Department of Homeland Security
COVID-19 Partner Threat Overview
April 17, 2020

Office of Strategy, Policy, and Plans (PLCY)

Cybersecurity and Infrastructure Security Agency (CISA)

Office of Intelligence and Analysis (I&A)

Office of Partnership and Engagement (OPE)

Homeland Security

(U) COVID -19 Partner Threat Overview

April 17, 2020

(U//FOUO) The Department of Homeland Security (DHS) is providing this product to assist state, local, tribal, and territorial partners, and critical infrastructure owners and operators, with information on how the COVID-19 pandemic is impacting the threat landscape across the U.S. This product provides a consolidated resource for partners as the threat environment has evolved during the course of the pandemic.

(U//FOUO) DHS' Office of Intelligence and Analysis (I&A) assesses that a broad range of illicit actors, including cyber attackers, nation-state actors, traditional criminals, and terrorists, are seeking to take advantage of the current COVID-19 pandemic within the United States. I&A has developed a number of intelligence assessments and products specific to the impacts from the COVID-19 pandemic. These products are available for review on the Homeland Security Information Network (HSIN).

(U//FOUO) Attacks by cyber actors likely represents the most significant near-term threat across the U.S. DHS' Cyber and Security Infrastructure Agency (CISA) is providing continual real-time updates to partners across the Homeland Security Information Network. CISA-developed products are available to registered stakeholders in authorized communities of interest. CISA uses the NCCIC Portal on HSIN to share threat indicators and advisory information with public, private, and international partners in the network defense community of practice (https://www.us-cert.gov/hsin).

(U//FOUO) According to a joint assessment by CISA and the United Kingdom's National Cyber Security Centre, cyber criminals and advanced persistent threat (APT) groups are targeting individuals and organizations with a range of ransomware and malware, exploiting the COVID-19 outbreak for their own personal gain.

(U//FOUO) Although a range of cyber threats is currently a critical area of concern, anti-government and racially and ethnically motivated violent extremists have already demonstrated intent to incite violence and conduct attacks as result of the COVID-19 pandemic. These efforts include increasing disinformation, recruiting through social media and the Internet, attacking governmental and perceived governmental response efforts, and targeting specific ethnic groups.

(U//FOUO) Impacts and implications from the pandemic may result in increased social isolation and financial hardships. These are known risk factors that motivate extremists to violence and could present a long-term challenge to law enforcement as well as the soft targets and crowded spaces sector once restrictions are relaxed later in the response. Additionally, extremists could increasingly be motivated to direct attention to public health and medical facilities. Partners may seek to consider additional measures for reducing vulnerabilities and better securing such facilities against both cyber and physical attacks from a range of diverse actors.

(U//FOUO) DHS recognizes that for many law enforcement agencies, this pandemic has resulted in a significant reduction in bandwidth and a need to balance response efforts with sustaining policing activities. However, it is imperative that law enforcement be aware of the second and third order effects and risks from the pandemic where violent extremists could be motivated to inflict additional harm, and to ensure communities have information that can help prevent potential attacks. *If You See Something, Say Something*^{TM} remains relevant in the midst of this national public health emergency.

(U//FOUO) DHS's Office of Targeted Violence and Terrorism Prevention (TVTP) has prepared a Community Awareness Briefing (CAB) and Law Enforcement Awareness Briefing (LAB) for interested partners. Please contact TVTP at the email addresses indicated in the attached brochures to arrange a briefing.

(U//FOUO) For additional details and products related to the COVID-19 impacts to security, Homeland Security Enterprise partners are encouraged to visit the HSIN (https://hsin.dhs.gov).

(U) Relevant Intelligence Products

(U) Cyber

(U//FOUO) Nation-State Cyber Actors Likely to Conduct COVID-19-Themed Spear-Phishing Against Homeland Targets
Product Date: 27 March 2020
Source: DHS Office of Intelligence and Analysis (I&A)

(U//FOUO) Cyber Actors Almost Certainly View Telework During the Coronavirus Pandemic as an Opportunity to Exploit Networks
Product Date: 30 March 2020
Source: DHS Office of Intelligence and Analysis (I&A)

(U//FOUO) Cyber Actors Sending Coronavirus-Themed Phishing E-mails
Product Date: 02 April 2020
Source: DHS Office of Intelligence and Analysis (I&A)

(U) Terrorism and Mass Violence

(U//FOUO) Disruption of a Racially or Ethnically Motivated Violent Extremist's Plot to Attack a Missouri Medical Center
Product Date: 30 March 2020
Source: DHS Office of Intelligence and Analysis (I&A); DOJ Federal Bureau of Investigation (FBI)

(U//FOUO) COVID-19: Violent Extremists' Social Media Bio Attack Calls – Crudely Viable, Warrants Attention, but Effects Likely Not Measurable
Product Date: 01 April 2020
Source: DHS Office of Intelligence and Analysis (I&A); DHS Office of Countering Weapons of Mass Destruction (CWMD)

(U) Attachments

I&A COVID-19 Intelligence Product
CISA Public Gathering Area Security Product
Sample Messages to Address Disinformation and Resilience Building
Community Awareness Briefing and Law Enforcement Awareness Briefing

INTELLIGENCE ENTERPRISE

INTELLIGENCE NOTE

Homeland Security

6 April 2020

(U) COVID-19 Task Force

(U//FOUO) Key COVID-19-Related Homeland Threats

(U//FOUO) Prepared by the DHS Intelligence Enterprise (DHS IE) COVID-19 Task Force.

(U//FOUO) We assess that a broad range of illicit actors are seeking to take advantage of the current COVID-19 pandemic within the United States and these efforts probably will intensify as new vulnerabilities arise from ongoing changes to mitigate the crisis. Cyber actors probably pose the most imminent threat, as much of the country is teleworking, followed by nation-states that have traditionally exploited similar crises, traditional criminals seeking to profit through fraudulent activities, and terrorists.

» (U//FOUO) Cyber actors: Nation-state cyber actors and cybercriminals will likely exploit the spread of COVID-19 to target homeland victims through spear-phishing e-mails. These actors probably will continue using a variety of COVID-19-themes to target US-based individuals and organizations, including requests for donations, updates on virus transmissions, safety measures, tax refunds, and fake vaccines, judging from information from a UK advisory and consultancy firm.

» (U//FOUO) Nation-state actors: Foreign actors will continue to use the COVID-19 pandemic to sow discord through malign foreign influence activities. Their likely goal is to stoke fear and weaken the USGovernment's global standing. Since January, Russian online influence actors have advanced misleading and inflammatory narratives about the COVID-19 outbreak in the United States and abroad. These actors have sought to exacerbate general concerns related to the virus by amplifying content critical of the US response.

» (U//FOUO) Traditional criminals: Violent crime will likely remain constant with pre-COVID-19 trends while non-violent crime—especially fraud—will increase. These trends are caused by social distancing and individuals staying in their residences, limiting the opportunity for opportunistic crimes against individuals. The current crisis provides criminals an opportunity to peddle fake cures and cleaning supplies to thepublic, leading to an increase in non-violent crimes. Some jurisdictions have reported increases in business thefts at unoccupied buildings and in domestic violence cases.

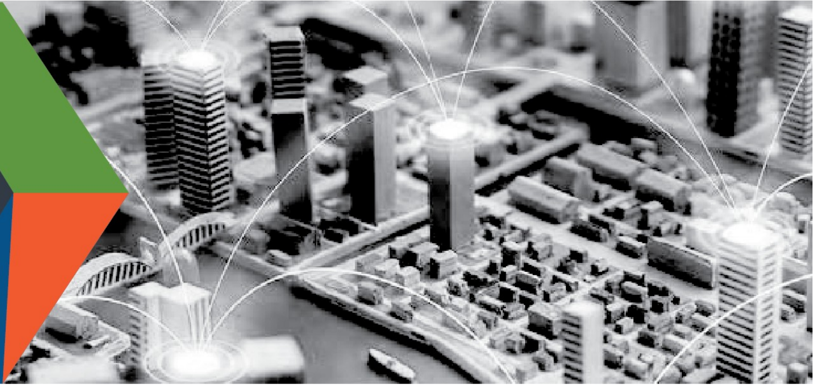
» (U//FOUO) Terrorists: Violent extremists probably are seeking to exploit public fears associated with the spread of COVID-19 to incite violence, intimidate targets, and promote their ideologies, judging from press and open source reporting. Increased travel restrictions and social distancing possibly will complicateviolent extremist efforts to operationalize attacks against more traditional terrorist targets in the Homeland, but the health care industry and ethnic and religious minorities probably are at greatest risk of suchattacks.

(U) Tracked by: HSEC-6.1.1

(U) Warning: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY, SECURE TOMORROW



PUBLIC GATHERING AREA SECURITY DURING THE PANDEMIC - INFORMATION FOR LAW ENFORCEMENT OFFICIALS

April 2020

OVERVIEW

The coronavirus pandemic is unprecedented, requiring all levels of government and the private sector to coordinate efforts in order to effectively mitigate community spread. Law enforcement officials are on the front line of this effort, often putting service before self in order to assist members of their community. For many law enforcement agencies, this pandemic has resulted in a significant reduction in bandwidth and a need to balance response efforts with sustaining policing activities. Nonetheless, it is imperative that law enforcement be alert for potential individuals triggered by the pandemic to inflict further harm, and to provide residents with information that can augment community safety and security.

POTENTIAL RISKS POSED TO PUBLIC GATHERING AREAS

During steady state conditions, threats evolve and include terrorists and other violent extremist actors attempting to disrupt the American way of life and democratic principles through a range of attack methods – active shooter, bombing, vehicle ramming, and others. Unfortunately, during circumstances such as a pandemic, individuals may be triggered by stressors (e.g., isolation, layoff, etc.) caused by the pandemic to also commit attacks. As captured in the U.S. Secret Service National Threat Assessment Center's 2018 *Mass Attacks in Public Spaces Report*, nearly all perpetrators had at least one significant stressor within five years prior to an attack, and over half had indications of financial instability in that same timeframe.

Although there are currently no imminent or credible threats, there has been an increase in online hate speech intended to incite violence and/or use the ongoing situation as an excuse to inflict hate. This is highlighted, for example, by the incident thwarted by the FBI in Missouri where a suspect was planning to bomb a hospital; even though the suspect was already planning the attack, he accelerated plans as a result of the pandemic.

The potential threat environment is particularly relevant to public gathering areas, which have shifted from the traditional special events in your area, such as a concert, to COVID-19 mobile screening stations, gas stations, still-open houses of worship, grocery stores and other retailers that have been approved to do business. As such, now is the time to engage community businesses and other stakeholders to encourage vigilance and awareness – particularly those who historically may have experienced hate crimes – and remind them to review security plans, policies, and procedures.

RESOURCES

To support law enforcement agencies in enhancing security within their communities, the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) provides access to a wide range of training, exercises, tools, and other materials focused on a wide range of attack methods; and other resources relating to behavioral indicator detection. These products can be easily downloaded, printed, and delivered to local establishments to assist them with their risk mitigation measures.

The resources below provide web-based entry points to many CISA resources.

- Hometown Security initiative (https://www.cisa.gov/hometown-security) provides access to resources with information regarding various threat types, potential impacts to operations resulting from an attack, and options for consideration to mitigate risk.
- A cadre of more than 100 Protective Security Advisors (PSA) located across the country who conduct infrastructure security and vulnerability mitigation activities at the local level. Their primary mission is to proactively engage with all levels of government and the private sector to protect infrastructure by conducting security and resilience surveys and assessments; providing access to security and resilience resources, training, and information; and serving as liaisons between government officials and the private sector during and after an incident. To connect with your local PSA, please contact CISA.CAT@cisa.dhs.gov.
- The Office for Bombing Prevention (https://www.cisa.gov/office-bombing-prevention-obp) has a range of actionable counter-improvised explosive device security and preparedness resources including those focused on how to safely respond to bomb threats or suspicious items, gain threat and incident information, or training and awareness videos to enhance preparedness.

Sample Messages to Address Disinformation & Resilience Building

April 7, 2020

Addressing Disinformation

Disinformation presents a threat to the United States. Disinformation can feed anxiety leading to violent responses, so it is critical to engage in the information environment. By proactively disseminating verifiable information daily, DHS can build its credibility to provide additional messaging that counters disinformation.

Sample messages from DHS may include…

Viral agents, like the Coronavirus, do not recognize race/ethnicity, religious beliefs, nationality, or socio-economic status.

The CDC maintains an active website with accurate information about the coronavirus. https://www.coronavirus.gov/

There is currently no cure or vaccine for Coronavirus. Social media posts that suggest otherwise are attempts to either steal your money or sow discord. The Federal Trade Commission has information on how to avoid scams. https://www.consumer.ftc.gov/features/coronavirus-scams-what-ftc-doing

Communities and members of the public should look to their local and state public health officials for the most accurate and up-to-date information about the coronavirus and its impacts on their communities.

Some social media posts may be made by deceptive foreign or domestic actors who are attempting to exploit the crisis to spread disinformation and destabilize our communities.

Rumors can easily circulate within communities during a crisis. FEMA can help you stay informed on what is rumor versus fact related to the coronavirus response.

https://www.fema.gov/Coronavirus-Rumor-Control

Reinforcing Resilience Building Within the Community

DHS can focus its messaging efforts on resilience building – particularly in light of social isolation. Sample messages, however, should be tailored to both local partners specifically and members of the public generally.

Communities should understand that **social distancing doesn't mean social isolation**: Communities should continually reinforce the need to stay in contact with their neighbors, friends, families, co-workers, and others through email, phone calls, and other types of distance communication.

Resilient communities are strong communities: Social distancing does not mean cutting off communication. Building social bridges to all members of communities requires providing information and interaction. Communities should work together with open communication to ensure all members of the community are informed and are able to maintain interactions with one another.

Communities should be aware of already isolated populations (such as linguistically or religious isolated populations, populations with lower socio-economic status who may not have electronic means of communication, etc.) and develop a plan to have regular contact with members of that population to provide information and to undertake welfare checks.

Possible Suggestions for Communities to do…

Share posts of examples of building resilience by staying connected

Social media has demonstrated this with videos of opera singers in Italy and musicians in Spain serenading their neighbors from their balconies.

Celebrities such as Melissa Ethridge and John Legend have provided free concerts.

Libraries and museums are making aspects of their collections available online.

There may be community-specific examples from our local partners that they can amplify to their communities

DHS can share examples from the U.S. of local communities building resilience by successfully navigating social distancing

Recommended messaging for members of the public may include…

Video chats can allow you to preserve, in a virtual setting, most of the benefits of in-person interactions.

Support ongoing hashtag campaigns, such as #FlattenTheCurve, #AloneTogether, #InThisTogether, and others

Viral agents, like the Coronavirus, do not recognize race/ethnicity, religious beliefs, nationality, or socio-economic status.

Ask the public: How Are You Staying Connected? This may be an inter-active social media campaign that asks members of the public to share their methods for staying resilient.

All disasters are local: Check with your state, local, tribal or territorial public health agencies and other partners for up-to-date information and developments in your local community.

Amplify FEMA, CDC, NIH, and other governmental information.

Community AwarenessBriefing (CAB)

Educate your community on preventing targeted violence and terrorism.

What's a CAB?

The Community Awareness Briefing is a one to two hour presentation designed to help participants develop an understanding of violent extremist recruitment tactics and explore ways to prevent such threats at the local level.

Members of the community can get involved earlier than government representatives, often during the critical window of opportunity when it's possible to offer alternatives to engaging in violence.

How do I host a CAB?

Organizations—such as schools, houses of worship, and others—may request a CAB from the TVTP Awareness Briefing Team. TVTP will provide the resources and materials, including a case studies-based presentation that empowers individuals to intervene.

What are the benefits?

The main goal of the CAB is to raise awareness of how violent extremist movements recruit individuals to commit violent or illegal acts, negatively impacting these individuals, their families, and their communities.

Interested in hosting a CAB?

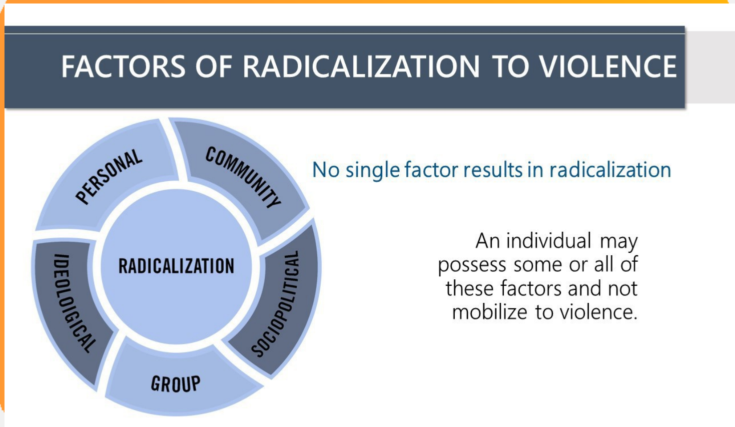
Contact the TVTP Awareness Briefing Team at:

CABbriefingrequests@hq.dhs.gov

Homeland Security

Included in the CAB presentation:

Learn what radicalization to violence looks like and what you can do to intervene

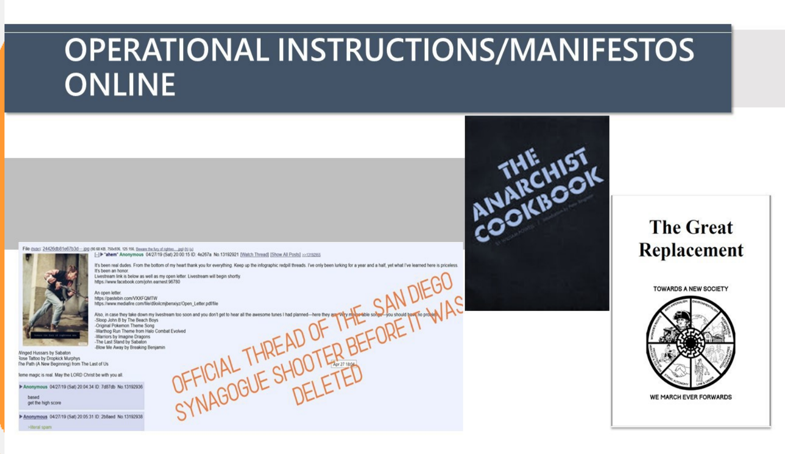


FACTORS OF RADICALIZATION TO VIOLENCE

No single factor results in radicalization

An individual may possess some or all of these factors and not mobilize to violence.

Discover how the internet and social media allow extremists to easily distribute operational instructions



OPERATIONAL INSTRUCTIONS/MANIFESTOS ONLINE

File (hide): 24426db81e67b3d-...jpg (90.68 KB, 750x936, 125:156, Beware the fury of righteo....jpg) [h] [s]

[–] ▶ "ahem" Anonymous 04/27/19 (Sat) 20:00:15 ID: 4e267a No.13192921 [Watch Thread] [Show All Posts] >>13192955

It's been real dudes. From the bottom of my heart thank you for everything. Keep up the infographic redpill threads. I've only been lurking for a year and a half, yet what I've learned here is priceless. It's been an honor.
Livestream link is below as well as my open letter. Livestream will begin shortly.
https://www.facebook.com/john.earnest.96780

An open letter.
https://pastebin.com/VXXFQMTW
https://www.mediafire.com/file/d9oilcmjbenxiyz/Open_Letter.pdf/file

Also, in case they take down my livestream too soon and you don't get to hear all the awesome tunes I had planned—here they are. Very meme-able songs—you should have no problem
-Sloop John B by The Beach Boys
-Original Pokemon Theme Song
-Warthog Run Theme from Halo Combat Evolved
-Warriors by Imagine Dragons
-The Last Stand by Sabaton
-Blow Me Away by Breaking Benjamin
Winged Hussars by Sabaton
Rose Tattoo by Dropkick Murphys
The Path (A New Beginning) from The Last of Us

Meme magic is real. May the LORD Christ be with you all.

▶ Anonymous 04/27/19 (Sat) 20:04:34 ID: 7d87db No.13192936

based
get the high score

▶ Anonymous 04/27/19 (Sat) 20:05:31 ID: 2b8aed No.13192938

>literal spam

Apr 27 18:04

OFFICIAL THREAD OF THE SAN DIEGO SYNAGOGUE SHOOTER BEFORE IT WAS DELETED

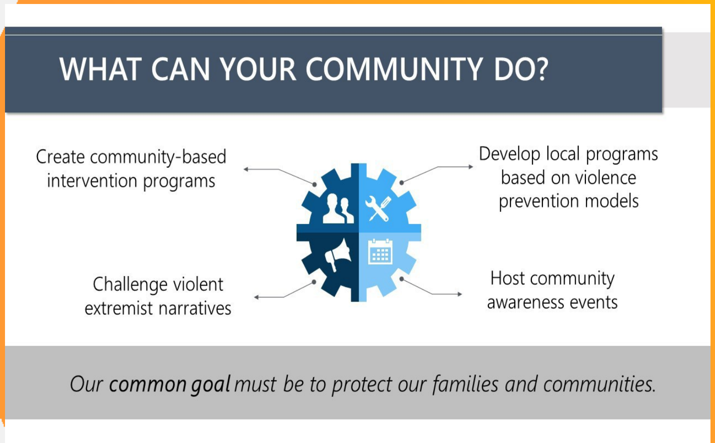
THE ANARCHIST COOKBOOK

The Great Replacement

TOWARDS A NEW SOCIETY

WE MARCH EVER FORWARDS

Understand how to utilize the numerous prevention programs in the U.S. and in your community



WHAT CAN YOUR COMMUNITY DO?

Create community-based intervention programs

Develop local programs based on violence prevention models

Challenge violent extremist narratives

Host community awareness events

*Our **common goal** must be to protect our families and communities.*

Law Enforcement Awareness Brief (LAB) on Terrorism Prevention

The Law Enforcement Awareness Brief (LAB) is a **2 - 5 hour** *customizable brief* designed for small and mid-sized state, local, tribal, and territorial (SLTT) law enforcement agencies on their role in the national terrorism prevention strategy.

- The brief is the central element of a broader Training-of-Trainers (ToT) program developed by Department of Homeland Security's Office for Targeted Violence and Terrorism Prevention (TVTP), Federal Law Enforcement Training Centers, and Office for Civil Rights and Civil Liberties (CRCL).
- The goal is to develop and support a national cadre of SLTT law enforcement instructors who, after completing the DHS ToT program, will be equipped to offer the brief in their home jurisdictions to other law enforcement personnel.
- The LAB is delivered *by* SLTT law enforcement *to* SLTT law enforcement.

Interested agencies should contact DHS HQ via email:

- TVTP Briefing Team at CABbriefingrequests@hq.dhs.gov , or
- CRCL staff at LAB-CABTraining@hq.dhs.gov

The LAB is coordinated via the federal interagency, yet customized by each jurisdiction.

The LAB addresses the unique role of SLTT law enforcement in the national terrorism prevention strategy by engaging with local communities.

The LAB discusses the multi-faceted terrorism threat as likely to be experienced by SLTT law enforcement by focusing on community engagement and "lessons learned" as related to terrorism prevention.

The research-driven LAB Program includes case studies, videos, relevant intel products and research-based InfoGfx.

Homeland Security