Cyber Updates

January - March 2020
# Table of Content

**Executive Summary** .................................................................................................................. 3

**Operational** ............................................................................................................................... 5

- Recruitment ................................................................................................................................. 5
- Finance .......................................................................................................................................... 6

**Defense** .................................................................................................................................... 7

**Offense** ..................................................................................................................................... 10

**Far Right** .................................................................................................................................. 11

**Operational** ................................................................................................................................ 11

- Propaganda and Radicalization .................................................................................................... 11
- Encouragement for Lone Wolf Attacks ......................................................................................... 13

**Defense** .................................................................................................................................... 14

**Offense** ..................................................................................................................................... 16

**International Response** .......................................................................................................... 19

- Government and Critical Infrastructure ......................................................................................... 19
- Legislation, Policy and Regulations ............................................................................................... 20
- Geopolitics and Terrorism .............................................................................................................. 21
- Cyberspace Collaboration ............................................................................................................... 22
Executive Summary

The potential of cyberspace has been 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. If at first terror organization had static web sites then later basic interactive elements have been incorporated and today, through social media and various applications, these organization are active online with full interactive suite. 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 one 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 (Jan-Mar 2020) terror activity in cyberspace has been identified in three major aspects:

**Operational** – Jihadi organizations keep using 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 keep their efforts to improve their offensive capabilities, especially in relation hacking social media accounts, defacing web sites 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 an 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 serve, 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 (Jan-Mar 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. Telegram channels in November 2019) and raise funds (increased use of jihadi activity of social media, especially in the Idlib region).

**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 one 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 several co-operations, either within the same country or cross border, between government entities and academia and the private sector to protect from cyber threats. It would seem that countries strive to develop AI systems to contend with cyber-attacks on the one hand and to protect the training modules of AI systems. That said, the UK has embarked on the formation of a new entity that will perform offensive cyber-attacks as part of the UK’s efforts to contend with cyber threats.
Operational

Within the operational uses jihadi organizations keep using cyberspace for a variety of uses, the most prominent of those were **propaganda to recruit activists and fundraising campaigns** as follows:

**Recruitment**

– In February 2020, Jihadists in Idlib launched, on the backdrop of the increased attacks by the Russians and the Syrian regime, a campaign titled “I am a Muslim” aimed at recruiting young men to the ranks of their organization. It was conducted in mosques and refugee camps as well as online under #I am Muslim. In response some Idlib residents expressed their solidarity and support with the jihadists¹ but its actual achievements are unknown.

![A jihadist with a banner of the "I am Muslim" campaign](image)

– **Saraya al-Muqawama al-Shabiyya**, a civilian organization supported by Hayat Tahrir al-Sham, launched, both in the public space and social media a campaign called “you will never pass”. It was meant to recruit civilians to assist with the fortification of the front lines vis a vis the Russians and the Assad forces, either financially or by joining jihadi ranks to assist with tunnel excavation².

¹ Feb, Telegram; Feb 11, 2020, Twitter. [https://twitter.com/mosleem77/status/1227315521013547010](https://twitter.com/mosleem77/status/1227315521013547010)
² Feb, Telegram; [https://www.facebook.com/PopResBr/](https://www.facebook.com/PopResBr/)
Finance

Terror finance via the internet within the reviewed period was mainly observed with jihadi organizations in Gaza, identifying with either ISIS or al-Qaeda. We will likely see continued efforts on this front.

– Al-Nasr Saladin Brigades, a Gaza jihadi organization supported by Iran kept running a fundraising campaign under the name Madid (Assist). The campaign has been running for two years on social media, mainly Twitter and telegram. Any potential donor is requested to contact a designated Telegram channel. Per the organizers, the campaign was meant to support mujahidin in Palestine and help them prepare for the war against the Jews. In January 2020 the cyber desk at ICT identified a money transfer from Iran to the organization’s Bitcoin wallet. For expansion see ICT’s article on the above.

3 Jan- Mar, 2020. Telegram
4 https://www.ict.org.il/Article/2488/Identifying_Money_Transfers_and_Terror_Finance_Infrastructure#gsc.tab=0
Defense
In the reviewed period no major innovation has been observed with the cyber defense strategies of terrorists. The trend of disseminating content on security and encryption, privacy and anonymity and instructions for a safe use of mobile devices continued, as follows:

- **Ibaa magazine, owned by Hayat Tahrir al-Sham**, posted during the reviewed period a section called “your technological security”. It included articles of safe web browsing, secure use of mobile devices and more. For example, in vol. 88 (February 15th, 2020) an article cautioning mujahidin from using BlueFrag operating system because it was full of security vulnerabilities capitalized on by hackers to steal personal information5.

- **Al-Qimmam al-Iliqtruniyya** media outlet, assisting with ISIS propaganda, mentioned that it renewed its Telegram, Riot.im and Rocket.Chat. In a banner posted by it, it mentioned that its job was to provide Muslims an information on electronic security, internet, social media, apps, software, computers and smart phones6.

![Banner explaining the organization’s role with online security](image)

- **Afaaq** media outlet, assisting with ISIS propaganda, posted in the reviewed period a series of manuals on secure web usage. Among other the following saw light:
  - A manual on the use of ESET mobile security software for Android7.

---

6 14.1.2020. [https://alshumukh.net/](https://alshumukh.net/)
7 3.2.2020. [https://ehorizons.info/?p=5919](https://ehorizons.info/?p=5919)
o A manual on the use of Gajim, an encrypted instant messaging platform\(^8\).

o A weekly update on security vulnerabilities, security add-ons and cyber world news. For example, update no\# 77 (March 20\(^{th}\), 2020) featured an article on a woman arrested in New York for an illegal Bitcoin trading.

o Encouragement to users to use VPNs in light of COVID-19 and office closures etc.\(^9\).

o A Q&A archive for web security and safe browsing\(^10\).

o An address (in Arabic and English) to users cautioning from logging into accounts posing as Afaaq accounts. Per Afaaq, these are fake accounts operated by intelligence agencies to capture ISIS supporters\(^11\).

---

\(^8\) 31.3.2020. [https://ehorizons.info/?p=6178](https://ehorizons.info/?p=6178)

\(^9\) 20.3.2020. [https://ehorizons.info/?p=6140](https://ehorizons.info/?p=6140)

\(^10\) 11.2.2020. [https://ehorizons.info/?p=4386](https://ehorizons.info/?p=4386)

\(^11\) 8.3.2020. [https://ehorizons.info/?p=5842](https://ehorizons.info/?p=5842)
On Shumukh al-Islam forum, identified with ISIS, some members discussed temporary replacement to Telegram in light of the mass removal of ISIS supporting accounts in November 2019 by Europol. One member suggested Tam Tam, another Riot.Chat however another member objected to the latter until it full advantages and disadvantages are known. “right now, we are using the Riot platform via Tor or VPN and we don’t need a number or an email address”12.

Offense

Terrorist organizations continued their efforts to improve their offensive capabilities, especially in connection to hacking social media accounts, Defacing web sites and planting malware. It seems that AQAP (al-Qaeda Arabian Peninsula) wished to motivate Muslims to allocate resources into cyber-attacks against the west. The following events have been observed:

- On February 3rd, 2020 AQAP posted a video featuring Qasim al-Rimi, its leader, claiming responsibility for an attack perpetrated by a Saudi gunman at a U.S. Navy base in Pensacola, FL on December 3rd, 2019. Alongside that, al-Rimi called upon Muslims residing in the west to attack (e.g. knifing) western targets, the U.S. especially. Additionally, he called upon people who possess cyber knowledge to cyber-attack American banks and corporations.\(^\text{13}\)

- APTC-23, a group identified with Hamas, planted malware into hundreds of IDF troops smart phones through fake profiles on social media. The malware was capable of letting the sender take control of the phone. To decrease suspicions the hackers used a variety of hashtags. Three apps used by the hackers to plant the malware were GrixyApp, ZatuApp, Catch&See. These apps are intended to transmit photos between users that shortly thereafter are being deleted, much like Snap. The apps were downloadable only via a link and they had requested multiple authorizations. Once downloaded and installed, the malware enabled Hamas to take control of the

\(^{13}\) 3.2.20. Rocket.Chat.
infected smartphone. For the first time, Hamas also used Telegram to start talking to IDF troops (February 16th, 2020)."}

Far Right

Far right activists have been active in cyberspace for years yet their presence in the medium has increased since February 2020, likely due to COVID-19 pandemic that forced people to stay indoors and caused an uptick of internet and social media use.

Operational

Far right activists are making extensive use of the internet for operational purposes, the most prominent of which are propaganda to disseminate their ideology, radicalization, recruitment and inspiration to perpetrate lone “wolf attacks”, as follows:

Propaganda and Radicalization

- Neinchchan forum on the dark web, home to many far-right activists, a post regarding the importance of propaganda, influencing people and recruiting them for white supremacy ideology (January 28th, 2020).

The importance of recruiting people to support white supremacy ideology (Neinchchan)

- 8Kun forum on the dark web is a place where many far-right activists write anonymous posts meant to disseminate far right ideology. Additionally, that forum enables the participants to anonymously consult with one another. Among the topics:

14 http://www.idftweets.co.il/article.php?id=730; https://tech.walla.co.il/item/3341198
- Lists of content recommended for dissemination including about the Holocaust, Israel, a conspiracy theory about a plan to “murder and expel the white race from Europe” (Kalergi Hooton Plan) and more (January 20th, 2020).

Disseminating radical content (8Kun)

- A post by a lecturer seeking advice on select chapters of Hitler’s Mein Kampf who have not been edited, in order to teach the students about race and struggle issues (February 19th, 2020).

Mein Kampf consultation (8Kun)

- Posts on activist recruitment. For example, a Bulgarian far right channel posted that due to the increased presence of paid informants they should beware and carefully vet new recruits. A list of rules to follow during a recruitment process was attached, such as: (i) any activist should recruit as many people as they can, preferably ones that they have known for a long time; (ii) the new recruit is to be introduced only after an approval of the leadership;
(iii) a determination regarding its new recruit’s security clearance has to be made etc. (March 6th, 2020).

Encouragement for Lone Wolf Attacks

Calls to perpetrate Lone Wolf attacks were made on forums and social media platforms, as follows:

- On Neinchan, which allows for anonymous postings, it was written that when Lone Wolves are concerned there are no commanders or cells. A person is his own commander and the one that selects the target and the time of the attack because organizations are doomed to fail and be persecuted by the FBI (January 24th, 2020).
What is a Lone Wolf attack (Neinchan)

Also on Neinchan, a post titled “How to Radicalize Yourself” said that in order to become a mass shooter one must forgo life as part of society for the ideals one believes in because society chains the individual and makes him a slave. That, per the writer is what separates a members of society who is a slave from heroes like Tarrant (the perpetrator of the Christchurch Massacre in 2019) and Breivik (who has killed dozens in Norway in 2011), who were willing to sacrifice everything for what they believed in (January 10th, 2020).

How to Radicalize Yourself

Defense

In the period reviewed trend of content dissemination on security and encryption, privacy and anonymity, warnings of imposters and instructions for secure use of mobile devices has been observed as follows:

On 8Kun forum, frequented by far-right activists, several posts were uploaded on net anonymity. For example, a link to a guide to anonymous browsing access to blocked sites was posted (February 3rd, 2020).
Link pointing to an anonymous browsing guide

- On a far-right Telegram channel instructions for maintaining web information security was posted. Among the recommendations: two step verification, not provide real phone number while signing up to Telegram and more (February 17th, 2020).

Further, a comprehensive 54 pages guide on web information security and anonymous browsing was posted on Telegram (March 11th, 2020).
Offense

During the pandemic one could observe a trend among far-right activists and organizations that encourages kinetic attack through cyber means. Yet their capabilities have not yet flourished and are still low level such as hacking social media accounts, Doxxing and Zoombombing, as follows:

- **Anonymous posts on 4 Chan** called upon far-right activists who have contracted COVID-19 to use the virus as a weapon and infect Jews, Asians and Blacks. For example, the following posts that called for the dissemination of the virus in synagogues and to die like a hero.

  ![A call to infect synagogues and mosques (4 Chan)](image)

- **On 8Kun**, calls for action were heard, although some were not specific. For example, a post that discussed immigration said: “we against them (the invaders)” and the manner Europe will change due to immigration. Therefore, the writer asked the activists to act and fight...
now. The post also mentioned Tarrant who perpetrated the Christchurch Massacre and said that everyone needs to remember their duty to the people. The duty is therefore to act without any limitation and any actions, as radical as it may be is possible (February 8th, 2020).

A call for action, as radical as it may be (8Kun)

- Another type of attack is Doxxing. Doxxing is a use of cyberspace to disseminate a person’s personal details and thus enable others to hurt them any way they like. For example, on a far-right Telegram channel, post that included the photograph and personal details of a Rabbi in Michigan as well as his wife’s, was uploaded.

Here’s the rabbi (Michael Schadick) who reported on our activity

And here’s his personal information: Fullname...
You have no house to run to now.
Disseminating a Rabbi’s personal details

Another type of attack is Zoombombing. Zoombombing is the abuse of the popular communications app Zoom (which became a world favorite communication method during COVID-19 pandemic) for the perpetration of barging in and interrupting video conferences, presenting hard graphic content and intimidating the participants. The phenomenon is mainly directed towards minority organizations, prayer centers and schools\textsuperscript{15}. For example, a white supremacy activist obtained the details of a Zoom conference attended by Jewish students in Massachusetts. He barged in and exposed a swastika tattoo on his chest.

Provision of the details of a Zoom conference of a Jewish school in Philadelphia to intimidate the attendees (Darknet)

International Response

Contending with cyber-attacks requires global cooperation and out-of-the-box thinking. The following are some of the actions taken by global actors to eradicate cyber-attacks.

Government and Critical Infrastructure

– The U.S. Army announced it was working with Duke University to develop a software that will assist in protecting the army’s AI system from cyber-attacks. The U.S. Army has been increasingly using AI systems embedded in various platforms (e.g. drones) to identify various objects. The concern in this matter is from hacking and corruption of the data used to train the systems (January 26th, 2020)16.

– More in the U.S., Sen. Josh Hawley, acts to pass a legislation that will prohibit federal employees to install TikTok on mobile devices provided to them by their employer to maintain national security as well as American citizens personal information protection. To date, several U.S. intelligence agencies dealing with national security have forbidden their employees to use the above app. Yet there is no blanket prohibition and military personnel for example continue to download and use it. the senator’s initiative came on the heels of warnings by legal scholar and intelligence people that under Chinese law corporations facing investigation are obligated to provide their users personal data, which elevates the risk for American citizens information security (that said, currently there is no data to support the claim that the Chinese government has access to personal information of U.S. citizens on Tik Tok) (March 4th, 2020)17.

– The Thai government announced it would establish within the year a Cyber Protection Ministry, to contend with cyber-attacks currently taking place against the government as well as the private sector (e.g. banks). The ministry is being formed further to the recommendation of the national committee for cyber protection headed by the Thai vice premier (January 14th, 2020)18.

– The UK announced the formation of a special task force which will include some 500 experts, including hackers, to conduct offensive cyber activity against hostile countries.

18 https://www.bangkokpost.com/thailand/general/1835054/govt-eyes-cyber-hq-to-combat-hacker-threat?&web_view=true
and terror organizations via disabling satellites, mobile devices, internet networks as well as communication networks being used by terror organizations. The task force is a joint initiative of the British Defense Ministry and the GCHQ (February 27th, 2020)\(^\text{19}\).

– The Japanese Minister of Defense announced an approx. $237 million USD to develop an AI based system to contend with cyber-attacks. The system is meant to autonomously locate malicious emails, rank the level of threat from them and respond accordingly (March 30th, 2020)\(^\text{20}\).

**Legislation, Policy and Regulations**

– **UK** – several bills co-authored by the Department for Digital, Culture, Media and Sport (DCMS) and the National Cyber Security Center (NCSC) requiring any device connected to the internet (IOT) to meet strict security standards. The bills are aimed at protecting customers and businesses being hurt by cyber-attacks (such as DDoS attacks) due to the fact that these devices do not include built in cyber security measures\(^\text{21}\).

– **U.S.A.** – the National Authority for Standards and Technology posted a draft of rules for organizations on ways to protect from ransomware attacks. There is a growing trend of organizations affected by this kind of attacks that in certain cases even paralyzes them completely. For example, in 2019, the City of New Orleans, the City of Baltimore and several small towns in Texas were hit by ransomware attacks. In October 2019 the FBI posted a warning to businesses on the subject. The cyber department of the Homeland Security Administration posted a similar warning a few months prior, in August, and described ransomware attacks and the most dangerous and prevalent kind of cyber-attacks (January 27th, 2020)\(^\text{22}\).

– The U.S. is considering passing a legislation that will require the states to appoint a cyber security czar for each state to promote cyber cooperation between the states and the federal government and speeding up the response in case of a cyber-attack. The cyber security czar will serve as the state’s cyber security advisor, will deal with preparedness for cyberattacks, development of potential responses and procuring technical, financial and

---


\(^\text{20}\) [https://www.defenseworld.net/news/26616/Japan_to_Develop_AI_based_System_to_Counter_Cyber_Attacks?&web_view=true#.Xrvx1mSuL_w](https://www.defenseworld.net/news/26616/Japan_to_Develop_AI_based_System_to_Counter_Cyber_Attacks?&web_view=true#.Xrvx1mSuL_w)


operational resources from the federal government for non-federal entities. The funding for this venture is supposed to be 100% federal (January 20th, 2020).  

- The federal government updated its remote working procedures due to COVID-19. Since federal agencies need to quickly adapt to handle a large quantity of employees that work remotely and therefore under threat of cyberattacks against federal networks capitalizing on the situation and the problems associated with VPN connections, the federal government issued instructions to assist federal employees and contractors to carry on with their jobs even when forced to work remotely. Among the instructions, authored by Jeff Green of the National Institute for Standards and Technology (NIST): using platforms and means that enable identification of authorized participants in meetings and blocks unauthorized persons, protection of sensitive conversations via a one-time identifying code, using an identifying sound once a person joins a conference etc. (March 26th, 2020).

Geopolitics and Terrorism

- A recent publication by the archive for national security at George Washington University (approved for dissemination by the Pentagon) reported that the U.S. Army successfully disrupted ISIS radicalization and recruitment propaganda on social media in an operation that took place in 2016. This is the first cyberattack that the Pentagon took responsibility for (January 25th, 2020).

- A new report cautions from military systems’ cyber vulnerabilities, especially command and control ones, within NATO member states. The report, titled “Cybersecurity of NATO’s Spaced-Based Strategic Assets” and published by the Royal Institute for International Relations, said that there was an immediate need to attend to cyber related issues revolving around NATO’s strategic assets in its key member states, especially as cyber threats relate to satellite based command and control systems. The uptick of vulnerabilities of satellites, ground stations, command and control systems and their teams has not yet gained the appropriate attention it deserved. There is a growing need to embed military grade cyber defense mechanisms into civilian system capable of supporting military application and should that fail to happen then items purchased on the free market who

---

may have design flaws in the above respect may expose NATO systems to additional vulnerabilities (July 29th, 2019)\textsuperscript{26}.

**Cyberspace Collaboration**

- The Homeland Security, the Dept. of Energy and the Department of Defense have announced an extension to their 2018 collaboration to establish cyberspace threats indicators systems and development of energy sector critical infrastructure protection capabilities. The three agencies executed mutual understandings on the need to develop a joint database and collaborate on providing guidelines to energy sector stakeholders on contending with cyber-attacks (February 5\textsuperscript{th}, 2020)\textsuperscript{27}.

- The U.S. and Estonia embarked on their first collaboration in the field and started building a platform that would assist in cyber threats intelligence information share and enrich their cyber defense capabilities. Both countries wish to present the system to additional potential partners. Per Kusti Salm\textsuperscript{28}, the director of the Estonian Center for Defense Investment, frequent exchange of intelligence among actors is one of the key principles of cyber defense (January 14\textsuperscript{th}, 2020).

\textsuperscript{26} https://www.fifthdomain.com/international/2019/07/30/the-next-cybersecurity-concern-for-nato-space/

\textsuperscript{27} https://fcw.com/articles/2020/02/05/energy-dod-dhs-infrastructure.aspx?web_view=true

\textsuperscript{28} https://cyber.ee/news/2020/01-14/
Cyber Desk Team:

Dr. Eitan Azani, Head of the Cyber Desk and Director of Research, ICT
Dr. Liram Koblenz-Stentzler, researcher, ICT
Dr. Michael Barak, Senior Researcher, ICT

Cyber Desk Assistance:

Ms. Delilah Meshulam, intern, ICT
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.