HARVARD LAW SCHOOL
NATIONAL SECURITY JOURNAL

ONLINE ARTICLE

Shining Light on the "Going Dark" Phenomenon: U.S. Efforts to Overcome the Use of End-to-End Encryption by Islamic State Supporters

RYAN PEREIRA[*]

Recommended Citation

Ryan Pereira, *Shining Light on the "Going Dark" Phenomenon: U.S. Efforts to Overcome the Use of End-to-End Encryption by Islamic State Supporters*, HARV. NAT'L SEC. J. ONLINE (Sep. 3, 2021), https://harvardnsj.org/wp-content/uploads/sites/13/2021/09/Shining-Light-On-Going-Dark.pdf.

[*] J.D., Georgetown University Law Center, Class of 2021; M.A., Georgetown University School of Foreign Service, 2016; B.A., University of Florida, 2013. I would like to thank the following individuals, listed alphabetically, for agreeing to speak with me about the topic: Jim Baker, Mary DeRosa, Joshua Geltzer, and Colin Kahl. I would also like to thank Professor David Koplow for providing motivation and guidance as well as substantive feedback that greatly strengthened the paper. These individuals have provided invaluable assistance in the process of completing this paper. All errors and mistakes are mine alone.

Contents

Introduction

On May 3, 2015, two individuals committed to the Islamic State (IS) and armed with high-powered assault rifles opened fire at a contest for cartoon depictions of the Prophet Muhammad held in Garland, Texas.[1] The two gunmen injured an off-duty police officer before another officer shot and killed them.[2] After the attack, the U.S. government disclosed that Elton Simpson, one of the two gunmen, had been in direct contact with Junaid Hussain, an IS external attack planner located in Syria, using Twitter direct message and Surespot, an end-to-end encrypted mobile messaging application.[3] Then-F.B.I. Director James Comey told the Senate Judiciary Committee that shortly before the Garland attack, Simpson had "exchanged 109 messages with an overseas terrorist" using an end-to-end encrypted messaging application.[4] Because those messages were encrypted, the F.B.I. was never able to learn what Simpson had discussed with that overseas terrorist on the morning of the attack.[5] Sally Yates, then-U.S. Department of Justice Deputy Attorney General, warned, "Even when we have the [legal] authority to search digital communications, we can't get the information that we need" because the government cannot intercept and decipher the encrypted communications.[6]

When new technologies hinder the government's technical ability to investigate and follow potential leads, law enforcement may fail to identify and stop terrorists before they act.[7] The U.S. law enforcement community calls these challenges "going dark." "Going dark" challenges arise when a criminal suspect's use of new methods of electronic communication such as end-to-end encryption impedes law enforcement's technical ability to obtain electronic information and evidence pursuant to a court order or warrant.[8] Director Comey warned, "[t]he use of encryption is part of terrorist tradecraft now because they understand the problems we have getting court orders to be effective."[9] End-to-end encryption is a method of secure communication that scrambles electronic messages in such a way that they can only be deciphered on the sender and intended recipient's electronic devices.[10] End-to-end encryption prevents law enforcement from eavesdropping on the contents of a message while it is in transit.[11]

---

[1] Greg Botelho, *Texas Shooting: Outgunned Traffic Officer Stopped 2 Attackers*, CNN (Mar. 5, 2015), https://www.cnn.com/2015/05/05/us/texas-police-shooting-hero/index.html [https://perma.cc/AGB6-J9WB].
[2] *Id.*
[3] Alexander Meleagrou-Hitchens & Seamus Hughes, *The Threat to the United States from the Islamic State's Virtual Entrepreneurs*, 10 CTCSENTINEL 1, 2 (2017).
[4] *Oversight of the Federal Bureau of Investigation: Hearing Before the Comm. on the Judiciary*, 114 Cong. (43:30-43:45) (2015) (statement of James B. Comey), https://www.judiciary.senate.gov/meetings/oversight-of-the-federal-bureau-of-investigation-12-2015 [https://perma.cc/D8RX-7U3C].
[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] *Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy: Hearing Before the Comm. on the Judiciary*, 114th Cong. (2015) (joint statement of James B. Comey and Sally Quillian Yates), https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy [https://perma.cc/2WHW-C4BM].
[9] *Id.* at 52:00-52:15.
[10] Nicole Perlroth, *What Is End-to-End Encryption? Another Bull's-Eye on Big Tech*, N.Y. TIMES (Nov. 19, 2019), https://www.nytimes.com/2019/11/19/technology/end-to-end-encryption.html [https://perma.cc/85CA-34EC].
[11] *Id.*

In June 2014, IS began to gain a global following after the terrorist group captured Mosul, Iraq's second largest city, and declared its so-called caliphate.[12] By strategically disseminating "Hollywood quality" propaganda on social media platforms, IS's media team helped to transform the group's real-world successes in holding and governing territory into an expansive and engaged online network of supporters. IS external attack planners[13] then leveraged this online network to fundraise, recruit new foreign fighters, and direct and inspire violent attacks around the globe.[14] The pervasiveness of social media platforms allowed IS external attack planners to establish contact with potential supporters in the United States.[15] After the potential recruit had established his or her bona fides, the external attack planner would instruct the individual to switch to encrypted messaging applications to avoid government surveillance. [16]

IS uses end-to-end encrypted communications platforms such as Telegram, Signal, and Surespot to maintain regular contact with U.S.-based supporters, providing moral encouragement to conduct violent attacks, helping would-be attackers select targets, tactics, and weapons, and trying to ensure that attacks would generate maximum publicity for the group.[17] Since IS began to gain a global following in June 2014, law enforcement and counterintelligence officials began warning that the use of end-to-end-encryption by U.S.-based supporters created risks of "going dark,"[18] leaving authorities unable to gain timely access to these individuals' communications

---

[12] Interview with Joshua Geltzer, Exec. Dir. of the Inst. for Constitutional Advocacy and Prot., Georgetown Univ. Law Ctr., in Wash., D.C. (Feb. 27, 2020).

[13] For the purposes of this paper, external attack planners are IS terrorists whom the U.S. government has identified for their role in planning, organizing, and directing international terrorist attacks. IS external attack planners, most commonly living and operating in IS-held territories, maintain regular online communication with IS supporters around the world in order to organize and direct international terrorist attacks.
See Press Release, U.S. Dep't of Def., Coalition Removes ISIS Terrorists from Battlefield (Aug. 3, 2017), https://www.defense.gov/Explore/News/Article/Article/1266520/coalition-removes-isis-terrorists-from-battlefield/source/GovDelivery [https://perma.cc/9XYQ-NPCJ][hereinafter DoD Press Release].

[14] *See* J.M. BERGER & JONATHON MORGAN, THE BROOKINGS PROJECT ON U.S. RELATIONS WITH THE ISLAMIC WORLD, THE ISIS TWITTER CENSUS: DEFINING AND DESCRIBING THE POPULATION OF ISIS SUPPORTERS ON TWITTER 2 (2015), https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf [https://perma.cc/8LCF-2RP3]; Cori E. Dauber & Mark Robinson, *ISIS and the Hollywood Visual Style*, JIHADOLOGY (July 6, 2015), https://jihadology.net/2015/07/06/guest-post-isis-and-the-hollywood-visual-style [https://perma.cc/WMT8-E5BT]; John P. Carlin, *Inside the Hunt for the World's Most Dangerous Terrorist*, POLITICO MAG. (Nov. 21, 2018), https://www.politico.com/magazine/story/2018/11/21/junaid-hussain-most-dangerous-terrorist-cyber-hacking-222643 [https://perma.cc/HEB9-UE9H].

[15] *E.g.*, J.M. Berger, *How Terrorists Recruit Online (and How to Stop It)*, BROOKINGS INSTITUTION (Nov. 9, 2015), https://www.brookings.edu/blog/markaz/2015/11/09/how-terrorists-recruit-online-and-how-to-stop-it [https://perma.cc/5KLL-NR7M].

[16] IS used a variety of encrypted messaging applications, including Telegram and the Swiss messaging application Threema, to communicate with followers. However, the IS was suspicious that encrypted messaging applications that were designed and managed by Western companies were less secure. For instance, the group reportedly urged followers not to use Facebook's WhatsApp. Harriet Taylor, *Islamic State's Favorite Technologies Outlined by Study*, CNBC (Jul. 22, 2016), https://www.cnbc.com/2016/07/22/islamic-states-favorite-technologies-outlined-by-study.html [https://perma.cc/5KLL-NR7M]; *see also* Berger, *supra* note 15.

[17] Andrew Zammit, *The Role of Virtual Planners in the 2015 Anzac Day Terror Plot*, 13 SEC. CHALLENGES 41, 42–44 (2017).

[18] "Going dark" refers to the government's decreasing ability to conduct effective lawful surveillance for many different technical reasons, including the widespread use of encryption by terrorists. Jim Baker, *Rethinking Encryption*, LAWFARE (Oct. 22, 2019), https://www.lawfareblog.com/rethinking-encryption [https://perma.cc/AU94-PAYS] (defining the "going dark" problem that government agencies face when dealing with a wide range of threat

despite a legal court order to do so.[19] By mid-2015, less than a year after IS declared its so-called caliphate, the group's virtual recruitment strategy had proved particularly effective.[20] IS's territorial gains, online propaganda, and recruitment inspired unprecedented numbers of U.S. residents to attempt or carry out terrorist attacks and engage in other activities supportive of the group.[21] Indeed, then-F.B.I. Director James Comey disclosed that "approximately 250 Americans had traveled or attempted to travel" to the Middle East to join IS.[22] Moreover, the terrorist group's ideological resonance stretched across the entire U.S. territory, with the F.B.I. actively investigating more than 900 suspected IS sympathizers across all fifty states.[23]

Because of the commercial availability of encrypted messaging applications that can help terrorists to communicate securely, it is likely that international terrorist groups and sophisticated criminal actors will continue to instruct followers and co-conspirators to use end-to-end-encryption in order to evade detection and incrimination.[24] Even if legislative efforts to mandate U.S. technology companies to install so-called backdoors in encrypted messaging applications or banning such apps altogether succeeded, [25] the "going dark" problem would not be completely resolved because criminals could still leverage non-U.S. encryption products and open source encryption tools.[26] Such legislation would likely make it easier to detect and surveil less

---

actors). Although terrorists use other technologies such as virtual private networks (VPNs) to try to "go dark," this paper focuses primarily on the use of end-to-end-encryption by U.S.-based supporters of the IS.

[19] *E.g.*, James B. Comey, Dir., Fed. Bureau of Investigation, Going Dark: Are Technology, Privacy, and Public Safety on a Collission Course?, Speech Before the Brookings Institution (Oct. 16, 2014), [hereinafter Comey Speech].

[20]Although the number of IS foreign fighters from the United States is unprecedented in U.S. history, on a per capita basis, countries in the Middle East and Europe contributed larger numbers of foreign fighters. *See* TSG FOREIGN FIGHTERS IN SYRIA, THE SOUFAN CENTER 5 (June 2014).

[21] *Global Terrorism: Threats to the Homeland, Part 1: Hearing Before the H. Comm. on Homeland Sec.*, 116th Cong. 2 (2019) (statement of Peter Bergen, Vice President, Global Studies & Fellows, New America) [hereinafter Bergen 2019 Testimony].

[22] *Threats to the Homeland: Hearing Before the S. Comm. on Homeland Sec. and Governmental Affairs*, 114th Cong. (2015) (statement of James B. Comey), https://www.fbi.gov/news/testimony/threats-to-the-homeland [https://perma.cc/8A8X-6CQK]; Jamie Novogrod, *FBI Director: Dozens of Americans Secretly Conversing with ISIS*, MSNBC (Oct. 08, 2015), http://www.msnbc.com/msnbc/fbi-director-dozens-americans-secretly-conversing-isis [https://perma.cc/ZA9Y-K4MJ].

[23] Kevin Johnson, *Comey: Feds Have Roughly 900 Domestic Probes About Islamic State Operatives, Other Extremists*, USA TODAY (Oct. 23, 2015), https://www.usatoday.com/story/news/politics/2015/10/23/fbi-comey-isil-domestic-probes/74455460 [https://perma.cc/PJ37-Z6KP].

[24] *See* Joshua Geltzer, *How to Move the Battle Lines in the Crypto-Wars*, JUST SEC. (Apr. 5, 2018), https://www.justsecurity.org/54552/move-battle-lines-crypto-wars [https://perma.cc/59JT-M35R].

[25] Proposals to mandate U.S. companies to install backdoors in end-to-end encrypted messaging applications are intended to provide government authorities with the ability to lawfully access and read particular encrypted communications, but critics argue that building backdoors in messaging apps would create a vulnerability in all communications systems and would weaken everyone's security from unlawful spying by nefarious actors. *See* Eric Geller, *Trump Officials Weigh Encryption Crackdown*, POLITICO (Jun. 27, 2019), https://www.politico.com/story/2019/06/27/trump-officials-weigh-encryption-crackdown-1385306 [https://perma.cc/TK3C-7N67].

[26] Robert Graham, *How Terrorists Use Encryption*, 9 CTC SENTINEL 20, 20 (2016) ("Legislative efforts to help law enforcement agencies wrestle with the phenomenon of "going dark" will never lead to a return to the status quo ante, however."); BRUCE SCHNEIER ET AL., THE BERKMAN CTR. FOR INTERNET & SOC'Y AT HARVARD UNIV., A WORLDWIDE SURVEY OF ENCRYPTION PRODUCTS 5-6 (2016), https://cdn0.vox-cdn.com/uploads/chorus_asset/file/6029389/2016-02_encryption1.0.pdf [https://perma.cc/S73W-5KG3] (noting that "anyone who wants to evade an encryption backdoor in US or UK encryption products has a wide variety of foreign products they can use instead to maintain online privacy").

sophisticated criminals who stop using encryption or use U.S. encryption products with backdoors. However, savvy extremists and criminals would either switch to using non-compromised platforms or would use and adapt widely available source code to create their own encrypted messaging applications.[27] Thus, U.S. authorities would still need to find ways to mitigate potential "going dark" threats as sophisticated, international terrorist groups and criminals will continue accessing strong encryption technologies.

Because IS is the most prominent terrorist group to have systematically encouraged its sympathizers to use encrypted messaging applications and provided detailed instructions on how to do so securely, this article focuses on the "going dark" threats created by U.S.-based supporters of the group. This paper argues that the government's counterterrorism efforts against U.S.-based supporters of IS illustrate how the aggressive use of traditional law enforcement tools, including physical and electronic surveillance, wiretaps, undercover informants, and targeted hacking, can help to reduce but not eliminate potential "going dark" threats. The U.S. government was largely successful at identifying and surveilling U.S.-based supporters of IS and disrupting their violent plots, despite many of these individuals using encryption.

To analyze the "going dark" challenges that U.S. authorities confronted during their counterterrorism efforts against U.S-based IS supporters, this paper uses news reports and unsealed court documents to compile a dataset of all U.S. residents both (1) accused of supporting IS and (2) indicted on terrorism-related offenses or killed while committing an attack between the years 2015 and 2019. The dataset consists of 181 individuals residing in 29 different states and the District of Columbia.[28] Because the U.S. residents who successfully joined and fought alongside IS initially managed to evade U.S. counterintelligence and law enforcement agencies, the dataset excludes those individuals, even if they were eventually captured on the battlefield and prosecuted in the United States.[29] This dataset shows that, while not perfect, the use of traditional law enforcement investigative and surveillance tools, including targeted hacks to try to access criminal suspects' mobile devices and read their messages before they are encrypted, is generally sufficient to combat the threat posed by many terrorists and nefarious actors who try to "go dark." However,

---

[27] SCHNEIER ET AL., *supra* note 26, at 20; Geltzer, *supra* note 24.

[28] The author used The George Washington University Program on Extremism's *ISIS in America* dataset as well as The Investigative Project on Terrorism research center's website to locate court documents related to IS arrestees between 2015 and 2019. *See* GEO. WASH. PROGRAM ON EXTREMISM, https://extremism.gwu.edu/isis-america (last visited Apr. 20, 2020) [https://perma.cc/F2ZB-ZP2Z]; THE INVESTIGATIVE PROJECT ON TERRORISM, https://www.investigativeproject.org (last visited Apr. 20, 2020) [https://perma.cc/74BJ-A5UL].

[29] The dataset excludes individuals who successfully managed to join IS because there is insufficient data on many of these individuals, including how or why they joined IS, and whether they were captured, killed on the battlefield, or remain at-large. Most of these IS recruits have not been prosecuted by U.S. authorities, and reports about the recruits are either unavailable, classified, or do not shed light on whether these recruits used end-to-end to communicate with IS external attack planners. As of May 2021, only one U.S. resident, Mohamad Jamal Kweis, who fought alongside IS before being captured, has been prosecuted and sentenced. Because Kweis' arrest report and complaint focus on his time fighting alongside IS, rather than his process of joining the group, his exclusion does not impact the dataset. Press Release, U.S. Dep't of Justice, American Sentenced to 20 Years for Joining ISIS (Oct. 27, 2017), https://www.justice.gov/opa/pr/american-sentenced-20-years-joining-isis [https://perma.cc/67TH-4BD5]. For a discussion about the potential prosecution of U.S. foreign fighter returnees in the future, see Robin Wright, *Despite Trump's Guantànamo Threats, Americans Who Joined ISIS Are Quietly Returning Home*, NEW YORKER (June 11, 2019), https://www.newyorker.com/news/news-desk/americas-isis-members-are-coming-home [https://perma.cc/923M-JLJ9].

the use of end-to-end encryption by nefarious actors with more sophisticated communications and operations security complicates law enforcement efforts to uncover and disrupt criminal activities.

The remainder of the paper is divided into five sections: Section I illustrates how IS external attack planners used encrypted messaging applications when directing terrorist attacks in the United States. Section II presents quantitative findings related to the use of encryption by U.S.-based supporters of the group and to the U.S. government's ability to mitigate "going dark" threats. Section III provides an overview of the dataset and methodology. Section IV illustrates how the government used traditional law enforcement techniques against IS supporters to address "going dark" threats and discusses the potential costs and limitations of the various law enforcement techniques that the authorities use to mitigate "going dark" threats. Section V concludes that "going dark" threats will persist because U.S.-based extremists will continue using end-to-end encryption, making it imperative that the authorities adapt to these threats.

I. The Role of External Attack Planners in Encouraging Violence in the United States

IS external attack planners use encryption to orchestrate and execute remotely directed attacks.[30] Remotely-directed attacks involve perpetrators who had not travelled to IS-held territories or terrorist safe havens to receive training or instructions, but who nevertheless maintained regular contact with external attack planners.[31]

Figure 1 is a social network map that illustrates IS external attack planners' direct influence over the U.S. residents who were involved in IS-directed plots and attacks between the years 2015 and 2019. By showing the lines of communication between external attack planners and connected U.S. residents, Figure 1 illustrates the role of IS external attack planners in encouraging and planning terrorist attacks in the United States from within IS-controlled territories. To illustrate, the top left of Figure 1 shows that Usaamah Rahim, a U.S.-based IS supporter who was shot after charging at law enforcement officers with a knife, communicated directly with external attack planner Junaid Hussain. Rahim was plotting an IS-directed attack with co-conspirators Nicholas Rovinski and David Daoud Wright, but there is no evidence indicating that either Rovinski or Wright were directly communicating with Hussain.[32] Similarly, the bottom left of Figure 1 shows that external attack planner Abu Sa'ad al-Sudani was directly communicating with Aaron Daniels, Emanuel Lutchman, and Mohamed Bailor Jalloh, U.S.-based IS supporters who were separately involved in three different IS-directed plots but were arrested without incident.

---

[30] Rukmini Callimachi, *Not "Lone Wolves" After All: How ISIS Guides World's Terror Plots from Afar*, N.Y. TIMES (Feb. 4, 2017), https://www.nytimes.com/2017/02/04/world/asia/isis-messaging-app-terror-plot.html [https://perma.cc/PB6B-4NFY].

[31] Zammit, *supra* note 17, at 43.

[32] *See* Adam Goldman & Eric Schmitt, *One by One, ISIS Social Media Experts Are Killed as Result of F.B.I. Program*, N.Y. TIMES (Nov. 24, 2016), https://www.nytimes.com/2016/11/24/world/middleeast/isis-recruiters-social-media.html [https://perma.cc/A3GM-5FMK] (explaining that Junaid Hussain communicated directly with Usaamah Rahim and encouraged Rahim and his co-conspirators to kill Pamela Gellar, a conservative activist who organized a cartoon contest for depictions of the Prophet Muhammad).

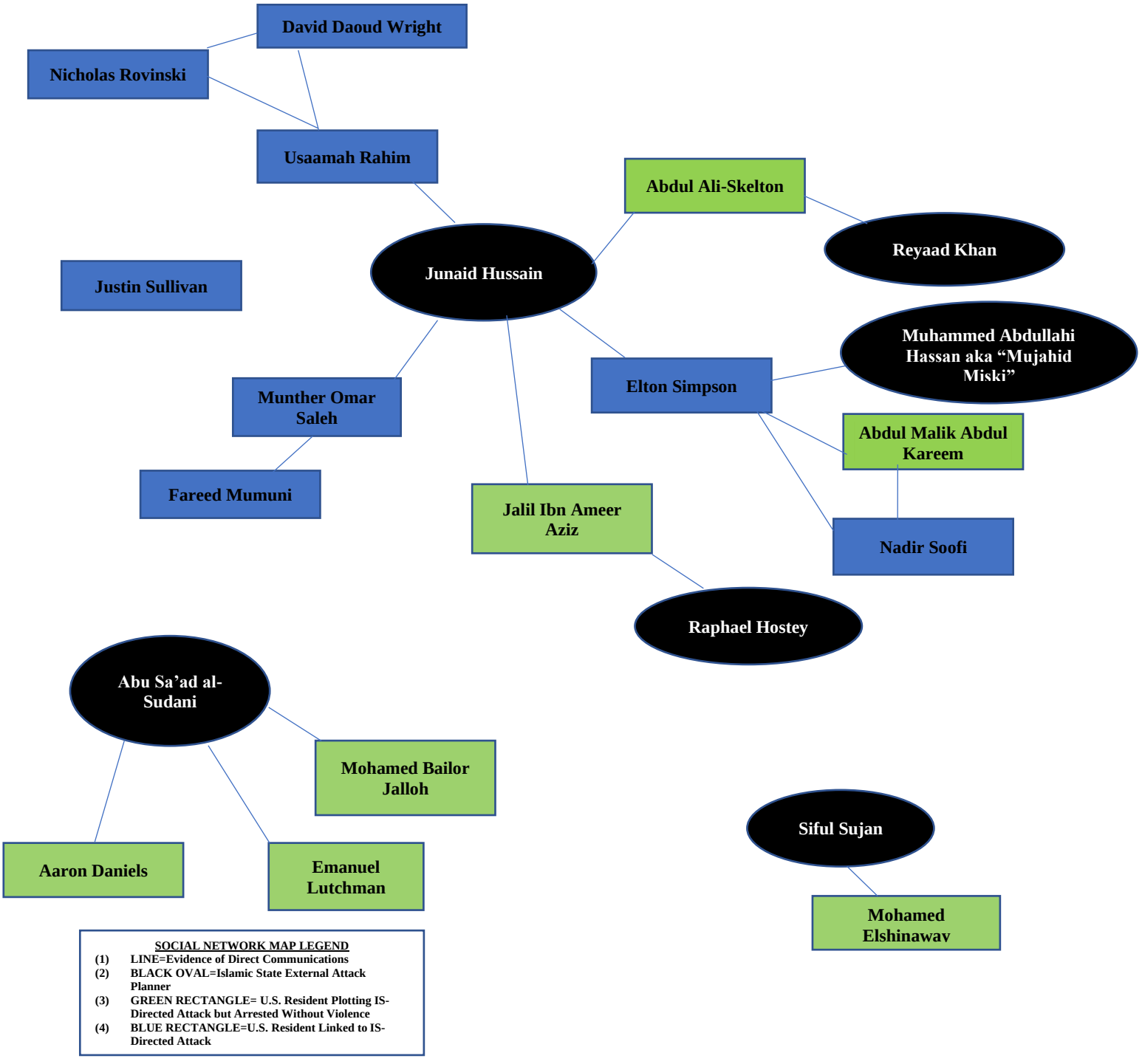

Figure 1

The following sections discuss how maintaining regular communication with U.S. residents enabled external attack planners to encourage and orchestrate IS-directed terrorist

attacks. First, maintaining regular communication with U.S. residents enables external attack planners to cultivate a sense of "remote intimacy" with potential recruits and provide moral encouragement in order to promote their radicalization towards violence. Second, communicating with U.S. residents allows external attack planners to help would-be attackers to select targets, tactics, and weapons and to develop contingency plans should law enforcement try to make arrests. Lastly, external attack planners seek to maximize the propaganda value of violent attacks committed in the group's name by highlighting IS's influence over U.S.-based attackers.[33]

A. *Providing Moral Encouragement*

IS's external attack planners regularly communicated with potential attackers in the United States in order to develop intimate and emotionally powerful connections with U.S.-based IS sympathizers. Attack planners did so by validating these sympathizers' personal beliefs, making them feel as if they were a part of a larger, worldwide movement, and promising them global fame and adulation if they followed through with external attack planners' instructions to commit violent attacks in IS's name.[34] Moral encouragement can motivate extremists to follow through with plans to conduct terrorist attacks by convincing the extremists of the religious and strategic importance of using violence to achieve their aims.[35] Consequently, IS external attack planners tried to provide such encouragement to U.S.-based supporters of the terrorist group.[36] For instance, Director Comey noted that IS external attack planners told U.S.-based extremists that, "if you can't travel [abroad to join IS],[37] kill where you are."[38] Director Comey further explained, "It's almost as if there is a devil sitting on the [U.S. resident's] shoulder saying, 'Kill, kill, kill, kill' all day long."[39]

---

[33] *Id.*

[34] *See* Daveed Gartenstein-Ross & Madeleine Blackman, *ISIL's Virtual Planners: A Critical Terrorist Innovation*, WAR ON THE ROCKS (Jan. 4, 2017), https://warontherocks.com/2017/01/isils-virtual-planners-a-critical-terrorist-innovation [https://perma.cc/QM44-FAP4]; Daniel L. Byman, *Omar Mateen, Lone-wolf Terrorist*, THE BROOKINGS INSTITUTION (June 13, 2018), https://www.brookings.edu/blog/markaz/2016/06/13/omar-mateen-lone-wolf-terrorist [https://perma.cc/TL5R-E7HV].

[35] *See* RANDY BORUM, PSYCHOLOGY OF TERRORISM 24-26 (2004), https://www.ncjrs.gov/pdffiles1/nij/grants/208552.pdf [https://perma.cc/CN38-L56N]; Coral Dando, *What Science Can Reveal About the Psychological Profiles of Terrorists*, THE CONVERSATION (May 26, 2017), http://theconversation.com/what-science-can-reveal-about-the-psychological-profiles-of-terrorists-78304 [https://perma.cc/44YH-JTW7].

[36] For an influential and provocative discussion of how IS and other jihadist groups use Islamic scriptures, history, and ideologies to convince extremists of the moral and religious justifications for violence, see Graeme Wood, *What ISIS Really Wants*, THE ATLANTIC (Mar. 2015), https://www.theatlantic.com/magazine/archive/2015/03/what-isis-really-wants/384980 [https://perma.cc/9CKZ-ZL3P].

[37] Although the IS's early English-language propaganda urged American Muslims to travel to the Middle East to join its so-called Caliphate, by early 2015 the terrorist group's messaging had shifted to encouraging U.S.-based supporters to commit attacks in the United States. *See ISIS Online: Countering Terrorist Radicalization & Recruitment on the Internet & Social Media: Hearing Before the U.S. S. Comm. on Homeland Sec., Permanent Subcomm. on Investigations*, 114th Cong. 12 (2016) (statement of Peter Bergen, Vice President, New America), https://www.govinfo.gov/content/pkg/CHRG-114shrg22476/pdf/CHRG-114shrg22476.pdf [https://perma.cc/U6U5-UYFZ].

[38] Pierre Thomas et al., *ISIS: Potentially "Thousands" of Online Followers Inside US Homeland, FBI Chief Warns*, ABC NEWS (May 7, 2015), https://abcnews.go.com/International/thousands-online-isis-followers-inside-us-homeland-fbi/story?id=30882077 [https://perma.cc/7ZGX-7VB7].

[39] *Id.*

The standard recruitment process begins with the U.S resident taking actions to self-identify as an IS supporter on social media, after which point either the U.S. resident or IS recruiter would reach out and initiate contact. By instant messaging potential recruits, often multiple times a day in private, one-on-one, or small group chats, IS external attack planners cultivated a sense of "remote intimacy" with potential violent extremists that helped to encourage their radicalization towards violence.[40]

The case of Munir Abdulkader, an IS supporter who plead guilty to plotting to attack U.S. government officers in 2015,[41] is illustrative. Sometime after Abdulkader began using Twitter to express his support for IS, he established contact with external attack planner Junaid Hussain.[42] Although Abdulkader was initially interested in travelling to Syria to join and fight alongside IS, "Hussain helped push him to a different course" and encouraged Abdulkader to conduct an attack in the United States "when they [Hussain and Abdulkader] decided it simply had gotten too dangerous to go to an airport."[43] After laying out an attack plan for Abdulkader to execute,[44] Junaid Hussain provided him with moral encouragement to follow through with the planned operation. For instance, when Abdulkader messaged Hussain that he had gone to the shooting range to practice using firearms, Hussain responded, "Next time ul [sic] be shooting kuffar [nonbelievers] in their face and stomach."[45] By predicting that Abdulkader would soon be killing nonbelievers, an act that IS promises will guarantee supporters their place in paradise,[46] Hussain tried to validate Abdulkader's radical religious beliefs and encourage him to follow through with their planned attack.

B. *Helping Potential Attackers to Select Appropriate Targets, Tactics, and Weapons*

The IS external attack planners used encrypted messaging applications to remotely direct terrorist plots globally by providing logistical and operational direction to potential attackers.[47] When it came to potential attackers within the United States, external attack planners helped the U.S. residents to select targets and develop attack plans.[48]

For instance, Munir Abdulkader's sentencing memorandum illustrates how IS external attack planners help would-be attackers to select targets, tactics, and weapons The sentencing memorandum details how "[Islamic State external attack planner Junaid] Hussain ultimately laid

---

[40] J.M. Berger, *The Metronome of Apocalyptic Time: Social Media as Carrier Wave for Millenarian Contagion*, 9 PERSPECTIVES ON TERRORISM 61, 66-67 (2015).

[41] Information at 4, United States v. Munir Abdulkader, No. 1:16-cr-019 (S.D. Ohio Feb. 26, 2016), https://www.investigativeproject.org/documents/case_docs/3024.pdf [https://perma.cc/S8G7-VRK4].

[42] Sentencing Memorandum of United States at 3, United States v. Munir Abdulkader, No. 1:16-CR-0019-MRB (S.D. Ohio Nov. 10, 2016), https://www.investigativeproject.org/documents/case_docs/3152.pdf [https://perma.cc/XAU6-AK55].

[43] Sentencing Proceedings at 55, United States v. Munir Abdulkader, No. 1:16-CR-019 (S.D. Ohio Nov. 23, 2016), https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/AbdulkaderSentencingProceedings.pdf [https://perma.cc/F9ST-C8WN].

[44] *Id.* at 10.

[45] *Id.* at 55.

[46] ALEX SCHMID, CHALLENGING THE NARRATIVE OF THE "ISLAMIC STATE," INTERNATIONAL CENTRE FOR COUNTER-TERRORISM - THE HAGUE 1, 7 (Jun. 2015), https://www.icct.nl/wp-content/uploads/2015/06/ICCT-Schmid-Challenging-the-Narrative-of-the-Islamic-State-June2015.pdf [https://perma.cc/B4X3-33XL].

[47] Callimachi, *supra* note 30.

[48] Meleagrou-Hitchens & Hughes, *supra* note 3.

out, through electronic communications, an overall terrorist attack plan for Abdulkader…to implement."[49] Junaid Hussain's operational plan was for Abdulkader to "raid a soldier's home, behead him, record it, [and then] send the recording to Hussain. Once this attack was completed, the Defendant [Abdulkader] was to go to a police station, throw pipe bombs, engage the police officers with firearms, and then fight to the death."[50]

Similarly, in another IS-directed plot involving communications between Hussain and Usaamah Rahim, an IS supporter, Hussain instructed Rahim and his accomplices to behead Pamela Geller, the organizer of the Prophet Muhammad cartoon contest in Garland, at her apartment in New York City.[51] By instructing Rahim to behead Geller, external attack planner Junaid Hussain tried to develop an attack plan that would enable IS to achieve its goal of eliminating a prominent critic of IS whom the group had unsuccessfully targeted in the Garland attack.

In addition to helping U.S.-based extremists develop operational attack plans, IS external attack planners provided would-be attackers with instructions on what to do if law enforcement attempted to arrest them before they could execute their attacks. For example, Hussain allegedly told Usaamah Rahim that he should always "carry a knife" on his person "in case the 'feds' try to arrest him."[52] When law enforcement officers attempted to question Rahim in connection with their ongoing counterterrorism investigation, Rahim was shot dead as he moved towards the officers, menacingly waving a 13-inch knife in the air, ignoring repeated demands to drop his weapon, and verbally daring the officers to shoot him.[53] In another plot, Junaid Hussain sent the would-be attackers detailed bomb-making instructions to construct explosive devices but told the individuals to attack law enforcement officers if the police attempted to thwart the attack.[54] When law enforcement attempted to arrest the individuals involved in the plot, they unsuccessfully tried to kill the officers.[55] Fareed Mumuni, one of the arrestees, told F.B.I. agents that, per Junaid Hussain's guidance, he kept one knife "wrapped in a T-shirt in his bed" and another knife in his "mother's vehicle for use in an encounter with law enforcement."[56] By instructing U.S. residents who were planning IS-directed attacks to try to kill arresting officers, IS was more likely to be able

[49] Sentencing Memorandum of United States, *supra* note 42, at 10.
[50] *Id.*
[51] Press Release, Office of Pub. Affairs, Dep't of Justice, Massachusetts Man Convicted of Supporting ISIS and Conspiring to Murder U.S. Citizens (2017), https://www.justice.gov/opa/pr/massachusetts-man-convicted-supporting-isis-and-conspiring-murder-us-citizens [https://perma.cc/RC4Q-HSA9].
[52] Second Superseding Indictment at 8, United States v. David Daoud Wright, No. 1:15-CR-10153-WGY (D. Mass. Feb. 15, 2017), https://www.investigativeproject.org/documents/case_docs/3231.pdf [https://perma.cc/6SBB-BDFT].
[53] Lauren Del Valle, *Usaamah Rahim Shooting by Police Yields No Charges*, CNN (Aug. 24, 2016), https://www.cnn.com/2016/08/24/us/no-charges-usaamah-rahim-boston-terror-suspect/index.html [https://perma.cc/R8NU-9T8P].
[54] Letter Regarding Sentencing of Munther Omar Saleh & Fareed Mumuni at 15, United States v. Munther Omar Saleh, No. 1:15-cr-00393-MKB (E.D.N.Y. Jan. 12, 2018), https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Saleh%20Government%20Submission.pdf [https://perma.cc/A9Q8-X5C4].
[55] *Id.* at 1.
[56] Complaint at 8, United States v. Fareed Mumuni, No. 1:15-mj-00554 (E.D.N.Y. June 17, 2015), https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Mumuni%20Criminal%20Complaint.pdf [https://perma.cc/Z8FE-5UTL].

to claim credit for violent incidents in the United States, even if law enforcement managed to successfully thwart the extremists' larger, underlying plot.[57]

C. *Using the Attack to Generate Maximum Publicity*

IS's use of encrypted messaging applications allowed IS external attack planners to publicize and offer concrete evidence of the group's influence over successful attackers, which helped to increase publicity for the terrorist group.[58] For instance, about an hour before the attack against the cartoon contest in Garland, external attack planner Junaid Hussain ominously tweeted, "The knives have been sharpened, soon we will come to your streets with death and slaughter!"[59] After the attack had taken place, Hussain tweeted, "They Thought They Was Safe In Texas From The Soldiers of The Islamic State."[60]

In other IS-directed plots, external attack planners instructed the individuals to send videos of themselves pledging allegiance to IS leader Abu Bakr al-Baghdadi, videos which the terrorist group would release after the attack.[61] For instance, when North Carolina native Justin Sullivan, who had hoped to create a new branch of IS in North America, messaged Junaid Hussain saying, "Very soon [I will be] carrying out 1st operation of Islamic State in North America," Hussain replied, "Can u make a video first?"[62] Junaid Hussain's request that Sullivan record himself pledging allegiance to IS's leader illustrates how IS external attack planners attempted to maximize the propaganda and shock value of violent attacks. By releasing pre-recorded videos made by the perpetrators of IS-directed attacks, the terrorist group's media team aimed to convince their followers and the wider public that the group's senior leaders in Syria carefully planned, orchestrated, and directed the violent attacks.[63]

---

[57] For instance, after law enforcement officers shot and killed Usaamah Rahim, Junaid Hussain tweeted that he had encouraged Rahim to carry a knife in case anybody attempted to arrest him. *See The Future of Counterterrorism: Addressing the Evolving Threat to Domestic Security: Hearing Before the Comm. on Homeland Sec.*, 115th Cong. (2017), https://www.govinfo.gov/content/pkg/CHRG-115hhrg26904/html/CHRG-115hhrg26904.htm [https://perma.cc/5SEL-CN6V] (statement of Thomas Joscelyn, Senior Fellow, The Foundation for the Defense of Democracies).

[58] *See* Charlie Winter & Aymenn al-Tamimi, *ISIS Relaunches as a Global Platform: The Sri Lanka Bombings Were a Preview of the Islamic State's Future.*, THE ATLANTIC (Apr. 27, 2019), https://www.theatlantic.com/ideas/archive/2019/04/the-sri-lanka-bombings-were-a-preview-of-isiss-future/588175 [https://perma.cc/T95B-6VP8].

[59] Rukmini Callimachi, *Clues on Twitter Show Ties Between Texas Gunman and ISIS Network*, N.Y. TIMES (May 11, 2015), https://www.nytimes.com/2015/05/12/us/twitter-clues-show-ties-between-isis-and-garland-texas-gunman.html [https://perma.cc/JW5D-APB6].

[60] Matt Pearce, *Outside Muhammad Cartoon Contest in Texas, 2 Gunmen Are Killed and Guard Is Shot*, L.A. TIMES (May 3, 2015), https://www.latimes.com/nation/la-na-texas-shooting-20150503-story.html [https://perma.cc/2H65-KA64].

[61] *See, e.g.*, Factual Basis in Support of the Plea Agreement at 15, United States v. Justin Nojan Sullivan, No. 1:16-cr-05-MR-DLH (W.D.N.C. Nov. 14, 2016), https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Sullivan%20Factual%20Basis.pdf [https://perma.cc/3JWU-G2JQ]; Elisabetta Povoledo et al., *Hunt for Berlin Suspect Ends in Gunfire on an Italian Plaza*, N.Y. TIMES (Dec. 23, 2016), https://www.nytimes.com/2016/12/23/world/europe/berlin-anis-amri-killed-milan.html?_r=0 [https://perma.cc/A5RQ-H7EB].

[62] Factual Basis in Support of the Plea Agreement, *supra* note 61, at 15.

[63] Although IS never released videos of U.S.-based attackers pledging allegiance to its leader before their attacks, IS used this propaganda tactic after several attacks in Europe. *See* Daveed Gartenstein-Ross & Madeleine Blackman, *ISIL's Virtual Planners: A Critical Terrorist Innovation*, WAR ON THE ROCKS (Jan. 4, 2017),

II. Dataset and Methodology

The dataset used in this paper consists of 181 U.S. residents who supported IS and who were arrested or killed while committing attacks in the United States between the years 2015 and 2019. The Department of Justice indicted 172 of these individuals.[64] The data reveal that nearly a quarter of all IS-related arrestees and attackers in the United States used encrypted messaging applications to communicate. Moreover, there is evidence that IS external attack planners communicated with at least 13 of the 172 IS-related arrestees and remotely directed at least 4 of the 18 IS-related attacks that occurred in the United States between 2015 and 2019.[65]

The 181 cases that occurred between 2015 and 2019 were coded along the following criteria: (1) the year that the arrest or violent attack took place; (2) whether there is evidence that the U.S.-based supporter of IS used encrypted messaging applications; (3) whether there is evidence that the U.S.-based supporter communicated with external attack planners; (4) whether there is evidence that an outside tip from a third-party alerted law enforcement to the individual's radicalization; and (5) whether undercover sources interacted with the IS supporter before the supporter's arrest or attack.[66]

In order to show how IS external attack planners influenced the expression of violence in the United States, each of the 18 IS-inspired and -directed attacks were coded for the following additional criteria: (1) whether there is evidence that at least one of the attackers communicated with external attack planners before the attack;[67] (2) the method of attack used;[68] and (3) the total

---

https://warontherocks.com/2017/01/isils-virtual-planners-a-critical-terrorist-innovation [https://perma.cc/6GRF-R3MK].

[64]See GEO. WASH. PROGRAM ON EXTREMISM, https://extremism.gwu.edu/isis-america (last visited Apr. 20, 2020) [https://perma.cc/BE43-4HPW] and THE INVESTIGATIVE PROJECT ON TERRORISM, https://www.investigativeproject.org (last visited Apr. 20, 2020) [https://perma.cc/6TRU-ZBEY] (determining the number of indictments by subtracting those criminal cases involving individuals who successfully joined IS from the total number of IS-related indictments between 2015 and 2019).

[65] The four known IS-directed attacks all occurred within 2015. The specific attacks were the shooting against the cartoon contest in Garland, Texas, Justin Sullivan's killing of his elderly neighbor, attacks against arresting officers by Usaamah Rahim and his co-conspirators, and attacks against arresting officers by Fareed Mumuni and his co-conspirators.

[66] The author coded an incident as involving the use of undercover sources if court documents or news reports mentioned the F.B.I.'s use of undercover informants or agents in order to try to establish in-person or online contact with the individual or the individual's co-conspirators.

[67] Callimachi, *supra* note 30.

[68] The author coded each violent incident for one of the following methods of attack–the attempted use of explosives, the use of firearms, knife attacks, or vehicular ramming attacks. Two attacks–Abdul Razak Ali Artan's attack at Ohio State University (OSU) and Ahmad Khan Rahami's attack in New York and New Jersey–involved the use of more than one method of attack. The author coded the OSU attack, which was a vehicular ramming attack that ended with the assailant trying to stab students, as a vehicular ramming attack. Ahmad Khan Rahami's attack, which involved the attempted use of explosives before Rahami was injured in a brief shootout with law enforcement officers, was coded as an attack involving the use of explosives. *See* Merrit Kennedy, *Suspect Killed After Knife and Vehicle Attack at Ohio State University*, NPR (Nov. 28, 2016), https://www.npr.org/sections/thetwo-way/2016/11/28/503589910/at-least-9-injured-following-report-of-active-shooter-at-ohio-state-university [https://perma.cc/PK7T-BJ46] ; Marc Santora, et al. *Ahmad Khan Rahami Is Arrested in Manhattan and New Jersey Bombings*, N.Y. TIMES (Sep. 19, 2016),

number of individuals, excluding the perpetrators, who were killed or seriously injured during the attack.

An arrest or attack was coded as involving the use of encryption if court documents, public officials, or news reports made reference to the individual's use of encrypted communications platforms, or specifically to the use of Telegram, Kik, Signal, or similar applications offering end-to-end encryption. To be certain, this variable likely underestimates the extent to which U.S.-based IS supporters used encrypted messaging applications. In some instances, the defendant's use of encryption might not have been "mentioned in the indictment . . . or the intelligence or law enforcement community may have been unaware"[69] that the encrypted communications even took place. Nevertheless, this variable provides a baseline number, which illustrates the significant use of end-to-end encryption by U.S.-based supporters of IS between the years 2015 and 2019.

The author coded an arrestee as having been directed by IS external attack planners if there were evidence of direct communications[70] between the arrestee and Junaid Hussain, Reyaad Khan, Abu Sa'ad al-Sudani, Siful Sujan, or any other individual labelled an IS external operations planner by the U.S. government.[71] Many individuals whom IS inspired regularly communicated with like-minded extremists on the Internet, social media, and encrypted messaging platforms.[72] However, this variable related to communications with external attack planners captures the use of multiple platforms, both encrypted and unencrypted, to remotely recruit and direct U.S.-based extremists to commit violent attacks in IS's name. It is certainly possible that some U.S.-based attackers

---

https://www.nytimes.com/2016/09/20/nyregion/nyc-nj-explosions-ahmad-khan-rahami.html [https://perma.cc/D7VZ-5ZA5].

[69] Interview with Joshua Geltzer, *supra* note 12.

[70] The strength of IS's direct influence over U.S.-based individuals varied across cases, but the author coded all cases involving direct communications between IS external attack planners and U.S.-based individuals or their co-conspirators as IS-directed cases. In contrast, the author coded incidents in which there was no evidence that the individual or the individual's co-conspirators communicated with IS external attack planners as IS-inspired attacks. Although there was no evidence in IS-inspired attacks of direct communications between the U.S.-based individuals and IS external attack planners, these individuals nevertheless regularly communicated with like-minded extremists on the Internet, social media, and encrypted messaging platforms. When coding, the key qualitative difference between IS-directed and -inspired attacks was whether or not the U.S.-based individuals or co-conspirators were directly communicating with individuals labelled IS external attack planners by the U.S. government. *See* Jen Easterly & Joshua A. Geltzer, *The Islamic State and the End of Lone-Wolf Terrorism*, FOREIGN POL'Y (May 23, 2017), https://foreignpolicy.com/2017/05/23/the-islamic-state-and-the-end-of-lone-wolf-terrorism [https://perma.cc/2Q55-MYJH] (explaining that even those terrorists who did not receive specific direction from IS external attack planners considered themselves to be a part of the Islamic State's global community).

[71] *See, e.g.*, DoD Press Release, *supra* note 13; Goldman & Schmitt, *supra* note 32;
Seamus Hughes & Alexander Meleagrou-Hitchens, *The Reach of ISIS's Virtual Entrepreneurs into the United States*, LAWFARE (Mar. 28, 2017), https://www.lawfareblog.com/reach-isiss-virtual-entrepreneurs-united-states [https://perma.cc/8KTS-6KA2]; Seamus Hughes, *The Only Islamic State-Funded Plot in the U.S.: The Curious Case of Mohamed Elshinawy*, LAWFARE (Mar. 7, 2018), https://www.lawfareblog.com/only-islamic-state-funded-plot-us-curious-case-mohamed-elshinawy [https://perma.cc/49XX-FBFQ].

[72] Many individuals who were inspired by the Islamic State were motivated, in part, by the allure of feeling like they were a part of IS's global community. In arguing that the term 'lone wolf' terrorism is misleading, former Obama Administration officials Jen Easterly and Joshua Geltzer elegantly explained that, "By taking up arms for [IS's] cause, getting behind the wheel of a truck, or building a pressure cooker bomb, these men become part of a community, part of something bigger than themselves, and indeed part of history–anything but alone." Easterly & Geltzer, *supra* note 70.

managed to successfully conceal their communications with external attack planners.[73] Although the variable may thus slightly underestimate the number of IS-directed plots and attacks, it nevertheless captures aggressive efforts by external attack planners to encourage violent attacks in the United States.

III. Law Enforcement Adapts to End-to-End Encryption

IS's strategy of using encrypted messaging applications to encourage American residents to conduct attacks on U.S. soil forced law enforcement to develop new strategies for identifying and arresting terrorists. For one, in the years after 9/11, the authorities became skilled at identifying potential attackers by detecting physical "signatures" of radicalization.[74] Common "signatures" of radicalization included, for instance, U.S. residents' attempted travel to conflict zones like the tribal areas of Pakistan or Yemen in order to receive combat training, their attempts to buy bomb-making components, or making money transfers between U.S. residents and individuals located in regions with ongoing jihadist conflicts.[75] However, many of these "signatures" of radicalization became less useful once IS started encouraging its supporters to remain at home and carry out attacks with weapons like vehicles, guns, and knives that could be acquired without raising red flags.[76]

Because many IS-linked plots were relatively unsophisticated, the would-be attackers could "buy [all of the weapons and supplies that they needed] in a way that was not going to alert authorities in the United States" to the individuals' radicalization or plots.[77] Moreover, compared to other violent extremists, the "flash-to-bang" period—the length of time an extremist takes to go from radicalization to a violent attack—was significantly shorter for IS supporters.[78] A shorter "flash-to-bang" period, combined with IS's aggressive efforts to encourage attacks in the United States, made it much more challenging for law enforcement to identify potential violent extremists and to uncover and disrupt plots before they were carried out. For instance, former F.B.I. General Counsel Jim Baker remarked that in the years after 9/11, most aspiring al-Qaeda recruits,

> would have to somehow come into contact with an al-Qaeda operative…figure out a way to go travel overseas, how to get to an al-Qaeda training camp, would have to plan the operation, be trained for the operation, and then come back to the United States and actually execute it. And the point is, there are multiple places where…we [the authorities] could detect them because we have electronic surveillance, we have data collection, [and] we have [human intelligence] sources all along that sort of chain of events.[79]

---

[73] For a discussion of how IS-directed attacks in Europe were initially incorrectly labelled 'lone wolf' attacks, see Daveed Gartenstein-Ross & Nathaniel Barr, *The Myth of Lone-Wolf Terrorism: The Attacks in Europe and Digital Extremism*, FOREIGN AFF. (Jul. 26, 2016), https://www.foreignaffairs.com/articles/western-europe/2016-07-26/myth-lone-wolf-terrorism [https://perma.cc/2QYP-7BSF].
[74] *Id.*
[75] *Id.*
[76] *Id.*
[77] Telephone Interview with Jim Baker, Mar. 3, 2020, Washington D.C.
[78] Carlin, *supra* note 14.
[79] Telephone Interview with Jim Baker, *supra* note 77.

For violent extremists influenced by IS, "the problem became very quickly that the flash-to-bang was much shorter,"[80] meaning fewer opportunities and less time existed for law enforcement to detect and arrest would-be attackers.

Further complicating law enforcement's task, online messaging companies such as Telegram, Signal, and Kik began to provide end-to-end encryption for private chats in recent years.[81] IS quickly adopted these encrypted messaging platforms, and provided supporters with direction online about which encrypted messaging applications and security protocols to use in order to maximize communications and operational security.[82] Because even unsophisticated U.S.-based extremists can learn which encryption products to use and which to avoid, the "going dark" problem will continue to bedevil national security and law enforcement officials.[83] As such, it is important to analyze how the use of encryption by U.S.-based IS supporters complicated law enforcement efforts, and whether and how the government managed to adapt to new challenges in identifying and surveilling extremists and preventing attacks.

On the one hand, extremists' use of end-to-end encryption may have stymied law enforcement's ability to identify U.S.-based supporters of IS as well as the nature and extent of these individuals' connections to external attack planners. Mary DeRosa, the Deputy Counsel to the President for National Security Affairs in the Obama Administration, noted that many people in the national security community believed that law enforcement's ability to physically access the content of extremists' communications was invaluable and worried that "stings [involving undercover informants]" and other traditional law enforcement tools "could not really uncover the full range of what is going on out there, particularly the influence from [external attack planners] abroad."[84]

Similarly, Baker explained that given the public perception that law enforcement needs to have a zero-failure rate, "…not being able to access the content of communications or the content of phones makes the investigators extremely anxious about what it is that they don't know..."[85] Although since leaving the F.B.I. Baker has emphasized the national security and societal benefits of end-to-end encryption technologies,[86] he acknowledges the potential costs of encryption to law enforcement.[87] When encryption prevents the authorities from accessing the contents of a terrorist's smartphone or from intercepting communications between two or more terrorists, it complicates efforts to understand and thwart the U.S.-based extremists' plans and to identify their

[80] *Id.*
[81] Graham, *supra* note 26, at 20.
[82] *Id.* at 23 (explaining that IS's French-language magazine *Dar al-Islam* instructed readers not to use Tor, an open-source software designed to allow users to anonymously browse the Internet, out of concern that the National Security Agency had compromised the software); Geltzer, *supra* note 28 (predicting that skilled terrorists will tell less savvy U.S.-based extremists which encrypted communications platforms to use in order to securely communicate).
[83] Geltzer, *supra* note 24.
[84] Interview with Mary DeRosa, Deputy Counsel to the President for Nat'l Sec. Affairs, Obama Administration, in Wash., D.C. (Mar. 5, 2020).
[85]Telephone Interview with Jim Baker, *supra* note 77.
[86] Phillip Bantz, *FBI General Counsel Who Battled Apple over Encryption Now Embraces "Going Dark,"* LAW.COM (Oct. 24, 2019), https://www.law.com/corpcounsel/2019/10/24/fbi-general-counsel-who-battled-apple-over-encryption-now-embraces-going-dark [https://perma.cc/72PM-RVLJ].
[87] Baker, *supra* note 18.

co-conspirators.[88] Successfully using end-to-end encryption may sometimes enable attacks that law enforcement otherwise would have detected.

On the other hand, the use of end-to-end encryption by itself does not guarantee that law enforcement will be unable to access the contents of digital communications or uncover the existence of influence from IS external operation planners. In instances where the external attack planners and U.S.-based individuals, in addition to using encrypted messaging applications when communicating, employ sound communications and operational security tactics, the "going dark" challenges will be more pronounced. In many other cases, however, the government has and will likely continue to be able to identify and arrest the U.S.-based extremists, despite their use of encryption. In this vein, Baker explained that,

> Bad guys are not a monolith, and they have different levels of adherence to good operational and communications security practices. However, it is hard not to make a mistake. It's certainly possible, and encryption helps bad guys who might make a mistake, but they often make mistakes…so they'll do something that will alert the F.B.I. to their location, to who they might be in communication with, that type of thing, and that can provide critical investigative leads that can be followed up…[89]

Colin Kahl, former National Security Advisor to Vice President Joe Biden, succinctly summarized the cat-and-mouse game played by U.S. authorities and violent extremists by noting that "there is a Darwinian thing–the more skilled the target [at operational and communications security], the more difficult it might be [for the government] to get access to their communications."[90]

In other words, end-to-end encryption is not a substitute for strong operational and communications security, and law enforcement has a variety of tactics and tools for detecting and disrupting plots even when extremists use encryption to "go dark." Indeed, the law enforcement campaign against U.S.-based supporters of IS shows that there are several tactics that law enforcement uses to try to mitigate "going dark" threats. These tactics include (A) identifying potential targets for surveillance through referrals and tips to law enforcement; (B) using undercover sources to infiltrate private chatrooms on encrypted messaging applications; (C) using traditional means of physical and electronic surveillance against suspects; and (D) employing technical means to gain lawful access to the individuals' communications devices.

A. *Referrals and Tips from Concerned Individuals*

Third-party referrals are reports from individuals or private companies to law enforcement agencies about another individual's concerning behaviors. Between 2015 and 2019, third-party referrals helped the authorities to identify and begin building cases against at least 30 different individuals suspected of supporting IS. Moreover, in at least two of the thirteen known cases in which U.S. residents were directly communicating with external attack planners, third-party referrals alerted the authorities to the individuals' potential radicalization.[91]

---

[88] Baker, *supra* note 18.
[89] Telephone Interview with Jim Baker, *supra* note 77.
[90] Telephone Interview with Colin Kahl, Nat'l Sec. Advisor to Vice President Joe Biden (Mar. 3, 2020).
[91] Those two defendants are Munther Omar Saleh and Justin Sullivan.

The case of Justin Sullivan illustrates how third-party referrals can help the authorities to identify violent extremists who might otherwise avoid detection.[92] In April 2015, Sullivan's concerned father called 911 to request police assistance to his house saying, "I don't know if it is ISIS or what, but [Justin] is destroying Buddhas, and figurines, and stuff."[93] As the father spoke, the 911 operator could hear Justin in the background yelling, "Why are you trying to say I am a terrorist?"[94]

About a month later, an undercover informant posing as a person willing to be recruited into IS began interacting online with Justin Sullivan, who unwittingly invited the informant to participate in his attack planning.[95] In ongoing messages with the informant, Sullivan laid out the plot that he and external attack planner Junaid Hussain concocted: Sullivan was to purchase AR-15s at a gun show in Manassas, Virginia and to attack a bar or nightclub.[96] Sullivan also asked the informant to construct a firearm silencer to use in the attack, sent the informant a YouTube video containing instructions on how to build one, and asked that the finished silencer be mailed to his parents' home.[97]

When a U.S. postal inspector posing as a mail carrier delivered the package to Sullivan's parents' home, his parents opened the package, found the silencer, and once again threatened to call the police. After Sullivan's parents threatened to call the authorities, Sullivan texted the informant and offered him "compensation" if he agreed to kill Sullivan's parents.[98] Immediately thereafter, the authorities arrested Sullivan at his parents' home.[99] A forensic search of Sullivan's cell phone uncovered deleted text messages with external attack planner Junaid Hussain in which Sullivan conspired and agreed with Hussain to commit an armed attack in the United States.[100]

Although third-party referrals may, in some cases, alert the authorities to violent extremists who might otherwise go undetected, there is no guarantee that parents, peers, religious leaders, community members, and other third parties will recognize concerning behaviors in every instance.[101] In other cases, concerned bystanders may naturally resist reporting the individual to law enforcement out of fear of the consequences for that individual.[102] An article in *The New York Times* poignantly explained the nature of the problem: "For parents, particularly those who see

---

[92] Press Release, Office of Pub. Affairs, Dep't of Justice, *North Carolina Man Pleads Guilty to Attempting to Commit an Act of Terrorism Transcending National Boundaries* (Nov. 29, 2016), https://www.justice.gov/opa/pr/north-carolina-man-pleads-guilty-attempting-commit-act-terrorism-transcending-national [https://perma.cc/7ZZX-F77S].

[93] Criminal Complaint at 4, United States v. Justin Nojan Sullivan, No. 1:15-mj-00082-DSC (W.D.N.C. June 22, 2015), https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Sullivan%20Criminal%20Complaint.pdf [https://perma.cc/7Z3N-X3R9].

[94] *Id.*

[95] *Id.* at 5-6.

[96] *Id.* at 6-7.

[97] *Id.* at 9-10.

[98] Factual Basis in Support of the Plea Agreement, *supra* note 61, at 12.

[99] *Id.*

[100] *Id.* at 13.

[101] LAUREN RICHARDS ET AL., FED. BUREAU OF INVESTIGATION BEHAVIORAL THREAT ASSESSMENT CTR., LONE OFFENDER TERRORISM REP. 52 (Nov. 2019).

[102] *Id.* at 2.

their children as misguided but not dangerous, the decision to make that call can be agonizing. Do you risk sending your son to prison? Or hope things improve, and he does not hurt anyone?"[103]

More broadly, the authorities will not have sufficient evidence after every third-party referral to open a predicate case involving the use of resources like wiretaps, surveillance, and human intelligence sources.[104] In some cases, this may mean that the authorities decline to open investigations into suspects who, in hindsight, seem like ideal candidates for lawfully authorized surveillance.[105] Indeed, this appears to have been what happened with Ahmad Khan Rahami, the perpetrator of two IS-inspired bombings that injured thirty-four civilians on September 17, 2016 in New York and New Jersey.[106]

In mid-2014, Rahami's father told the authorities that he worried his son might be a terrorist, prompting the F.B.I. to open a so-called "Guardian"[107] file on the son in order to look into the specific behaviors alleged.[108] However, the initial assessment produced no clear evidence of radicalization, and the authorities declined to investigate further.[109] A little over two years later,[110] Ahmad Khan Rahami carried out his attack. As the Rahami case demonstrates, an outside referral is no guarantee that the authorities will uncover and thwart a determined attacker.

B. *Penetrating Private Chatrooms on Encrypted Messaging Platforms*

Between 2015 and 2019, IS extensively used Telegram, an online messaging platform, in order to disseminate propaganda and to orchestrate and direct violent plots outside IS-held territories.[111] IS's media team used Telegram's public channels, which are searchable and

---

[103] Matt Apuzzo, *Only Hard Choices for Parents Whose Children Flirt with Terror*, N.Y. TIMES (Apr. 9, 2016), https://www.nytimes.com/2016/04/10/us/parents-face-limited-options-to-keep-children-from-terrorism.html [https://perma.cc/J8X8-NMVN].

[104] *Morning Edition: FBI's Challenges in Fighting Domestic Terrorism* (David Greene, National Public Radio radio broadcast Aug. 8, 2019), https://www.npr.org/2019/08/08/749303220/fbis-challenges-in-fighting-domestic-terrorism [https://perma.cc/TJ6H-RGHD].

[105] Faiza Patel, *More Surveillance Doesn't Mean Greater Safety*, N.Y. TIMES (Sept. 22, 2016), https://www.nytimes.com/roomfordebate/2016/09/22/can-the-fbi-do-more-to-investigate-suspected-extremists-3.

[106] Mike Levine & Pierre Thomas, *FBI Opened Previous Inquiry into Bombing Suspect Ahmad Khan Rahami*, ABC NEWS (Sept. 20, 2016), https://abcnews.go.com/US/fbi-opened-previous-inquiry-bombing-suspect-ahmad-khan/story?id=42201580 [https://perma.cc/68CF-VXMP].

[107] Guardian is the F.B.I.'s terrorism threat tracking and management system that serves as the primary database for sending leads to other F.B.I. Field Offices and various Joint Terrorism Task Forces in order to open new terrorism-related assessments or investigations into individuals. WILLIAM H. WEBSTER, REDACTED REPORT OF THE WILLIAM H. WEBSTER COMMISSION ON THE FEDERAL BUREAU OF INVESTIGATION, COUNTERTERRORISM INTELLIGENCE, AND THE EVENTS AT FORT HOOD, TEXAS, 32-69 (Nov. 5, 2009), https://abcnews.go.com/images/Blotter/ft_hood_webster_redact.pdf?SITE=ABCNEWS [https://perma.cc/2LUD-8A3L].

[108] Levine & Thomas, *supra* note 106.

[109] *Id.*

[110] The F.B.I. did not continue to conduct surveillance on Ahmad Khan Rahami after the Bureau's initial assessment in 2014 that Rahami did not have ties to terrorists. *See id.*

[111] Palko Karasz, *What Is Telegram, and Why Are Iran and Russia Trying to Ban It?*, N.Y. TIMES (May 2, 2018), https://www.nytimes.com/2018/05/02/world/europe/telegram-iran-russia.html [https://perma.cc/EN9A-5BRV].

accessible to all Telegram users, to broadcast propaganda, claims of responsibility for terrorist attacks, and messages to an indefinite online audience.[112]

External attack planners have used private group chats, which are only accessible via time-limited URL links that are disseminated within existing IS channels, to incite and direct attacks against Western targets.[113] Some private chatrooms contain membership lists and indications of who is online, which allows all members of the private chatroom to engage other members directly in one-on-one encrypted chats.[114]

One of the ways that the authorities seek to mitigate the "going dark" problem is by using traditional law enforcement methods such as having undercover sources pose as IS supporters in order to gain access to these private chatrooms. Doing so allows the authorities to access otherwise encrypted communications and can help them to identify violent extremists in the United States. Geltzer notes that "if you're ISIS, you need to let some circle of new participants into [the private chatrooms] if you want to broaden your reach, but everyone new you let in is a potential vulnerability [to IS supporters in the chatroom]."[115]

For instance, beginning in July 2016, "a nationwide team of F.B.I. agents worked around the clock" to identify an avowed IS supporter who had posted in a private encrypted chatroom that he was planning "to explode a car bomb outside a gay nightclub in San Francisco, and plant backpack bombs on routes known to be used by emergency vehicles…."[116] Sometime in July, an undercover F.B.I. informant who had managed to join the private chatroom by posing as an IS supporter directly messaged the individual.[117] The F.B.I. informant sought to establish a rapport with the individual by saying, "[B]ro, I'm sorry to bother you, but I think we both know someone. Bro abu ali," which was the username that the administrator of the private IS chatroom went by.[118] Over the course of several days, the informant and individual communicated on the encrypted messaging application as the informant worked to gain the individual's trust. During this period, the F.B.I. managed to establish the individual's true identity by locating a Twitter account that had similar account identifiers[119] to the individual's username on the encrypted platform; the authorities then worked "their way backwards from information provided by Twitter" to identify the individual as Samer Anan Alhaggagi.[120]

---

[112] *Id.*

[113] BENNETT CLIFFORD & HELEN POWELL, THE GEORGE WASHINGTON UNIV. PROGRAM ON EXTREMISM, ENCRYPTED EXTREMISM: INSIDE THE ENGLISH-SPEAKING ISLAMIC STATE ECOSYSTEM ON TELEGRAM 37 (June 2019), https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/EncryptedExtremism.pdf [https://perma.cc/9WL5-XHT3].

[114] Mia Bloom et al., *Navigating ISIS's Preferred Platform: Telegram*, 31 TERRORISM & POL. VIOLENCE 1242, 1245 (2019).

[115] Interview with Joshua Geltzer, *supra* note 12.

[116] United States Sentencing Memorandum at 1, United States v. Amer Sinan Alhaggagi, No. CR-17-0387-CRB-1 (N.D. Cal. Dec. 4, 2018), https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/alhaggagi%20government%20sentencing%20memorandum.pdf [https://perma.cc/9WL5-XHT3].

[117] *Id.* at 2.

[118] *Id.*

[119] An account identifier, sometimes called a social media "handle," is any username that an individual uses on social media platforms such as Facebook, Twitter, and Instagram.

[120] *Id.* at 11.

The undercover informant eventually gained Alhaggagi's trust through conversations on encrypted messaging applications,[121] and by late July, Alhaggagi agreed to meet in-person with the informant and the informant's purported cousin, an undercover F.B.I. agent who claimed to know how to construct bombs.[122] During the in-person meeting, Alhaggagi mentioned that he had been in touch with "the brothers" and had sent IS pictures of sites that he was considering attacking as well as a video of himself pledging allegiance to the group's leader.[123]

Although Alhaggagi ceased communications with the informant and undercover agent after growing suspicious that they were associated with law enforcement, the authorities arrested Alhaggagi before he could execute his plans.[124] Alhaggagi's case reveals how the authorities can infiltrate encrypted messaging platforms in order to try to identify, contact, and lawfully surveil suspected violent extremists. At the same time, Alhaggagi's case shows that the use of informants carries other risks, including the possibility that the target will grow suspicious of monitoring efforts and accelerate his plans to commit a violent attack.[125]

In another instance involving the use of informants, an F.B.I. source managed to directly contact an external attack planner, Abu Sa'ad al-Sudani. Around this time period, al-Sudani had been in contact with Mohamed Bailor Jalloh, an IS supporter in the United States who told al-Sudani that he wanted to conduct an attack but was unsure whether he could "ensure his heart would be strong and not fail him" during the operation.[126] Al-Sudani then put Jalloh in touch with a purported IS supporter living in the United States hoping that he could help Jalloh to execute the plot.[127] Unbeknownst to al-Sudani and Jalloh, the purported supporter was the F.B.I source, and the authorities arrested Jalloh before he could carry out an attack.[128]

According to the data, there is evidence that the authorities used undercover sources to gather intelligence against at least six of the thirteen U.S. residents who were directly communicating with external attack planners between 2015 and 2019.[129] As such, undercover informant networks, both in the physical and online worlds, were critical to law enforcement's efforts to adapt to "going dark" challenges.

Although informants can provide invaluable human intelligence on surveillance targets, using informants carries its own set of risks. Baker explained,

> putting an undercover operative into…contact with an individual, increases the risk to the investigative personnel and to the investigation, meaning that there's an enhanced risk that

[121] *Id.* at 3-4.
[122] *Id.* at 24.
[123] *Id.* at 7.
[124] *Id.* at 55.
[125] Garrett M. Graff, *The FBI's Growing Surveillance Gap*, POLITICO MAG. (June 16, 2016).
[126] Position of the United States with Respect to Sentencing at 4, United States v. Mohamed Bailor Jalloh, No. 1:16-cr-00163-LO (E.D. Va. Feb. 2, 2017), https://www.investigativeproject.org/documents/case_docs/3222.pdf [https://perma.cc/HRG6-P44D].
[127] *Id.*
[128] *Id.* at 5.
[129] These six individuals were Elton Simpson, Mohamed Bailor Jalloh, Emanuel Lutchman, Justin Sullivan, Munther Omar Saleh, and Munir Abdulkader.

> the subject will find out that he or she is under investigation which could either make it difficult to figure out exactly what the person is up to so [that] the authorities can arrest them, or it encourages them to…escalate and engage in an attack more quickly [before the authorities can intervene and make an arrest].[130]

Although using undercover informants entails risks that using electronic surveillance does not, the aggressive use of undercover informants and other human intelligence collection methods was critical to law enforcement efforts to adapt to "going dark" threats.

C. *Using Physical and Electronic Surveillance*

Physical and electronic surveillance–including monitoring Internet activity–played a key role in helping the authorities to build criminal cases against dozens of suspected IS supporters in the United States, even though many of these individuals used encryption.[131] The investigation into and arrest of Munther Omar Saleh, a college student who used encrypted messaging applications[132] to communicate with Junaid Hussain, shows how IS supporters' online activities can undermine their efforts to use encryption to "go dark."

Munther Omar Saleh initially came to law enforcement's attention after tweeting that al-Qaeda was "getting too moderate" and praising IS for their "high end videos, great weaponry, and quality fighters."[133] Junaid Hussain, after connecting with Saleh online, used an encrypted messaging application to send him instructions for constructing a pressure cooker bomb; Saleh then emailed himself a copy of the instructions,[134] which could have been intercepted by the authorities with effective electronic surveillance. According to the government's sentencing memorandum, "on the same date that Saleh received the bomb-making instructions [from Junaid Hussain], the F.B.I. directed a confidential human source ("CHS 1") to initiate an online conversation with Saleh."[135]

When the confidential informant reached out pretending to be an IS supporter living in the United States, Saleh initially revealed that, "I'm in NY and trying to do an Op [an attack]" before asking the informant, "Who is the akh [brother] who sent you to me?" When the F.B.I. informant replied that he was sent by a "brother" in IS, Saleh responded, "I understand akhi [my brother], but as the system works, example: abuFulan sent u, u have to tell me 'abu fulan sent me', i would go to abuFulan to confirm and then we can safely and freely, [this messaging application] is fully

---

[130] Telephone Interview with Jim Baker, *supra* note 77.
[131] Michael S. Schmidt et al., *U.S. Investigators Struggle to Track Homegrown ISIS Suspects*, N.Y. TIMES (Nov. 19, 2015), https://www.nytimes.com/2015/11/20/us/us-investigators-struggle-to-track-homegrown-isis-suspects.html [https://perma.cc/36ZL-P4QA]; OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S EFFORTS TO IDENTIFY HOMEGROWN VIOLENT EXTREMISTS THROUGH COUNTERTERRORISM ASSESSMENTS 5 (Mar. 2020), https://oig.justice.gov/sites/default/files/reports/a20030_0.pdf [https://perma.cc/LQ27-Y89J].
[132] U.S. authorities can obtain and use traffic analysis and other metadata from U.S.-based encrypted messaging providers in order to discover whom a particular U.S. resident is sending encrypted data to. However, non-U.S. providers such as Telegram and Signal may only provide minimal amounts of metadata to U.S. authorities, or may altogether refuse to cooperate with U.S. investigators. *See* Baker, *supra* note 18.
[133] Letter Regarding Sentencing of Munther Omar Saleh & Fareed Mumuni, *supra* note 54, at 3.
[134] *Id.* at 4.
[135] *Id.*

encrypted….We can *talk* safely…"[136] The informant attempted to gain Saleh's trust by providing the name of a known external attack facilitator, but Saleh responded, "I'm very sorry, but I was ordered by dawlah [IS] officials not to talk to anyone until they produce an akh [brother] of authority to vouch for them."[137]

Although Saleh unknowingly thwarted the government's attempt to ensnare him in a sting by following IS's communications security protocols, the authorities did not give up: law enforcement continuously surveilled Saleh and his co-conspirators over the course of several months during summer 2015 in an attempt to head off the cell's planned attack.[138] Electronic surveillance established that Saleh searched online for targets in New York as well as for different components required to build an explosive device, and sent his co-conspirators links to IS propaganda videos on YouTube.[139] While physically surveilling Saleh, law enforcement agents observed him purchase a black digital wristwatch–which could be used as a timer in an explosive device–at a store in Queens, New York.[140] The plot fell apart after Saleh and one of his co-conspirators, convinced that the authorities were following them, ran towards a law enforcement vehicle that was trailing them and unsuccessfully attempted to attack the officer inside.[141]

Saleh's case illustrates that the use of end-to-end encryption is not a substitute for good operational and communications security. Even for those violent extremists who practice sound operational and communications security practices, it is hard for the extremists not to make a mistake in practice. [142] Making such mistakes risks undermining the extremists' efforts to use encryption to "go dark" and evade government detection and surveillance.

Although the IS has distributed lengthy guides on operational and communications security,[143] it is one thing for U.S.-based supporters of the terrorist group to read abstract technical instructions about how to maintain online anonymity and another for these individuals to flawlessly translate that knowledge into practice.[144] An additional complication when "going dark" is that IS's recruitment efforts depended upon the group and its supporters actively using social media to broadcast IS-produced propaganda to as many persons as possible.[145] IS's outsized presence[146] on social media allowed the group to identify, assess, and radicalize potential recruits who were sharing the group's propaganda or interacting with other self-proclaimed IS supporters, but online supporters' activism also created a digital trail that helped law enforcement to identify potential violent extremists and to determine which U.S.-based individuals to investigate most

---

[136] *Id*.
[137] *Id.* at 10.
[138] Press Release, Dep't of Justice U.S. Attorney's Office E. Dist. of New York, Queens Man Sentenced to 18 Years' Imprisonment for ISIS-Directed Terrorist Attacks in New York City (Feb. 6, 2018), https://www.justice.gov/usao-edny/pr/queens-man-sentenced-18-years-imprisonment-isis-directed-terrorist-attacks-new-york [https://perma.cc/9VNF-C9TR].
[139] Letter Regarding Sentencing of Munther Omar Saleh & Fareed Mumuni, *supra* note 54, at 10-11.
[140] *Id.* at 10.
[141] *Id.* at 13-14.
[142] Telephone Interview with Jim Baker, *supra* note 77.
[143] Kim Zetter, *Security Manual Reveals the OPSEC Advice ISIS Gives Recruits*, WIRED MAG. (Nov. 19, 2015).
[144] *See* Michael Kenney, *Beyond the Internet: Mētis, Techne, and the Limitations of Online Artifacts for Islamist Terrorists*, 22 TERRORISM & POL. VIOLENCE 177, 179-182 (2010).
[145] *See* Berger & Morgan, *supra* note 14, at 2.
[146] *Id*.

thoroughly. In other words, while IS skillfully exploited new communications platforms like Twitter and YouTube to gain power and influence, these same tools also made IS's followers vulnerable to detection and surveillance.

If these surveillance targets later switched to using encrypted messaging applications to communicate, as many IS supporters did, the authorities often were able to mitigate "going dark" threats through the use of human intelligence. If those efforts failed, physical and electronic surveillance could be used to build cases against suspected IS supporters, particularly if the individuals were not properly maintaining anonymity online, communicating via encrypted messaging applications, and using virtual private networks (VPNs) to conceal their location data from the authorities.[147]

Physical and electronic surveillance can help the authorities to continue to monitor extremists when they try to "go dark," but intensive, around-the-clock surveillance of a single suspect may require as many as thirty to forty F.B.I. agents, technicians, and analysts, meaning that this level of surveillance cannot be done at scale.[148] For instance, when it came to law enforcement efforts against suspected U.S.-based supporters of IS, the F.B.I. reportedly only had sufficient resources to conduct around-the-clock surveillance on about five to ten percent of the 1,000 U.S. residents deemed most at risk of radicalizing to violence.[149] Although the other ninety to ninety-five percent were subjected to varying levels of surveillance,[150] some of these individuals may have been able to conceal their radicalization from authorities, particularly if they were following sound operational and communications security practices, including the use of end-to-end encryption.[151] Thus, like other law enforcement tools, physical and electronic surveillance can help the authorities to reduce but not eliminate "going dark" threats.

D. *Employing Technical Means to Gain Lawful Access to Communications Devices*

If law enforcement becomes aware that an individual is using encrypted messaging applications to communicate with external attack planners, there are a number of technical means that the authorities can use to gain access to the device. After receiving appropriate judicial authorization, the F.B.I. can try to do some type of focused hacking on the device to try to get into the device of either the person in the United States or the person abroad to read the communications before they are encrypted.[152] Similarly, a senior Obama Administration official argued that, "end-to-end encryption is only useful if [the authorities] can't get a piece of malware onto their actual

---

[147] A Virtual Private Network (VPN) allows users to connect to proxy servers for the purposes of protecting personal identifying information and geo-location data when accessing the Internet. *See* BONNIE MITCHELL ET AL., OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, GOING DARK: IMPACT TO INTELLIGENCE AND LAW ENFORCEMENT AND THREAT MITIGATION 7 (2017), https://www.odni.gov/files/PE/Documents/10---2017-AEP_Going-Dark.pdf [https://perma.cc/3SUP-T6PE].

[148] Graff, *supra* note 125.

[149] *Id.*

[150] *Id.*

[151] It is not possible to determine with publicly available information how many of the individuals who could not be surveilled around the clock attempted terrorist attacks in the United States.

[152] Carlos Liguori, *Exploring Lawful Hacking as a Possible Answer to the "Going Dark" Debate*, 26 MICH. TECH. L. REV. 317, 320 (2020).

phone…If you can actually get ahold of the device or get somebody to download an app or click on a link then you might be able to get access to somebody's phone even with the encryption."[153]

Although data related to the government's use of targeted hacking to try to circumvent end-to-end encryption is classified, the authorities likely used targeted hacking to locate, monitor, and eliminate many of IS's external attack planners in Syria.[154] For instance, British agents who were posing as IS supporters on Surespot reportedly hacked Junaid Hussain's cellphone by sending him a phishing message with a link; when Hussain clicked the link, the authorities gained access to Hussain's phone, which enabled them to identify individuals in the West with whom Hussain was communicating and to monitor Hussain's physical movements in Syria.[155] Beginning in August 2015, the United States and United Kingdom conducted a series of drone strikes that killed Junaid Hussain and other key external attack planners who were based in Syria.[156]

The ability of U.S. authorities and foreign partners to bypass end-to-end encryption does not mean that there are simple technical fixes to "going dark" challenges. As Baker noted,

> while [hacking communications devices] can be successful, it's not guaranteed to be successful and it's not guaranteed to be durable. So, for example, even if you get onto somebody's device, if the person updates their operating system, as we get notices to do on a regular basis…that could disrupt the surveillance…So it's a fragile system that also cannot be done at scale…[157]

Nevertheless, when targeted hacking efforts are successful, the authorities can circumvent the target's efforts to "go dark," gain access to the contents of their communications, and learn new investigative leads, all of which may help the authorities to identify the target's co-conspirators as well as the wider social network that encouraged the target's radicalization towards violence.

IV. Interpreting the Quantitative Findings

The quantitative findings show that the authorities successfully used traditional law enforcement techniques, including human intelligence efforts, to mitigate the "going dark" challenges created by IS supporters' use of end-to-end encryption. For the purposes of this paper, success is defined as the prevention and disruption of large-scale terrorist attacks by U.S.-based individuals who attempted to "go dark." Part A below first analyzes how law enforcement aggressively responded to the threats posed by IS supporters in the United States. Part B compares the methods of attack and lethality for IS-directed and -inspired attacks. Finally, Part C concludes

---

[153]Telephone Interview with senior Obama Administration official (Mar. 3, 2020). The interviewee requested anonymity because (s)he thought that (s)he might be considered for a senior position in the Biden Administration and did not want to make statements on-the-record about law enforcement's ability to circumvent end-to-end encryption through targeted hacking techniques.

[154] Lizzie Dearden, *British Isis Jihadists "Had Phones Hacked by GCHQ" Before They Were Killed by Drone Strikes*, INDEPENDENT (Sept. 16, 2015), https://www.independent.co.uk/news/uk/home-news/british-isis-jihadists-had-phones-hacked-by-gchq-before-they-were-killed-by-drone-strikes-10503076.html [https://perma.cc/P99M-2X3Q].

[155] *Id.*

[156] Goldman & Schmitt, *supra* note 32.

[157] Telephone Interview with Jim Baker, *supra* note 77.

by arguing that U.S. counterintelligence and law enforcement agencies were largely successful in adapting to the threats posed by IS's supporters use of end-to-end encryption.

A. *Counterterrorism and Law Enforcement Efforts Against Islamic State Supporters*

As mentioned earlier, the U.S. government made 172 IS-related arrests in the five years between 2015 and 2019. For comparison, the U.S. government charged ninety individuals with terrorism-related offenses in connection with al-Qaeda in the five years after 9/11.[158] These arrest statistics help to illustrate IS's comparatively greater success than al-Qaeda in directing and inspiring terrorist plots in the United States as well as how the U.S. government significantly increased its law enforcement efforts in order to address the threat of IS-directed and-inspired attacks. Indeed, John Carlin, the former chief of staff to then-F.B.I. director Robert Mueller, wrote that, "Earlier in my career at F.B.I., we thought ten simultaneous terror cases represented a huge number; at this point [with IS supporters in the United States] we faced dozens."[159] Figure 2[160] illustrates that after the first IS-related arrests in the United States in March 2014, the government dramatically increased law enforcement efforts against the group's U.S.-based followers. Figure 2 shows the total number of IS-related arrests peaking in 2015 and gradually declining over the following years.[161]

[158] BRIAN MICHAEL JENKINS, RAND CORP., STRAY DOGS AND VIRTUAL ARMIES RADICALIZATION AND RECRUITMENT TO JIHADIST TERRORISM IN THE UNITED STATES SINCE 9/11 6 (2011), https://www.rand.org/pubs/occasional_papers/OP343.html [https://perma.cc/377D-FVZK].

[159] Carlin, *supra* note 14.

[160] The arrest statistics for the year 2014 were compiled by the George Washington University Program on Extremism. *See The Islamic State in America: GW Extremism Tracker 5 Year Review*, GEO. WASH. U. , https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/ISIS%20in%20America%205%20Year%20Review.pdf [https://perma.cc/Z3ST-TSZ4].

[161] Adam Goldman et al., *The Islamic State's Suspected Inroads into America*, WASH. POST (June 22, 2015), https://www.washingtonpost.com/graphics/national/isis-suspects [https://perma.cc/BP3W-HSGY].

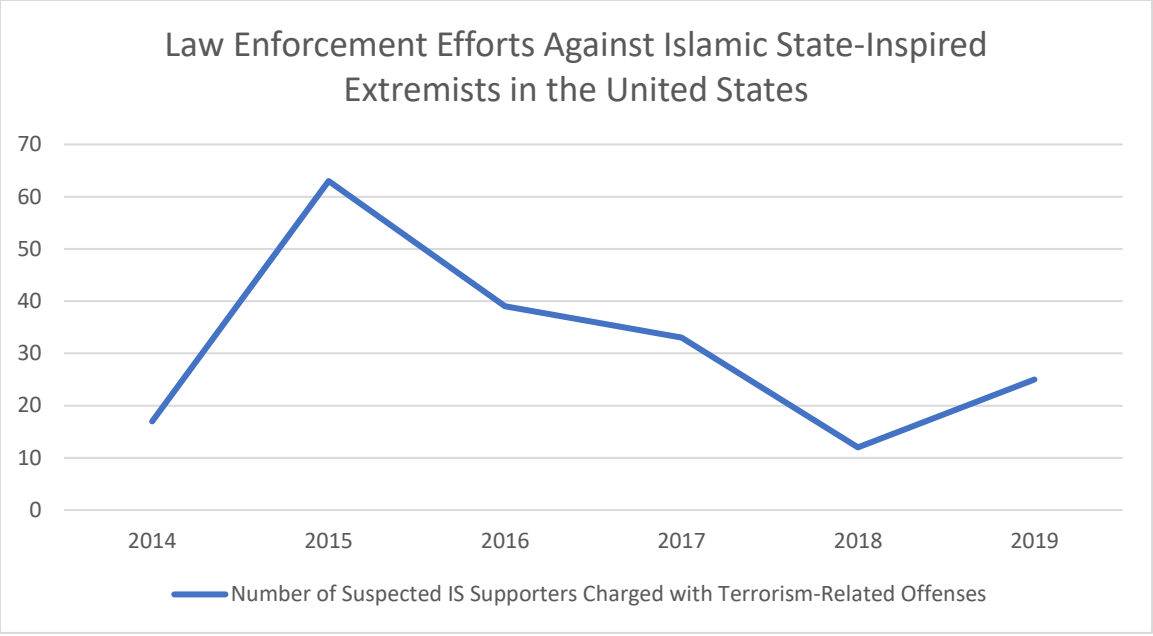

Figure 2

Human intelligence, including the use of undercover informants, played a critical role in these efforts by helping law enforcement to mitigate "going dark" threats.[162] One senior F.B.I. official argued that, "When the bad guys turn to encrypted areas, we're dark, and the only way to gain a better understanding of what we're up against may be through an undercover."[163] Similarly, Baker, explained that, "Human sources [including undercover informants] often produce the best intelligence because they're in the most direct contact with people….They understand the context, they understand the players, and they have direct interactions with people that are engaged in those types of activities."[164] By establishing a personal relationship with potential suspects, human sources are often able to elicit incriminating information that the authorities can use to make arrests and stop attacks.

The arrest data illustrate how law enforcement aggressively utilized human sources to try to monitor and disrupt potential plots involving IS-related extremists. The data show that undercover sources were interacting with at least sixty-four percent of IS-related extremists arrested or killed between 2015 and 2019. Furthermore, the percentage of IS-related cases involving the use of undercover sources increased from a low of about fifty-four percent in 2015 to eighty percent of cases in 2019.

Third-party referrals by concerned individuals to law enforcement were an additional and invaluable source of human intelligence on U.S.-based supporters of IS.[165] Figure 3 illustrates how

[162] *See Final Report of the Task Force on Combating Terrorist and Foreign Fighter Travel: H. Comm. on Homeland Sec.*, 114th Cong. 18 (2015), https://fas.org/irp/congress/2015_rpt/travel.pdf [https://perma.cc/AX25-RAY3].
[163] Eric Lichtblau, *F.B.I. Steps up Use of Stings in ISIS Cases*, N.Y. TIMES (June 7, 2016), https://www.nytimes.com/2016/06/08/us/fbi-isis-terrorism-stings.html [https://perma.cc/3G46-HK8Q].
[164] Telephone Interview with Jim Baker, *supra* note 77.
[165] Eric Rosand, *Fixing CVE in the United States Requires More Than Just a Name Change*, BROOKINGS INSTITUTION (Feb. 16, 2017), https://www.brookings.edu/blog/order-from-chaos/2017/02/16/fixing-cve-in-the-united-states-requires-more-than-just-a-name-change [https://perma.cc/MF3X-WTSX].

U.S. law enforcement relied upon third-party referrals and undercover sources to respond to IS supporters' attempts to carry out violent attacks.[166] Because the government is rarely in a position to observe behavioral changes that might signal an individual's radicalization towards violence, referrals from concerned family members, peers, professionals, and community or religious leaders can help the authorities to identify potential violent extremists who might otherwise go undetected.[167] According to the data, in roughly seventeen percent of the IS-related cases between 2015 and 2019, an outside tip alerted the authorities to the U.S.-based individual's potential radicalization. Third-party referrals can alert the government to potential extremists and provide the predicate information needed to open criminal investigations, but the relatively small number of referrals in IS-related cases indicates that they were of limited use in ameliorating "going dark" challenges. The statistics show that the authorities were far less successful in encouraging third parties from within the community to alert law enforcement about potential extremists.

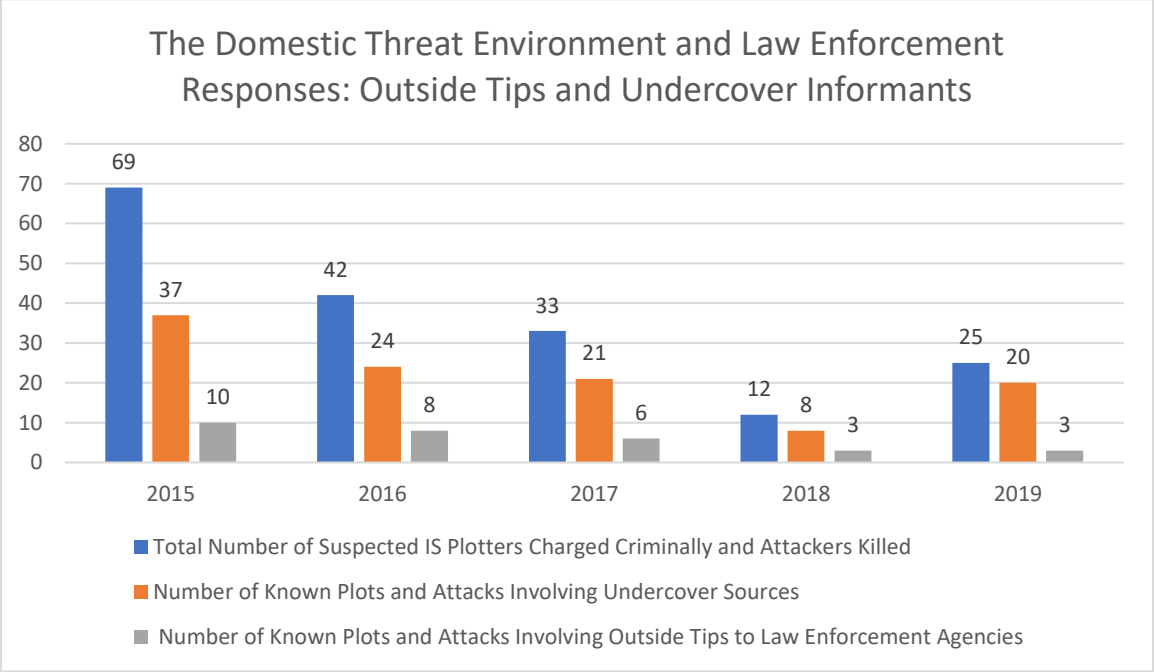

Figure 3

B. *Islamic State-Related Violence in the United States: Directed Versus Inspired Attacks*

Quantitative analyses can reveal differences in the failure rate and lethality of IS-directed and -inspired plots in the United States.[168] Figure 4 illustrates the lethality of IS-directed and -inspired attacks between 2015 and 2019. Directed attacks refer to attacks in which there is evidence of direct communications between at least one of the perpetrators and any IS external attack

[166] The majority of cases in the author's dataset involving third-party referrals also involved the use of undercover sources by the U.S. authorities.

[167] Lorenzo Vidino & Seamus Hughes, *Countering Violent Extremism in America*, GEO WASH. U. 9 (June 2015), https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/downloads/CVE%20in%20America.pdf [https://perma.cc/SH5G-NR9T].

[168] For the purposes of this analysis, the author coded an attack as IS-directed if there was any direct communication between the individual or the individual's co-conspirators and IS external attack planners.

planner. Inspired attacks refer to attacks committed by IS sympathizers where there is no evidence of direct communications between any one of the perpetrators and external attack planners. Between the years 2015 and 2019, there is evidence that IS external attack planners directly communicated with at least thirteen U.S. residents as part of the terrorist group's efforts to plan and direct violent attacks in America from within the group's safe havens in the Middle East. Four of the thirteen known IS-directed plots reached the execution stage, with IS supporters carrying out their original terrorist plots or attacking arresting officers. Law enforcement disrupted the other nine IS-directed plots without any violent incident. These statistics reveal that the authorities successfully uncovered and thwarted roughly seventy percent of IS-directed plots in the United States. The sizeable failure rate for directed attacks illustrates the difficulty in evading law enforcement detection and incrimination despite the use of encryption and other means of "going dark."

Between the years 2015 and 2019, there were fourteen instances of IS-inspired attacks without evidence of communications between the perpetrators and external attack planners. Roughly forty-three percent of inspired attacks involved the use of knives, twenty-nine percent involved the use of firearms, fourteen percent involved the attempted use of explosive devices, and another fourteen percent involved vehicular attacks. The fourteen IS-inspired attacks collectively left 73 people dead and 159 individuals seriously wounded, an average of about 6 fatalities and 12 individuals seriously wounded per attack.

Although the attack statistics show that the average IS-inspired attacker killed and injured far more victims than IS-directed attackers in the United States, two incidents-deadly shootings in Orlando and San Bernardino-skewed the data on inspired attacks.[169] For instance, Omar Mateen's IS-inspired attack on the Pulse Nightclub in Orlando, which resulted in forty-nine casualties, caused roughly 350% more casualties than the second deadliest inspired attack.[170] The Orlando attack accounts for nearly sixty-seven percent of the fatalities and thirty-three percent of the serious injuries that resulted from IS-inspired attacks during the five-year period. Furthermore, the two deadliest IS-inspired attacks, the shootings in Orlando, Florida and San Bernardino, California, were responsible for roughly eighty-six percent of the fatalities caused by IS-inspired attacks in the United States between 2015 and 2019.

[169]Although the two inspired attacks in Orlando and San Bernardino skewed the attack statistics, these statistics fail to capture certain advantages of directed attacks. Following successful directed attacks, IS could release evidence of the group's connections to and communications with the attackers. This evidence could maximize publicity for the group and help to further terrorize the population. In contrast, with inspired attacks, IS cannot provide any evidence of the group's influence over the attackers other than what the attackers do to signal their support for the group.

[170] The next deadliest attack, the IS-inspired attack in San Bernardino, resulted in fourteen deaths.

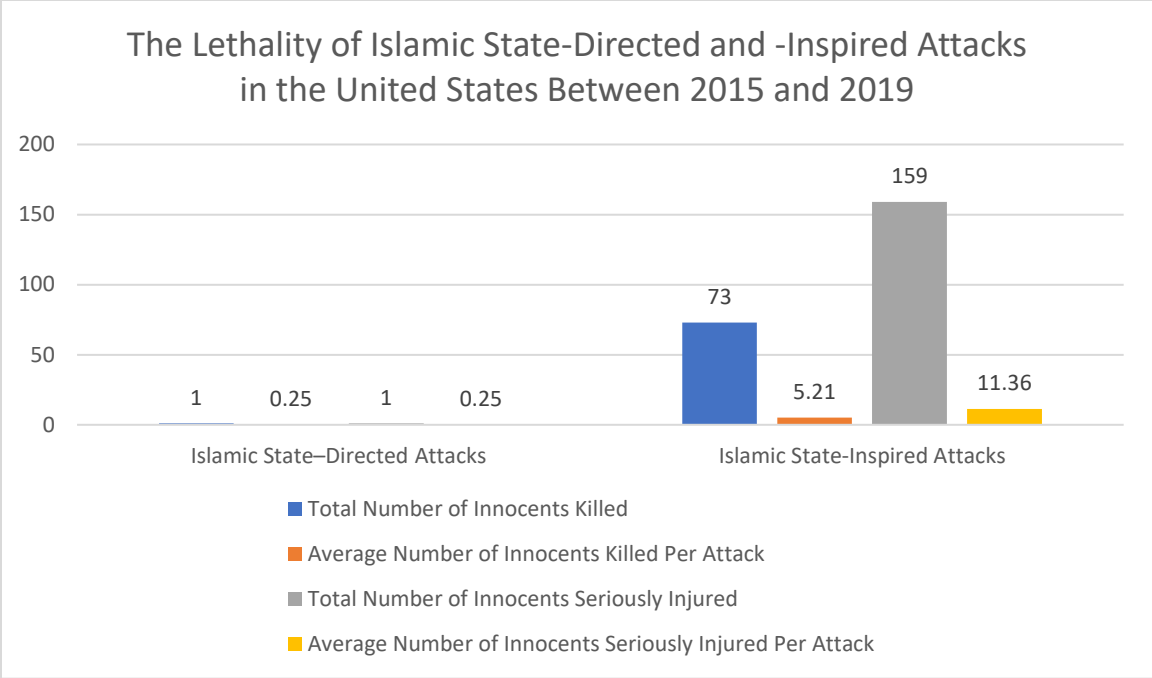

Figure 4

On average, directed attacks resulted in fewer than one death per attack, while inspired attacks resulted in more than five deaths per attack. However, Figure 5 illustrates that when the outlier of the Pulse nightclub shooting is removed from the dataset, IS-inspired attacks collectively resulted in twenty-four deaths or an average of fewer than two victims per attack. Even after removing the Pulse Nightclub shooting from the dataset, the average inspired attack was still deadlier than all directed attacks. This finding suggests that IS external attack planners' direct influence over attackers is not correlated with higher fatality rates when compared to IS-inspired attackers. This may indicate that the benefit for U.S.-based extremists of directly communicating with international terrorist groups' external attack planners is not worth the difficulty of trying to use encryption and other measures to successfully conceal those conversations from law enforcement.

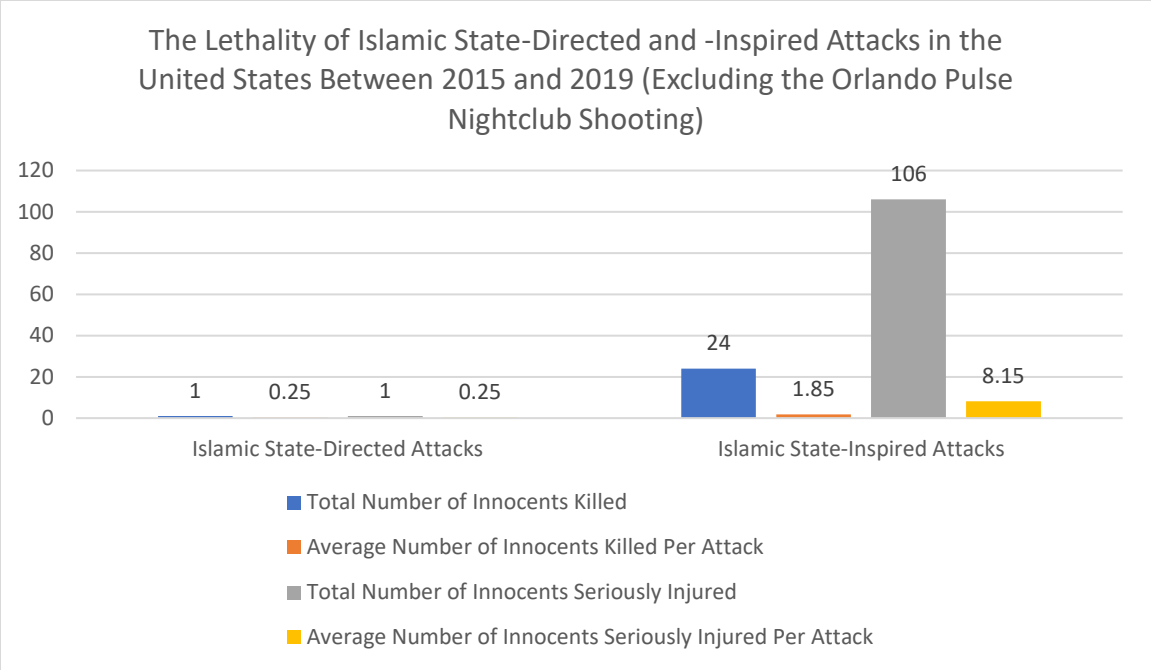

Figure 5

C. *U.S. Counterterrorism and Law Enforcement Efforts: Measuring Success*

Measuring how U.S. counterterrorism efforts against IS succeeded can help the authorities to develop a strategy for dealing with other terrorists and criminals that use encryption and other measures to evade detection and incrimination. Defining counterterrorism success depends on "what interests are prioritized and which perspective one takes."[171] This article measures counterterrorism success by evaluating the degree to which the authorities prevented and disrupted violent attacks.[172] Because it is difficult to obtain data on terrorist organizations' morale, recruitment, and ability to conduct attacks, the number or arrests and disruptions can serve as a proxy for such indicators of terrorist groups' health as well as the success of counterterrorism efforts.[173]

As Figure 6 illustrates, the number of IS-related attacks and fatalities in the United States declined from a peak of seven attacks that resulted in sixty-four fatalities in 2015 to one non-lethal attack in 2019.

[171] Daniel Byman, *Eighteen Years on: The War on Terror Comes of Age*, 12 CTCSENTINEL 1, 1 (2019).
[172] *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, THE NATIONAL INTELLIGENCE STRATEGY OF THE UNITED STATES OF AMERICA 12 (2019), https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf (defining counterterrorism success similarly) [https://perma.cc/7L6D-PYSJ].
[173] Daniel Byman, *Are We Winning the War on Terrorism?*, BROOKINGS INSTITUTION (May 23, 2003), https://www.brookings.edu/research/are-we-winning-the-war-on-terrorism [https://perma.cc/2PED-BBET].

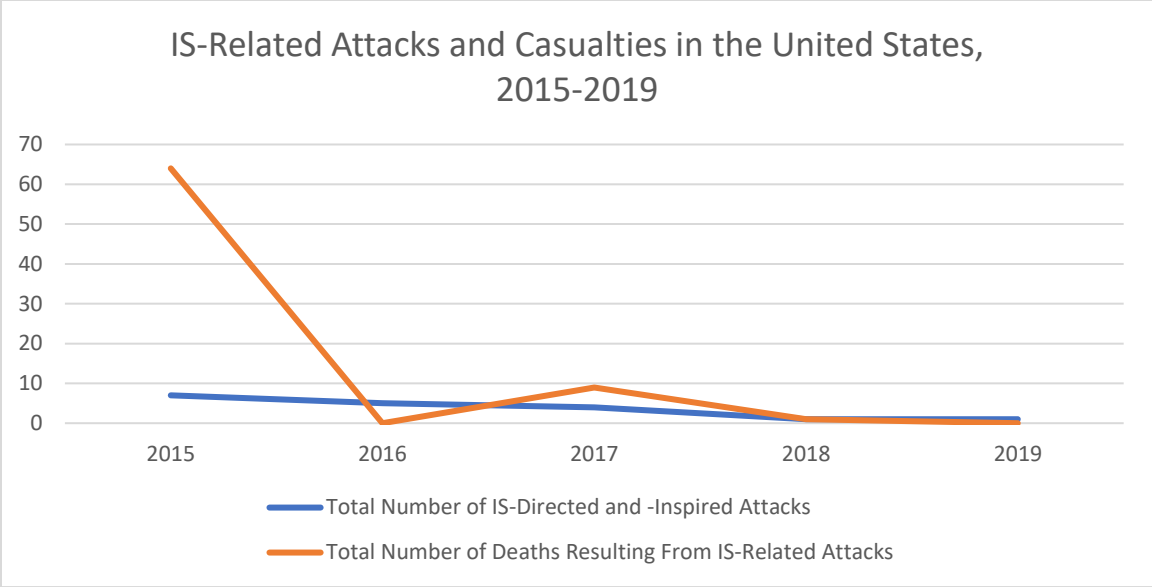

Figure 6

However, measuring counterterrorism success through attack statistics alone is misleading; for instance, attack statistics cannot capture how attacks influenced public opinion, how much U.S. law enforcement activities contributed to the decline in IS attacks, or how U.S. communities responded to violence. In this vein, Baker explained that "especially post-9/11, the F.B.I. has been expected to have a zero-failure rate with respect to counterterrorism. So, it induces an incredible stress on everyone in the system to try…to stop every possible attack." Viewed through the lens of the law enforcement community in the post-9/11 political environment, the U.S. counterterrorism effort failed to achieve its goal of preventing every deadly terrorist-related incident. Nevertheless, the statistics showed that law enforcement successfully adapted to the threat posed by IS and managed to disrupt most large-scale plots by the terrorist group's U.S.-based supporters.

V. Lessons Learned and the Way Forward

Given the strong likelihood that international terrorists will continue to use encryption in order to communicate securely,[174] studying how the government attempted to address the "going dark" phenomenon can provide important lessons for the U.S. national security community. The law enforcement campaign against suspected IS supporters in the United States provides a template for confronting future "going dark" threats. Examining how law enforcement adapted to U.S.-based supporters of IS's use of encryption is particularly useful because the perceived need to gain timely access to these individuals' encrypted communications was particularly acute. Just like IS,

[174] For a discussion of how extremist groups are likely to replicate and refine IS's success at using modern communications technologies, including professionally produced propaganda, social media platforms, and end-to-end encrypted messaging applications, to recruit individuals who feel vulnerable and detached from their communities, see *Stepping out of the Shadows: How Violent White Supremacists Have Used Technology to Pose a Transnational Threat: Hearing Before the H. Subcomm. on Civil Rights & Civil Liberties and on Nat'l Sec.*, 116th Cong. 2 (2019) (statement of Joshua A. Geltzer, Executive Director Georgetown Law's Institute for Constitutional Advocacy & Protection), https://docs.house.gov/meetings/GO/GO02/20190920/109977/HHRG-116-GO02-Wstate-GeltzerJ-20190920.pdf [https://perma.cc/6PKS-T5SF].

other terrorist and criminal groups will try to use encryption to conceal the content of their communications from law enforcement.

The law enforcement campaign against U.S.-based IS supporters illustrates the nature of "going dark" challenges as well as the authorities' ability to adapt to new realities. In particular cases, the use of end-to-end encryption may stymie the authorities' ability to gain timely access to content for which they have obtained lawful authorization.[175] In many other cases, however, the authorities will be able to successfully surveil potential targets despite their use of end-to-end encryption. The use of traditional law enforcement tools, including undercover informants, physical and electronic surveillance, outside tips, and targeted hacking were instrumental in the U.S. counterterrorism campaign against IS and can help the authorities to mitigate future "going dark" threats.

The data also reveals that IS-inspired attacks were, on average, deadlier than IS-directed attacks. This suggests that there was not a strong, positive correlation between external attack planners' direct influence over attackers and attack lethality. This may indicate that the benefit for U.S.-based extremists of directly communicating with international terrorist groups' external attack planners is not worth the difficulty of trying to use encryption and other measures to successfully conceal those conversations from law enforcement.

That at least 4 of the 18 IS-related attacks inside the United States were remotely directed and roughly 25 percent of IS-related arrestees and attackers used end-to-end encryption to communicate substantiates law enforcement's concerns about the extensive use of end-to-end encryption by U.S.-based supporters of IS. At the same time, the authorities were able to use human and signals intelligence and targeted hacking to effectively surveil many extremists attempting to "go dark." The authorities should replicate these tactics to deal with future "going dark" challenges.

In particular, two law enforcement techniques—the use of human sources and targeted hacking—can help the U.S. government to handle future "going dark" challenges. The data on the government's targeted hacking efforts are classified. However, the authorities' ability to use targeted hacking to gain access to external attack planners' mobile devices enabled the authorities to locate and eliminate many of the individuals responsible for instigating terrorism within the United States. The targeted hacking of high-profile targets' mobile devices can help to mitigate future "going dark" challenges.

When law enforcement hacks into a suspect's mobile device, the government can circumvent end-to-end encryption, read encrypted messages that are stored on the device, and develop and pursue potential leads against co-conspirators. Although the targeted hacking of mobile devices cannot be done at scale, the authorities can prioritize identifying and hacking those high-profile targets who are well-connected within a terrorist or criminal organization. After identifying individuals who are directly communicating with these targets, the authorities can utilize undercover sources to monitor and build criminal cases against U.S.-based co-conspirators. While international terrorists and other nefarious actors will continue to embrace new technologies

[175] Baker, *supra* note 18.

in their quest to “go dark,” the authorities have a potent arsenal of investigative tools that they can use to shine light on “going dark” threats.