



BULLETIN

SECURE COMMUNITY NETWORK

Phone: 844.SCN.DESK
Website: www.securecommunitynetwork.org

Michael Masters
National Director & CEO

29 June 2020
No. 30

Please report all relevant information and direct all media inquiries to the SCN Duty Desk

Email: dutydesk@securecommunitynetwork.org | Phone: 844.SCN.DESK

SCN BULLETIN: Threat and Security Update

Distribution: Organizational Leadership and Security Directors

Scope

The following bulletin provides an overview of the current threat environment for the Jewish community, specifically in the context of current conditions related to the novel coronavirus (COVID-19) and recent civil unrest. As local, state and federal guidance metrics begin to be met, and restrictions are lifted, concern remains regarding possible operational changes by domestic violent extremists (DVE), international terrorist organizations, and other entities that seek to harm the Jewish community, both domestically and overseas. All data included in this bulletin was obtained through open-sources and is current as of 29 June 2020.

Assessment

Lockdown measures and disinformation campaigns regarding the current social and political situation within the U.S. have likely led to an increase in recruitment and radicalization by DVEs and like-minded groups. As such, the reported presence of individuals motivated by extremist ideologies, who may be attempting to spread disinformation and encourage discord as well as violence at demonstrations and protests across the country, present a potential threat that may need to be addressed in both the short and long term. At this time, there are currently no known credible threats directed at Jewish institutions or organizations. However, social media accounts have been observed noting, encouraging, and/or implying that the Jewish community could/should be targeted, to include the hypothetical notion of attacking synagogues, and while federal and local law enforcement resources may be strained.

In the long term, this predicted increase in recruitment by domestic and international violent extremist groups may result in an environment conducive to anti-Semitic behavior. This lends credence to expert opinions that attacks against soft targets, such as synagogues and schools, are likely to increase as the nation returns to standard operations.

Overview

Extremist groups and criminal enterprises have utilized the uncertainty surrounding COVID-19 as well as recent protests, demonstrations and other activity, to take aim at vulnerable populations and expand operations, specifically online. While

lockdown procedures have temporarily reduced some forms of extremist activities and criminal behavior, issues related to COVID-19 and recent civil unrest have also, in some instances, placed a strain on law enforcement and security-related resources at the local level.

In response, and as lockdown measures begin to lift, domestic and international security agencies have warned of a possible spike in anti-Semitism and violent extremist activity. Experts anticipate that this activity will manifest in a number of different ways:

- **Domestic Violent Extremism:** Prolonged public exposure to anti-Semitic or anti-government rhetoric may inspire attacks, particularly against soft targets such as religious and cultural facilities.
- **International Terrorism:** Local governments may struggle to quickly and fully return to pre-pandemic effectiveness in the fight against terrorism, especially as terrorist organizations may have recouped previous losses in territory, manpower, and/or supplies during the lockdown.
- **Cybersecurity:** As operations resume and organizations undertake recovery efforts and adopt new business practices, cybercriminals may increase efforts to target organizations with phishing scams, ransomware attacks, and other sophisticated methods.
- **Geopolitical Tensions:** Political tension within the Middle East may increase in severity as global leaders take hardline postures in an attempt to regain public support after a global health crisis.

Domestic Threats

Since October 2018, the Jewish community within the United States has been the target of multiple violent hate crimes, including two attacks at houses of worship, a shooting at a Jewish kosher supermarket, and a stabbing during a Hanukkah celebration. During the same time period, at least two dozen individuals were arrested for alleged plots, attacks or threats against the Jewish community. According to the latest hate crime statistics released by the Federal Bureau of Investigation (FBI), of the total number of hate crime offenses motivated by religious bias, 57.8% were due to anti-Jewish bias, the highest level in decades, and three times higher than the next religious group.

While the pandemic may have temporarily contributed to a reduction in domestic violent attacks, research indicates a significant increase in online hate speech and rhetoric from extremist networks. According to the Institute for Strategic Dialogue, white supremacist Telegram channels grew by more than 6,000 users over the month of March. During that same month, one examined channel grew from approximately 300 users to nearly 2,700 — an increase of 800%.

Similar increases in activity have also been observed on platforms such as Facebook, Twitter, Imgur, Reddit, and online gaming communities. Research conducted by the Tech Transparency Project (TTP) discovered at least 125 Facebook groups dedicated to the concept of the “boogaloo,” a term referring to a hypothetical civil war and commonly associated with DVE agendas. According to TTP, “More than 60% of the groups were created in the last three months, as COVID-19 quarantines took hold in the U.S., and they’ve attracted tens of thousands of members in the last 30 days.” These online platforms have been used to increase the reach of DVE ideologies and serve as a means of recruitment for potential members – which is further enhanced by the current stay-at-home orders, providing a nearly captive audience.

This increase in rhetoric has been reflected by the recent touting of white supremacist culture and anti-Semitic hate during various protests and demonstrations across the country:

- **18 April 2020:** A pair of protestors were observed in Columbus, Ohio carrying a sign reading "the real plague," with imagery of a blue and white rat wearing a yarmulke.

- **30 April 2020:** A protestor in Lansing, Michigan was seen holding a sign depicting the governor with a Hitler mustache on the steps of the state capitol.
- **03 May 2020:** A shopper in Santee, California was photographed wearing what appeared to be a Ku Klux Klan hood as a face covering while at a grocery store.
- **04 May 2020:** A protestor in Chicago, Illinois was seen holding a sign with the Nazi slogan from the gates of Auschwitz Concentration Camp.
- **May 2020:** Several anti-Semitic social media posts were discovered attempting to direct hatred and national protests towards the Jewish population.
- **03 June 2020:** A synagogue and several Jewish-owned businesses in Los Angeles, California were vandalized with phrases such as "Free Palestine" and "F*** Israel."

International Threats and Concerns

International terrorist organizations such as the so-called Islamic State in Iraq and Syria (ISIS) and al-Qaeda have also reduced attacks as a result of COVID-19. In a newsletter to their followers, leaders within ISIS directed operatives to "not enter the land of the epidemic" and stated that they should not return home if they become sick. Furthermore, the leaders of al-Qaeda suggested that COVID-19 would devastate the United States economy and requested that their followers use these times of illness to study the Quran instead of conducting attacks.

Despite these orders, countries such as the Philippines, Mozambique, Iraq, and Germany have reported extremist activities within their borders since the beginning of the pandemic. On 15 April, police arrested four suspected ISIS members in Berlin, Germany believed to be planning an attack against U.S. military facilities in the area. Similarly, on 28 April, ISIS claimed responsibility for a suicide-bomb that occurred in Kirkuk, Iraq. These reports have led intelligence agencies to warn that a surge in attacks is possible as lockdown measures begin to lift.

Warnings have also been issued by the international community regarding extremist attempts to sow discord and foster mistrust of local governments. Similar to DVE tactics, these efforts have included spreading disinformation while simultaneously using propaganda narratives to bolster and promote their ideologies. Foreign-state media and international entities have already shown the desire to weaponize COVID-19 through the use of anti-Semitic rhetoric. These efforts often align with historic canards, such as those used during the Middle Ages, suggesting that the Jewish community is somehow responsible for the spread of the virus:

- **04 March 2020:** Alain Mondino, a far-right French politician, posted a video on social media suggesting that the Jewish community was responsible for COVID-19.
- **05 March 2020:** Iranian Press TV reported that "Zionist elements developed a deadlier strain of coronavirus against Iran."
- **15 March 2020:** Herritar Batasuna, a far-left politician from Spain, published an opinion article suggesting that COVID-19 was a weapon of the Third World War, created by "the Anglo-Saxon and Zionist elite."
- **10 April 2020:** At least two stickers were found on a subway car in Hamburg, Germany with the quote "Coronavirus Fake!" The stickers were shaped like yellow Stars of David, similar to the patch the Jewish community was forced to wear in concentration camps.

- **30 April 2020:** Social media comments from Australia were documented suggesting that COVID-19 should be renamed the "Jew flu."

Cybersecurity

Despite the diligent work of experts in the field of cybersecurity, expanding dependence on and rapid advances in technology continue to present attractive opportunities for cybercriminals. There is an increasingly large gap between the number of cybersecurity professionals mitigating the effects of cybercrime and the number of bad actors scaling up their cybercrime campaigns. An increased dependence on technology, and a nationwide shift to telework during the pandemic, has created ample opportunity for cybercriminals to deploy their tactics on a much larger audience. According to the FBI, reports of cybercrime have spiked since the pandemic began and several new patterns have emerged.

Zoombombing: Attempts to disrupt online presentations, ceremonies, and/or conference calls are colloquially called "Zoombombing." Bad actors have proven capable of infiltrating virtual meetings with the intent to disrupt public video conferencing calls – primarily using the Zoom platform. These attempts often use the platform's screen-sharing feature to project graphic content to unwitting conference participants, which can force hosts to shut down their events. In addition to private corporations and general community events, this activity has also impacted Jewish institutions. Reports include instances of white supremacist and/or neo-Nazi material being used to disrupt meetings. The risk of Zoombombing can be mitigated through the use of security settings already available on the platform. These functions, combined with basic guidance on how to properly utilize them, can significantly decrease the likelihood of disruption.

Phishing: The FBI defines phishing as unsolicited emails, text messages, or telephone calls purportedly from a legitimate company or individual requesting personal, financial, and/or login credentials. Spoofing is defined as contact information (phone number, email, and website) that is deliberately falsified to mislead and appear to be from a legitimate source. According to the FBI, between 2018 and 2019, the number of Americans who were victimized by phishing scams increased by 430% and the economic loss from spoofing scams increased by 428%.

Phishing and spoofing scams regularly impact members of the Jewish community. Over the last six months, members of numerous Jewish organizations around the country have received spoofing emails with fraudulent email addresses that appear, at a glance, to be from local rabbis or organization executives. The emails follow a general pattern in which the sender requests a favor and requests the recipient to purchase gift cards and provide the personal identification number (PIN) information via email.

Business Email Compromise (BEC) and Email Account Compromise (EAC): BEC and EAC are sophisticated scams targeting both businesses and individuals during the transfer of funds. These scams account for the majority of financial loss associated with cybercrime. The scams are frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds. Recent examples of BEC or EAC attempts include the compromise of personal and professional email accounts, requests for confidential business information, and fraudulent requests for changes to financial records.

Recently, several Jewish institutions have been impacted by BEC or EAC scams. In two reported incidents, bookkeepers received emails from fraudulent email addresses that appeared to belong to the executive directors of their organizations. The emails stated that the executive director had changed banks and was requesting that their banking information be updated.

Ransomware: Ransomware attacks occur when a cybercriminal takes control of computer files and data and extorts money from the victim in exchange for the release of the same. While local governments, schools, law enforcement, court systems,

and libraries are targeted most frequently, Jewish organizations, houses of worship, and non-profits also present attractive targets for ransomware attacks.

- **April 2019:** A Cleveland, Ohio church was targeted as cybercriminals impersonated business contractors providing services to the church and sent a number of emails in which they provided "updated instructions" for carrying out the wire transfer of the scheduled payments. The church made the payments as directed, and only realized the scam when they were contacted by the contractors a couple months later because of missed payments.
- **April 2019:** A Massachusetts-based non-profit running a homeless shelter was the target of a ransomware attack. The president of the organization claimed that an anti-virus software used by the organization detected the attack and shut it down within 30 seconds, preventing any files from being compromised or lost.
- **August 2019:** A synagogue in Maitland, Florida was targeted in a ransomware attack. After identifying the breach, the synagogue's leadership decided against paying the ransom and worked with the FBI to secure their systems. The attack resulted in a complete loss of information for the synagogue, as no files were able to be recovered.
- **January 2020:** A large Jewish Federation's information technology (IT) system was infected with a crypto-virus, which was not recognized by their anti-virus software. The crypto-virus was delivered through a link in an email and resulted in significant damage to the servers. The attack did not lead to a loss of information, as the Federation had recently backed-up their files.

Geopolitical Tensions

United States and Iran

Despite a recent period of relative calm while world governments focused on COVID-19 related issues, geopolitical tensions remain elevated. Of particular concern is the continued escalation of tensions between the United States and Iran and the likelihood of renewed confrontation between the two countries as lockdowns continue to lift.

In early April, Iran began a gradual resumption of government operations. In spite of increasing economic strain, Iran has boldly resumed pre-pandemic activities in the region to include defiantly challenging the U.S. military in the Persian Gulf and supporting pro-Iranian Shi'ite militia actions against U.S. forces in Iraq. These activities come after more than a year of escalating tensions between Iran and the United States. Recent notable incidents include:

- **31 October 2019:** The U.S. extended sanctions on Iran, specifically targeting "four strategic materials as being used in connection with Iran's nuclear, military, or ballistic missile programs." Iran responded by further suspending a portion of its compliance with the 2015 Nuclear Deal.
- **17 November 2019:** Leaked intelligence information revealed the extent of Iranian influence on neighboring Iraq. In one document, it was suggested that Prime Minister Adil Abdul Mahdi of Iraq has a "special relationship with the Islamic Republic of Iran."
- **27 December 2019:** A rocket attack on the K1 military base near Kirkuk killed one U.S. civilian contractor and wounded "several" U.S. service members and Iraqi personnel. According to reports by Reuters, several rockets were launched at the base.
- **29 December 2019:** The U.S. conducted airstrikes in Iraq and Syria against targets associated with the Kata'ib Hezbollah (KH). The airstrikes killed approximately 25 people overnight. KH leadership warned of a "strong response" to the attack.

- **31 December 2019:** Protestors backed by Iran stormed and damaged U.S. Embassy compound in Baghdad, forcing the Department of State to suspend public consular services.
- **03 January 2020:** The U.S. conducted an airstrike on the leader of Iran's Islamic Revolutionary Guard Corps (IRGC) Quds Force, Qassem Soleimani. Also killed in the strike was Abu Mahdi al-Muhandis, a high-level deputy within the KH, an Iranian-sponsored Shi'ite militia operating in Iraq. The Department of State also issued an alert for all U.S. citizens to leave Iraq while advising U.S. citizens not to travel to Iraq.
- **05 January 2020:** Reports by the Iraqi military said that six rockets landed in Baghdad, three of which landed in the Green Zone (where the U.S. Embassy is located).
- **10 January 2020:** The U.S. administration imposed economic sanctions on Iran that targeted multiple sectors of the Islamic Republic's economy.
- **11 March 2020:** Two Americans and a British national were killed in a rocket attack on a military base in Taji, Iraq. Based on the weapons and tactics used, a U.S. defense official stated they had every reason to believe Iranian-backed fighters or the IRGC were behind the attack.
- **12 March 2020:** U.S. warplanes, backed by British military, carried out airstrikes on five targets in southern Iraq where KH, an Iraqi militia with ties to Iran, were believed to be storing the rockets used to attack coalition forces the night before.
- **15 April 2020:** Eleven Iranian warships approached six U.S. warships in the Persian Gulf, coming within a 30-foot distance before retreating. On 22 April 2020, U.S. President Donald Trump revealed that he ordered U.S. naval forces to shoot at any Iranian ship demonstrating harassing behavior. In response, the Commander of the IRGC, Hossein Salami, announced that Iranian warships would open fire on any U.S. ship threatening their security.

While it is unlikely that Iran will start a conventional war with the United States, asymmetric and unconventional attacks remain a risk. Experts at the U.S. Department of Homeland Security have previously stated that Iran likely views terrorist activities as an option to deter or retaliate against its perceived adversaries.

Israel and Iran

Israel and Iran have not always been direct adversaries. However, since the early 2000s, Iranian rhetoric towards Israel has become more openly hostile and proxy conflict between the two countries continues to increase. Successful military efforts to reduce Iran's influence in the Middle East, a long-standing alliance with the United States, and the ongoing Israeli-Palestinian conflict has made Israel a prime target for threats of retaliatory attacks by the Iranian regime and its proxies.

Since the beginning of 2020, Israel has increased military efforts to counter Iranian militia positions in Syria. During March and April, airstrikes from the Israeli Defense Force (IDF) targeted Iranian military weapons and transportation hubs in southern and central Syria.

- **31 March 2020:** According to Syrian media reports, Israeli warplanes were responsible for an airstrike on the Shayrat airbase south of Homs. The base was allegedly used as a forward base for Iran to bring weapons into the country.

- **15 April 2020:** A Hezbollah vehicle, suspected of transporting group members and precision missiles components, was destroyed by an Israeli drone strike near the border of Syria and Lebanon. The first strike prompted the occupants to exit the vehicle before the second strike destroyed it.
- **20 April 2020:** Syrian air defenses shot down several missiles launched by Israeli warplanes over the historic city of Palmyra in the central Homs province. The United Kingdom-based Syrian Observatory for Human Rights (SOHR) stated that Israeli air raids were targeting Iranian and Iran-backed fighters in the desert near Palmyra.
- **27 April 2020:** Syrian state media accused Israel of conducting an airstrike on the Mezzeh military airfield on the outskirts of Damascus. According to the SOHR, the strike destroyed a number of Iranian buildings and killed at least four pro-Iranian fighters.
- **30 April 2020:** Israeli shells targeted military posts of regime forces and Iranian militias in Tal Ahmar and rural Ma'ariya, west of Daraa, and the Tal al-Ahmar al-Gharbi area in Al-Quneitra near the administrative border with Daraa governorate in southern Syria, according to a report from the SOHR.

Israel-Palestinian Conflict

The conflict between Israel and Palestine persists, despite a brief period of cooperation during pandemic response efforts. This fragile calm followed a series of deadly conflicts between the IDF and Palestinian Islamic Jihad (PIJ) along the Gaza border in late February, and recent incidents indicate an imminent return to pre-pandemic conflict.

- **23 February 2020:** PIJ member Mohammed al-Naim was shot and killed by the IDF while planting explosives along an Israeli fence in Southern Gaza.
- **27 March 2020:** Rockets launched from Gaza landed in Israeli territory. The IDF responded with strikes against military positions and infrastructure used for underground Hamas activity in the northern Gaza Strip. Palestinian media reports later stated that Israeli Air Force jets also struck several targets in the Hamas-run coastal enclave.
- **05 May 2020:** A rocket launched from Gaza landed in an open area of the Eshkol region of Israel. The IDF responded, using tanks to shell three Hamas military positions in the northern Gaza Strip.

Additionally, Israel's new unity government, formed under an agreement between Benjamin Netanyahu and Benny Gantz, is set to begin considering the annexation of occupied areas in the West Bank on 01 July 2020. The result of those deliberations is expected to increase tensions.

Impact to the Jewish Community

Although there are currently no known credible threats directed at Jewish institutions or organizations, it is assessed that stressors caused by the pandemic, as well as increased exposure to online hate speech, may contribute to the decision of an individual or group to undertake an attack. SCN and other partners have observed an increase in rhetoric across multiple social media platforms and during nationwide protests, which further suggests that the environment is conducive to potentially violent anti-Semitic behavior, both inside the United States and abroad. Open-source research shows that many individuals desiring to conduct an attack against the Jewish community have co-opted ideas of attacking soft targets, such as synagogues, schools, or hospitals. Discussions observed between violent extremists have often concluded that such targets are likely to have the most traumatic effect on the population. Other discussions observed have included the idea of spreading COVID-19 to the Jewish community or have involved the promotion of conspiracy theories that suggest COVID-19 was created by Israel or the Jewish community.

Over the past year, there has been an increase in the number of arrests of individuals motivated by violent anti-Semitic ideology for allegedly planning and/or carrying out attacks against the Jewish community. As organizations work to resume operations, leadership and security personnel are encouraged to remain situationally aware of individuals and groups who espouse similar violent ideology and seek to exploit the current environment to promote extremist rhetoric, spread disinformation, foster discord, and incite violence.

Knowing how to report incidents to both local and federal law enforcement and implementing a comprehensive security plan can substantially decrease the perception of being a "soft target" to individuals that may wish to cause harm.

Organizations and institutions should work to proactively review, adapt, and implement any security plans and procedures to protect staff, visitors, and facilities during times when public safety and security resources are stretched thin.

Even as communities work to resume in-person operations and trainings, many opportunities for virtual training exist. SCN and the network of Federation security directors are actively providing virtual trainings for organizations across North America, to include:

- Situational Awareness
- Community Active Threat Training
- Greeter/Usher Training
- Stop the Bleed Training

Organizations interested in learning more about in-person and virtual training opportunities should contact their local Federation security director or email training@securecommunitynetwork.org.

For additional resources, please visit the SCN [website](#).

Report Suspicious Activity

Follow established protocols to report suspicious activity – to include contacting local law enforcement and/or the relevant suspicious activity reporting authority – and contact the SCN Duty Desk at DutyDesk@securecommunitynetwork.org or by calling 844-SCN-DESK.

For questions, please contact the SCN Duty Desk at DutyDesk@securecommunitynetwork.org

FOUO

For Official Use Only

This bulletin was compiled by the Secure Community Network, utilizing open-source information and relevant details provided by non-profit and federal partners. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact the SCN Duty Desk at 844.SCN.DESK if you have any questions or need additional information.

Information labeled FOUO should be safeguarded and withheld from public release until approved for release by the originating agency.

Dissemination of FOUO is restricted to persons with “need-to-know.” Need-to-know is defined as the determination made by an authorized holder of the information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties.

Typical FOUO requirements include:

- FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.
- The holder of the information will comply with access and dissemination restrictions.
- Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.