Violent Extremists Likely Will Continue to Use Disinformation on Social Media Outlets to Instill Fear and Radicalize Others

Terrorist disinformation may be used to attract attention, harass people, drain public safety resources, and incite others to violence. Disinformation, including that which is in the form of manipulated images and videos, can create challenges for public safety stakeholders in evaluating the credibility of the information and determining whether a threat exists. This product highlights manipulated violent extremist messaging, so that public safety and private sector stakeholders may better identify and assess terrorist disinformation.

SCOPE: This product highlights examples of official media releases by designated foreign terrorist organizations, such as ISIS, and unofficial media releases by auxiliary news agencies and terrorist supporters. It is intended to describe how terrorists use disinformation to potentially influence Homeland and Western audiences, and introduce steps that can be taken to determine the credibility of the messaging.

Terrorists often use manipulated and fictitious images to enhance their messaging efforts. In comparison to media released by al-Qa'ida which tends to rely on pre-recorded videography often highlighting historical events, ISIS generally tends to feature aspirational threats using better quality imagery or infographics. Although these images may not be indicative of an ongoing plot, they sometimes combine background images of actual US locations with unrelated images of terrorists, weapons, terrorist symbols, and attacks.

- In December 2017, a screenshot from an ISIS-Somalia video of a sniper on top of a building in Denver, Colorado was released, which may have been intended to inspire fellow supporters or to create a sense of fear. A technical assessment indicated that the individual portrayed, as well as the sniper rifle and accessories, were doctored into the image using editing software.

Screenshot depicting Denver from ISIS-Somalia video, December 2017

- Also, in December 2017, ISIS supporters released a video via social media during the holiday season and included pictures of the Statue of Liberty, the Eiffel Tower and a beheading of Santa Claus, which demonstrates aspirational threats towards US and Western targets.

9 AUGUST 2018
AUTHORED BY NCTC, DHS, FBI

- In May 2017, a pro-ISIS media outlet posted a video highlighting potential targets in the US, including Las Vegas, New York and Washington, DC, which may also be representative of ISIS's use of media to spread fear and encourage attacks.

The general public plays a key role in the identification of terrorist disinformation on the Internet. Public safety personnel are encouraged to perform preventative outreach efforts, such as hosting town halls which cover material that helps demystify and dispel narratives that violence is necessary and justified, and instead frame these actions as selfish and harmful to a would-be attacker's community and family. Additionally, such outreach efforts may also help increase bystander reporting.

Steps for Dealing with Violent Extremist Social Media Messaging: Social media messaging is a legal, constitutionally-protected activity and no single factor should be considered on its own to signify terrorism, but when observed in conjunction with violent extremist rhetoric and other cautionary behaviors, may provide warning of mobilization to violence.

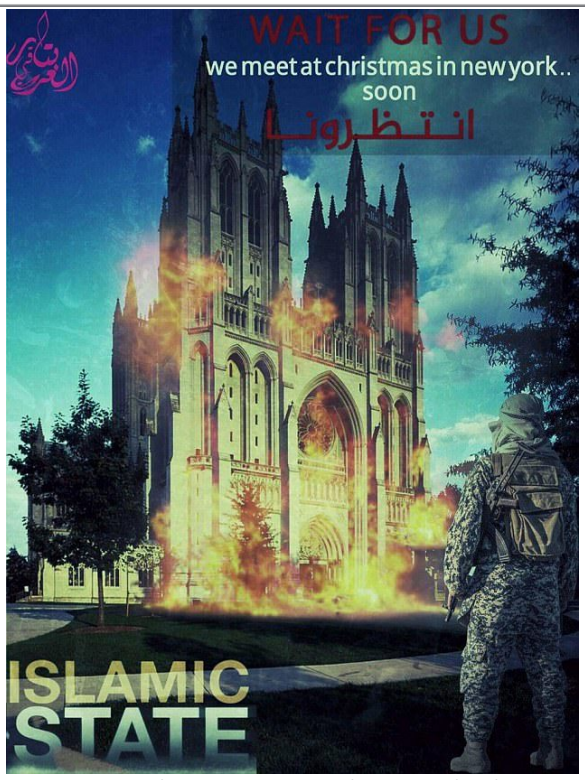
Identify: Awareness and vigilance are crucial to identifying suspicious behaviors online. Familiarity with tactics, techniques, and procedures (TTPs) in violent extremist messaging can help public safety and private sector stakeholders identify suspicious behaviors on social media (characteristic of similar postings from online ISIS supporters threatening locations around the world).

Document: Similar to evidence found at a traditional crime scene, evidence within the cyber realm should be properly collected, documented and maintained through a chain-of-custody. Gathering possible evidence can assist law enforcement in identifying at-risk individuals, facilitate information sharing between public safety and private sector entities, and even be used in court.

Analyze and Evaluate: Allows public safety and private sector partners to understand the purpose of the identified online message and determine how to respond to the potential threat. In this product, we provide a list of questions to ask when encountering terrorist disinformation. Answers to these questions may assist in understanding the type of disinformation (credible or aspirational), capability, and how to respond to or mitigate any threat to public safety.

Report and Respond: Reporting indicators of suspicious activity through established reporting mechanisms is a vital step and helps the investigating law enforcement agencies to carefully assess the information. Sharing pre-incident terrorism indicators and other related criminal activity is key to preventing acts of terrorism while protecting privacy, and civil rights and liberties.

Questions to Ask When Encountering Violent Extremist Messaging:



Pro-ISIS image threatening an attack. Depicted is the National Cathedral in Washington, DC

- **WHAT IS BEING SAID?**
  - ***Does the message contain a last will, manifesto, or martyrdom statement?*** Preparing and disseminating a last will or martyrdom statement that is shared online and to social media contacts should be of immediate concern and is highly indicative of an individual mobilizing to violence.
  - ***Is the message attempting to mobilize others to violence****?* This behavior may not present a direct and imminent threat but is an indicator of someone who is mobilizing and is a near-term concern.
  - ***Is the message a fictional, vague, and/or aspirational threat?*** If yes, the threat may not be credible but should still be considered in the context of all available information. Additionally, non-credible threats can also serve ISIS's purposes.
  - ***Does the message express acceptance of violence as a necessary means to achieve ideological goals?*** Behavior associated with acceptance for acts of violence is typically considered a long-term concern. Other indicators signifying intent to commit violence would generally be needed to confirm an individual's mobilization to violence.
- **WHO IS SAYING IT?**
  - ***Is it a media release by a designated foreign terrorist organization (FTO)?*** Designated FTO media releases may not present a credible threat but should still be considered in the context of all available information. Such releases could also help inspire supporters to conduct an attack.
  - ***Has the social media account been verified through public records or other means?*** If the account can't be verified, the threat may not be credible but should still be considered in the context of all available information.
  - ***Has this image previously been recycled, repurposed, linked from another author, or used elsewhere?*** Recycled messages may not be credible but should still be considered in the context of all available information.
  - ***Has the online content received multiple posts or does it contain "live feed"?*** Understanding who and how many people are tracking the message will assist in identifying who the author is, its intended audience, and the purpose of the message.

- **WHAT ARE THE POTENTIAL EFFECTS?**
  - ***Does the message present a specific and credible threat to the general public?*** The main purpose of the message may be to attract attention, harass people, drain public safety resources, instill fear, and radicalize and incite others to violence. Early analysis of the message will assist in determining the tactical approach to the threat; including the amount of resources needed to appropriately address security concerns and how to effectively investigate the incident.
  - ***What is the TTP or target (location, entity, facility, or person)?*** Online threats can be directed to many different persons, groups, and infrastructures. Understanding the threat's target will assist in identifying the experts and resources needed to properly investigate and provide effective security measures to mitigate potential danger.
  - ***Aside from addressing the credibility and potential danger of the threat, what does the message mean?*** Violent extremist social media messaging can be analyzed to identify long-term information that can be used to strategize for future threats. The messages can provide insight into current trends and TTPs, and can provide insight as to when, where, and how future threats or attacks may happen.

Pro-ISIS image threatening an attack

Evidence Collection and Documentation Considerations:

- Public safety entities should consider establishing policies and procedures with respect to handling online terrorist disinformation.
- Cyber security precautions should be taken when collecting internet data (downloading content vs taking a screenshot) in case of malicious code.

- Online documentation and analysis tools can be used to document and determine reliability and validity of threat information posted on social media. Resources include:
  - **Real-Time and Open Source Analysis (ROSA) Resource Guide**: https://it.ojp.gov/GIST/1200/Real-Time-and-Open-Source-Analysis--ROSA--Resource-Guide
  - **International Association of Chiefs of Police Social Media Resources**: http://www.iacpsocialmedia.org/resources/tools-tutorials/law-enforcement-investigative-guides/ and http://www.iacpcybercenter.org
  - **The National Cyber-Forensics and Training Alliance (NCFTAS):** A nonprofit partnership between private industry, government, and academia for the sole purpose of providing a neutral, trusted environment that enables two-way collaboration and cooperation to identify, mitigate, and disrupt cyber-crime. (http://www.ncfta.net/)
  - **Tech Against Terrorism:** A UN-mandated initiative that helps tech companies prevent their platforms from being exploited by terrorists, while also respecting human rights. Tech Against Terrorism works with the global tech sector to share best practice (policy, guidelines, learning materials, practical workshops, and tools) within the tech industry and with governments. Go to www.techagainstterrorism.org or reach out to Contact@TechAgainstTerrorism.org with the subject line "Training."

Additional Resources: It is important to include public safety and private security stakeholders in the analysis of online violent-extremist messages and images, so they may be able to understand and respond to threats associated with such disinformation. When an online violent-extremist post is identified, public safety personnel should collaborate with other stakeholders who may assist in analyzing, investigating and responding to the threat. These stakeholders include:

- **The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI):** A joint collaborative effort by the U.S. Department of Homeland Security, the Federal Bureau of Investigation, and 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. SARS Training can be found at: http://nsi.ncirc.gov/training_online.aspx
- **State and Major Urban Area Fusion Centers:** The principal role of the fusion center is to compile, analyze, and disseminate criminal and terrorism information and intelligence (including, but not limited to, threat, public safety, law enforcement, public health, social services, and public works) to anticipate, identify, prevent, and/or monitor criminal and terrorist activity. (https://www.dhs.gov/fusion-center-locations-and-contact-information)
- **Fusion Liaison Officers (FLO):** FLO programs may also be referred to as Intelligence Liaison Officer (ILO), Terrorism Liaison Officer (TLO), or Liaison Officer (LNO) programs. Different jurisdictions may use a slightly different term in their respective centers, but for the purposes of the National Strategy, the program is referred to as FLO. (https://www.dhs.gov/state-and-major-urban-area-fusion-centers)

- **Regional Computer Forensic Lab (RCFL):** A one-stop, full-service forensics laboratory and training center entirely devoted to the examination of digital evidence in support of criminal investigations such as terrorism. (https://www.rcfl.gov/)
- **FBI Joint Terrorism Task Forces (JTTF):** The United States' front line on terrorism: small cells of highly trained, locally based, passionately committed investigators, analysts, linguists, SWAT experts, and other specialists from dozens of US law enforcement and intelligence agencies.
    - Field Offices: http://www.fbi.gov/contact-us/field
    - Terrorism Online Tips: https://tips.fbi.gov/
    - Internet Crime Complaint Center Online Tips (IC3): http://www.ic3.gov
- **National Counterterrorism Center (NCTC) Domestic Representatives**: NCTC Domestic Representatives are stationed in 11 strategic locations across the US and serve as NCTC's touch point with federal, state, local, tribal and territorial government partners. (https://www.dni.gov/index.php/nctc-home)
- **DHS Intelligence Officers (IOs) and Protective Service Advisors (PSAs):** Deployed throughout the US, IOs and PSAs support state, local, tribal, territorial, and private sector partners through collaboration, information sharing, and outreach activities. IOs share threat-related information and assist with the implementation and execution of the intelligence cycle. PSAs are regional critical infrastructure security and resilience specialists, who provide local perspective to and support the development of the national risk picture by identifying, assessing, monitoring, and minimizing risk to critical infrastructure. (https://www.dhs.gov/publication/deployed-intelligence-officers-and-protective-security-advisors)
- **National Geospatial Intelligence Agency (NGA):** Delivers world-class geospatial intelligence that provides a decisive advantage to policymakers, warfighters, intelligence professionals, and first responders. (https://www.nga.mil/ProductsServices/Pages/default.aspx)
- **The National Virtual Translation Center (NVTC):** An FBI-managed federal government center created to serve the US government's translation needs. The NVTC was established by Congress in 2003 to provide timely, accurate, and cost-effective translations in support of national interests. (https://www.fbi.gov/about/leadership-and-structure/intelligence-branch/national-virtual-translation-center)
- **Private Sector Partners:**
    - **FBI Private Sector Coordinators**: The Office of Private Sector provides an organized, coordinated, and horizontal approach to how the FBI engages with the private sector. It serves as the entity within the FBI that has a 360 degree understanding of the FBI's engagement with the private sector, enterprise-wide. (https://www.fbi.gov/contact-us/field-offices)
    - **INFRAGARD**: A partnership between the FBI and the private sector. It is an association of persons who represent businesses, academic institutions, law enforcement agencies, and other

participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. (https://www.infragard.org/)

- **Domestic Security Alliance Council (DSAC)**: A strategic partnership between the US Government and US private industry that enhances communication and promotes the timely and effective exchange of security and intelligence information. (https://www.dsac.gov/)
- **Information Sharing and Analysis Center (ISAC)**: ISACs help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards. ISACs collect, analyze, and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency. (https://www.nationalisacs.org/)

JOINT COUNTERTERRORISM ASSESSMENT TEAM | JCAT

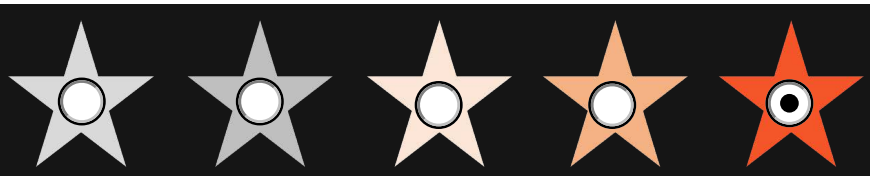
PRODUCT FEEDBACK FORM

(U) JCAT MISSION: To improve information sharing and enhance public safety. In coordination with the FBI and DHS, collaborate with other members of the IC to research, produce, and disseminate counterterrorism (CT) intelligence products for federal, state, local, tribal and territorial government agencies and the private sector. Advocate for the CT intelligence requirements and needs of these partners throughout the IC.

NAME and/or ORG:

DISCIPLINE: ☐ LE ☐ FIRE ☐ EMS ☐ HEALTH ☐ ANALYSIS ☐ PRIVATE SECTOR DATE:

PRODUCT TITLE: Violent Extremists Likely Will Continue to Use Disinformation on Social Media

POOR  GREAT

ADDITIONAL COMMENTS, SUGGESTIONS, OR QUESTIONS. HOW DOES JCAT MAKE PRODUCTS BETTER?

WHAT TOPICS DO YOU RECOMMEND?

SUBMIT