Received: 6 July 2020 | Revised: 15 December 2020 | Accepted: 17 December 2020

DOI: 10.1111/1745-9133.12537

CRIMINOLOGY & Public Policy

ORIGINAL ARTICLE

The online behaviors of Islamic state terrorists in the United States

Joe Whittaker

Department of Criminology, College of Law, Swansea University, Swansea, Wales, UK

Correspondence
Joe Whittaker, Department of Criminology, College of Law, Swansea University, Richard Price Building, Swansea, SA2 8PP, Wales, UK.
Email: j.j.whittaker@swansea.ac.uk

Research Summary: This study offers an empirical insight into terrorists' use of the Internet. Although criminology has previously been quiet on this topic, behavior-based studies can aid in understanding the interactions between terrorists and their environments. Using a database of 231 US-based Islamic State terrorists, four important findings are offered: (1) This cohort utilized the Internet heavily for the purposes of both networking with co-ideologues and learning about their intended activity. (2) There is little reason to believe that these online interactions are replacing offline ones, as has previously been suggested. Rather, terrorists tend to operate in both domains. (3) Online activity seems to be similar across the sample, regardless of the number of co-offenders or the sophistication of attack. (4) There is reason to believe that using the Internet may be an impediment to terrorists' success.

Policy Implications: The findings of this study have two important policy implications. First, it is vital to understand the multiplicity of environments in which terrorists inhabit. Policy makers have tended to emphasize the online domain as particularly dangerous and ripe for exploitation. While this is understandable from one perspective, simplistic and monocausal explanations for radicalization must be avoided. Terrorists operate in both the online and offline domain and there is

little reason to believe that the former is replacing the latter. The two may offer different criminogenic inducements to would-be terrorists, and at times they may be inseparably intertwined. Second, when policy responses do focus on online interventions, it is vital to understand the unintended consequences. This is particularly the case for content removal, which may inadvertently be aiding terrorists and hampering law enforcement investigations.

KEYWORDS
Extremism, online radicalization, terrorism

1 | INTRODUCTION

The Internet has changed the nature of terrorism and by extension, policy responses to it. With this change, the notion of "online radicalization" has emerged which, despite being a nebulous concept (Macdonald & Whittaker, 2019), implies a causal relationship between interacting with extremist content and/or co-ideologues on the Internet and engaging in terrorist activity. Governments and security services around the world have signaled the Internet as the key domain by which individuals become involved in terrorism. The Federal Bureau of Investigation (FBI), for example, highlights both "the Internet" and "social media" as having the ability to recruit and radicalize individuals that are receptive to extremist messaging (Federal Bureau of Investigation, n.d.). Across the Atlantic, the U.K. Government has made clear that they consider online terror content a key feature in radicalizing individuals (HM Government, 2019) and have recently increased the penalty for viewing terrorist propaganda from 10 to 15 years (HM Parliament, 2019:Counter-Terrorism and Border Security Act, 2019). In Europe, countering online radicalization is repeatedly emphasized as a policy priority (for example, see: EU Council, 2014; European Commission, 2015; Europol, 2016).

As has been noted previously, criminology has been remarkably quiet on this subject (Gill, Corner, Thornton, & Conway, 2015), with scholarship instead coming more from political science and sociology (Neumann & Kleinmann, 2013). However, criminological methods and theory can add a great deal to the accumulated knowledge and policy perspectives. In recent years, both Gruenewald, Chermak, & Freilich (2013) and Gill et al. (2017) offer data-driven studies that disaggregate the complex roles and behaviors of different terrorists which assess how different individuals use the Internet in their eventual activity. Moreover, theories such as Situational Action Theory (SAT) can offer an explanation of how terrorists' interactions with their environments, analyzing how the latter can affect norm-based motivations of the former (Wikström & Bouhana, 2017).

The goal of this study is to empirically analyze the interactions between terrorists and the radical online milieu. What follows below is a brief discussion of the previous literature which is developed into one subresearch question and three sets of hypotheses: First, the extent to which terrorists are engaging online; second, whether online interactions are replacing the need for face-to-face ones; third, whether differences in terrorist plots result in the Internet being used more

heavily; and finally, questioning whether online interactions lower the chance of terrorist success. After this, the data and methodological considerations are outlined, which is followed by both descriptive and multivariate findings, before discussing two ways in which the findings affect policy decisions to counter violent extremism: Policy must not overrate the importance of interactions in the online environments at the expense of offline ones and where online interventions—such as content removal—are made, policy makers must be cognizant of the unintended consequences, such as stifling criminal investigations.

This research draws from a database of 231 Islamic State (IS) inspired terrorists that acted in the United States from the years 2012–2020. The sample includes a range of different types of terrorists, including: those that have been arrested and charged, and in some cases, convicted; those that successfully traveled abroad to join IS; as well as those that died conducting attacks. In doing so, it makes two important contributions to the field: First, despite the aforementioned articles, there is still a paucity of research which analyses the online antecedent and event behaviors of terrorists in a rigorous manner. The field is still dominated by research that assesses the "supply-side"—that is to say, the content with which would-be terrorists could engage (von Behr, Reding, Edwards, & Gribbon, 2013). This includes research on jihadist online magazines (Ingram, 2016a; Watkin & Looney, 2018), social network analyses of sympathizers (Berger & Morgan, 2015; Klausen, 2015), or even examinations into online meme culture (Huey, 2015). These are all undoubtedly important topics that help elucidate the online ecosystem, but one must take a causal inferential leap before understanding how this actually affects those plotting acts of terrorism. Fundamentally, we still know little about how terrorists use the Internet, or conversely, how using the Internet affects the pathways of terrorists.

Second, it is the first article to analyze the online behaviors of the cohort of American IS terrorists in a quantitative manner. The group presented one of the most sophisticated and tech-savvy propaganda operations of any terrorist group (Berger & Morgan, 2015; Ingram, 2016b; Winter, 2017). If there is an argument to be made that links the consumption of online terrorist content to engaging violently—an "online radicalization" thesis—this is a prime place to test it. Furthermore, it is one of the most contemporary threats. Previous studies have not, for example, coded for whether terrorists used end-to-end encryption or identified which social media platform was used, reflecting the current online criminogenic environment of which terrorists are part.

1.1 | The ubiquity of the internet

Terrorists' use of the Internet has been extremely well-documented within the academic literature in recent years. Studies have highlighted the reach that groups like IS have on social media platforms (Berger & Morgan, 2015; Carter, Maher, & Neumann, 2014; Fisher, 2015; Klausen, 2015), as well as the sophistication of their propaganda campaigns (Ingram, 2015; Winter, 2015b; Zelin, 2015), which are largely online, covering video (Botz-Bornstein, 2017; Lakomy, 2017a; Winter, 2015a), magazines (Ingram, 2016a; Novenario, 2016; Wilbur, 2017), and game iconography (Al-Rawi, 2016; Dauber, Robinson, Baslious, & Blair, 2019; Lakomy, 2017b). Beyond propaganda, the Internet has been highlighted as providing a means for instructing individuals to commit acts of terror (Alexander & Clifford, 2019; Hughes & Meleagrou-Hitchens, 2017; Reed & Ingram, 2017). Within the United States, studies have suggested that IS terrorists have used social media platforms heavily as part of their recruitment (Soufan Group, 2015; Vidino & Hughes, 2015).

Despite a wide literature, there are still relatively few data-driven studies that focus exclusively how individual terrorists have utilized the Internet. In their study on convicted British

terrorists from 1995–2015, Gill et al. (2017) find that 61% of cases showed evidence of online activity that related to the eventual plot. They also find that 54% used the Internet to learn about their eventual activity, which rises to 76% when the date range is narrowed to 2012–2015. Jensen, James, LaFree, Safer-Lichtenstein, and Yates (2018) find that U.S. terrorists' use of social media had grown steadily in recent years, up to around 75% in the years 2011–2016. Similarly, in their study on Canadian terrorists, Bastug, Douai, and Akca (2018) found that social media and the Internet played a role in at least 76% of their sample either during or after radicalization. In their qualitative study on 15 U.K.-based terrorists and extremists, von Behr, Reding, Edwards, and Gribbon (2013) found that the Internet was present in every case, acting as a key source of information, means of communication, and a platform for propaganda. In short, the small amount of empirical literature suggests that the vast majority of terrorists use the Internet as part of their plot. Therefore, this research seeks to add to this by questioning:

> *Subresearch Question 1: How frequently do terrorists in this sample use the Internet, and in what ways?*

1.2 | Online replacing offline

Considering the high use of the Internet by terrorists, it has also been claimed that the online domain is replacing the offline one as the primary venue in which individuals are radicalized. Sageman (2008a) noted that the Internet had transformed jihad; previously most terror networks were the result of face-to-face communications, but that the Internet had become the central hub of communications. He even went as far as to state that 'face-to-face radicalization has been replaced by online radicalization' (Sageman, 2008b, p. 41). Similar sentiments were offered by Weimann, who notes that the formal face-to-face networks no longer present the biggest threat, but instead, "the real threat now comes from the single individual, the 'lone wolf', living next door, radicalized on the internet, and plotting strikes in the dark" (Weimann, 2012). However, the difficulty in generating empirical data on terrorists' online behaviors led to an overreliance on anecdotal evidence when making these types of claims (Gill et al., 2015).

In recent years, there has been an increase in research that explores the relationship between online and offline dynamics. Gill et al. (2017) find that those that used the Internet to learn about their eventual activity were 4.39 times more likely to experience nonvirtual network activity and 3.17 times more likely to have engaged in nonvirtual place interaction. In their study of German foreign fighters, Reynolds and Hafez (2017) reject the hypothesis that online radicalization drives mobilization, instead finding greater support for the notion that offline social networks play a strong role. When discussing the consumption of propaganda, Baugut and Neumann (2019) find that the online and offline domain are inseparably intertwined. Many would watch online propaganda and then discuss it with their peers offline, and vice versa; discussions with friends would lead to further viewing online. This has led to a point in which most scholars in the field take the nuanced view that despite a prevalence of the Internet, in most cases, the Internet has not replaced nonvirtual interactions. Rather, online and offline dynamics tend to complement each other (Meleagrou-Hitchens & Kaderbhai, 2017). Given this, it is hypothesized that:

> *Hypothesis 1a*: Individuals that engage in an online network will be more likely to engage in a nonvirtual network than those that do not.

Hypothesis 1b: Individuals that learn about or plan their activity online will be more likely to also do so offline than those that do not.

1.3 | Opportunities for online learning

One might be inclined to think that the Internet benefits some would-be terrorists more than others. Those that conduct their plot alone could make up for the lack of co-offenders by learning about their activity online. In their study on lone actor terrorists, Gill, Corner, McKee, Hitchen, and Betley (2019) find that 82% learned about their attack using virtual sources. When comparing lone actors to their group-based counterparts, Gill et al. (2017) find that they were 2.64 times more likely to learn about their activity than those that were members of a cell, suggesting that "within a cell, there is a likely pooling of human, social, technical, and financial capital, the absence of which leads individuals to go online to learn how to conduct attacks and for other purposes" (Gill et al., 2017, p. 110). Given this, it is expected that:

Hypothesis 2a: Lone actor terrorists will be more likely to learn about or plan their activities than those that operate as part of a cell.

It is also expected that plots that require a degree of sophistication may rely more heavily on the Internet. For example, terrorists that conduct attacks using improvised explosive devices may be drawn to learn how to construct the bomb via the array of online instructional guides (Conway, Parker, & Looney, 2017; Reed & Ingram, 2017). Gill et al. (2017) find that those that planned to use improvised explosive devices (IEDs) were 3.34 times more likely to learn online than those that did not, which they argue reflects the ease with which individuals can obtain bomb-making instructions on the Internet. Conversely, they find that those who conducted more primitive attacks—such as unarmed assault—were significantly less likely to learn online. Similarly, attacks on targets with additional security, such as government, armed forces, or police may require a degree of online learning. Gill et al. (2017) find that those that plotted against a government target were 4.50 times more likely to learn via the Internet, which they attribute to the risk that is involved, requiring the need to utilize online affordances to prepare. Taken together, suggests that terrorists may learn take opportunities to facilitate more sophisticated attacks by learning online:

Hypothesis 2b: Individuals that plan to attack using IEDs are more likely to learn about their intended activities via the Internet than those that do not.

Hypothesis 2c: Individuals that plan to attack better defended targets are more likely to learn about their intended activities via the Internet than those that do not.

1.4 | Online activity as an impediment to success

The Internet can offer a host of network and operational benefits to would-be terrorists, such as cheap and immediate connection around the world which permit the transmission of propaganda and the ability to give and receive operational guidance. However, these benefits may be counterweighed by other factors that make using the Internet a net negative. Benson (2014)

argues that the Internet is not increasing terrorism because many of these operational benefits also benefit security services, which are able to use the Internet to conduct investigations; that terrorists inadvertently disclose information and that a large number of online platforms are easily subpoenaed. Jensen et al. (2018) find that terrorists that were active on social media had lower success rates than those that were not, suggesting that activity on these platforms helped security services identify them. Similarly, in Gill and Corner's (2015) study on U.S. and European-based lone actor terrorists, they find that those that learned about or planned their eventual activity online were significantly less likely to kill or injure anyone. It is therefore hypothesized that:

> *Hypothesis 3a*: Individuals that engage in an online network will be less likely to be successful than those that do not.

> *Hypothesis 3b*: Individuals that learn about or plan their event online will be less likely to be successful than those that do not.

However, not all levels of online interaction are created equal. In recent years, there have been a number of studies which discuss terrorists' utilization of end-to-end encrypted platforms, particularly as they have been pushed away from mainstream social media sites (Conway et al., 2018; Macdonald, Correia, & Watkin, 2019). These platforms offer a higher level of operational security and, by their nature, are not compliant to subpoena. One example of this is Telegram, which offers encrypted chats and has been noted as a platform on which IS were particularly active (Bloom, Tiflati, & Horgan, 2017; Clifford & Powell, 2019; Fisher, Prucha, & Winterbotham, 2019). Other online encrypted applications, such as WhatsApp, The Onion Router (TOR), and cryptocurrencies such as Bitcoin also offer an opportunity for would-be terrorists to evade law enforcement surveillance. Given this, it is expected that:

> *Hypothesis 3c*: The use of end-to-end encrypted platforms will increase as the range of event dates progresses.

> *Hypothesis 3d*: Individuals that utilize end-to-end encryption will be more likely to be successful than those that do not.

2 | METHODOLOGY

2.1 | Data

To analyze online behaviors, a database was created of all known terrorists acting on behalf of IS within the United States. This includes those that plotted attacks, those that attempted to travel to the caliphate, as well as individuals that played a more peripheral role, such as those that facilitated other's plots. Importantly, it includes both those that were successful and unsuccessful in their endeavors, so as not to rely on inferences on individuals that were apprehended, which may produce biasing effects.

To begin, a directory of terrorists was created by triangulating data sources, which is important because, as Behlendorf, Belur, and Kumar (2016) show, single data sources may miss a large

number of terrorist events, and may privilege attacks, particularly those that are larger and more newsworthy (Chermak, Freilich, Parkin, & Lynch, 2012). The directory was created using three approaches, first by collating the names on the George Washington University's *Program on Extremism* IS repository (Program on Extremism, n.d.), which details the criminal investigation of 205 IS terrorists in the United States. Second, two reports were consulted which outline and list 100 individuals that successfully or unsuccessfully traveled from the United States to join jihadist groups[1] (Hughes, Blackburn, & Mines, 2019; Meleagrou-Hitchens, Hughes, & Clifford, 2018). Finally, a list of terror attacks was generated from the Global Terrorism Database (GTD) by conducting searches for incidents in the United States from 2010–2018.[2] Because the GTD is focused on attacks rather than individual terrorists, names were identified from the entry or the sources attributed to it.

Having created a directory of terrorists, case files were created for each using a range of different sources. Firstly, U.S. court documents were utilized from repositories such as the *Program on Extremism's* IS repository, the Department of Justice Web site, the Investigative Project on Terrorism, as well as legal search engines such as Courtlistener. These made up the bulk of the database and include criminal complaints, affidavits, indictments, sentencing memoranda, and plea agreements. Secondly, data were collected via academic and gray literature which details terrorist behaviors such as case studies and qualitative database studies (e.g: Alexander, 2016; Clifford & Hughes, 2018; Klausen, 2016a, 2016b; Klausen, Campion, Needle, Nguyen, & Libretti, 2016). Finally, journalistic data were collected on each of the terrorists via news search engines such as LexisNexus News and Media Monitoring and Google News. To be included, sources must include new information beyond what was already in the case file, or the same information from a more reliable source. This was important for keeping the cases at a manageable size, as many terrorists had hundreds of articles written about them, but few added new information.

As with the creation of the directory, it is important to triangulate data via multiple sources as a reliance on a single type of source when build databases because it can lead to selectivity bias and produce unstable results (Behlendorf et al., 2016; Chermak et al., 2012). Where accounts conflicted, a hierarchy of data was used which deemed official transcripts most reliable, followed by affidavits, then local journalism, followed by national journalism (Gill, 2020). The reliability of academic and gray documents depended on which of these sources were cited.

It would have been beneficial to include data directly from terrorists' social media accounts. However, given the crackdown on terrorist accounts by social media platforms around 2016 (Conway, 2016), it was not possible to find this data in its primary form. However, many of the court documents detailed individuals' social media presence.

As Gill et al. correctly assert, it is important when analyzing the role of the Internet to not simply collect data for terrorists that are alleged to have radicalized online—this would be sampling the dependent variable; that is to say, "selecting cases only on the basis of a certain criteria being met, and only making use of these cases as evidence for the criteria" (Gill et al., 2015, p. 3). Rather, this study collects data for each identified IS terrorist to assure that the research is as representative as possible.

After collecting data, several inclusion and exclusion criteria were applied. To be deemed an IS terrorist, collecting data on those that were "formal" members is too narrow and would miss the large number of IS activity that is inspired rather than directed by the group (Europol, 2017). I follow the lead of the Profiles of Individual Radicalization in the United States (PIRUS) codebook, who define member broadly, even if the group does not acknowledge membership (START, 2018). Members are deemed to be IS inspired if they either explicitly support the group or if they consume ideological material. Moreover, their actions must be seen in furtherance of the group's goals. For

example, cases are excluded if they are judged to be motivated by other factors such as monetary gain.

Defining what constitutes as operating within the United States also needs clarification. To be included, the terrorist must have:

1. Been charged in the United States, or
2. Be a U.S. Citizen or permanent resident *and* resided in the United States until 5 years before their event, or
3. Resided in the United States at the time of their activity.

The directory includes those that acted from the earliest identified instance of an individual joining the group[3] in 2012 until data collection was completed in May of 2020. Given it is a point of contention as to whether Syrian Islamist group Jabhat al-Nusra was formally part of the group (or if it was, when it stopped being part of it), those that acted on behalf of that group were excluded. Finally, following the lead of Gill et al. (2015), individuals are excluded based on a lack of evidence. If there are no data (either online or offline) regarding the antecedent or event behaviors, then they are excluded (this amounted to 21 in total-mostly individuals included in a list of successful travelers with no other information). After applying these criteria, the database consists of 231 terrorist case studies. A random selection of 10% of these ($n = 23$), show that each case file is on average 5,600 words long (around 10 pages), with eight sources per file (an average of 2.8 criminal documents and 5.2 journalistic/academic/gray). However, the court documents were considerably richer in detail and longer, making up an average of around 3,500 words per file (63%), while the other documents made up around 2,100 words (37%).

2.2 | Coding

The study aims to build on the database research of Gill et al. (2017) by disaggregating online behaviors into two categories: interactions with co-ideologues and online learning and planning. Each of these are coded as a variable and split into subvariables identified by Gill et al. These include:

2.2.1 | Online network behaviors

a. Reinforcing prior beliefs; b) seeking legitimization; c) disseminating propaganda and providing material support; d) attack signaling; and e) attempting to recruit others.

2.2.2 | Online learning/planning

a. Accessing ideological content; b) opting for violence after witnessing something online; c) target selection; d) preparing an attack; and e) overcoming hurdles.

Several other demographic and event behaviors were also identified to assess whether those that used the Internet had different experiences from those that did not. These include: the number of terrorists that were involved in the execution of the plot; the role that the attacker played in

their event; if they plotted an attack, a categorization of the type of attack and its target; as well as arrest, conviction, and sentence details if applicable.

Beyond the Gill et al. (2017) study, several extra variables were also coded, including whether the individual used social media (and which platforms if so) and the use of end-to-end encryption. A data point is also created for whether the terrorist's plot is successful. In the case of those that plot an attack, this is fulfilled if the attack goes ahead (regardless of fatalities) and would-be travelers are deemed to be successful if they reach IS territory (rather than just leaving the US). Importantly, for those playing facilitative or financing roles, the success is dependent on whether the plot they are supporting is successful. In total, the codebook consists of 91 variables.

This article also follows Gill et al. (2017) as well as a number of other database studies (Clemmow, Bouhana, & Gill, 2020; Gill, Horgan, & Deckert, 2014; Silver, Horgan, & Gill, 2018) in coding most of the variables in a dichotomous manner—that is to say behaviors were coded as "present" or "not enough information to code as present" as opposed to a three-answer coding system of "Yes," "No," and "Not enough information" (e.g: Horgan, Shortland, Abbasciano, & Walsh, 2016; Lafree, Jensen, James, & Safer-Lichtenstein, 2018). The two-answer system is used by Gill et al. (2017), who justify it on the grounds that most open-sourcing reporting on terrorism does not detail what an individual *did not* do, and as such:

> Definitive "no" answers were a rarity (less than 5%) within the data collection process. This percentage was generally uniform across most variables. Usually these "no" answers only occurred in response to incorrect reporting earlier in the news cycle about a particular offender. (Gill et al. 2017, pp. 105–106)

They suggest that there are so few cases which confirm a negative that it would present findings heavily skewed against the true representation of these negatives, however, they do suggest that using multiple imputation methods may be possible if there were more definitive "No" answers in the data, positing that this level of granularity necessitates access to closed-source data (Gill et al. 2017).

Another reason for utilizing a dichotomous coding system is for reasons of comparison. There are still relatively few data-driven studies which seek to disaggregate the behaviors associated with online radicalization. As such, meaningful comparisons can be drawn between the findings of this dataset and that of Gill et al. (2017), hence the reason to utilize many of the same coding variables. To draw comparisons, it makes sense to utilize the same coding system.

All else being equal, it is good practice to minimize assumptions when coding. Safer-Lichtenstein, LaFree, and Loughran (2017) argue that research on terrorism has not thoroughly considered the reprecussions of assumptions around missing data, empirically demonstrating that different assumptions can create misleading findings that are not reflected when the assumptions are removed. In doing so, they call on researchers to be more transparent regarding coding assumptions. As such, this study is both limited by a lack of granular open-source data that describes what terrorists *did not* do, and is open about the assumptions that go with coding data dichotomously, that is, that missing data is more likely to be "No" than "Yes".

Another important assumption to note is the presence of undercover agents. In the US, security services regularly use undercover agents and informants as part of counterterror investigations (Greenberg & Weiner, 2017; Horgan et al., 2016). This raises the question of how to code behaviors in which an individual believes they are speaking to a co-ideologue but are, in fact, speaking to an agent. Given that this research's aim is to analyze terrorists' trajectories and group dynamics, network behaviors with undercover agents are included—it is more important to discern what

the individual did do and who they believed they were speaking to than to establish the number of "true" terrorists in a plot.

The data were coded by four individuals in June 2020. Before beginning, training was conducted in which the codebook and overall strategy was explained to the coders. The individuals independently coded the same case file and then met to compare and discuss results. Agreement was generally high and ambiguous points were clarified. After this, an intercoder reliability process was conducted in which 10 case files were selected and coded independently by each individual. The categorical variables ($n = 73$) were then tested for reliability. Some variables were omitted as to not unfairly skew to the data. For example, demographic data were collected including the country and (if applicable) state of birth. While it would be possible to treat these as categorical variables, agreement in the high number of categories would be misleadingly rewarded by statistical models (Joyce, 2013). Fleiss' kappa was calculated for agreement between the coders (730 observations by each coder in total), resulting in a kappa of 0.643 ($p = 0.000$) 95% CI (0.642–0.643). This is comfortably into what Landis and Koch (1977) describe as "Substantial Agreement," which is deemed acceptable from which to draw tentative conclusions.

The remaining cases were then split between the four coders and were completed independently. At the end of the coding period, 10 more cases were selected at random and coded by each individual. The Fleiss' kappa for these 730 observations was 0.710 ($p = 0.000$) 95% CI (0.709–0.711), suggesting that the raters increased in reliability over the coding process. The combined intercoder reliability for the 20 cases (1460 observations and around 9% of the sample) was $k = 0.675$ ($p = 0.000$) 95% CI (0.674–0.675), comfortably placing it in the "Substantial Agreement" category (Landis & Koch, 1977).

2.3 | Methods

Following the lead of Gruenewald, Chermak, and Freilich (2013), Gill and Corner (2015), and Gill et al. (2017), the descriptive findings are presented below. For the variables where missing data is permitted, such as age, occupation, and highest level of education, the total number of observations are included. This is followed by the online behaviors that are hypothesized above. Pearson's chi-square and Fisher's exact tests (where applicable) are used to compare categorical variables. The chi-square value, the p value, and the odds ratios of the significant correlates are presented.

2.4 | Limitations

There are several limitations to be noted. Most pertinently, secondary data can be problematic because the original author may have different goals to a researcher. For example, criminal complaints are drafted to secure a conviction rather than to outline the online and offline antecedent behaviors of terrorists, while journalists write stories that are newsworthy. Both write what is needed to fulfil their own goals and may omit information that could be important to researchers. However, given the methods of data collection outlined above, which provide varying types of data, this is likely mitigated to some extent because there are a number of different authors all aiming to fulfil their own goals, which should offer a balanced picture.

It is also important to note that there are varying levels of data for different types of terrorist. This is seen clearest in the difference between those that have been charged, and therefore have

court filings, and those that do not—that is, most successful travelers. The criminal justice information provides the richest data available and therefore, in many instances, far less is known about those that traveled to Iraq and Syria. Similarly, the newsworthiness of stories affected the amount of data available too. Some received far more attention, such as those that conducted successful large-scale attacks, or females, or white American converts to Islam. In comparison, those that committed crimes that did not involve an attack, such as facilitating or financing, gathered far less press coverage than their violent counterparts. Moreover, there is also a time consideration. Cases that occurred in 2020 and 2019 are likely to contain less information than those that took place in 2014 because there is more time for prosecutors or journalists to write their respective resources. These factors are important because a lack of coverage may cause a coder to incorrectly infer that they did not act in specific ways, which can potentially skew results. The decision to remove the cases for which there is very little information is, in part, informed by these two limitations.

This study collected data on all the known IS terrorists at the time of data collection in May 2020. However, it is likely that there are others that are not captured within the data sources available. This is shown by the slow but steady flow of new cases that are appearing from previous years, particularly of individuals that successfully traveled to the caliphate. For example, Omer Kuzu traveled from Houston, TX, to join IS in October 2014, but was only charged in the summer of 2019 after his capture (USA vs. Kuzu, 2020). There are undoubtedly terrorists that slip through the cracks and it may take the criminal justice system a while to catch up to these cases, and it is possible that many may not be identified, particularly if they died while travelling.

Finally, it also must be noted that there is a lack of comparable base rates with which to compare online behaviors against. Beyond general Internet penetration and usage of particular platforms, it is not easy to establish the ways in which nonterrorists use the Internet. Gill notes that "we have no grasp on the societal prevalence of the vast majority of online radicalisation indicators… Behaviours, like making threats online, are a far more difficult task to quantify" (Gill, 2016, pp. 6–7). Relatedly, there is no control group, meaning that the research is not able to discern the relationship between, for example, online behaviors and engaging on behalf of IS. As such, the findings must be interpreted against basic statistics such as total internet usage as well as compared against previous samples of terrorists, particularly that of Gill et al. (2017), from whom this study's codebook is drawn.

3 | RESULTS

3.1 | Demographic and event variables

Before discussing online behaviors, it is prudent to give an overview of the demographic details of the sample. The vast majority of the individuals in this sample are male (90%) and relatively young ($n = 223$ mean = 27, median = 26, mode = 20) but with a distribution between 15–55[4]. This is in keeping with previous studies on terrorist populations (Bakker, 2006; Gill et al., 2017; Horgan et al., 2016). With regards to family ($n = 151$), 42% of the sample were single, compared to 41% that were married with a further 11% having a partner and 7% were divorced. Finding an accurate comparison for this is difficult, but census data in 2018 suggested that 29% of the 18—34-year olds in the United States were married, which roughly aligns with the age range of most of this cohort. Twenty-nine percent had children, and 23% had a family member that also displayed a radical ideology.

The cohort is mostly toward the bottom end of the socioeconomic spectrum. Of the 186 individuals with employment information, 40% did not have a job[5] and a further 34% worked in the service or low-skilled sector. Similarly, in terms of education ($n = 141$), for two-thirds of the sample a high school diploma was the highest level of education completed, with a further 16% not achieving this, and 14% completing a university degree and 1% attaining a postgraduate qualification. This is somewhat lower than would be expected given the Muslim population in the United States, of whom 31% are college graduates (Pew Research Center, 2017).

A quarter of the sample converted to Islam from a different (or no) religion, which is similar to the 21% of US-based Muslims that are converts (Pew Research Center, 2017). Around 10% of the sample had previous military experience. The majority were not purported to suffer from mental health problems (77%); 10% were professionally diagnosed, while a further 13% being credibly speculated as having a condition (for example, by friends, family members or defense counsel). This is in line with the U.S. population, of whom one in five experience a mental illness each year (National Alliance on Mental Illness, n.d.). One in four had a previous criminal conviction of some kind, although only 15% of these 55 (eight in total) were terror-related offences; the vast majority could be better described as "petty crime", offering support to Basra, Neumann, and Brunner (2016) who argue that a number of terrorists have low-level criminal backgrounds, but a life in crime may have given them important skills such as understanding how to deal with law enforcement.

With regards to the terrorists' events, the date (i.e., the date of an attack/travel/arrest) were mostly around the back end of IS' peak (mean = Feb 27, 2016, median = September 17, 2015). Eighteen percent executed their plot alone without any support or facilitation and were therefore classified as lone actors while 24% conducted their plot alone but *with* outside guidance and were coded as solo actors. Fewer still (13%) acted as a dyad, while a plurality (45%) was operating as part of a group or cell of larger than two. Twenty-nine percent of individuals plotted an attack, while almost half (49%) either attempted to, or successfully, traveled to join IS. A smaller number played peripheral roles such as financier (17%), offering nonfinancial facilitative support (28%), or creating explosives (8%).

Only 39% of these plots were deemed to be successful, and the vast majority (83%) were arrested for their activity. At time of coding in June 2020, legal proceedings had been publicly announced against 197 (85%), with 60% of these individuals pleading guilty, 13% being found guilty at trial, and 27% having not faced trial or made a plea. The most common charge was material support to a foreign terrorist organization,[6] with which 147 individuals—three quarters of those that were charged. This is in line with previous research which has highlighted an increase in this charge in recent years; Berkell notes that material support far exceeds other crimes in IS-related cases due in large part to its broad interpretation spanning from low-level nonviolent conduct such as raising small amounts of money to providing oneself by way of traveling to the caliphate (Berkell, 2017). Other types of charges include making false statements to the FBI (13%), gun-related charges (12%), explosive-related (10%), crimes of violence such as murder and assault (10%), other terrorism-related charges (7%), obstruction of justice (4%), threat-based charges (4%), solicitation of violent crimes (3%), financial crimes (2%), citizenship-related (2%) and all other crimes (3%). 120 terrorists had been sentenced (52%) and the average is around 15 years (mean = 183 months, median = 178 months, mode = 180 months).[7]

3.2 | Online behaviors

Terrorists in this sample used the Internet overwhelmingly; it was present for either network activity or online learning in 92% of cases. Breaking this number down, over four-fifths interacted virtually with co-ideologues, including 55% that went online to reinforce their beliefs, often on social media platforms or online fora. Propaganda was disseminated online to co-ideologues by 36% of the sample, including jihadist magazines, execution videos and lectures. Interestingly, there was still a sizable crossover between IS propaganda and other jihadist groups. For example, while IS's *Dabiq* and *Rumiyah* magazines were disseminated among these networks, so too was al-Qaeda in the Arabian Peninsula's *Inspire* magazine. A similar number (38%) used the Internet to support others, including offering operational advice for travelers that sought to travel to Syria—such as which border town in Turkey to travel to or what to say to officials at Istanbul airport to avoid suspicion. Just under a third (29%) sought legitimization from a spiritual authority figure, while almost half (47%) attempted to recruit others to the movement, for example by soliciting funds or trying to convince people to engage in attacks.

The vast majority (80%) turned to social media to fulfil some part of their activity. When breaking these platforms down there are several interesting findings. Intuitively, the largest platforms appear the most frequently: Facebook ($n = 108$), Twitter (54), YouTube (50)—suggesting that, like most people, terrorists use the most popular platforms. However, despite Facebook being the most frequently used, fewer than 60% of social media users in the sample (and fewer than 50% overall) used the site. Furthermore, 28 different online platforms were identified, including messaging services and file hosting sites.[8] However, only around 20% of the sample utilized end-to-end encrypted technologies such as Telegram ($n = 14$), WhatsApp (10), and Surespot (6).

Eighty four percent used the Internet to learn about or plan their event online, including 70% that accessed ideological content. This includes formal IS material made by its media arms, including infamous videos such *Healing the Believer's Chests*—the immolation of Jordanian pilot Muath Safi Yousef al-Kasasbeh and or *The Flames of War*, as well as informal content such as sympathetic memes and gifs. Almost 60% used the Internet to prepare for their eventual activity, such as searching and booking flights for travel. For those that planned an attack ($n = 68$), 25% selected their target online. Eighteen percent cited something that they witnessed online as a motivation for action. These include pictures of dead Muslims (at the hands of both Syrian and Western forces) from conflicts dating back a number of years. Finally, around 7% used the Internet to overcome a hurdle in their plan, such as requesting funds from another party to finance a plot.

The data presented above clearly show that the Internet has become a central part of contemporary cases of terrorism in the United States. The sample used the internet for a wide range of antecedent and event behaviors and there is a wide ecology of online platforms.

It should be noted that this finding should not be altogether surprising. Benson (2014) notes that the Internet is the dominant mode of communication and it would be surprising if terrorists were not using the Internet. Around nine in 10 used the Internet as part of their plot, which matches similarly to the nine in 10 U.S. adults that use the Internet (Pew Research Center, 2019). Neumann also makes this point: "Like everyone else, they disseminate their ideas and promote their causes, they search for information, and they connect and communicate with like-minded people, often across great distances" (Neumann, 2013, p. 433). Even if the finding that most terrorists use the Internet is not surprising, the descriptive statistics offered above give an empirical snapshot of the wide array of online behaviors and Internet ecosystem inhabited by jihadists.

TABLE 1 Online network activity behavioral correlates

Online network activity behavioral correlates			
Behavior	**χ^2 value**	***p* value (Sig.)**	**Odds ratio**
Offline network interaction	32.334	0.000	6.952
Try to recruit others offline	7.693	0.002	10.318
Learn/plan offline	6.084	0.011	2.319

TABLE 2 Online learning/planning behavioral correlates

Learn/plan online behavioral correlates			
Behavior	**χ^2 value**	***p* value (Sig.)**	**Odds ratio**
Learn/plan offline	14.997	0.000	4.075
Try to recruit others offline	4.376	0.024	4.296
Attended in person meeting with co-ideologues	12.807	0.000	4.009

3.3 | Online replacing offline

Descriptive findings show that more than nine in 10 terrorists in this sample use the Internet to learn about their activity or interact virtually and that they do this in several different ways. It may, therefore, be tempting to conclude that the Internet has become the primary domain for terrorist activity. To assess whether this is the case, a series of bivariate tests are conducted which analyze the experiences of individuals that used the Internet against those that did not.

Table 1 shows that those that engaged in an online network were 6.95 times more likely to also engage in an offline one too. As well as this, those that engaged in an online network were 10.32 times more likely to attempt to recruit others offline. Take the example of Mahmoud Amin Mohamed Elhassan, who in the offline domain associated with Joseph Hassan Farrokh and facilitated his travel to Syria, while simultaneously kept online contact with radical cleric Mohammed Ali al Jazouly (USA vs. Elhassan, 2017). Similarly, those that engaged in a virtual network were also 2.32 times more likely to learn about or plan their event offline too. Emmanuel Lutchman was in contact with Abu Sa'ad Al-Sudani, who was located in Syria, who directed him in his plot to attack a bar in Rochester, NY on New Year's Eve 2015. Lutchman also planned his attack via a series of meetings with three undercover agents before his eventual arrest (USA vs. Lutchman, 2015). These examples are relatively typical—even though most are part of an online network of co-ideologues, they are also engaging in the offline domain too.

Table 2 shows that terrorists that learned about or planned their activity online were also significantly more likely—4.08 times—to learn about or plan their activities offline. Omar Mateen, the Pulse Nightclub shooter, conducted physical surveillance of a number of targets around Orlando in his car over a week in advance of the attack, but also in the minutes directly preceding the attack, Googled "downtown Orlando nightclubs" (USA vs. Salman, 2018). Although there is no significance with offline network interaction on the whole, two of the subvariables (attempting to recruit others offline and attending an in-person meeting) are significantly correlated. Again, despite the operational benefits that the Internet can provide, terrorists tend to operate within both domains.

TABLE 3 Lone actor behavioral correlates

Lone actor behavioral correlates			
Behavior	**χ^2 Value**	***p* Value (Sig.)**	**Odds Ratio**
Learn/plan online	11.357	0.002	0.279
Prepare event online	4.338	0.029	0.488
Learn/plan offline	6.923	0.007	0.404
Attacker	11.686	0.001	3.195
Successful event	8.426	0.004	2.715
Deadly attack	8.267	0.009	9.000

The results suggest that there is a strong relationship between online behaviors and offline ones. Rather than replacing the offline domain, both virtual network activities and online learning are strongly associated with nonvirtual activities. As such, *both Hypothesis 1a and 1b are supported*.

3.4 | Opportunities for online learning

It was expected that certain subsets of terrorists would be more likely to utilize the Internet to learn about their plots than others given the affordances that the Internet can offer. However, the data do not bear this out. Not only were lone actors not more likely to learn about their intended activity online, but they were significantly less likely to do so. Furthermore, this is accounted for by lone actor using the internet for preparatory activities rather than ideological learning (as can be seen in Table 3). Given the fact that the Internet affords an opportunity to supplement a lack of operational expertise, this is a surprising finding. One possible explanation is that several of the lone actors in the sample appeared to attack on the spur of the moment rather than planning their event. Individuals such as Edward Archer (Associated Press, 2018), Mahad Abdiaziz Abdiraham (USA vs. Abdiraham, 2017), and Esteban Santiago (Sanchez, 2017) displayed little-to-no preparatory behaviors in either domain (lone actors were also significantly less likely to learn or plan offline). As such, *Hypothesis 2a is not supported* in this sample. Interestingly, despite a lack of online learning, lone actors, who overwhelming plotted attacks, were 2.72 times more likely to be successful and nine times more likely to conduct a deadly attack. This may suggest that these types of spur of the moment attacks may provide a substantial risk due to their difficulty in detection.

When looking at the subset of attackers, it was expected that those that plotted more sophisticated attacks would utilize the Internet more than those that did not. However, this does not seem to be the case. Those that plotted to conduct attacks involving IEDs were no more likely to learn about their event online, nor were there any significant correlates between any of the methods of attack (unarmed assault, armed assault, and vehicle-based attack) and learning online, meaning that *Hypothesis 2b is not supported*. Furthermore, there is no discernible relationship between the target of the attack and online learning. It was hypothesized that targets with greater security may require a higher degree of learning, but attacks on government, police, and military targets each had no significance with virtual learning. Moreover, if these categories are grouped together as "Hard Targets," the new category also holds no significance with online learning. As a result, *Hypothesis 2c is not supported*.

Despite well-reasoned hypotheses developed from the academic literature, specific subsets of terrorists do not seem to be more likely to learn about their activity online. There does not seem to

TABLE 4 Online network activity success correlates

Online network activity success correlates			
Behavior	**χ^2 Value**	***p* Value (Sig.)**	**Odds ratio**
Successful event	9.554	0.002	0.348
Known to security services	27.382	0.000	6.043
Arrested	4.998	0.026	2.400

TABLE 5 Online learning/planning success correlates

Learn/plan online success correlates			
Behavior	**χ^2 Value**	***p* Value (Sig.)**	**Odds ratio**
Successful event	20.314	0.000	0.193
Known to security services	16.331	0.000	4.158
Arrested	9.731	0.003	3.340

be an obvious reason for why this is the case. Digging deeper into the subvariables associated with online learning and planning, the same lack of correlates holds for: online preparatory behaviors, selecting targets, overcoming hurdles, and accessing ideological content. Perhaps the best explanation for this is, as established above, that the Internet is so ubiquitous that it is used in almost every case for learning and planning, regardless of whether the individual acts alone or plots a sophisticated attack.

4 | ONLINE ACTIVITY AS AN IMPEDIMENT TO SUCCESS

The descriptive results showed that terrorists in this sample utilized the Internet for a range of different network and learning behaviors. Despite the technical affordances that the Internet can offer, it may act as an impediment to success. Table 4 shows that the individuals that engaged in an online network were 0.35 times as likely to succeed in their plot as those that did not. The case of Heather Coffman represents a relatively typical example. Coffman was sentenced to four and half years for facilitating an accomplice's travel to Syria and her social media accounts alerted her attention to law enforcement because they contained several expressions of support for IS. For example, her Facebook profile picture included an image of armed men with the text "VIRTUES OF THE MUJIHADEEN" and IS's black standard flag. After the FBI was notified to the presence of Coffman, they deployed an undercover agent, for whom Coffman would also attempt to facilitate travel (USA vs. Coffman, 2015). Coffman is no outlier in this sample; many were identified by recklessly displaying their ideology at the expense of operational security. Terrorists that engaged in an online network were also 6.04 times more likely to be previously known to the security services and 2.40 times more likely to be arrested for their activity. As a result, *Hypothesis 3a is supported*.

A similar story can be seen via those that learned about or planned their activity online; individuals that learned virtually were 0.19 times as likely to succeed as those that did not, as well as being 4.12 times more likely to be known to security services, and 3.34 times more likely to be arrested for their actions (Table 5). When investigating a case, if the FBI deems it to be serious enough, it can open a "full investigation" which allows it to conduct full searches with a warrant or court order (Ellingsen, 2016). This can include online messaging history, such as in the case

TABLE 6 End-to-end encryption usage over time

End-to-end encryption over time			
Behavior	**χ^2 Value**	***p* Value (Sig.)**	**Odds ratio**
All years	21.927	0.003	*
2013	3.519	0.047	0.784
2019	11.902	0.002	4.380

*Odds ratio only be computed for 2 × 2 tables.

of Said Azzam Mohamad Rahim—after the FBI became aware of his support for IS, executed a search warrant on his social media accounts which illustrated key details of Rahim's case (USA vs. Rahim, 2017). Unlike those engaging in an online network who recklessly alert law enforcement to them, this may work the opposite way, using methods of investigation that rely on terrorists using sites that comply with subpoenas and have access to user data—that is, not end-to-end encrypted platforms. Given this, *Hypothesis 3b is supported*.

To test whether the use of end-to-end encrypted platforms increased over time, the event date variables were recoded into categorical ones (i.e., 2012, 2013, 2014, and so on) and were subjected to chi-square tests (and Fisher's exact where appropriate) against the dichotomous variable of end-to-end encryption (Table 6). When considering each of the years together, there is a significant difference between the individual years ($p = 0.003$). However, this is accounted for almost entirely by events in the year 2019, in which terrorists were 4.38 times more likely to use end-to-end encryption; in no other year were they more likely to use it. In the year 2013, they were significantly less likely to use it. Taken together, *these findings do support Hypothesis 3c*—there is an increase over time—but perhaps is not the widespread migration from around 2016 that is often posited (Macdonald et al., 2019; Prucha, 2016).

Finally, with regards to the use of end-to-end encrypted platforms, there is no significant relationship with the successfulness of terrorists' events, and therefore *Hypothesis 3d is not supported*. It could be interpreted that the lack of a negative correlation—which exists for other online behaviors—suggests that it is a *safer* way of acting on the Internet, given the hostile ecosystem that would-be jihadist terrorists find themselves. This seems to make sense, although end-to-end encryption does offer operational security benefits, it is not impenetrable to security services. Rather, investigations utilize undercover agents that are invited by ideologues into encrypted messenger services, such as in the case of Tayyab Tahir Ismail, in which a substantial amount of evidence was gathered from an FBI undercover employee, which the prosecutors were able to triangulate with Ismail's Google search data (USA vs. Ismail, 2018). This is an interesting null finding and requires further investigation in future research.

Given that the chi-square analyses find that terrorists that engage in an online network and learn or plan online are less likely to be successful, it is prudent to explore whether a type of online behavior predicts success. Furthermore, given that the use of end-to-end encryption may be a safer way of terrorists to communicate, it is worthwhile to establish whether it mitigates any predictive effect. To do this, a binary logistic regression is conducted with event success as the dependent variable. The independent variables are acting in an online network, learning or planning online, and the use of end-to-end encryption. The terrorist being a lone actor was chosen as the control variable as it holds a significant positive correlation with event success ($\chi^2 = 8.426$, $p = 0.004$, OR = 2.715) which seems to make logical sense given that lone actors "pose a threat that is particularly difficult to detect and preempt because of their lack of operational ties to co-conspirators" (Schuurman et al., 2018, p.1,198). Given that the online behaviors are significantly

TABLE 7 Event success binary logistic regression

Event success binary logistic regression				
Behavior	**B(SE)**	**D*f***	***p* Value (Sig.)**	**Exp(B)**
Online network interaction	0.075(0.469)	1	0.873	1.078
Learn/plan online	1.478(0.442)	1	0.001	4.386
End-to-end encryption	0.014(0.367)	1	0.971	1.014
Lone actor	−0.723(0.418)	1	0.084	0.486
Constant	−0.154(0.483)	1	0.749	0.857

correlated, tests for multicollinearity are undertaken by running regression diagnostics. In each iteration the variance inflation factor (VIF) is <1.7, suggesting that there are no biasing effects. Given that there are more instances of event failure (61%) than success (39%), the former is selected as the baseline, this means that a positive odds ratio — Exp(B) — represents the chances of failure. The results show that learning or planning one's event online is predictive of event success, even when controlling for factors such as the use of end-to-end encryption and the terrorist being a lone actor (Table 7). As suggested above, the causative nature of this is unclear; it is possible that it is terrorists acting recklessly or it could suggest that law enforcement have greater reach to investigate online activities.

5 | POLICY DISCUSSION AND CONCLUSION

Studying the environments in which terrorists interact is vital to understanding why these crimes occur and therefore shapes methods to counter it. Wikström and Bouhana (2017) propose that Situational Action Theory (SAT) can help to explain terrorism by examining the criminogenic inducements of environments which can affect a would-be terrorist's norm-based motivations. The types of environments in which individuals find themselves are dictated by processes of both social selection (for example, residence and socioeconomic status) as well as self-selection—where individuals choose to spend their time, such as political rallies or on the Internet (Bouhana, 2019). The interplay between the individual and environment help explain why individuals perceive their actions as morally acceptable or fail to adhere to personal morals when incited to break them (Wikström & Bouhana, 2017). The findings of this research offer two important insights into understanding such environments, which in turn informs policy discussion: First, it is necessary to understand the multitude of environments in which terrorists inhabit rather than privileging the online milieu, and secondly, to recognize that interventions to counter extremist activity in the online environment may have unintended consequences on law enforcement investigations.

5.1 | Understanding a multitude of environments and the interplay between them

In contemporary cases of IS-related terrorism in the US, the use of the Internet is high for several observable behaviors. It is, perhaps, unsurprising that policy makers have concluded that the Internet poses some kind of radicalizing agency. If case after case shows that terrorists were networking with co-ideologues online or used the Internet to plan their event, it seems reasonable to assume that it plays a driving role. However, findings here and elsewhere suggest that this is

misplaced— actors engage in both online and offline environments (Gill, 2016; Gill & Corner, 2015; Gill et al., 2017; Reynolds & Hafez, 2017; von Behr et al., 2013). Corner, Bouhana, and Gill note that 'public discourse, government bodies, and the media all reinforce the perception of the danger posed by online environments, which are presumed to be ripe for exploitation by radicalizing agents' (Corner et al., 2018, p. 28). Take, for example, the United Kingdom, which has recently published its Online Harms White Paper, which leans heavily on online terrorist content without giving due to the offline radical milieu (Bishop, Looney, Macdonald, Pearson, & Whittaker, 2019; HM Government, 2019). As long as policy responses are fixated to a specific location rather than taking in a multiplicity of environments, then simplistic monocausal explanations will continue to be propagated. In short, if policy keeps dictating that people look for radicalization on the Internet, they will find it.

This melding of the online and offline environment lends further credence to the argument that it is a false dichotomy, as is suggested by Gill et al. (2017). Conway (2017) makes an important point that this false dichotomy implies that there is a "real world" in which harm can be done and a virtual world consisting only of 1s or 0s. This distinction is reminiscent of the 1990s and early 2000s in which "going online" was a deliberate act. Today, this is not reflective of reality. The majority of the 250 million smartphone users in the United States (Statista, 2019), which utilize push notifications, are always online and social media platforms represent an integral part of the offline lived experience. A number of the cells within this sample held "viewing parties" in which members of the sample would gather, socialize, and watch videos of online IS propaganda (see: Goldman, 2015; Koerner, 2017;), while Haris Qamar went to shops to purchase Google Play gift cards, which were sent via online encrypted messaging services to what he believed were IS fighters in the caliphate (USA vs. Qamar, 2016). Drawing a distinction between online and offline behaviors is not easy and it is important to understand the intertwined nature of the two domains; a focus primarily on online activities will miss the environmental interactions which shape terrorists' dynamics. In the example of the "viewing parties," a focus on the online propaganda rather than the offline interaction in watching and discussing it together may lead policy makers to overinflate the importance of the former, and as a result, missing the criminogenic inducements that are offered by the latter.

5.2 | Policy responses that alter the online radical milieu may have unintended consequences

Although it is important not to overrate the importance of the online environment, the findings of this research do show terrorists overwhelmingly interact on the Internet. In recent years, there has been a policy move toward the removal of terror content, particularly in Europe where lawmakers are clear that social media companies will be held accountable for terror content on their platforms. The EU Parliament recently passed a proposal that compels companies to remove terror content within one hour of law enforcement notification or face a fine of up to 4% of global turnover (EU Parliament, 2019). In the United Kingdom, the Online Harms White Paper suggests several regulatory tactics, including the blocking of platforms and members of senior management may be held legally accountable (HM Government, 2019). In the aftermath of the terror attack in Christchurch, New Zealand in 2019, which was live streamed on Facebook, a total of 48 nation states, three international institutions, and eight tech companies, have signed up to the "Christchurch Call," whose underlying goal is to eliminate terrorist and extremist content from the Internet (Christchurch Call, nd). This is important in the context of the US, who is not

signed up to the Call. Terrorist content, including instructional material, has typically not passed the "true threat" test of Brandenburg versus Ohio (1969) (Raban, 2018). While the United States sticks to its First Amendment principles, much of the rest of the world is moving in the opposite direction. However, the Internet cannot easily be divided up to reflect these policy differences; responses on the Internet have transnational effects. It is likely that, as long as the incentives are heavily aligned—such as heavy fines, geo-blocking, or personal accountability for executives—the more restrictive policy is likely to be adopted by platforms.

Despite the concern from policy makers over the threat of terror content, this research shows that online activities may actually aid law enforcement in apprehending would-be terrorists, supporting the findings of Jensen et al. (2018). Many of the terrorists in this sample recklessly telegraphed their ideological leanings to law enforcement and the most frequently used platforms (which coincidentally are the platforms that have taken the greatest steps to remove content) were able to aid law enforcement by complying with subpoena requests. This could result in an unintended consequence of forcing would-be terrorists to act in environments that provide a greater degree of security. This could be by the utilization of end-to-end encrypted platforms (although the findings here only partially support that this is a safer way of operating), or by forgoing online activity altogether. Research has repeatedly shown that terrorists are adaptive to hostile online ecosystems (Bloom et al., 2017; Fisher et al., 2019; Weimann, 2018). It is important to understand how policy positions such as the removal of content affect the interactions between individuals and their environment. At first glance, it may seem that removing accounts and materials reduces exposure to interactions which encourage and facilitate terrorism. However, this may not be the case, it may be spurring innovation and sending would-be terrorists to platforms in which communities are more radical, are not compliant with subpoena request, and cannot be targeted by strategic communication campaigns.

It should be underscored that this is not a call for a return to the online Wild West in which content was rarely, if ever, removed. Remedying the utility of removing content against its consequences is not an easy problem to resolve because there are substantial benefits to driving terrorists from the mainstream platforms—IS was severely degraded in its ability reach to potentially interested audiences. Berger and Morgan (2015) found that in late 2014, there were between 46,000–70,000 sympathizers on Twitter alone, but in a follow up study a year later, fewer than 3,000 accounts were readily discoverable (Berger & Perez, 2016). More recent studies have painted a similar picture, suggesting that social media platforms are adept at removing content and accounts promoting IS content (Conway et al., 2018; Grinnell, Macdonald, & Mair, 2017). For their part, IS supporters have been clear that they would rather stay on mainstream platforms:

> Telegram is not a media platform for dawa [proselytization] to all Muslims and the West. No one will enter your channel except for the Ansar [supporters] who already know the truth… Rarely would you find someone from the general public following you. That's why our main platform is where the General Public is found. Like on Twitter and Facebook. (MEMRI, Quoted in: Clifford & Powell, 2019, p. 9)

Simply put, degrading IS and other terrorist groups on large platforms limit their ability to recruit new members. Ultimately, there are many factors involved in the online regulation debate, many of which go beyond the scope of this research (for example, freedom of speech and rule of law issues). However, this study shows that like most other ecosystems, the online radical milieu is a fragile one and altering it may produce unintended consequences that affect the relationship between individuals and their environment.

This study has sought to empirically analyze terrorists' use of the Internet and assess the ramifications online behaviors. This can be expanded upon in future by introducing a qualitative analysis which is able to dig deeper into these behaviors; a quantitative coding system will invariably paint with a broad brush and not capture certain differences. Given the findings surround use of the Internet and success, it would be fruitful to explore the varying degrees of sophistication. For example, this study has discussed the use of end-to-end encryption, but this could be expanded upon substantially by exploring the ways terrorists countered the ever-growing hostile online ecosystem, like the use of fake names, VPNs, multiple accounts and so on. Conducting both qualitative and quantitative analyses in this manner will help to provide a much clearer picture of the contemporary online terrorist threat.

ACKNOWLEDGMENTS

I am deeply grateful to Angharad Devereux, Chamin Herath, Ben O'Sullivan, and Dylan Samuel for their hard work coding the data that were used in this study. I also with to thank my friend Audrey Alexander for her valuable feedback on an earlier draft, and my Ph.D. advisors, who provided feedback throughout the project: Lella Nouri, Stuart Macdonald, Alastair Reed, and Edwin Bakker.

CONFLICT OF INTEREST STATEMENT

The author confirms that he has no conflict of interest to declare.

ORCID

Joe Whittaker https://orcid.org/0000-0001-7342-6369

ENDNOTES

[1] The first report outlines 64 individuals that successfully traveled to Iraq or Syria, but not exclusively to IS (Meleagrou-Hitchens et al., 2018), while the latter summarizes 36 cases of individuals that either successfully or unsuccessfully traveled to jihadist groups *not* in Iraq or Syria (Hughes et al., 2019). All of these entries were tested against the inclusion and exclusion criteria.

[2] Many cases in the GTD are not attributed to IS because they are not formally directed or claimed by the group. As such, a search was run for all incidents of terrorism within the United States between 2005 and 2018 using the widest definition of terrorism "The act must be aimed at attaining a political, economic, religious, or social goal," which returned 365 responses, of which each case was tested against the inclusion and exclusion criteria.

[3] Joining the group directly from the United States to IS. Some left the country much earlier before eventually joining the group. These were excluded.

[4] The sample includes only three individuals under the age of 18 because they were tried as adults. The standard procedure for minors is to seal the document and leave the individual unnamed. Minors that successfully traveled to the Iraq or Syria were not included. This means that the distribution and average age is probably somewhat lower than presented above.

[5] It should be noted that this should not be compared with official U.S. unemployment rates, which track those who are not employed but are willing and able to work, while this study coded for affirmation of or lack of employment.

[6] This includes conspiracy to provide material support and attempt to provide material support.

[7] I follow the lead of the George Washington University's Program on Extremism, who record life sentences (in this sample $n = 6$) as 470 months, as per United States Sentencing Commission practice (Schmitt and Konfrst, 2015)

[8] In some instances, the name of the platform is redacted in the court filings. In these cases, the platform is not included.

REFERENCES

Al-Rawi, A. (2016). Video games, terrorism, and ISIS's Jihad 3.0. *Terrorism and Political Violence*, 1–21. https://doi.org/10.1080/09546553.2016.1207633

Alexander, A. (2016). Cruel intentions: Female jihadists in America. Report. Washington, DC: GW Program on Extremism.

Alexander, A., & Clifford, B. (2019). Doxing and defacements: Examining the Islamic state's hacking capabilities. *CTC Sentinel*, *12*(4), 22–28.

Associated Press, (2018, February 1). Man accused of shooting Philly officer convicted of attempted murder, *ABC News*. https://6abc.com/man-accused-of-shooting-philly-officer-found-guilty/3018942/

Bakker, E. (2006). *Jihadi terrorists in Europe: Their characteristics and the circumstances in which they joined the jihad*. The Hague, The Netherlands: Clingendael Institue.

Basra, R., Neumann, P., & Brunner, C. (2016). *Criminal pasts, terrorist futures: European jihadists and the new crime-terror nexus*. Report. London, UK: ICSR.

Bastug, M. F., Douai, A., & Akca, D. (2018). Exploring the "demand side" of online radicalization: Evidence from the Canadian context. *Studies in Conflict & Terrorism*, *43*(7), 616–637. https://doi.org/10.1080/1057610X.2018.1494409

Baugut, P., & Neumann, K. (2019). Online propaganda use during Islamist radicalization. *Information Communication and Society*, 1–23. https://doi.org/10.1080/1369118X.2019.1594333

Behlendorf, B., Belur, J., & Kumar, S. (2016). Peering through the kaleidoscope: Variation and validity in data collection on terrorist attacks. *Studies in Conflict and Terrorism*, *39*(7–8), 641–667. https://doi.org/10.1080/1057610X.2016.1141004

Benson, D. C. (2014). Why the Internet is not increasing terrorism. *Security Studies*, *23*(2), 293–328. https://doi.org/10.1080/09636412.2014.905353

Berger, J. M., & Morgan, J. (2015). The ISIS twitter census: Defining and describing the population of ISIS supporters on twitter. The Brookings Project on U.S. Relations with the Islamic World. Analysis Paper.

Berger, J. M., & Perez, H. (2016). *The Islamic state's diminishing returns on Twitter: How suspensions are limiting the social networks of English-speaking ISIS supporters*. Washington, DC: George Washington University: Program on Extremism, 1–20. Retrieved from https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/Berger_Occasional_Paper.pdf

Berkell, K. (2017). Risk reduction in terrorism cases: Sentencing and the post- conviction environment. *Journal for Deradicalization*, *13*, 276–341.

Bishop, P., Looney, S., Macdonald, S., Pearson, E., & Whittaker, J. (2019). Response to the Online Harms White Paper. *Cyber Threats Research Centre*. https://doi.org/10.11588/heidok.00005826

Bloom, M., Tiflati, H., & Horgan, J. (2017). Navigating ISIS's preferred platform: Telegram. *Terrorism and Political Violence*, 1–13. https://doi.org/10.1080/09546553.2017.1339695

Botz-Bornstein, T. (2017). The "futurist" aesthetics of ISIS. *Journal of Aesthetics and Culture*, *9*(1), 1271528. https://doi.org/10.1080/20004214.2017.1271528

Bouhana, N. (2019). The moral ecology of extremism: A systemic perspective. London, UK: UCL Department of Security and Crime Science. Prepared for the UK Commission for Countering Extremism.

Carter, J., Maher, S., & Neumann, P. (2014). *#Greenbirds: Measuring importance and influence in Syrian foreign fighter networks*. Report. London, UK: The International Centre for the Study of Radicalisation and Political Violence.

Chermak, S., Freilich, J. D., Parkin, W. S., & Lynch, J. P. (2012). American terrorism and extremist crime data sources and selectivity bias: An investigation focusing on homicide events committed by far-right extremists. *Journal of Quantitative Criminology*, *28*(1), 191–218. https://doi.org/10.1007/s10940-011-9156-4

Christchurch Call, (n.d.). *Supporters*. https://www.christchurchcall.com/supporters.html

Clemmow, C., Bouhana, N., & Gill, P. (2020). Analyzing person-exposure patterns in lone-actor terrorism: Implications for threat assessment and intelligence gathering. *Criminology & Public Policy*. https://doi.org/10.1111/1745-9133.12466

Clifford, B., & Hughes, S. (2018). United States v. Aws Mohammed Younis al-Jayab: A case study on transnational prosecutions of jihadi foreign fighter networks. *CTC Sentinel*, *11*(1), 26–30.

Clifford, B., & Powell, H. (2019). Encrypted extremism: Inside the English-speaking Islamic state ecosystem on telegram. Report. Washington, DC: Program on Extremism.

Conway, M. (2016). Violent extremism and terrorism online in 2016: The year in review. Report, (December). Vox Pol Publications. https://www.voxpol.eu/download/vox-pol_publication/Year-in-Review-2018.pdf

Conway, M. (2017). Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research. *Studies in Conflict & Terrorism*, *40*(1), 77–98

Conway, M., Khawaja, M., Lakhani, S., Reffin, J., Robertson, A., & Weir, D. (2018). Disrupting Daesh: Measuring takedown of online terrorist material and its impacts. *Studies in Conflict and Terrorism*, *42*(1–2), 141–160. https://doi.org/10.1080/1057610X.2018.1513984

Conway, M., Parker, J., & Looney, S. (2017). Online jihadi instructional content: The role of magazines. In L. Jarvis & O. Lehane (Eds.), *Terrorists' use of the internet: Assessment and response* (pp. 182–193). Amsterdam: The Netherlands: IOS Press.

Corner, E., Bouhana, N., & Gill, P. (2018). The multifinality of vulnerability indicators in lone-actor terrorists. *Psychology, Crime and Law*, *25*(2), 111–132. https://doi.org/10.1080/1068316X.2018.1503664

Council of the European Union. (2014). Revised EU strategy for combatting radicalisation and recruitment to terrorism. 9956/14. Brussels, Belgium: Council of the European Union. Retrieved from https://data.consilium.europa.eu/doc/document/ST-9956-2014-INIT/en/pdf

Dauber, C. E., Robinson, M. D., Baslious, J. J., & Blair, A. G. (2019). Call of duty: Jihad – How the video game motif has migrated downstream from Islamic state propaganda videos. *Perspectives on Terrorism*, *13*(3), 17–31.

Ellingsen, N. (2016, June 20). The life cycle of an FBI Investigation. *Lawfare Blog*. https://www.lawfareblog.com/life-cycle-fbi-terrorism-investigation.

European Commission. (2015). The European Agenda on Security. Com. 185.

European Parliament. (2019). *Terrorist content online should be removed within one hour, says EP*. April 17. http://www.europarl.europa.eu/news/en/pressroom/20190410IPR37571/terrorist-content-online-should-be-removed-within-one-hour-saysep.

Europol. (2016). *Terrorism situation and trend report (TE-SAT) 2016*. The Hague, The Netherlands: European Police Office.

Europol. (2017). *Terrorism situation and trend report (TE-SAT) 2017*. The Hague, The Netherlands: European Police Office.

Federal Bureau of Investigation. (n.d). What we investigate – Terrorism. Retrived from https://www.fbi.gov/investigate/terrorism.

Fisher, A. (2015). Swarmcast: How jihadist networks maintain a persistent online presence. *Perspectives on Terrorism*, *9*(3), 3–20.

Fisher, A., Prucha, N., & Winterbotham, E. (2019). Mapping the jihadist information ecosystem: Towards the next generation of disruption capability. *Global Research Network on Terrorism and Technology*, (6).

Gill, P. (2016). Online behaviours of convicted terrorists. Vox Pol.

Gill, P. (2020, February). The data collection challenge: Experiences studying lone-actor terrorism. Washington, DC: RESOLVE Network.

Gill, P., & Corner, E. (2015). Lone actor terrorist use of the internet and behavioural correlates. In L. Jarvis, S. Macdonald, & T. M. Chen (Eds.), *Terrorism online: Politics law and technology* (pp. 35–53). Abingdon, UK: Routledge.

Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M., & Horgan, J. (2017). Terrorist use of the internet by the numbers: Quantifying behaviors, patterns, and processes. *Criminology and Public Policy*, *16*(1), 99–117. https://doi.org/10.1111/1745-9133.12249

Gill, P., Corner, E., McKee, A., Hitchen, P., & Betley, P. (2019). What do closed source data tell us about lone actor terrorist behavior? A research note. *Terrorism and Political Violence*, 1–8. https://doi.org/10.1080/09546553.2019.1668781

Gill, P., Corner, E., Thornton, A., & Conway, M. (2015). What are the roles of the internet in terrorism? Vox Pol. Retrieved from http://voxpol.eu/wp-content/uploads/2015/11/DCUJ3518_VOX_Lone_Actors_report_02.11.15_WEB.pdf

Gill, P., Horgan, J., & Deckert, P. (2014). Bombing Alone: Tracing the motivations and antecedent behaviors of lone-actor terrorists. *Journal of Forensic Sciences*, *59*(2), 425–435. https://doi.org/10.1111/1556-4029.12312

Goldman, A. (2015, Sep 16). An American family saved their son from joining the Islamic state. Now he might go to prison. *Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/an-american-family-saved-theirson-from-joining-the-islamic-state-now-he-might-go-to-prison/2015/09/06/2d3d0f48-44ef11e5-8ab4-c73967a143d3_story.html?noredirect=on&utm_term=.47868926f3b3

Greenberg, K. J., & Weiner, S. (2017). The American exception. Terrorism prosecution in the United States: The ISIS cases March 2014 - August 2017. New York: Center on National Security At Fordham Law.

Grinnell, D., Macdonald, S., & Mair, D. (2017). The response of, and on, twitter to the release of Dabiq issue 15. Paper presented at the 1st European Counter Terrorism Centre (ECTC) Conference on Online Terrorist Propaganda, April 10—11, The Hague, The Netherlands.

Gruenewald, J., Chermak, S., & Freilich, J. D. (2013). Distinguishing "loner" attacks from other domestic extremist violence: A comparison of far-right homicide incident and offender characteristics. *Criminology and Public Policy*, *12*(1), 65–91. https://doi.org/10.1111/1745-9133.12008

HM Government. (2019). *Online Harms White Paper*. London, UK: The Stationary Office. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf

HM Parliament. (2019). Counter-Terrorism and Border Security Act 2019. Retrieved from: http://www.legislation.gov.uk/ukpga/2019/3/section/9/enacted

Horgan, J., Shortland, N., Abbasciano, S., & Walsh, S. (2016). Actions speak louder than words: A behavioral analysis of 183 individuals convicted for terrorist offenses in the United States from 1995 to 2012. *Journal of Forensic Sciences*, *61*(5), 1228–1237. https://doi.org/10.1111/1556-4029.13115

Huey, L. (2015). This is not your mother's terrorism: Social media, online radicalization and the practice of political jamming. *Journal of Terrorism Research*, *6*(2), 1–16. https://doi.org/10.15664/jtr.1159

Hughes, S., Blackburn, E., & Mines, A. (2019). The other travelers: American jihadists beyond Syria and Iraq. Report. Washington, DC: Program on Extremism.

Hughes, S., & Meleagrou-Hitchens, A. (2017). The threat to the United States from the Islamic state's virtual entrepreneurs. *CTC Sentinel*, *10*(3), 1–9.

Ingram, H. (2015). The strategic logic of Islamic State information operations. *Australian Journal of International Affairs*, *69*(6), 729–752. https://doi.org/10.1080/10357718.2015.1059799

Ingram, H. (2016a). An analysis of Islamic State's Dabiq magazine. *Australian Journal of Political Science*, *51*(3), 458–477. https://doi.org/10.1080/10361146.2016.1174188

Ingram, H. (2016b). Deciphering the siren call of militant Islamist propaganda: Meaning, credibility & behavioural change. ICCT Research Paper, September. The Hague, The Netherlands: International Centre for Counter-Terrorism. https://doi.org/10.19165/2016.1.12

Jensen, M., James, P., LaFree, G., Safer-Lichtenstein, A., & Yates, E. (2018). The use of social media by United States extremists. National Consortium for the Study of Terrorism and Responses to Terrorism. Retrieved from http://www.start.umd.edu/data-

Joyce, M. (2013). Picking the best intercoder reliability statistic for your digital activism content analysis. *Digital Activism Research Project: Investigating the Global Impact of Digital Media on Political Contention*, (i), 1–10. Retrieved from http://digital-activism.org/2013/05/picking-the-best-intercoder-reliability-statistic-for-your-digital-activism-content-analysis/

Klausen, J. (2015). Tweeting the jihad: Social media networks of western foreign Fighters in Syria and Iraq. *Studies in Conflict & Terrorism*, *38*(1), 1–22. https://doi.org/10.1080/1057610X.2014.974948

Klausen, J. (2016a). A behavioral study of the radicalization trajectories of American "homegrown" Al Qaeda-inspired terrorist offenders. Final Report. Office of Justice Programs' National Criminal Justice Reference Service

Klausen, J. (2016b). *The role of social networks in the evolution of Al Qaeda-inspired violent extremism in the United States, 1990–2015*. Nation Institute of Justice. https://nij.ojp.gov/topics/articles/role-social-media-evolution-al-qaeda-inspired-terrorism

Klausen, J., Campion, S., Needle, N., Nguyen, G., & Libretti, R. (2016). Towards a behavioral model of "homegrown" radicalization trajectories. *Studies in Conflict & Terrorism*, *39*(1), 67–83. https://doi.org/10.1080/1057610X.2015.1099995

Koerner, B. I. (2017, January 14). A controversial new program aims to reform homegrown ISIS recruits back into normal young Americans. *Wired*. Retrieved from https://www.wired.com/2017/01/can-you-turn-terrorist-back-into-citizen/.

Lafree, G., Jensen, M., James, P. A., & Safer-Lichtenstein, A. (2018). Correlates of violent political extremism in the United States. *Criminology*, *56*(2), 233–268. https://doi.org/10.1111/1745-9125.12169

Lakomy, M. (2017a). Cracks in the online "caliphate": How the Islamic state is losing ground in the battle for cyberspace. *Perspectives on Terrorism*, *11*(3), 40–53. Retrieved from http://www.terrorismanalysts.com/pt/index.php/pot/article/viewFile/607/1200

Lakomy, M. (2017b). Let's Play a video game: Jihadi propaganda in the world of electronic entertainment. *Studies in Conflict & Terrorism*. https://doi.org/10.1080/1057610X.2017.1385903

Landis, J. R., & Koch, G. C. (1977). The Measurement of observer agreement for categorical data. *Biometrics*, *33*(1), 159–174. https://doi.org/10.2307/2529310

Macdonald, S., Correia, S. G., & Watkin, A.-L. (2019). Regulating terrorist content on social media: Automation and the rule of law. *International Journal of Law in Context*, *15*(2), 183–197. https://doi.org/10.1017/S1744552319000119

Macdonald, S., & Whittaker, J. (2019). Online radicalization: Contested terms and conceptual clarity. In *Online Terrorist Propaganda, Recruitment, and Radicalisation* (pp. 33–46). Boca Raton, FL: CRC Press.

Meleagrou-Hitchens, A., Hughes, S., & Clifford, B. (2018). The Travelers: American jihadists in Syria and Iraq. Washington, DC: Program on Extremism, George Washington University.

Meleagrou-Hitchens, A., & Kaderbhai, N. (2017). *Research perspectives on online radicalisation: A Literature Review, 2006–2016*. Dublin, Ireland: VOX-Pol Network of Excellence.

National Alliance on Mental Illness. (n.d). *Mental health by the numbers*. https://www.nami.org/mhstats.

Neumann, P. (2013). Options and strategies for countering online radicalization in the United States. *Studies in Conflict & Terrorism*, *36*(6), 431–459. https://doi.org/10.1080/1057610X.2013.784568

Neumann, P., & Kleinmann, S. (2013). How rigorous is radicalization research? *Democracy and Security*, *9*(4), 360–382. https://doi.org/10.1080/17419166.2013.802984

Novenario, C. M. I. (2016). Differentiating Al Qaeda and the Islamic state through strategies publicized in jihadist magazines. *Studies in Conflict & Terrorism*, *39*(11), 953–967. https://doi.org/10.1080/1057610X.2016.1151679

Pew Research Center. (2017). *U.S. Muslims concerned about their place in society, but continue to believe in the American dream: Findings from pew research center's 2017 survey of U.S. Muslims*. https://www.pewforum.org/2017/07/26/findings-from-pew-research-centers-2017-survey-of-us-muslims/.

Pew Research Center. (2019). *Internet/broadband fact sheet*. https://www.pewresearch.org/internet/fact-sheet/internet-broadband/.

Program on Extremism. (n.d). *ISIS in America, the cases*. Retrieved from https://extremism.gwu.edu/cases.

Prucha, N. (2016). IS and the jihadist information highway – projecting influence and religious identity via telegram. *Perspectives on Terrorism*, *10*(6), 48–58.

Raban, O. (2018). Observations on the first amendment and the war on terror. *Tulsa Law Review*, *53*(2), 141–157

Reed, A., & Ingram, H. (2017). Exploring the role of instructional material in AQAP's inspire and ISIS' Rumiyah. Paper presented at the 1st European Counter Terrorism Centre (ECTC) Conference on Online Terrorist Propaganda, April 10—11, The Hague, The Netherlands.

Reynolds, S. C., & Hafez, M. M. (2017). Social network analysis of German foreign fighters in Syria and Iraq. *Terrorism and Political Violence* (April). https://doi.org/10.1080/09546553.2016.1272456

Safer-Lichtenstein, A., LaFree, G., & Loughran, T. (2017). Studying terrorism empirically: What we know about what we don't know. *Journal of Contemporary Criminal Justice*, *33*(3), 273–291. https://doi.org/10.1177/1043986217697873

Sageman, M. (2008a). *Leaderless jihad: Terror networks in the twenty-first century*. Philadelphia, PA: University of Pennsylvania Press.

Sageman, M. (2008b, March/April). The next generation of terror. *Foreign Policy*, 36–42. https://doi.org/10.2307/25462270

Sanchez, R., (2017, January 8). What we know about the fort lauderdale airport shooting suspect. *CNN*. https://edition.cnn.com/2017/01/06/us/fort-lauderdale-airport-shooting-suspect/index.html

Schmitt, G.R. & Konfrst, H.J., (2015). *Life sentences in the federal system*. Washington, DC: United States Sentencing Commission.

Schuurman, B., Bakker, E., Gill, P., & Bouhana, N., (2018). Lone actor terrorist attack planning and preparation: A data-driven analysis, *Journal of Forensic Sciences*, *63*(4), 1191–1200.

Silver, J., Horgan, J., & Gill, P. (2018). Foreshadowing targeted violence: Assessing leakage of intent by public mass murderers. *Aggression and Violent Behavior*, *38*(December), 94–100. https://doi.org/10.1016/j.avb.2017.12.002

Soufan Group. (2015). Foreign fighters: An updated assessment of the flow of foreign fighters to Syria and Iraq. New York: Soufan Group.

START. (2018). *Profiles of Individual Radicalization in the United States (PIRUS) codebook*. Retrieved from www.start.umd.edu

Statista. (2019). *Number of smartphone users in the United States from 2010 to 2023 (in millions)*. https://www.statista.com/statistics/201182/forecast-of-smartphone-users-inthe-us/.

Vidino, L., & Hughes, S. (2015). ISIS in America: from retweets to Raqqa. Report. Washington, DC: GW Program on Extremism. https://doi.org/10.1017/CBO9781107415324.004

von Behr, I., Reding, A., Edwards, C., & Gribbon, L. (2013). Radicalisation in the digital era: The use of the internet in 15 cases of terrorism and extremism. Report. Cambridge, UK: RAND.

Watkin, A.-L., & Looney, S. (2018). "The lions of tomorrow": A news value analysis of child images in jihadi magazines. *Studies in Conflict & Terrorism*, *42*(1–2), 120–140. https://doi.org/10.1080/1057610X.2018.1513696

Weimann, G. (2012). Lone wolves in cyberspace. *Journal of Terrorism Research*, *3*(2), 75–90.

Weimann, G. J. (2018). Competition and innovation in a hostile environment: How Jabhat Al-Nusra and Islamic state moved to twitter in 2013–2014. *Studies in Conflict and Terrorism*, *42*(1–2), 25–42. https://doi.org/10.1080/1057610X.2018.1513692

Wikström, P. O. H., & Bouhana, N. (2017). Analyzing radicalization and terrorism: A situational action theory. In G. LaFree & J. D. Freilich (Eds.), *The handbook of the criminology of terrorism* (pp. 175–186). Chichester, UK: John Wiley & Sons. https://doi.org/10.1002/9781118923986.ch11

Wilbur, D. (2017). propaganda's place in strategic communication: The case of ISIL's Dabiq magazine. *International Journal of Strategic Communication*, 1–15. https://doi.org/10.1080/1553118X.2017.1317636

Winter, C. (2015a). *Detailed analysis of Islamic state propaganda video: Although the disbelievers dislike it*. London, UK: Quilliam Foundation.

Winter, C. (2015b). *The virtual "caliphate": Understanding Islamic state's propaganda strategy*. London, UK: Quilliam Foundation. Retrieved from http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/the-virtual-caliphate-understanding-islamic-states-propaganda-strategy.pdf

Winter, C. (2017). Media jihad: The Islamic state's doctrine for information warfare. Report. London, UK: International Centre for the Study of Radicalisation and Political Violence.

Zelin, A. Y. (2015). Picture or it didn't happen: A Snapshot of the Islamic state's official media output. *Perspectives on Terrorism*, *9*(4), 85–97.

USA v. Mahad Abdiaziz Abdiraham. Criminal complaint, 4th Judicial District Court, 27-CR-17-28647. State of Minnesota, County of Hennepin. (2017).

USA v. Heather Coffman. Statement of facts. Case 3:15-cr-00016. United States District Court for the Eastern District of Virginia. (2015).

USA v. Mahmoud Amin Mohamed Elhassan. Government's sentencing memorandum. Case 1:16-cr00064. United States District Court for the Eastern District of Virginia. (2017).

USA v. Tayyab Tahir Ismail, Criminal complaint, Case 0:18-mj-06588-PMH, United States District Court for the Southern District of Florida (2018).

USA v. Omer Kuzu, Factual basis, Case Case 3:19-cr-00327-M, United States District Court for the Northern District of Texas (2020).

USA v. Emanuel L. Lutchman. Criminal complaint. Case 6:15-mj-04212-MWP. United Sates District Court for the Western District of New York (2015).

USA v. Haris Qamar. Statement of Facts. Case 1:16-cr-00227. United States District Court for the Eastern District of Virginia. (2016).

USA v. Said Azzam Mohamad Rahim. Case 3:17-mj-00171. United States District Court for the Northern District of Texas. (2017).

USA v. Noor Zahi Salman. Defendant's motion to preclude improper argument in government's opening statement. Case 6:17-cr-00018. United States District Court Middle District of Florida Orlando Division. (2018).

AUTHOR BIOGRAPHY

Joe Whittaker is a lecturer in the Department of Criminology at Swansea University and is a research fellow at the International Centre for Counter-Terrorism. He researches terrorists' and extremists' use of the Internet as well as the methods employed to counter them.

How to cite this article: Whittaker J. The online behaviors of Islamic state terrorists in the United States. *Criminol Public Policy*. 2021;1–27. https://doi.org/10.1111/1745-9133.12537