Evaluating and Responding to Violent Extremist Hoax Threats

SCOPE: This product is intended to assist public safety officials and other security stakeholders in detecting, evaluating, responding to, and mitigating violent extremist hoax threats and online harassment tactics. This product is not a response to a specific threat against the United States. It provides information and resources related to international terrorism threats and/or threats resulting from violent extremist tactics, techniques, and procedures. In this product, NCTC uses the term "violent extremists" to refer to foreign violent extremists, including foreign terrorist organization members, and those US-based violent extremists who are directed, enabled, inspired by, or who otherwise affiliate or collaborate with foreign violent extremists.

Violent extremists continue to use online harassment and hoax threats such as swatting, fedposting, fearmongering, and doxing as low-cost, low-risk tactics to instill a fear in people that they may be a victim of a violent extremist attack and to incite others to engage in violence. These threats may divert attention and drain public safety resources and could inspire other illicit actors to engage in these practices. While these tactics are not new, the media attention garnered by hoax threats and to operations at government facilities, commercial facilities, faith-based organizations, and schools may further drive violent extremists to adopt these tactics for use against various targets. Awareness of hoax trends and tactics may better position public safety officials to assess, identify, allocate resources, and provide intelligence and warning to first responders.

Online Email Mail Phone

	SWATTING	FEDPOSTING	FEARMONGERING[a]	DOXING
				
DEFINITON	*Falsely reporting an emergency via online tip or phone call to emergency services to provoke a law enforcement reaction, particularly from SWAT teams who show up to the unwitting target's location*	*Posting false threats of violence against a specific target*	*Publishing online media content—often featuring manipulated or fictious images—with threats of violence against a specific target*	*Gathering an individual's personally identifiable information (PII)—or an organization's sensitive information— from open source or compromised material and publishing it online for malicious purposes*
EXAMPLE	In 2020, a Texas-based leader of the transnational racially or ethnically motivated violent extremist (REMVE) group Atomwaffen Division was arrested and sentenced to 41 months in prison for conducting more than 130 swatting attacks in 2018 and 2019 against a variety of perceived ideological opponents, including a US Cabinet official, a historic African-American church, and an Islamic center.	In April 2024, a minor from a European country who supported REMVE ideology posted threats against mosques in Oslo, Norway, probably to intimidate the local Muslim community and waste law enforcement resources. The threat coincided with Ramadan festivities and led to a national arming of police and increased presence at mosques in Oslo through the end of Ramadan, even though the police quickly determined the threat was not credible.	Pro-ISIS media outlet, al-Wafaa Media Foundation, published dozens of online videos and images that encouraged violent attacks against the 2018 World Cup in Russia using easily accessible weapons such as guns, knives, and vehicles. Some of the threatening messaging also depicted UAS dropping bombs on crowded stadiums.	In 2016, a member of an ISIS-affiliated online group recruited others to carry out online attacks and cyber intrusions to collect PII and used the information to disseminate "kill lists" of potential victims. The person responsible for this activity pleaded guilty and was sentenced in 2019 for conspiring to provide material support to ISIS.
POTENTIAL MITIGATION[b]	• Maintain awareness of hoax threat tactics to assist with threat identification and response. • Assess for inconsistent noises in the background or the caller's demeanor, which may not match the reported threat. • Evaluate for inconsistent responses or demeanor when the caller is challenged. • Confirm if the call was made through voice over Internet protocol (VoIP) services by checking if the number appears as all zeros, nines, blocked, unavailable, or a default VoIP number.	• Assess the demeanor of a caller as well as background noises for inconsistencies with the reported crisis or threat. • Consider the threat and information surrounding the threat for vagueness, inconsistencies, or implausibility. • Check emails that do not contain a direct threat to a specific location or may include many locations. • Evaluate emails containing the same or similar language sent to multiple targets.	• Determine if the media was previously released by a designated foreign terrorist organization. • Check if images were recycled, repurposed, linked from another author, or used elsewhere. • Determine if the social media account can be verified through public records or other means.	• Review online security and privacy settings and implement the strongest controls possible. • Remove PII from social media profiles. • Update all software, operating systems, and applications to the most recent versions, and only apply updates from a trusted source. • Refrain from responding to unsolicited phone calls, visits, or emails asking about employees or other potential sensitive information.

[a] While one of the goals of this type of threat is to incite lone offenders to violence, people rarely mobilize to violence solely through their engagement with online violent extremist content.
[b] These considerations are not exhaustive. No single factor should be considered on its own but the totality of circumstances may provide warning of the potential threat scenario. For additional information, refer to the resources highlighted throughout this product.

NCTC-JFRT-2024-17093
7 NOVEMBER 2024
AUTHORED BY NCTC, DHS, FBI

CONSIDERATIONS

Public safety officials are encouraged to take steps prior to and while they respond to an incident to help reduce risks associated with violent extremist online harassment incidents and hoax threats. There are many resources available on this topic. This product highlights options that first responder partners may incorporate or use in accordance with existing departmental guidelines or standard operating procedures.

PLANNING AND TRAINING

Awareness of hoax tactics can help public safety organizations prepare and respond to potential threat incidents.

Cybersecurity and Infrastructure Security Agency (CISA) Mitigating the Impacts of Doxing on Critical Infrastructure provides information, guidance, and resources to help organizations assess their cybersecurity and improve mitigation against evolving online threats. https://www.cisa.gov/resources-tools/resources/cisa-insights-mitigating-impacts-doxing-critical-infrastructure

CISA and FBI provide information on cybersecurity best practices to help individuals and organizations implement preventative measures and manage cyber risks. https://www.cisa.gov/topics/cybersecurity-best-practices

CISA Office for Bombing Prevention offers training and products to build counter-improvised explosive device core capabilities and enhance awareness of terrorist threats. Course offerings provide education on strategies to prevent, protect against, respond to, and mitigate bombing incidents. https://www.cisa.gov/topics/physical-security/bombing-prevention

DHS Resources for Individuals on the Threat of Doxing provides ways to protect sensitive information from the threat of doxing and additional government resources. https://www.dhs.gov/sites/default/files/2024-01/24_0117_ope_resources-for-individuals-on-the-threat-of-doxing-508.pdf

FBI Characteristics of Swatting Calls provides swatting call indicators and de-escalation strategies (available on Law Enforcement Enterprise Portal (LEEP) via Justice Connect).

FBI Quick Response Guide to Internet Based Threat Investigations is a response guide to assist law enforcement in their investigation of Internet based threats (available on LEEP via Justice Connect).

REPORTING AND EVALUATING

In the event of a hoax threat or online harassment incident, the following resources provide first responder partners with initial reporting guidance and strategies for threat identification and assessment of the information.

The **FBI** encourages reporting of any perceived threat of violence, harassment, or intimidation to the local FBI Field Office and the FBI National Threat Operations Center by calling 1-800-CALL-FBI (225-5324) or visiting https://tips.fbi.gov.

eGuardian migrated to the FBI's internal Guardian system, where it is assigned to the appropriate squad or Joint Terrorism Task Force (JTTF) for further investigative action, as required. https://le.fbi.gov/informational-tools/eguardian

FBI Internet Crime Complaint Center is the central site for victims to file a complaint or report cybercrime and receive training and updates about cyber threats. https://www.ic3.gov/default.aspx

FBI Virtual Command Center National Common Operational Picture—SWATTING, available through LEEP, is a collaborative space for public safety partners to share information on swatting incidents and create a real-time operational picture.

CISA Social Media Threat Guidance for School Staff and Authorities highlights considerations for reporting and responding to social media threats to schools. https://www.cisa.gov/resources-tools/resources/social-media-threat-guidance-school-staff-and-authorities-infographic

State And Major Urban Fusion Centers are focal points for the receipt, analysis, gathering, and sharing of threat-related information. https://www.dhs.gov/fusion-centers

RESPONSE AND INVESTIGATION

Recipients of threats should follow departmental guidelines and emergency procedures, as applicable, until the threat is deemed noncredible and determined to be a hoax. Determining the credibility of a threat can help a decisionmaker dispatch appropriate resources.

CISA and FBI Bomb Threat Guide provides guidance to decisionmakers to help assess bomb threats, provide response guidance, and protect critical infrastructure. https://www.cisa.gov/resources-tools/resources/bomb-threat-guide

FBI National Cyber Investigative Joint Task Force coordinates, integrates, and shares information to support cyber threat investigations. https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force

FBI Joint Terrorism Task Forces are highly trained and locally based investigators and analysts from dozens of US law enforcement and intelligence agencies. www.fbi.gov/contact-us/field-offices

CISA and FBI Anonymized Threat Response Guidance: A Toolkit for K-12 Schools helps local education facilities and law enforcement agencies develop tailored approaches for assessing and responding to anonymous threats. https://www.cisa.gov/resources-tools/resources/k-12-anonymized-threat-response-guidance

COLLABORATION AND OUTREACH

Timely and effective incident responses rely on pre-incident collaboration, information sharing, and engagement across public and private sector partners to improve reporting and response capabilities.

FBI "Think Before You Post" campaign highlights the impact of hoax threats that disrupt workplaces, schools, waste limited resources, and divert law enforcement from potential threats. https://www.fbi.gov/news/stories/hoax-threats-awareness-100518

FBI Threat and Intimidation Response Guide provides information about types of threats and what to do if threatened. https://www.fcc.gov/sites/default/files/threat_guide_english_final.pdf

Technical Resource for Incident Prevention (TRIPwire) is an online, information-sharing and resource portal to help users anticipate, identify, and prevent IED incidents. https://www.cisa.gov/resources-tools/resources/technical-resource-incident-prevention-tripwire-portal

DHS and FBI Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) is a collaborative effort with state, local, tribal, and territorial law enforcement partners. This initiative helps prevent terrorism and related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information. Training can be found at: https://nsi.ncirc.gov/training_online.aspx

NCTC-JFRT-2024-17093

7 NOVEMBER 2024
AUTHORED BY NCTC, DHS, FBI

JCAT

JOINT COUNTERTERRORISM ASSESSMENT TEAM

PRODUCT FEEDBACK

Please use the link below to complete a short survey. Your feedback will help JCAT develop counterterrorism products that support the public safety and private sector community.

https://www.JCAT-url.com

For further information, please email JCAT
jcat@odni.gov

(U) The Joint Counterterrorism Assessment Team (JCAT) is a collaboration by NCTC, DHS, FBI, state, local, tribal, and territorial government personnel to improve information sharing and enhance public safety. The First Responder's Toolbox is an ad hoc, unclassified reference aid intended to promote counterterrorism coordination among federal, state, local, tribal, and territorial government authorities and partnerships with private sector officials in deterring, preventing, disrupting, and responding to terrorist attacks.