INTELLIGENCE NOTE

Homeland Security

22 May 2020

(U) Counterterrorism Mission Center

(U//FOUO) Violent Adversaries Likely to Use Protective Masks to Evade Face Recognition Systems

(U//FOUO) Scope. This *Intelligence Note* (*IN*) examines the potential impacts that widespread use of protective masks could have on security operations that incorporate face recognition systems—such as video cameras, image processing hardware and software, and image recognition algorithms—to monitor public spaces during the ongoing COVID-19 public health emergency and in the months after the pandemic subsides. This *IN* focuses on face recognition systems used in public spaces to support security operations during mass gatherings and outdoor events. Face recognition used at single-person entry security checkpoints, such as airports and US points of entry, are not included in this assessment, as those systems typically require the removal of face coverings or a second form of identification such as a government issued identification card. This *IN* is current as of 1 May 2020.

(U//FOUO) Prepared by the DHS Intelligence Enterprise (DHS IE) Counterterrorism Mission Center (CTMC). Coordinated with CBP, CISA, CWMD, NCTC-JCAT, ICE, TSA, and USCG.

(U) Interest in Avoiding Face Recognition Continues, May Use Current Public Safety Guidance to Evade Detection

(U//FOUO) We assess violent extremists and other criminals who have historically maintained an interest in avoiding face recognition are likely to opportunistically seize upon public safety measures recommending the wearing of face masks to hinder the effectiveness of face recognition systems in public spaces by security partners. Current recommendations by the Centers for Disease Control and Prevention, posted online on 10 April, recommend wearing face masks in public spaces to limit the person-to-person transmission of COVID-19 in situations when maintaining social distancing is not feasible.[1] While we have no specific information that violent extremists or other criminals in the United States are using protective face coverings to conduct attacks, some of these entities have previously expressed interest in avoiding face recognition and promulgated simple instructions to conceal one's identity, both prior to and during the current COVID-19 pandemic.

» (U//FOUO) On 21 March, members of a white supremacist extremist (WSE) online forum discussed attacking critical infrastructure, causing damage and disruption to vital services during the COVID-19 pandemic, and spreading COVID-19 intentionally.[a] A group member suggested targeting critical infrastructure—specifically power lines, wastewater facilities, and rail—while wearing a breathing mask to hide a perpetrators identity.[2]

» (U//FOUO) An anonymous social media user posted tactics, techniques, and procedures for disrupting airport operations, which also included general methods to avoid face recognition systems in late August 2019. This included the use of make-up, hairstyles, and a link to a website advertising glasses for sale that prevent face recognition and mapping.[3]

» (U//FOUO) In early February 2018 an individual on an internet messaging board posted a series of techniques for conducting attacks without exposing ones' identity. This included the wearing of a "dust mask" (possibly a respirator), "hard hat," and "goggles".[4]

[a] (U) Please see DHS Definition box at end of the document.

(U//FOUO) Face Recognition Systems Likely to be Less Effective as Widespread Wear of Face Coverings for Public Safety Purposes Continue

(U//FOUO) We assess face recognition systems used to support security operations in public spaces will be less effective while widespread public use of face masks, including partial and full face covering, is practiced by the public to limit the spread of COVID-19. Independent, third-party testing of the effectiveness of face recognition algorithms in identifying subjects wearing face coverings is being developed by the Department of Commerce's National Institute of Standards and Technology, but these efforts are on hold due to the current COVID-19 public health emergency, according to a 1 May 2020 media account.[5] While the use of face coverings is recommended in the interest of public safety during the COVID-19 pandemic, security partners that leverage face recognition systems will likely have to rely on other means of detecting suspicious activity in the near to mid-term. We assess the widespread use of masks for public safety could likely continue to impact the effectiveness of face recognition systems even after federal or state mandates for their use are withdrawn as portions of the general population will likely continue to voluntarily wear face coverings in public even after restrictions on social gatherings are lifted or until an effective COVID-19 vaccine is publicly available.

(U//FOUO) Other Means of Avoiding Face Recognition Systems

(U//FOUO) Masks or face coverings remain a simple, readily available means to avoid detection by face recognition systems however, some states and localities have anti-mask laws that generally prohibit the wearing of face coverings under normal circumstances. The use of face covering by violent extremists or criminals to avoid identification is typically easily noticeable by security partners. Other means of evading face recognition are commercially available, with no acquisition barriers, and may be less noticeable than masks to security partners. As the use and capability of face recognition systems expand typically innocuous items such as laser pointers, accessories, and clothing capable of interrupting such systems may become a feature in violent activity. While the wearing or possession of these items may not be explicitly prohibited by federal, state or local statues, such items could be misused by violent extremists or other criminals intending to cause disruption to critical infrastructure.

(U) Blue or green lasers pointed directly at security cameras. Blue and green lasers have very high bandwidth, project over a relatively long distance, and may be able to temporary "blind" a video camera.

(U) Crowd using lasers during 2019 pro-democracy protest in Hong Kong.[6] Note this example is offered only to illustrate how violent extremists might employ similar tactics.

(U) Clothing or accessories with images of faces, license plates, or pixelated images. Face recognition algorithms are unable to deconflict images resulting in a false positive or unresolved detection.

(U) Backpack with pixelated images of faces.[7]

(U) Specialized clothing, such as hats, which use visible infrared lights to obscure the face. The results may appear as a white blob on camera or cause shadows, which cannot be resolved by face recognition algorithms.

(U) Research version of hat with light emitting diodes (LEDs).[8]

(U) DHS Definition

(U//FOUO) DHS defines **white supremacist extremists (WSE)** as groups or individuals who facilitate or engage in acts of unlawful violence directed at the federal government, ethnic minorities, or Jewish persons in support of their belief that Caucasians are intellectually and morally superior to other races and their perception that the government is controlled by Jewish persons.

(U) Report Suspicious Activity
(U) **To report suspicious activity, law enforcement, Fire-EMS, private security personnel, and emergency managers should follow established protocols; all other personnel should call 911 or contact local law enforcement.** Suspicious activity reports (SARs) will be forwarded to the appropriate fusion center and FBI Joint Terrorism Task Force for further action. For more information on the Nationwide SAR Initiative, visit http://nsi.ncirc.gov/resources.aspx.

(U) **Tracked by:** HSEC-8.2, HSEC 8.3, HSEC-8.8, HSEC-8.9

(U) Source Summary Statement

(U//FOUO) We have **high confidence** in our assessment that violent extremists and other criminals will maintain interest in avoiding face recognition recognition systems in public spaces by security partners based off direct reporting of the promulgation of this technique by violent extremists as recently as March 2020. Our assessment could be strengthened further by reporting of specific technical information and placement of face recognition systems.

(U//FOUO) We have **medium confidence** in our assessment that face recognition systems will be less effective while public safety measures during the COVID-19 emergency that recommend wearing face covering. We based this on available research of face recognition system effectiveness when a video is unable to capture a full-face profile. Our confidence could increase based off reporting indicating that violent extremists are specifically aware of face recognition limitations.

---

[1] (U) [US Center for Disease Control | 10 APR 2020 | "Use of Face Covering to Help Slow the Spread of COVID-19" | https://www.cdc.gov/coronavirus/2019-ncov/downloads/DIY-cloth-face-covering-instructions.pdf | | (U) | (U) |]

[2] (U//FOUO) [DHS | FIR-0032-20 | 26 MAR 2020 | 21-25 MAR 2020 |"SUBSTANTIVE REVISION: COVID-19 - White Supremacy Extremist Telegram Users Discuss Attacking Critical Infrastructure, Spreading COVID-19, and Causing Disruption to Vital Services During National Emergency" | (U//FOUO) | (U//FOUO) |]

[3] (U//FOUO) [DHS | OSIR-04001-1576-19 | 26 AUG 2019 | 26 AUG 2019 | (U//FOUO) "TTPs to avoid face recognition and drone use as an easy way to attack and disrupt airport operations" | | (U//FOUO) | (U//FOUO) |]

[4] (U//FOUO) [DHS |OSIR-04001-0437-18 | 8 FEB 2018 | 8 FEB 2018 | (U//FOUO) "Anti-fascist social media user incites violence against White Supremacist Extremists" | | (U//FOUO) | (U//FOUO) |]

[5] (U) [Wired | 1 MAY 2020 | "How Well Can Algorithms Recognize Your Masked Face?" | https://www.wired.com/story/algorithms-recognize-masked-face/ | | (U) | (U) |]

[6] (U) [Laserpointersafety.com | "Laser use during protests"; 2019-2020 | https://www.laserpointersafety.com/protests/index.html | | (U) | (U) |]

[7] (U) [The Economist | 16 AUG 2019 | "Fooling Big Brother, Face off" | page 60 | https://articles.cafeyn.co/34e71f/the-economist/2019-08-16/face-o%EF%AC%80 | | (U) | (U) |]

[8] (U); [University of Cambridge, National Institute of Technology (Warangal, India: and the Indian Institute of Science | 30 AUG 2017 | "Disguised Face Identification (DFI) with Facial KeyPoints using Spatial Fusion Convolutional Network" | pg. 4 | https://arxiv.org/pdf/1803.04683.pdf | | (U) | (U) |]

CLASSIFICATION: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

Homeland Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title: (U//FOUO) Violent Adversaries Likely to Use Protective Masks to Evade Face Recognition Systems

All survey responses are completely anonymous. No personally identifiable information is captured unless you voluntarily offer personal or contact information in any of the comment fields. Additionally, your responses are combined with those of many others and summarized in a report to further protect your anonymity.

1. Please select partner type: Select One **and function:** Select One

2. What is the highest level of intelligence information that you receive? Select One

3. Please complete the following sentence: "I focus most of my time on:" Select One

4. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	○	○	○	○	○	○
Product's relevance to your mission	○	○	○	○	○	○
Product's timeliness	○	○	○	○	○	○
Product's responsiveness to your intelligence needs	○	○	○	○	○	○

5. How do you plan to use this product in support of your mission? ***(Check all that apply.)***

- ☐ Drive planning and preparedness efforts, training, and/or emergency response operations
- ☐ Observe, identify, and/or disrupt threats
- ☐ Share with partners
- ☐ Allocate resources (e.g. equipment and personnel)
- ☐ Reprioritize organizational focus
- ☐ Author or adjust policies and guidelines
- ☐ Initiate a law enforcement investigation
- ☐ Intiate your own regional-specific analysis
- ☐ Intiate your own topic-specific analysis
- ☐ Develop long-term homeland security strategies
- ☐ Do not plan to use
- ☐ Other:

6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.

7. What did this product *not* address that you anticipated it would?

8. To what extent do you agree with the following two statements?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disgree	N/A
This product will enable me to make better decisions regarding this topic.	○	○	○	○	○	○
This product provided me with intelligence information I did not find elsewhere.	○	○	○	○	○	○

9. How did you obtain this product? Select One

10. Would you be willing to participate in a follow-up conversation about your feedback? Yes

To help us understand more about your organization so we can better tailor future products, please provide:

Name: *Position:*
Organization: *State:*
Contact Number: *Email:*

Submit Feedback

Privacy Act Statement

CLASSIFICATION: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

Product Serial Number: IA-44196-20 REV: 01 August 2017