker groups that would learn about electronic attacks, to the point of crystallization into an electronic army.

  It is also written that the Mujahideen have in recent years been able to develop their cyber capabilities in the field of information, indoctrination, and training, as well as in the field of hacking, which is manifested in hacking into enemy servers and Internet networks, hacking online financial activity, hacking banks, stealing vital information and leaking sensitive information. However, according to the leadership, there is still ample room to develop hacking capabilities. The leadership stressed that jihadist organizations must invest considerable resources in human capital to develop offensive cyber capabilities that will be capable of harming critical infrastructure and major online networks.[4]

[4] June 2020, Telegram.



Article published in the second issue of the magazine "One Ummah"

Radicalization

During the period under review, radicalization activity on the Internet continued (in addition to similar activity in the physical world), as part of a general trend of increasing use in the cyber world. Thus, the terrorist organizations and their affiliates make use of widely distributed platforms but at the same time keep their identity and traffic as modest as possible.

Terror fundraising

The practice of financing terrorism through the Internet during the period under review was mainly the domain of jihadist organizations in the Gaza Strip, which identify with ISIS and al-Qaeda. 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 despite being a hybrid organization, which to some extent also affects the bodies affiliated with it. It can be assumed that in this state of affairs the efforts to raise funds through internet platforms will be magnified.

- A financial center in Idlib, Syria, called the **Bitcoin Transfer Center**, which maintains contacts with jihadist activists in the aforementioned region, published leaflets and banners about its financial services on social media. (In Western translation): "Do you want to transfer money from Belgium or the Netherlands to Syria, but do not know how to do it? Or does anyone who wants to send you [money] not know how to buy Bitcoin? Are you afraid to expose your friend or family members to

danger due to the transfer of funds? Do not worry and do not burden yourself with this. Bitcoin Transfer will do this on your behalf. You only need to buy a certain type of tickets, we will inform you about them privately, and we will transfer your money to the Levant with the help of Allah. No identification documents are required at the time of purchasing the tickets. This way is successful with the help of Allah because it has been practically tested in France for several months." The center also provided means of communication with him via WhatsApp and the Telegram.[5]

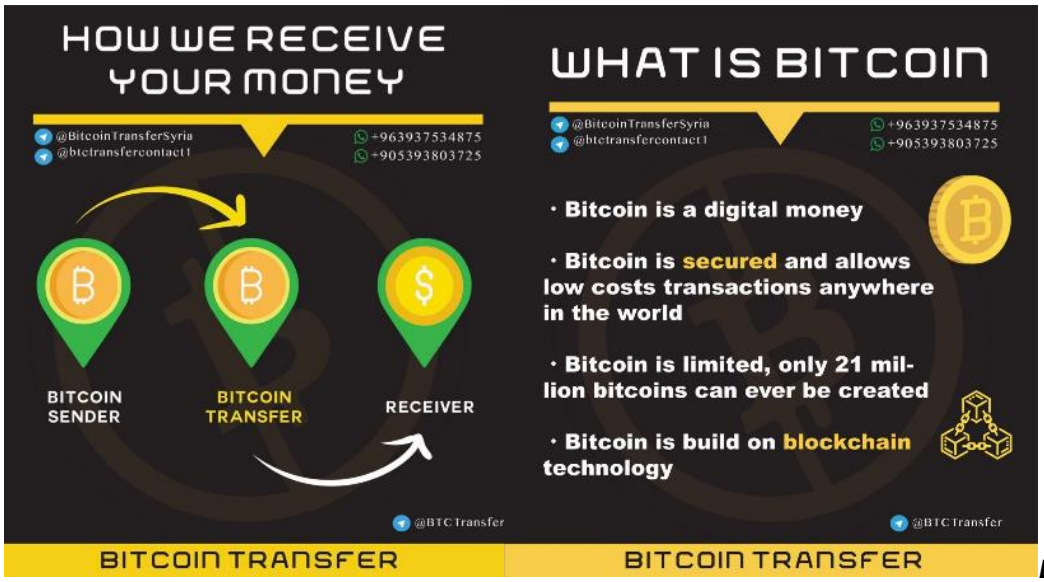
The Bitcoin Transfer Center Finance Center

[5] Apr-Jun, 2020. Telgeram.

Announcement in Arabic, English and Dutch about the center's activities

Purchase card for bitcoin transfer

A banner distributed by the center detailing electronic payment methods

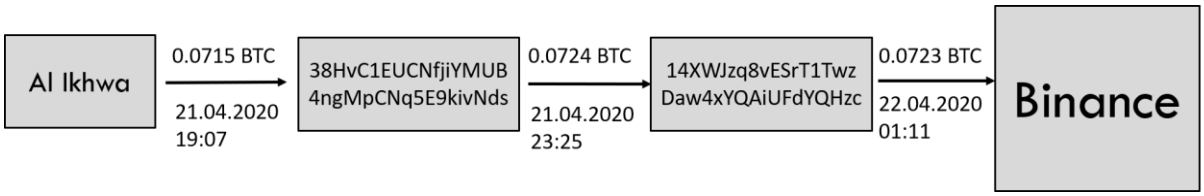


Banners explaining what Bitcoin is and how Bitcoin transfers work

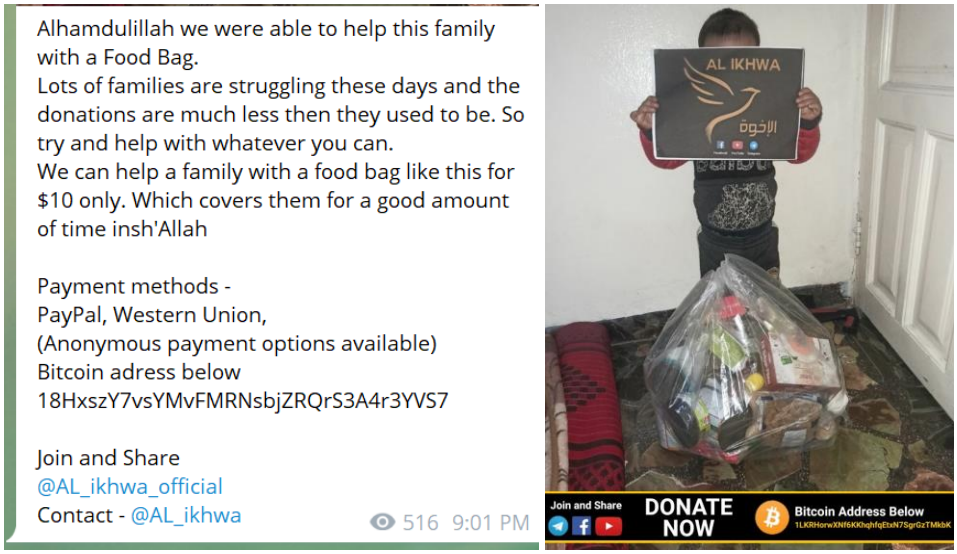
- **Al Ikhwa** - Al Ikhwa is a group that claims to be an independent charity in Syria and that they do not support terrorism. However, analysis of the group's usage of cryptocurrency and social media postings demonstrates otherwise. Al Ikhwa has been linked to Malhama Tactical, a jihadist military company.[6]
    - Many of Al Ikhwa's Telegram posts request donations through PayPal, Western Union and Bitcoin. Their first post stated, in part: "…supporting the brothers in Syria, Wives of [martyrs] and their families…[and] We help those who defend the Muslims in [Syria]. "
    - The Al Ikhwa administrator posted 11 BTC addresses at various points in time asking for potential donations.

[6] August 2020, *United States Department of Justice*

- Al Ikhwa follows a technique called layering, in which it transfers bitcoin through several addresses in a very fast chain to obscure who the intended recipient is. These chains often lead to the virtual exchange, Binance, where it is then impossible to follow.



A chain of transactions demonstrating the layering method used by Al Ikhwa



Telegram post by Al Ikhwa soliciting donations to their Bitcoin address

Defense

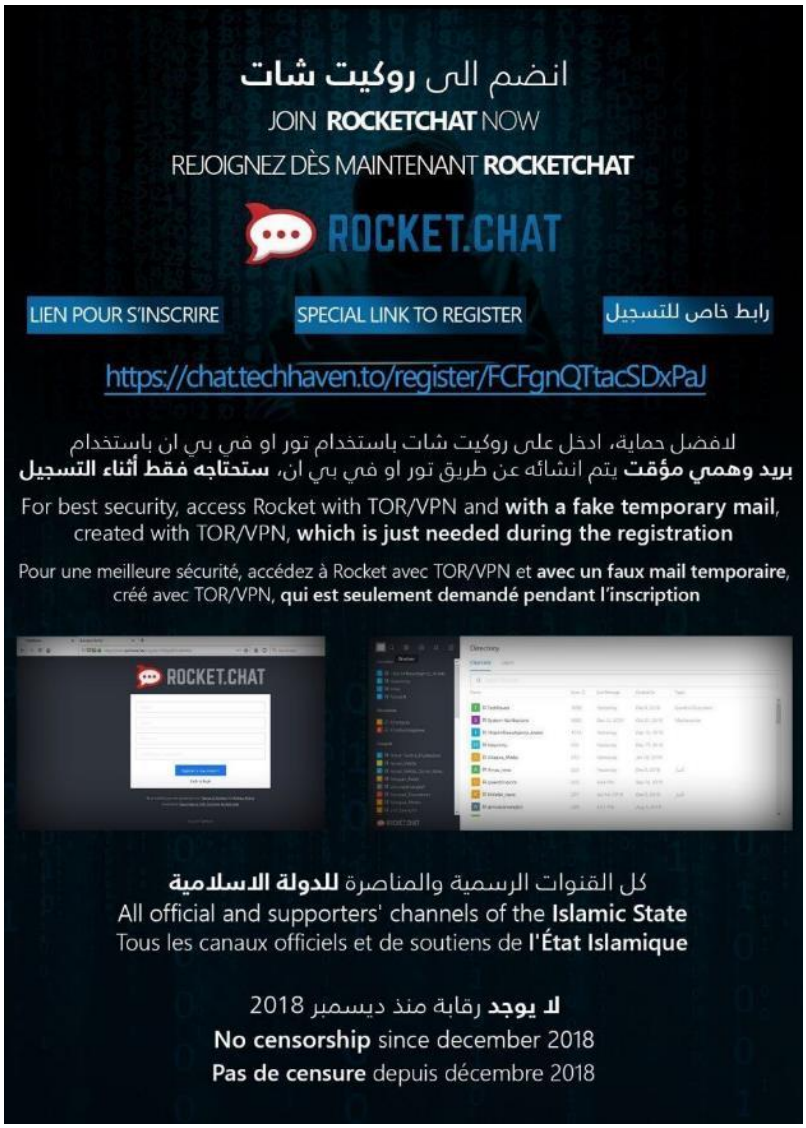
Terrorist organizations are aware of the tireless preventative efforts of security agencies and the activities of the major players on the internet in general and in the social networks in particular, to remove Jihadist content from their platforms. Terrorist organizations continuing therefore to distribute guidelines and instructions and continued to move to the darknet where they claimed to be better able to protect the traffic and anonymity of the organizations themselves, as well as their supporters, from the tracking software of intelligence agencies and activists who operate against terrorist organization on the Internet.

Organizational support for cyber-defense continued with the translation of guidebooks produced by elements unconnected to terrorism, and with the independent production of guidebooks, instructions, and warnings about malware.

- From the publications of the computer section of the jihadist forum **"Shamuh al-Al-Islam"** affiliated with ISIS[7]:
    - A user recommended using the website https://10minutemail.net to distribute the organization's propaganda materials to email addresses. He warned against using Gmail claiming that Google collects information about users through its various services. He also recommended using a VPN like GateVPN to disguise personal computer information.
    - A guide to using the RocketChat encrypted messaging software from a communications agency called Qimmam. The opening remarks of the guide state that since 2018 there has been no supervision of the application, so that it is a "technological safe haven" (TechHeaven) for ISIS supporters. The tyrannical regimes in the West. "In the correspondence, the media institution recommended using the chat applications RockeChat and Hoop.[8]

[7] June 2020, https://alshumukh.net/forum/

[8] June 2020, https://alshumukh.net/forum/



A banner posted on the Shmuh al-Islam forum calling on ISIS supporters to continue consuming the organization's propaganda materials through the Rocket Chat application

- From the publications of the technology section of the weekly publication **"Ibaa"**, which publishes on behalf of the **"Hayat Tahrir al-Sham"** organization in Idlib, Syria[9]:
    - An article on the importance of saving passwords for websites and emails against theft. The article also mentioned tips for keeping passwords secure. For example, it was recommended to write a password that is difficult to identify.
    - An article about alternative search engines for Google on the web. According to the author of the article, the search in the Google engine is not safe because the company collects information about the users and therefore more secure search engines such as DuckDuckGo must be used.

[9] Apr-Jun, 2020. *Ibaa*.

- An article on the importance of using encrypted chats such as Riot.im, Wire, Signal and Conversations. The author warned not to use Messenger, Viber, Whatup chats because they are linked to intelligence means that collect information about users, and also warned against using the Telegram application.
- An article on the importance of saving the user's personal information when surfing the Internet. For example, it is written that it is better to encrypt the data as well as the computer's IP by using the TOR browser while browsing the Internet.
- An article about hacking and encouraging readers to deepen their knowledge of computing and programming to become hackers.
- An article regarding the correct and secure use of mobile Android devices. For example, it is recommended to install encrypted chat applications such as Conversations.

The "Technology Security" section

Defense Guidebooks

- From the publications of the **Al-Afaq Communication Institute**, which is affiliated with the Islamic State and focuses on information for secure web browsing:
  - A message that draws users' attention to the possibility of contacting Al-Afaq's technical staff with questions about technical problems with their computer or mobile phones. To this end, addresses of accounts set up by al-Afaq on the RiotChat, Threema, and Conversations platforms were provided.
  - An article entitled "How do intelligence agents track you?". According to the authors of the article, intelligence agencies are building databases on civilians and taking every step to track people in the name of fighting terrorism. This is done in various ways, such as: intercepting text messages on cell phones; Locating the geographical location of users on the network and cell phones; Hacking attempts at computers, smartphones and social media accounts;

Use of mobile towers and UAVs that track user movements; technology companies like Twitter, Facebook, Telegram; electronic devices that governments use to track the movements of people such as Saudi Arabia that uses a GPS device.

- Instructional video for installing Debian software on a computer running a Linux operating system.
- A new English-language journal called The Supporter's Security. The first issue dealt with tips on securely using a smartphone, surfing the net, and using a computer.

Title Page "The Supporter's Security"

- From the publications of the **Al-Kamam al-Al-Khtronia** media group, which assists in advocacy for ISIS, in April-June 2020[10]:
  - A warning against using Zoom messenger software. This is on the grounds that it has flaws in its security and is under surveillance by intelligence means.
  - A warning about a security breach in Samsung mobile devices that has existed since 2014 .
  - A warning about spying activity on linkedin and TikTok.
  - Technical tips on how to avoid hackers on the WhatsApp application.

[10] Apr-Jun, 2020. RocketChat

Warning against using Zoom messenger software

Offense

Terrorist organizations continued their efforts to improve their offensive capabilities, but at this stage they do not reveal significant technological abilities in this area. Nevertheless, it should be taken into account that these organizations can hire external bodies, such as those who identify with terrorist ideas or organized crime, and can acquire such abilities from terror-supporting states.

- In April 2020, the hacker group **Cyber Caliphate Shield**, which is affiliated with the Islamic State, released a video documenting hacks that its members committed on websites in South Africa and amounted to corruption (DeFacement). They claimed the attacks were carried out in retaliation for their alleged involvement in activities against jihadist operatives.[11]

[11] April, 2020. Telegram.

Banner of the video, and images of vandalism of South African websites

- In another video released by the hacker group **Cyber Caliphate Shield** in June 2020, hacks were recorded on websites in the United States, including the Los Angeles Police Officers Association website, which contained personal information from within the department.[12]

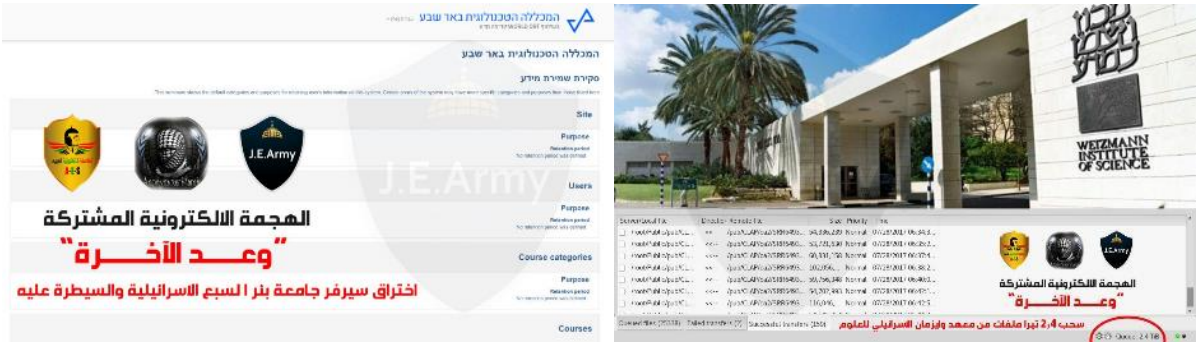
Banner of a video documenting activities for websites

- During April – May 2020, The **Jerusalem Electronic Army**, a group of hackers from Arab countries along with other countries, claimed responsibility for hacking into a series of Israeli academic servers and websites and accounts of Israelis. They took responsibility for a breach at the Be'er Sheva College of Technology, the Weizmann Institute and the bank account of a chemical plant manager in Israel. The group released a video called "The Last Promise" documenting some of the hacking operations it carried out in conjunction with two other hackers, AES and Anonymous Islamic. In addition, the group published a banner detailing the attacks and another banner in which it stated that Israel was hiding the wave of electronic attacks on its servers and sites from the eyes of the Israeli public.
- On May 22, the group claimed responsibility for further hacking operations to mark Jerusalem Day, which was set by former Iranian President Khomeini. This is what she noted in a video and a series of banners that she announced that she had managed to break into four central Israeli servers, including the Knesset website; Institute for Strategic Studies; David College; Served at a yeshiva university and sent training videos of the Izz al-Din al-Qassam Brigades, Hamas' military wing. The

[12] June, 2020. Telegram.

group also claimed that it had hacked into 12,000 Israeli accounts on social media, including 8,000 Facebook accounts and 4,000 email accounts.

Banner of the video of hacking attacks on Israeli servers and websites



Photos showing alleged evidence of the group breaking into Israeli websites

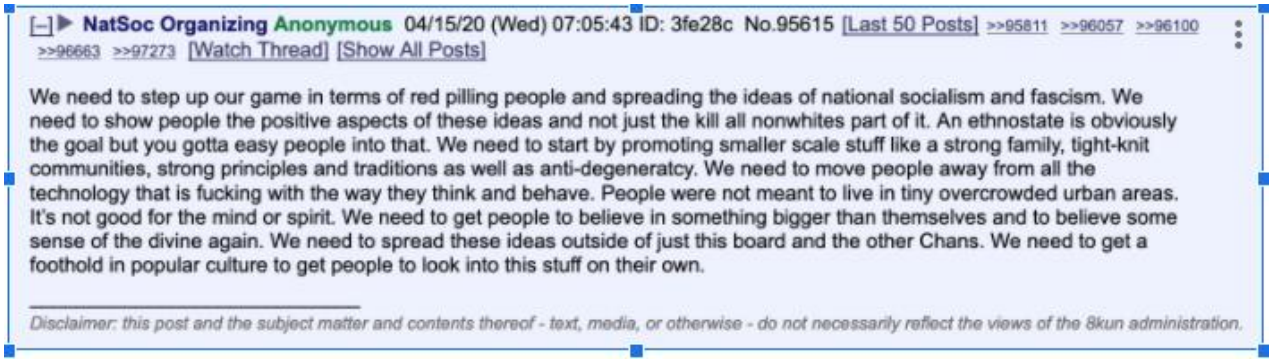
Far-right Extremism

Operational

Propaganda and radicalization

The various forums of the far-right continue spreading propaganda for the purpose of radicalization.

On April 15, 2020, an 8Kun board on the darknet published a post describing the desire to spread the ideas of nationalism, and make people believe in something bigger than themselves. The intent is to spread the idea in more places outside of this board.

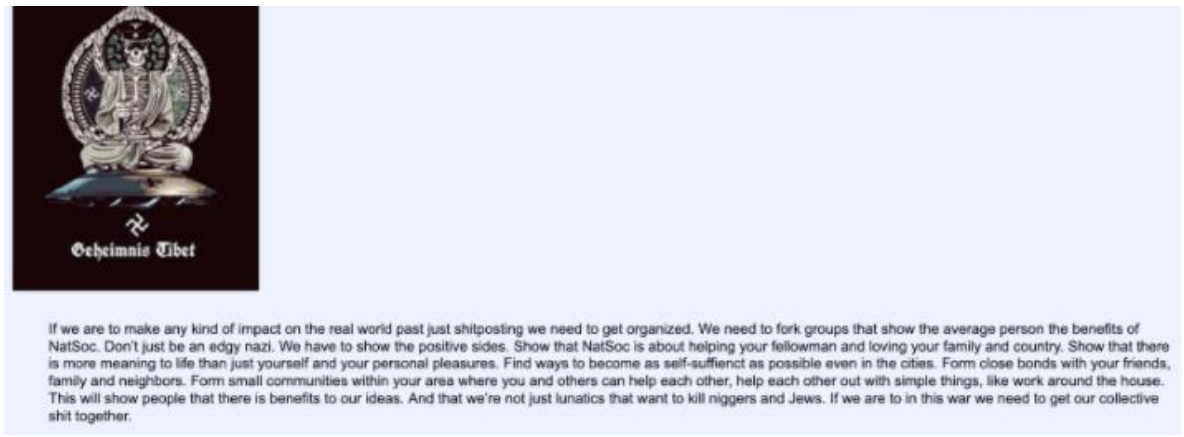


[–] ▶ **NatSoc Organizing Anonymous** 04/15/20 (Wed) 07:05:43 ID: 3fe28c No.95615 [Last 50 Posts] >>95811 >>96057 >>96100 >>96663 >>97273 [Watch Thread] [Show All Posts]

We need to step up our game in terms of red pilling people and spreading the ideas of national socialism and fascism. We need to show people the positive aspects of these ideas and not just the kill all nonwhites part of it. An ethnostate is obviously the goal but you gotta easy people into that. We need to start by promoting smaller scale stuff like a strong family, tight-knit communities, strong principles and traditions as well as anti-degeneratcy. We need to move people away from all the technology that is fucking with the way they think and behave. People were not meant to live in tiny overcrowded urban areas. It's not good for the mind or spirit. We need to get people to believe in something bigger than themselves and to believe some sense of the divine again. We need to spread these ideas outside of just this board and the other Chans. We need to get a foothold in popular culture to get people to look into this stuff on their own.

Disclaimer: this post and the subject matter and contents thereof - text, media, or otherwise - do not necessarily reflect the views of the 8kun administration.

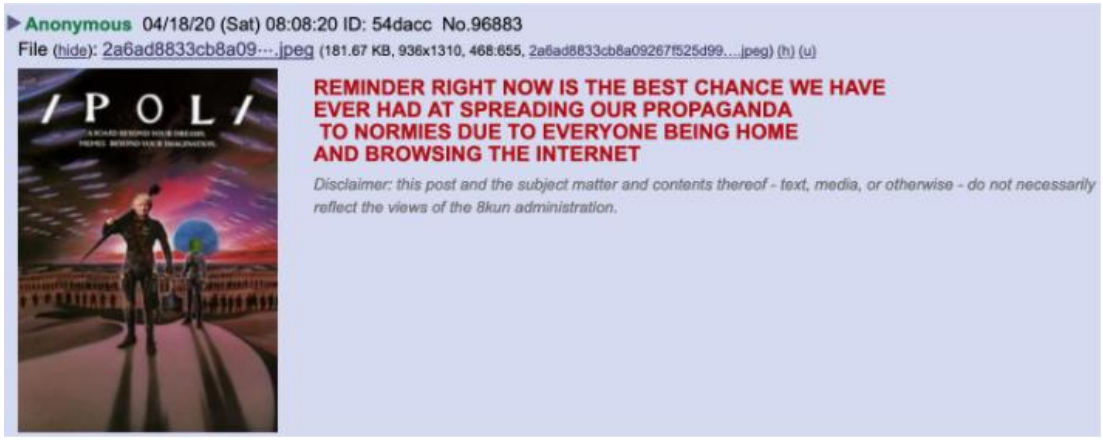
Additionally, on another anonymous board, Endchan (April 13, 2020) the poster intends to convert others to radicalization. The post suggests organizing into groups to spread propaganda. Not to talk about Nazism, but to show that the goal is to help people, to love your family and your country. It is also recommended to establish small communities in the residential area so that it will be possible to help each other. This way people will see that it is not just a group of "crazy" people who want to kill blacks and people will want to join and believe in these ideas.



If we are to make any kind of impact on the real world past just shitposting we need to get organized. We need to fork groups that show the average person the benefits of NatSoc. Don't just be an edgy nazi. We have to show the positive sides. Show that NatSoc is about helping your fellowman and loving your family and country. Show that there is more meaning to life than just yourself and your personal pleasures. Find ways to become as self-suffienct as possible even in the cities. Form close bonds with your friends, family and neighbors. Form small communities within your area where you and others can help each other, help each other out with simple things, like work around the house. This will show people that there is benefits to our ideas. And that we're not just lunatics that want to kill niggers and Jews. If we are to in this war we need to get our collective shit together.

Far-right activists see the fact that people lost their jobs due to the coronavirus as an opportunity to radicalize them.

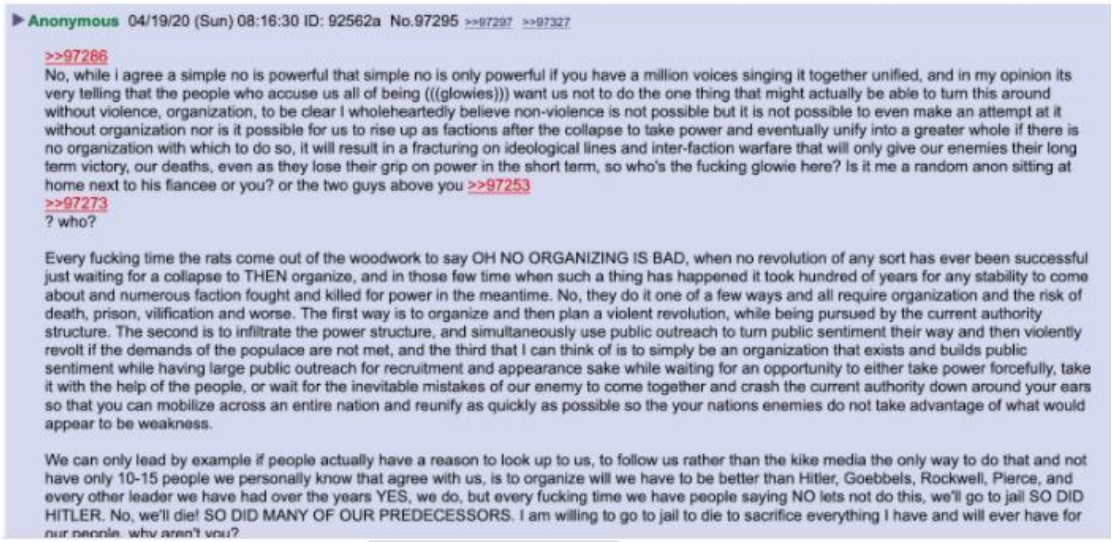
For example, it was claimed in a post published on 8KUN on April 18, 2020 that this is now the most appropriate opportunity for spreading propaganda, since everyone is at home and surfing the Internet.



Another post published on the 8kun board on April 16th claimed that nationalist ideology could be spread through the production of music and games that would be distributed via the Internet and social media. The post claims that many Americans have lost their jobs and therefore this is an opportunity that has never been like it to convince people to support them.

The propaganda includes suggestions for ways to organize and act to recruit people.

For example, a post published on 8Kun on April 19th stated that power will only come if there is unity. It is impossible to act if you do not organize and operate within an organization. The author of this post says that no revolution was successful in which the instigators sat and waited for those in power to fall before they decided to organize and fight back. The author says that in the few occurrences when this did happen, it took hundreds of years to achieve stability afterwards and the interim was filled with violence and needless fatalities. They must therefore act as an organization that recruits people to its ranks. The writer of the post even claims that he is willing to go to jail or even die for the cause and asks others why they are not willing to do the same.



Anonymous 04/19/20 (Sun) 08:16:30 ID: 92562a No.97295 >>97297 >>97327

>>97286
No, while i agree a simple no is powerful that simple no is only powerful if you have a million voices singing it together unified, and in my opinion its very telling that the people who accuse us all of being (((glowies))) want us not to do the one thing that might actually be able to turn this around without violence, organization, to be clear I wholeheartedly believe non-violence is not possible but it is not possible to even make an attempt at it without organization nor is it possible for us to rise up as factions after the collapse to take power and eventually unify into a greater whole if there is no organization with which to do so, it will result in a fracturing on ideological lines and inter-faction warfare that will only give our enemies their long term victory, our deaths, even as they lose their grip on power in the short term, so who's the fucking glowie here? Is it me a random anon sitting at home next to his fiancee or you? or the two guys above you >>97253
>>97273
? who?

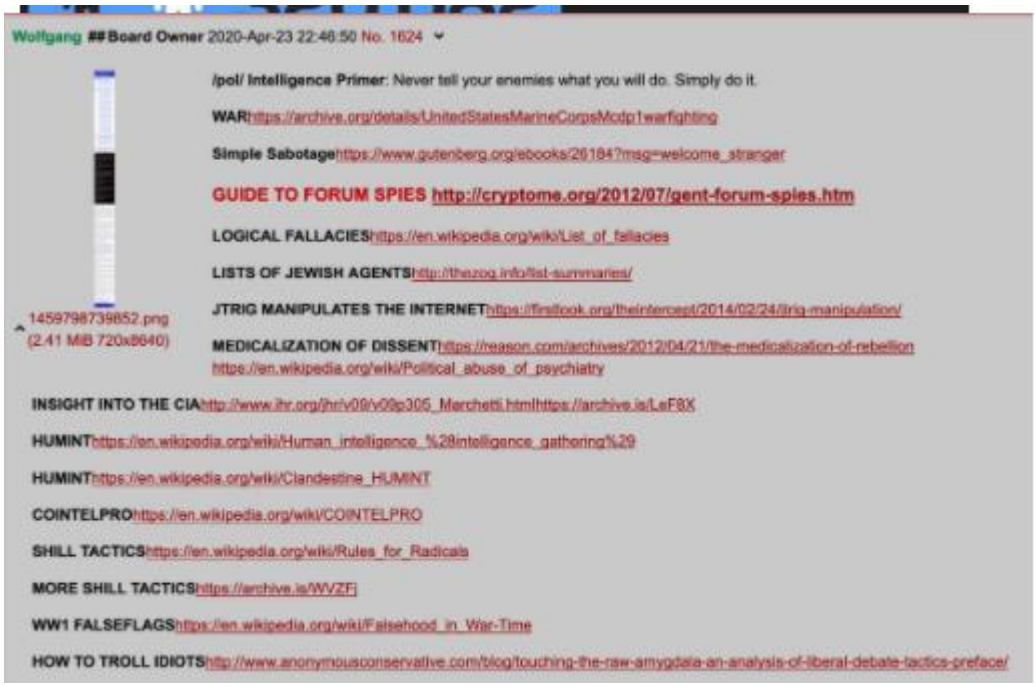
Every fucking time the rats come out of the woodwork to say OH NO ORGANIZING IS BAD, when no revolution of any sort has ever been successful just waiting for a collapse to THEN organize, and in those few time when such a thing has happened it took hundred of years for any stability to come about and numerous faction fought and killed for power in the meantime. No, they do it one of a few ways and all require organization and the risk of death, prison, vilification and worse. The first way is to organize and then plan a violent revolution, while being pursued by the current authority structure. The second is to infiltrate the power structure, and simultaneously use public outreach to turn public sentiment their way and then violently revolt if the demands of the populace are not met, and the third that I can think of is to simply be an organization that exists and builds public sentiment while having large public outreach for recruitment and appearance sake while waiting for an opportunity to either take power forcefully, take it with the help of the people, or wait for the inevitable mistakes of our enemy to come together and crash the current authority down around your ears so that you can mobilize across an entire nation and reunify as quickly as possible so the your nations enemies do not take advantage of what would appear to be weakness.

We can only lead by example if people actually have a reason to look up to us, to follow us rather than the kike media the only way to do that and not have only 10-15 people we personally know that agree with us, is to organize will we have to be better than Hitler, Goebbels, Rockwell, Pierce, and every other leader we have had over the years YES, we do, but every fucking time we have people saying NO lets not do this, we'll go to jail SO DID HITLER. No, we'll die! SO DID MANY OF OUR PREDECESSORS. I am willing to go to jail to die to sacrifice everything I have and will ever have for our people, why aren't you?

Defense

Far-right activists are striving to protect their identity in cyberspace.

For example, a post was published on 9Chan (April 23, 2020) that provides links that instruct how to maintain anonymity online and how to identify "agents".



Wolfgang ## Board Owner 2020-Apr-23 22:46:50 No. 1624

1459798739852.png
(2.41 MiB 720x8640)

/pol/ Intelligence Primer: Never tell your enemies what you will do. Simply do it.

WAR https://archive.org/details/UnitedStatesMarineCorpsMcdp1warfighting

Simple Sabotage https://www.gutenberg.org/ebooks/26184?msg=welcome_stranger

GUIDE TO FORUM SPIES http://cryptome.org/2012/07/gent-forum-spies.htm

LOGICAL FALLACIES https://en.wikipedia.org/wiki/List_of_fallacies

LISTS OF JEWISH AGENTS http://thezog.info/list-summaries/

JTRIG MANIPULATES THE INTERNET https://firstlook.org/theintercept/2014/02/24/jtrig-manipulation/

MEDICALIZATION OF DISSENT https://reason.com/archives/2012/04/21/the-medicalization-of-rebellion
https://en.wikipedia.org/wiki/Political_abuse_of_psychiatry

INSIGHT INTO THE CIA http://www.ihr.org/jhr/v09/v09p305_Marchetti.html https://archive.is/LeF8X

HUMINT https://en.wikipedia.org/wiki/Human_intelligence_%28intelligence_gathering%29

HUMINT https://en.wikipedia.org/wiki/Clandestine_HUMINT

COINTELPRO https://en.wikipedia.org/wiki/COINTELPRO

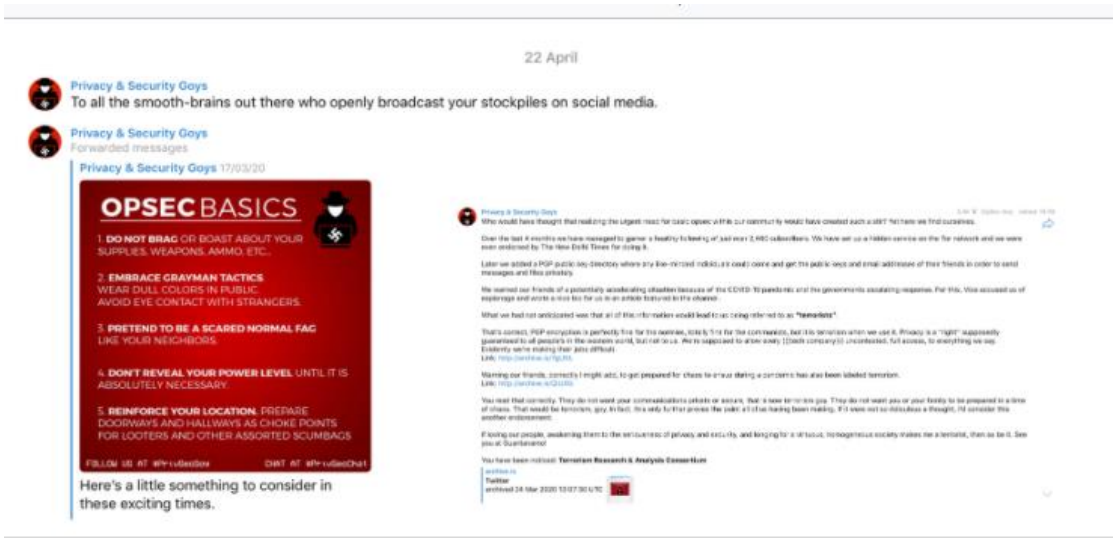
SHILL TACTICS https://en.wikipedia.org/wiki/Rules_for_Radicals

MORE SHILL TACTICS https://archive.is/WVZFi

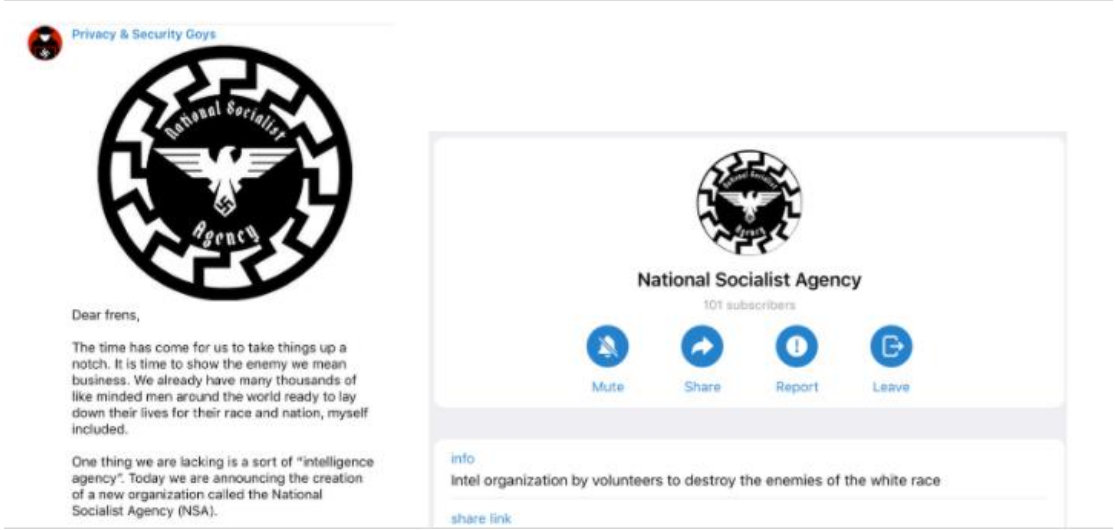
WW1 FALSEFLAGS https://en.wikipedia.org/wiki/Falsehood_in_War-Time

HOW TO TROLL IDIOTS http://www.anonymousconservative.com/blog/touching-the-raw-amygdala-an-analysis-of-liberal-debate-tactics-preface/

On the Telegram channel (April 22, 2020), additional rules were published explaining how to maintain anonymity online.



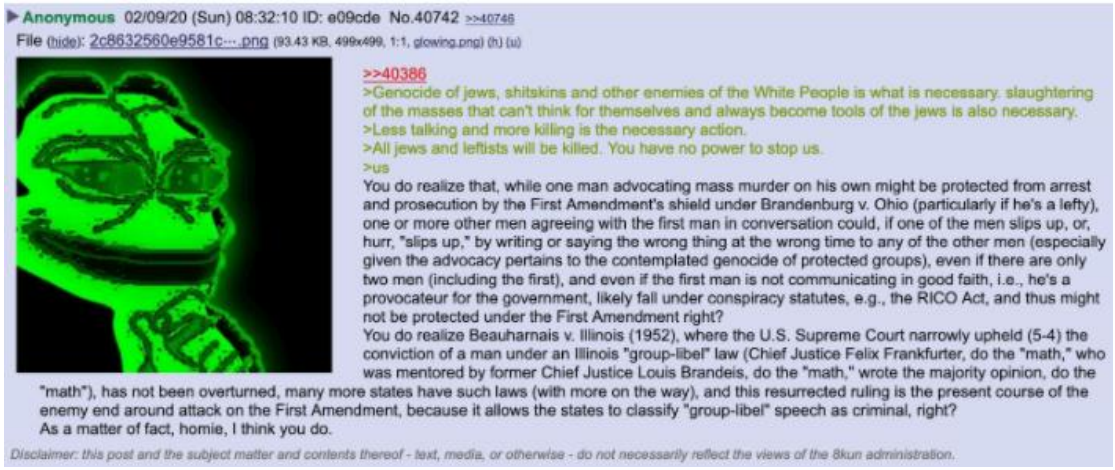
In order to protect themselves from security forces and "traitors", on April 15, 2020, the National Socialist Agency (NSA) announced the establishment of an "intelligence agency" – the agency will take part in people from all over the world who share the same views concerning racial ideology.



Offense

Right-wing activists are writing posts calling for the killing of minorities.

For example, 8Kun published a call for the killing of Jews, leftists, and other enemies of "whites", such as people who are led by the Jews and do not know how to think for themselves.



Anonymous 02/09/20 (Sun) 08:32:10 ID: e09cde No.40742 >>40746

File (hide): 2c8632560e9581c···.png (93.43 KB, 499x499, 1:1, glowing.png) (h) (u)

>>40386

>Genocide of jews, shitskins and other enemies of the White People is what is necessary. slaughtering of the masses that can't think for themselves and always become tools of the jews is also necessary.

>Less talking and more killing is the necessary action.

>All jews and leftists will be killed. You have no power to stop us.

>us

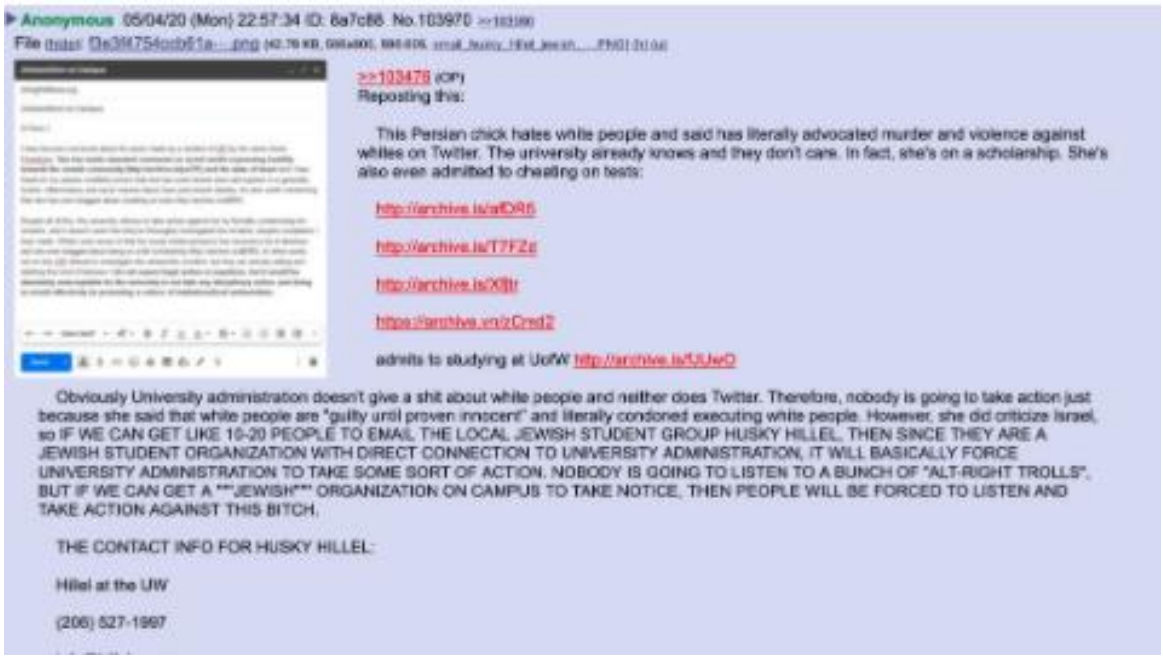
You do realize that, while one man advocating mass murder on his own might be protected from arrest and prosecution by the First Amendment's shield under Brandenburg v. Ohio (particularly if he's a lefty), one or more other men agreeing with the first man in conversation could, if one of the men slips up, or, hurr, "slips up," by writing or saying the wrong thing at the wrong time to any of the other men (especially given the advocacy pertains to the contemplated genocide of protected groups), even if there are only two men (including the first), and even if the first man is not communicating in good faith, i.e., he's a provocateur for the government, likely fall under conspiracy statutes, e.g., the RICO Act, and thus might not be protected under the First Amendment right?

You do realize Beauharnais v. Illinois (1952), where the U.S. Supreme Court narrowly upheld (5-4) the conviction of a man under an Illinois "group-libel" law (Chief Justice Felix Frankfurter, do the "math," who was mentored by former Chief Justice Louis Brandeis, do the "math," wrote the majority opinion, do the "math"), has not been overturned, many more states have such laws (with more on the way), and this resurrected ruling is the present course of the enemy end around attack on the First Amendment, because it allows the states to classify "group-libel" speech as criminal, right?

As a matter of fact, homie, I think you do.

Disclaimer: this post and the subject matter and contents thereof - text, media, or otherwise - do not necessarily reflect the views of the 8kun administration.

Far-right activists continue to implement doxxing. In a post on 8Chan (May 4, 2020) details were published of a student of Persian descent who is alleged to have said on Twitter that she hates boys and is willing to kill them. According to the writers of the post, the university where she studies were aware of the situation, but did nothing. The post contains the student's personal details, including telephone and address.



Anonymous 05/04/20 (Mon) 22:57:34 ID: 8a7c88 No.103970

>>103478 (OP)

Reposting this:

This Persian chick hates white people and said has literally advocated murder and violence against whites on Twitter. The university already knows and they don't care. In fact, she's on a scholarship. She's also even admitted to cheating on tests:

http://archive.is/atDAt

http://archive.is/T7FZz

http://archive.is/XBtr

https://archive.vn/zCred2

admits to studying at UofW http://archive.is/UUwO

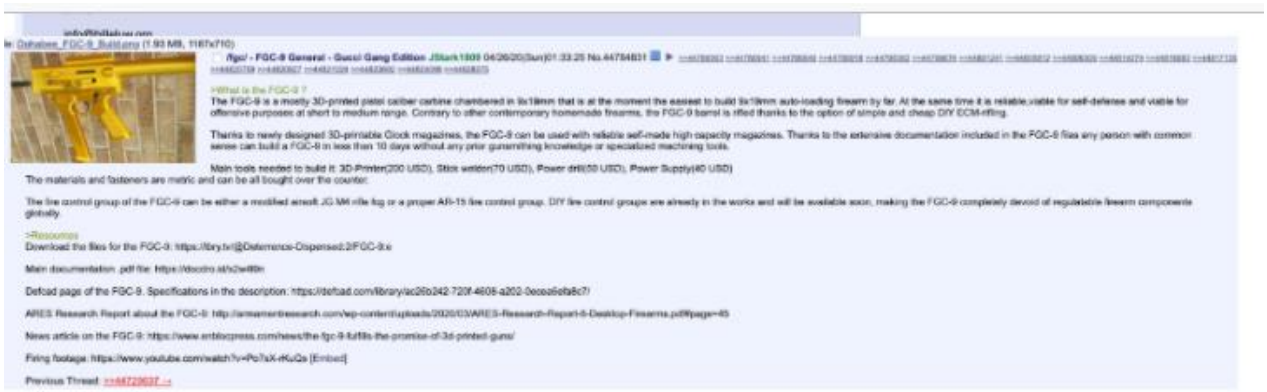
Obviously University administration doesn't give a shit about white people and neither does Twitter. Therefore, nobody is going to take action just because she said that white people are "guilty until proven innocent" and literally condoned executing white people. However, she did criticize Israel, so IF WE CAN GET LIKE 10-20 PEOPLE TO EMAIL THE LOCAL JEWISH STUDENT GROUP HUSKY HILLEL, THEN SINCE THEY ARE A JEWISH STUDENT ORGANIZATION WITH DIRECT CONNECTION TO UNIVERSITY ADMINISTRATION, IT WILL BASICALLY FORCE UNIVERSITY ADMINISTRATION TO TAKE SOME SORT OF ACTION. NOBODY IS GOING TO LISTEN TO A BUNCH OF "ALT-RIGHT TROLLS", BUT IF WE CAN GET A ""JEWISH"" ORGANIZATION ON CAMPUS TO TAKE NOTICE, THEN PEOPLE WILL BE FORCED TO LISTEN AND TAKE ACTION AGAINST THIS BITCH.

THE CONTACT INFO FOR HUSKY HILLEL:

Hillel at the UW

(206) 527-1997

Various posts publish guidelines for printing weapons with a 3D printer. In April, a post was published on 8Kun (April 26, 2020) with a link for 3D printing of weapons.



/fgc/ - FGC-9 General - Gucci Gang Edition

>What is the FGC-9 ?

The FGC-9 is a mostly 3D-printed pistol caliber carbine chambered in 9x19mm that is at the moment the easiest to build 9x19mm auto-loading firearm by far. At the same time it is reliable,viable for self-defense and viable for offensive purposes at short to medium range. Contrary to other contemporary homemade firearms, the FGC-9 barrel is rifled thanks to the option of simple and cheap DIY ECM-rifling.

Thanks to newly designed 3D-printable Glock magazines, the FGC-9 can be used with reliable self-made high capacity magazines. Thanks to the extensive documentation included in the FGC-9 files any person with common sense can build a FGC-9 in less than 10 days without any prior gunsmithing knowledge or specialized machining tools.

Main tools needed to build it: 3D-Printer(200 USD), Stick welder(70 USD), Power drill(50 USD), Power Supply(40 USD)

The materials and fasteners are metric and can be all bought over the counter.

The fire control group of the FGC-9 can be either a modified airsoft JG M4 rifle fcg or a proper AR-15 fire control group. DIY fire control groups are already in the works and will be available soon, making the FGC-9 completely devoid of regulatable firearm components globally.

>Resources

Download the files for the FGC-9:

Main documentation .pdf file:

Defcad page of the FGC-9. Specifications in the description:

ARES Research Report about the FGC-9:

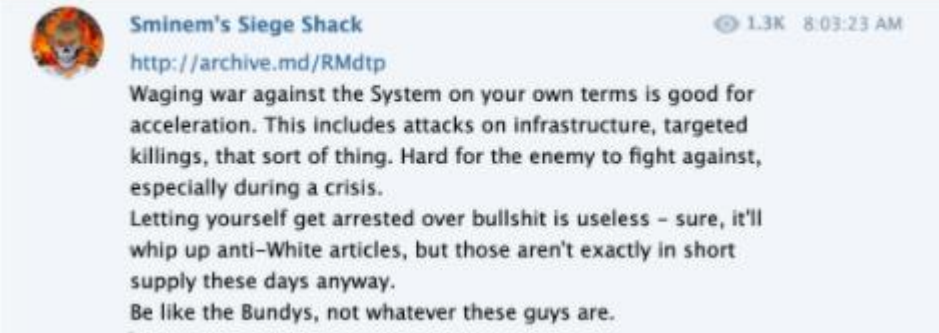
News article on the FGC-9:

Firing footage:

Previous Thread:

Various posts call for kinetic attacks.

In one of the posts on Telegram (May 06, 2020), for example, they call for a war against infrastructure and targeted killings, claiming that it is difficult for the enemy to fight against this type of attacks, especially during the coronavirus period.



Sminem's Siege Shack 1.3K 8:03:23 AM

http://archive.md/RMdtp

Waging war against the System on your own terms is good for acceleration. This includes attacks on infrastructure, targeted killings, that sort of thing. Hard for the enemy to fight against, especially during a crisis.

Letting yourself get arrested over bullshit is useless - sure, it'll whip up anti-White articles, but those aren't exactly in short supply these days anyway.

Be like the Bundys, not whatever these guys are.

Geopolitics and Terrorism

- Germany - On May 28, The German Ministry of Foreign Affairs announced that the German federal prosecutor had issued a sealed arrest warrant for Dmitry Sergeyevich Badin, a Russian military intelligence officer, over the 2015 **Bundestag hack**. The breach led to the infiltration of 16 GB of sensitive emails and documents, and caused other damage to the extent that the Parliament's information technology network had to be completely reworked. The ministry also announced that they would pressure the EU to implement restrictive measures (EU cyber sanctions) against Badin and anyone involved in the Bundestag hack. [13]
- The EU is preparing to impose sanctions on a group of Russian hackers, after the German government announced it "has evidence" related to members of a Russian hacking group in the 2015 Bundestag. Implementing restrictions in response to an attack like this would signal that sanctions would likely be imposed on anyone who commits a similar attack. [14]
- Australia - The Australian government announced plans to set up the country's first task force dedicated to combating disinformation campaigns, under the Ministry of Foreign Affairs and Trade (DFAT). Foreign Minister Maris Payne accused China and Russia of "using the pandemic to undermine liberal democracy" by spreading misinformation to manipulate the discussion on social media. [15]
- Israel - In April, Israel foiled an attempted cyberattack against its water systems, allegedly by Iran. The head of Israel's national cyber network, Yigal Unna, stated that the goal was to disrupt Israel's humanitarian water system. The attack was designed to cause physical damage through hacked command and control systems. This is a sign of the transition to the use of cyberattacks aimed at humanitarian purposes. [16]

[13] https://www.lawfareblog.com/case-against-eu-cyber-sanctions-bundestag-hack

[14] https://www.politico.eu/article/europe-reached-its-tipping-point-on-russian-hacking-germany-bundestag-cyberattack/

[15] https://theconversation.com/chinas-disinformation-threat-is-real-we-need-better-defences-against-state-based-cyber-campaigns-141044?&web_view=true

[16] https://www.israelhayom.com/2020/05/28/failed-cyberattack-on-israel-was-designed-to-trigger-a-humanitarian-disaster/

Legislation, Policy, and Regulations

- Hundreds of professionals in the field from the Department of Defense, other federal agencies, along with other countries worked together at the Joint Headquarters in Suffolk, Virginia, as part of the 19-1 **Cyber Flag**, a cyber exercise meant to help prepare for cyber-attacks and build partnerships between participants.[17]
- U.S. Cyber Command and the National Guard created a new portal called **Cyber 9-Line** to provide a two-way interface for sharing malware and gaining understanding of the cyber threats facing the state. With this new interface, those on guard can relay events to cyber control, who can respond quickly, offer analysis, and help address any problems. [18]
- The UK Ministry of Defense (MoD) has officially executed a cyber security division, called **The13th Signal Regiment**, dedicated to the protection of the UK defense networks for operations taking place within the UK and overseas.

  The 13th Signal Regiment will be in charge of providing "digital armor" to members of the armed forces in order to provide security to military personnel in the use of their IT and communications systems while under fire. The ministry said competitors and hostile players were already forming a “cyber frontline”, and as the landscape of the fighting develops, digital and cyber capabilities could be increasingly important to national security. [19]

Government and Critical Infrastructure

- A bipartisan group of lawmakers introduced legislation in the House of Representatives that will create a position for a national cyber security director who will be responsible for the cybersecurity efforts of the government. The person in this position will serve as the president's key adviser on cybersecurity along with other technological issues. The director

[17] https://www.defense.gov/Explore/News/Article/Article/1896846/cyber-flag-exercise-focuses-on-partnerships/

[18] https://www.defensenews.com/dod/cybercom/2020/06/09/cyber-command-creates-new-malware-sharing-portal-with-national-guard/?&web_view=true

[19] https://www.computerweekly.com/news/252484225/Ministry-of-Defence-forms-new-cyber-security-regiment#:~:text=Based%20at%20Blandford%20in%20Dorset,comms%20systems%20while%20under%20fire.

will be responsible for overseeing the formation and implementation of a national cybersecurity strategy for the US. [20]

[20] https://thehill.com/policy/cybersecurity/504605-lawmakers-introduce-legislation-to-establish-national-cybersecurity?&web_view=true

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