

An exploratory analysis of leakage warning behavior in lone-actor terrorists

Miss Menna Rose & John Morrison

To cite this article: Miss Menna Rose & John Morrison (2023) An exploratory analysis of leakage warning behavior in lone-actor terrorists, Behavioral Sciences of Terrorism and Political Aggression, 15:2, 179-214, DOI: [10.1080/19434472.2021.1900325](https://doi.org/10.1080/19434472.2021.1900325)

To link to this article: <https://doi.org/10.1080/19434472.2021.1900325>



© 2021 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



[View supplementary material](#)



Published online: 17 Mar 2021.



[Submit your article to this journal](#)



Article views: 2703



[View related articles](#)




[View Crossmark data](#)



Citing articles: 5 [View citing articles](#)

An exploratory analysis of leakage warning behavior in lone-actor terrorists

Miss Menna Rose and John Morrison 

Royal Holloway and New Bedford College, Egham, UK

ABSTRACT

Leakage is one of the eight warning behaviors referred to in the violence risk and threat assessment literature. Previous research has highlighted the relevance and prevalence of leakage in lone-actor terrorists; however, a more detailed understanding of this phenomenon is lacking. This study sets out to expand our knowledge of this behavior by conducting an exploratory analysis using court records relating to IS-inspired lone-actor terrorism cases in the United States. The general patterns in leakage warning behavior were analyzed, and different types of leakage were examined with regard to from whom they were leaked, how they were leaked, their presence online, and whether or not they occurred before certain types of attacks more than others. It was found that leakage in the form of support tended to be leaked most frequently to members of the public, via written text and online, whilst the leakage of intent and specifics appeared to be more regularly leaked to co-conspirators and through verbal communication that avoided the online world. Significant relationships were also found between leakage, FBI interaction and attack initiation, but no significant relationship was found between leakage and mental health. The implications of these findings are discussed.

ARTICLE HISTORY


Received 17 August 2020
Accepted 3 March 2021

KEYWORDS

Leakage; lone actor; warning behavior; mental health

Introduction

Despite appearing counterproductive in nature, research has found leakage warning behavior to be prevalent across lone-actor terrorists. For example, when Gill et al. (2014) examined the motivations and antecedent behaviors of 119 individuals who had engaged in, or planned to engage in, lone-actor terrorism, they found that in 79% of cases others were aware of the lone actor's commitment to an extremist ideology; in 64% of cases family and friends were aware of the individual's specific intent to engage in terrorist activity; and, in 58% of the cases other individuals knew about the specifics of the lone actor's preparation for the attack. Similarly, Schuurman, Bakker, et al. (2018) found that 86% of their lone-actor sample communicated their radical or extremist convictions to third parties. Importantly, leakage warning behavior may indicate

CONTACT Miss Menna Rose  mennarose@wonderglobe.co.uk  Royal Holloway and New Bedford College, Egham TW20 0EX, UK

© 2021 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group
This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way.

the research, planning, and implementation of a violent event (Meloy & O'Toole, 2011), and it could therefore provide crucial opportunities for early detection and intervention by law enforcement.

Whilst existing research does provide an important introduction to this risk behavior, building on this with a more nuanced understanding of leakage, including what sort of content tends to be leaked to which specific individuals via which mediums in the run up to a specific form of attack, would be of great benefit to those attempting to identify potential lone-actor terrorists. By examining this chain of events in more detail, one might be able to more readily deduce whether certain kinds of material tend to be leaked to specific individuals, and whether different forms of leakage are more predictive of particular kinds of lone-actor attacks. The present research, therefore, aims to expand our knowledge of leakage warning behavior in these areas by conducting an exploratory analysis of 31 ISIS inspired lone-actor terrorists in the United States using court reports. Importantly, it was found that leakage is by no means a uniform concept. More specifically leakage of support tended to be leaked most frequently to members of the public, via written text and online, whilst intent and attack specifics were more frequently leaked verbally to other perceived ISIS sympathizers.

Lone-actor leakage

Over recent years, lone-actor terrorism has become an increasingly concerning and prevalent phenomenon (Borum et al., 2012). It poses a considerable risk to contemporary society (Brynielsson et al., 2013), and a recent surge of lone-actor attacks in Europe and the United States has highlighted the lethality of this ever-evolving aspect of terrorism (Schuurman, Lindekilde, et al., 2018). Resultantly it is perhaps unsurprising that in recent years lone-actor terrorism has been considered a major national security threat in both Europe and North America (Meloy & Gill, 2016). One of the challenges of the lone-actor threat is that traditional intelligence techniques have, at times, struggled to intercept lone-actor attackers. Whilst some argue that it is the absence of multiple co-conspirators that renders lone actors less vulnerable to detection and infiltration (Schuurman et al., 2018), it is important to emphasize that this does not mean that there is nothing counter-terrorism practitioners can do to stop them (Brynielsson et al., 2013). But in order to successfully deter and counter the lone-actor terrorist threat, the lone-actor terrorists, their actions and their motivations, need to first be better understood.

For some time, research into the psychology of terrorism has focused on identifying the presence or absence of mental disorders and illnesses. For instance, throughout the 1970s, studies tended to emphasize the popular opinion that all terrorists were either insane or psychopathic individuals (Cooper, 1977; Hacker & Hacker, 1976; Pearce & Macmillan, 1977; Victoroff, 2005). More specifically, Pearce and Macmillan (1977) speculated that all terrorists were sociopaths who engaged in extremism as a way of relieving their mental health problems, and Cooper (1977) argued that all terrorists possessed psychopathic personalities. Then, slightly later throughout the 1980s, the idea that all terrorists were psychologically damaged youths became the most common and widespread belief (Billig, 1985; Böllinger, 1985; Gill & Corner, 2017).

In response to these psychopathological and personality-driven explanations of terrorism, a number of reviews were synthesized throughout the 1990s and early 2000s in order

to analyze the evidence that supported them (Borum, 2004; Corner & Gill, 2015; Gill & Corner, 2017; Horgan, 2003; Silke, 1998, 2003; Victoroff, 2005). Importantly, these reviews collectively argued that such propositions were 'built on unsteady empirical, theoretical and conceptual foundations' (Horgan, 2003, p. 23), and with this came the belief that terrorists were essentially 'normal individuals' (Silke, 1998, p. 53) who lacked mental illness altogether. More recently, however, Corner and Gill (2015) have argued that the presence or absence of mental illness in terrorism is, conceivably, less clear-cut. Perhaps most importantly for the present paper, they argue that previous research into the psychology of terrorism and the role of mental illness has focused too heavily on group-based actors, and that there is, in fact, a greater prevalence of mental illness within the lone-actor category. Investigating this concept, Corner and Gill (2015) utilized a unique dataset of 199 lone actors, and carefully matched them to a sample of group-based terrorists. In line with their hypothesis, they found that the chance of a lone actor having a mental illness was 13.49 times higher than that of a group actor. This finding is in line with previous research conducted by Gruenewald et al. (2013), which found that lone extreme right-wing offenders had significantly higher rates of mental illness than group offenders. It is important to understand that while Corner and Gill (2015) note the higher prevalence of mental illness, they emphasize that the very presence of mental illness does not necessarily indicate any causal relationship between mental health and engagement in terrorist activity.

Despite this notable inflation in the prevalence of mental illness in lone-actor terrorists, research suggests that the operational importance of mental illness and diagnoses is comparatively low (Meloy et al., 2015; Meloy & Yakeley, 2014). That is, diagnoses have been deemed to offer little assistance when determining the level of risk and concern prior to a possible terrorist attack. This is primarily due to the fact that lone-actor terrorists represent an infinitesimal number of all those who are mentally ill (Meloy et al., 2015), but also due to the fact as detailed above that the presence of a mental illness does not necessarily mean that it is the root cause of the violent activity. Instead, Meloy and colleagues suggest that whilst an understanding of mental illness could have some relevance when managing and mitigating an identified threat, understanding and assessing a string of so-called warning behaviors could offer an additional, invaluable lens through which a potential risk can be first identified, thoroughly assessed, and then effectively countered.

Warning behaviors are defined as '... particularly toxic changes in patterns of behavior which require an operational response' (Meloy et al., 2012, p. 260). Importantly, a typology of eight different warning behaviors has been published in the violence risk and threat assessment literature (Meloy et al., 2012) with the aim to capture '... superordinate behavioral or psychological patterns that constitute change and may evidence accelerating risk' (Meloy et al., 2014, p. 203). The eight different behaviors included within this typology are leakage, fixation, identification, pathway, novel aggression, energy burst, last resort and directly communicated threat, and whilst it is by no means expected that each one is presented before any given attack, every warning behavior is said to consist of discrete behaviors that can be considered risk variables for targeted violence (Meloy et al., 2014). Notably, this typology has received empirical support, and has been found to have ecological validity across a range of targeted violence domains (Meloy & Gill, 2016). For example, in one study, Meloy et al. (2014) examined whether the occurrence of warning behaviors differed between a group of school shooters and

a group of other students of concern. They found that five warning behaviors (namely pathway, fixation, identification, novel aggression and last resort) occurred with significantly greater frequency in the school shooters. Furthermore, Hoffmann et al. (2011) applied the typology to a dataset of fourteen non-terrorist attackers of public figures in Germany, and found that all warning behaviors were present. Considering lone-actor terrorists, Meloy and Gill (2016) investigated the validity of these behaviors as part of the Terrorist Radicalization Assessment Protocol (TRAP-18) risk assessment tool. The TRAP-18 was developed to aid the assessment of risk in lone-actor terrorists and considers the eight different warning behaviors as one set of indicators. In their study, Meloy and Gill (2016) viewed a large open source database of lone-actor terrorists through the lens of the TRAP-18 with the aim to test its criterion validity. Importantly, they found that 70% of the 111 lone actors included in their sample were positive on at least half the TRAP-18 indicators, and 77% or more exhibited four warning behaviors: pathway, fixation, identification and leakage. Of particular note, leakage behavior was the most prevalent TRAP-18 indicator, occurring in 85% of the lone-actor sample. Given this frequency and the nature of this behavior, leakage may well act as the point of entry for a threat assessor in any given case (Meloy & Gill, 2016) – making it an incredibly important topic for research, and the focus of this study.

The concept of leakage in threat assessment was first proposed by O'Toole (2000) in a study examining school violence (Meloy & O'Toole, 2011). In this study, O'Toole offered that leakage occurred when a student revealed clues, in the form of subtle threats, boasts or ultimatums, to thoughts, attitudes or intentions that may have signaled an impending violent attack. Today, in the context of lone-actor terrorist research, leakage can be defined as '... the behavior of a (would be) lone actor terrorist who intentionally or unintentionally divulge their motivation or capability to commit acts of violence' (Schuurman, Baker, et al., 2018, p. 1196). It can cover a range of behaviors; such as letting others know about ones' support for an ideology, intent to attack, and/or sharing specific information about the preparation of an attack (Gill et al., 2014; Spaaij, 2011). As discussed at the beginning of this article, research has found leakage warning behaviors to be prevalent across lone-actor terrorists (Gill et al., 2014; Schuurman, Bakker, et al. 2018). Of particular note, Schuurman, Bakker, et al. 2018 highlighted that it was infact often only after leakage behavior had begun that other forms of preparatory behavior were found. This emphasizes the importance and significance of the behavior with regards to counter-terrorism interventions, and largely constitutes the motivation of this study.

The relationship between leakage warning behavior and mental health does not appear to have been considered in lone-actor terrorists before. Whilst the operational utility of mental health alone has been deemed to be low, examining its relationship with leakage in lone actors is of interest given that Silver et al. (2018) found a potentially interesting association in public mass murderers (significant to the 0.1 level).

Previous research lacks a focus on the specific role of the Internet in terms of leakage behavior. Some researchers have suggested that the contemporary lone-actor terrorist is dependent upon the Internet as a 'virtual community' for a multitude of reasons ranging from seeking reinforcement of beliefs and legitimization for ones' actions, to simply preparing for an attack (Meloy & Yakeley, 2014; Gill, 2015). Some have argued that the anonymity that comes with virtual communities on the Internet additionally increases the

likelihood of self-disclosure, and increases a lone-actor's willingness to express their radical ideologies, views, and in some cases, their behavioral intentions online (Bargh & McKenna, 2004; Meloy & Yakeley, 2014). With this considered, research should also aim to more carefully examine the frequency of, and the particular platforms through which, lone actors might be leaking their views and intentions online.

Finally, previous research has also abstained from examining possible relationships between leakage and other warning behaviors. This area of research warrants further attention given that understanding leakage in the context of other warning behaviors might be beneficial when determining its dangerousness and its predictive value (Meloy & O'Toole, 2011).

The present study

The present research aims to expand our understanding of leakage warning-behavior in lone-actor terrorists by conducting an exploratory analysis. This research uses court reports sourced from the Program on Extremism at George Washington University to assess the general patterns of leakage behavior in US-based lone actors. Given the exploratory nature of this research, no hypotheses are given. Nonetheless, it examines the following:

- who is on the receiving end of leakage (the 'recipients'),
- how leakage is being leaked, whether or not this behavior is taking place online,
- and before what sort of attacks (if any) leakage is most prevalent.

Secondly, this research will break down leakage behavior into three different forms – (i) support – a type of leakage that indicates one's support for radicalized violence, ISIS and/or previous attack and attackers (ii) intent – a type of leakage that indicates an individuals' violent intent and (iii) specifics – a type of leakage that gives an indication towards the details of the research, plans and preparations of a particular event. It then examines whether these different forms of leakage vary in terms of to whom they are leaked and how they are leaked, whether or not they differ in terms of online prevalence, and whether the different kinds of leakage are more closely linked to specific sorts of attacks. Thirdly, this study will examine whether any relationships between leakage behavior and other factors, such as FBI interaction and mental health, exist. In this study, FBI interaction will be defined as the engagement in conversation, either virtual or face-to-face, between an undercover FBI agent and a lone-actor terrorist. Examples of these interactions will be outlined in the results section of this article. Finally, this study builds upon previous research by considering potential relationships between leakage and other warning behaviors. For the purpose of this study, these behaviors include fixation and identification only. Previous research has similarly grouped these two behaviors together with leakage and labeled them as 'weak signals' due to the fact that they can each be identified through written communication, and subsequently found on the Internet (Brynielsson et al., 2013; Cohen et al., 2014; Zeman et al., 2017). Fixation warning behavior refers to '... any behavior that indicates an increasingly pathological preoccupation with a person or a cause' (Meloy et al., 2015, p. 215), and in written text this would be observed through

repeated commentary on an issue or particular individual (Brynielsson et al., 2013). In addition, identification warning behavior can be defined as ‘... any behavior that indicates a psychological desire to be a ‘pseudo-commando’, have a ‘warrior mentality’, closely associate with weapons or other military or law enforcement paraphernalia, identify with previous attackers or assassins, or identify oneself as an agent to advance a particular cause or belief system.’ (Meloy et al., 2015, p. 215). Importantly, identification can often be recognized when there is a notable shift from crediting what others do (seen through fixation), to wanting to become exactly who they are (Meloy & Gill, 2016).

Method

Sample

The sample for this study includes 31 individuals who engaged in, or planned to engage in, lone-actor terrorism within the United States (US). Each member of the sample was subsequently convicted for his or her actions. In addition to those who actively planned and/or conducted violent attacks, the sample includes facilitators – individuals who engage in nonviolent behaviors that facilitate or encourage others to carry out violent actions that intend to cause terror and do harm to others. In addition to individual terrorists, the sample includes isolated dyads (pairs of lone-actor terrorists operating independently of a group) and triads (three lone-actor terrorists operating independently of a group). Although not technically ‘lone’ actors these subgroups are included because, firstly, they are not members of any specific terrorist group, and secondly, because it has been found that dyads and triads are often only formed when one lone-actor terrorist recruits others specifically for the execution of an attack (Gill et al., 2014). The individuals included in these dyads and triads ‘... may [have] become radicalised to violence on their own (or one may have radicalized the other)’ (Gill et al., 2014, p. 426). To note, whilst some lone actors included in this sample are believed to have been in dyads or a triads, the sample does not include their co-conspirators and therefore there are a total of 31 plots included in this study.

All lone actors, dyads and triads included in this sample were inspired by the Islamic State of Iraq and Syria (ISIS), but operated without any command or control links. They, therefore, operated autonomously and independently of the group in terms of training, preparation, target selection and execution. The original sample consisted of three additional cases that were subsequently removed because further analysis showed that the lone actors in question believed that they were under the command of ISIS officials ($n=3$). In each of these three cases, undercover FBI agents led the individuals to believe that they were interacting with official members of ISIS. It was therefore deemed necessary to remove these individuals from the analysis because it was thought that the mindset and psychology of these individuals would have been similar to that of those who were actually under command. All individuals in this sample planned to or successfully committed or facilitated an attack between 31st January 2014 and 31st January 2019. The specification of these dates is based on the fact that at the beginning of 2014, ISIS began to use social media to call for more lone-actor attacks (United States v Abdin, 2017, p. 4).

Design, data collection and analysis

This research has an exploratory multiple-case study design. To begin the data collection, criminal complaints, indictments, affidavits and courtroom transcripts stored on the Program on Extremism website, detailing Islamic State-related legal proceedings for 191 individuals charged for IS-related activities, were examined. From this set of cases, and whilst referring to the inclusion criteria specified above, an original list of 34 lone-actor terrorists was selected. The names of these selected individuals made up the 'actor dictionary', which was subsequently stored in a secure word file for ethical reasons. The legal documents, hosted by the Program on Extremism website, for each selected case were analyzed in more detail. Throughout this process, data were collected on the socio-demographic information (age, gender, and mental health), the antecedent event behaviors (FBI interaction, leakage, fixation and identification) and the event specific behaviors (date of attack, type of planned attack, type of executed attack, attack initiation, target, cell number and role of lone actor) of each member of the sample. Data were also collected on the recipients of leakage (other perceived ISIS sympathizers, family and friends, the public or law enforcement), the mode through which leakage was leaked (verbal, written or both), and the platforms through which information was leaked online (Twitter, Facebook, messaging application or other). In this study, 'other perceived ISIS sympathisers' can be defined as other individuals or strangers who are perceived to have similar views and ideas with regards to the Islamic State. The lone actors might have met these individuals online and/or in person. We included this recipient group in this study for internal security purposes attack and non-attack information and logistics is not always freely shared throughout ISIS. Therefore, in this study, as and when then lone actors *did* share information with other ISIS sympathizers, a form of leakage was recorded. Importantly, whilst previous research does not seem to have overtly specified this group as recipients of leakage, Schuurman, Baker, et al. (2018) did specify that 86% of the lone actors in their sample leaked to family members, friends, colleagues or 'strangers online' (p. 1196). This carries significance for the inclusion of other perceived ISIS sympathizers in this study, as in most instances, these recipients merely started out as online strangers who appeared to sympathize with the lone actors' radical views.

The data were originally recorded qualitatively (see Appendix 1). It is important to note that not all relevant information was found within the court documents, and when this was the case, missing information was located (where possible) in open source news reports that were primarily found using tailored LexisNexis searches, using the 'All English News' option. It was during this stage that the three cases mentioned previously were excluded.

Following this sampling procedure, a codebook was developed (see Appendix 2). This was influenced by the codebook of 'Profiles of Individual Radicalization in the United States' (PIRUS), published by the National Consortium for the Study of Terrorism and responses to Terrorism (START). The codebook for the current study specified the inclusion criteria, included the definitions of key terms, and set out the coding options for each variable. The final version of this codebook contained 72 variables. Using the codebook as reference, the qualitative data collected at the beginning of this process were coded quantitatively in SPSS and were subsequently analyzed. Given the exploratory

nature of this research, the statistics run were mainly descriptive, looking at patterns of frequencies and percentages. However, where appropriate, inferential statistics were run and the Fischer's Exact Test was utilized.

Ethical considerations

Considering the court reports/indictments analyzed in this study were public documents, taking steps to protect the lone-actors names was not deemed ethically mandatory but was implemented, nonetheless. Firstly, for data storage and analysis all the lone-actors names were made anonymous; secondly, all data were stored and saved in protected files in order to avoid unintentional and/or potentially intentional access by unauthorized persons, and thirdly, the researcher only collected and stored information that was deemed critical for the research project. This anonymity was not possible at the point of publication as it was deemed necessary to have illustrative examples to emphasize the points raised throughout the analysis. Within the article, there are a number of examples used within the name of the defendant accessible in the citation and/or in the court reports/indictments.

In total, this sample consisted of 31 lone-actor terrorists. Given that *N* is small, percentages should be interpreted with caution throughout the following section.

Results

The sample was predominantly male ($n = 27$), with only four lone actors being female. The majority of the sample targeted either civilians (51.6%; $n = 16$), or law enforcement (35.5%, $n = 11$). A smaller number of cases targeted military personnel (19.4, $n = 6$) and government officials (6.24%, $n = 2$), and only one case was found to target a specified individual. Within this sample, 38.7% ($n = 12$) of the sample was acting entirely alone, 32.3% ($n = 10$) of the sample were in dyads, and 29% ($n = 9$) of the sample were in triads.

In total, 83.9% ($n = 26$) of the lone-actor sample demonstrated leakage warning behavior. This reiterates the prevalence of leakage found in lone-actor terrorists, as highlighted by previous research. Out of the 26 leakage cases, 76.9% ($n = 20$) were 'attackers', and only 3.8% ($n = 1$) were 'facilitators'. In some instances (19.2%, $n = 5$) the lone actor acted as both an attacker and a facilitator.

A majority of the sample leaked to other perceived ISIS sympathizers (80.8%, $n = 21$). In a slightly smaller majority the lone actors leaked to members of the public (65.4%). Instances of leakage to the public included written statements that were posted on Twitter – for example, case nine publicly tweeted, 'al-Qa'ida said it loud and clear: we are fighting the American invasion and their hegemony over the earth and the people'.¹ Ten individuals (38.5%) leaked to family and friends. For example, case 10 told an acquaintance of whom he had known for two and a half years that he 'loves Allah' and believes that all non-Muslim Americans should be killed.² Only one lone actor leaked to known law enforcement. To note, in the majority of cases ($n = 20$), the lone actor leaked to two or more of the recipient groups mentioned here. For example, 17 out of the 21 lone actors that leaked to other perceived ISIS sympathizers also leaked to either members of the public, or family and friends. This means that if the 'other perceived ISIS sympathisers' recipient group were to be removed from

the sample, the number of leakage cases would be reduced by just four (as seen in Table 2, p. 18).

Additionally, 84.6% ($n = 22$) verbally leaked information. For example, during a meeting between case 6 and another perceived ISIS sympathizer, the lone actor described himself as a 'lone wolf' for ISIS and talked of his desire to kill people using a Savage .308 bolt action rifle.³ A similar 88.5% ($n = 23$) of the sample leaked through written communication. For instance, case 31 pledged his support for ISIS on Facebook by posting a profile picture of a flag with the words 'ALLAH IS MY LORD, ISLAM IS MY LIFE, QURAN IS MY GUIDE, SUNNAH IS MY PRACTISE, JIHAD IS MY SPIRIT, RIGHTEOUS IS MY CHARACTER, PARADISE IS MY GOAL ... I WILL DIE TO ESTABLISH ISLAM' written across it.⁴ Other written leakage included that on instant messaging platforms. For example, case 2 wrote to another perceived ISIS sympathizer, 'I believe that we should just wage jihad under our own orders and plan attacks and everything'.⁵ A calculated 80.8% ($n = 21$) of those that did leak did (at some point) do so online, highlighting the potential relevance of 'virtual communities'. Perhaps unsurprisingly given its relative privacy, the most widely used online platform was Facebook – used by 61.9% ($n = 13$) of those leaking online. In addition, unspecified online platforms were used by 33.3% ($n = 7$) of all those who leaked online; online messaging apps were used by 28.6% ($n = 6$), and Twitter, perhaps the most 'public' platform, was used by 23.8% ($n = 5$) of the sample. Leakage warning behavior occurred 88.9% ($n = 16$) of the time before planned shooting attacks and 83.3% ($n = 10$) of the time before planned bombing attacks. It also occurred before all planned stabbing attacks ($n = 2$) and 50% of the time before planned vehicle attacks ($n = 1$); however, we must note that N is particularly small for these latter types of attacks and thus these results should be treated with caution.

With regards to mental health, 38.7% ($n = 12$) of the lone-actor sample was reported as having a mental illness. To note, seven of these cases were undiagnosed but deemed mentally unwell through reported speculation, and five were recorded as professionally diagnosed. Figure 1 shows what raw numbers of lone actors were diagnosed with various mental illnesses (both professionally and through speculation). Out of those with no mental illness ($n = 19$), 84.2% ($n = 16$) demonstrated leakage warning behavior. In comparison, 71.4% ($n = 5$) of all those undiagnosed exhibited leakage behavior, whilst 100% ($n = 5$) of those professionally diagnosed with mental illness were found to have leaked. Table 1 shows the raw number of lone actors who exhibited leakage behavior in each mental health group. No significant relationship between leakage and mental health was found (Fisher's test; $p = .641$), and mental health did not appear to influence whether the lone actors acted alone or in dyads or triads.

A significant relationship was, however, found between leakage and FBI Interaction (Fisher's test; $p = .001$). Figure 2 shows that FBI interaction was not recorded in any of the 'no leakage' ($n = 5$) cases but was evident in 22 of the 26 cases in which leakage was detected. The leakage identified and the subsequent information gathered by the FBI tended to develop gradually. More specifically, the lone actors often began by expressing their support of ISIS to undercover FBI agents, before they leaked and communicated more specific ideas and/or hypothetical plans. For example, in case 3, the lone actor '... sent the FBI Confidential Human Source (CHS) various types of ISIS propaganda' before expressing at a later date that '... there is a Hindu temple I want to shoot up...'. To this latter statement, the CHS replied, 'when are you thinking about executing this?'.⁶

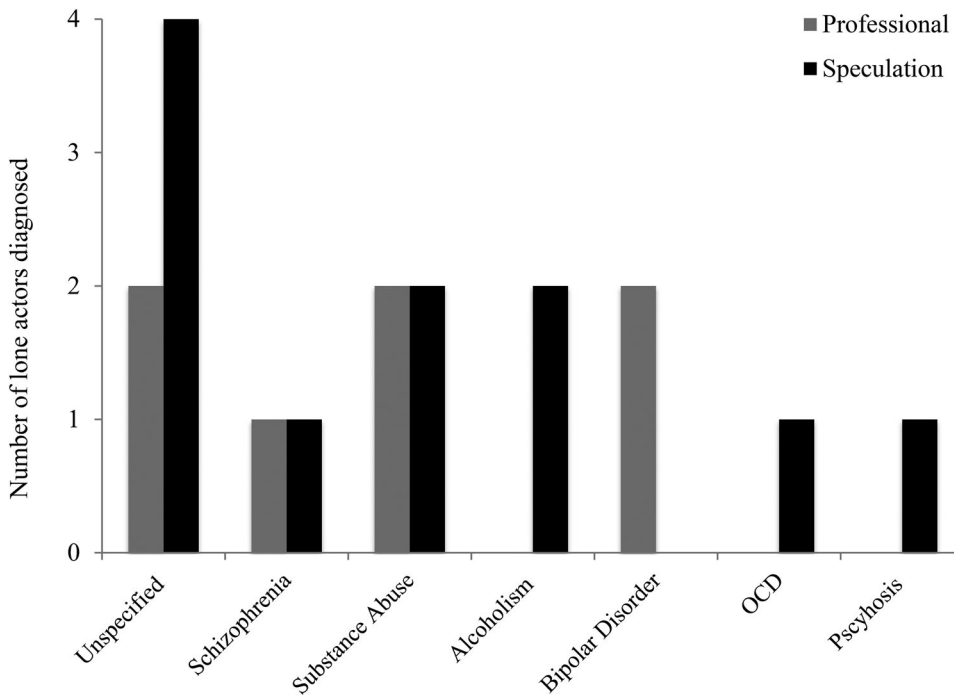


Figure 1. The number of lone actors either professionally diagnosed, or diagnosed through speculation, with one of the specified mental illnesses.

Table 1. Number of lone actors who leaked within each mental health group.

Mental health group	<i>n</i> (%)	<i>N</i>
No mental illness	16 (84.2)	19
Mental illness – speculation	5 (71.4)	7
Mental illness – professionally diagnosed	5 (100)	5

In some cases, but not all, this communication progressed towards what might be more readily defined as ‘attack planning’. For example, in case 6, the lone actor asked the CHS if he could purchase a ‘baby Glock’ for him.⁷ The lone actor ‘... then described how the CHS could purchase several weapons for him, and then indicated that he would arrange to have the guns stolen from the CHS’s car so that the CHS could just claim they were stolen’. Importantly, the meetings and interactions that took place between this lone actor and the CHS were preceded by the lone actor expressing his support for ISIS via his Facebook page.

To note, similar to that of other perceived ISIS sympathizer cases, 18 of the 22 FBI interaction cases also leaked to other recipients. These two sets of findings are summarized in Table 2, which shows that if cases of FBI interaction and other perceived ISIS sympathizer cases were dismissed from this sample, the overall presence of leakage would be reduced by four cases only.

A significant relationship was also found between leakage and attack initiation (Fisher’s test; $p = .02$). Out of those individuals who did leak, 7.7% initiated their attack. In contrast,

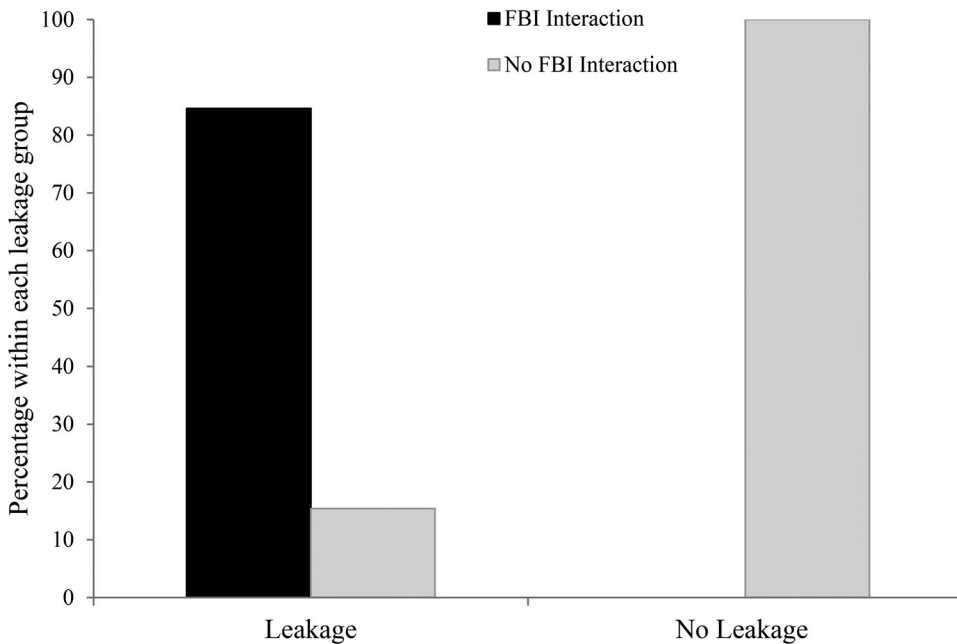


Figure 2. The percentages of those who did or did not leak interacting with the FBI in the build up to their plot.

Table 2. Number of leakage cases after FBI Interaction and other perceived ISIS sympathizer cases have been removed.

	Overall leakage	Leakage without other perceived ISIS sympathizers	Leakage without FBI interaction	Leakage without other perceived ISIS sympathizers + FBI interaction
<i>n</i>	26	22	22	22
% of sample (<i>n</i> = 31)	83.9	71.0	71.0	71.0

60% of those who did not demonstrate leakage behavior initiated their attack. All these findings suggest the importance of leakage in terms of counterterrorism interventions. **Table 3** shows the raw numbers of lone actors initiating their attacks in each leakage group.

Out of those who did demonstrate leakage warning behavior, 96.2% leaked intent. For example, in case 26, the lone actor declared, whilst in conversation with another perceived ISIS sympathizer, ‘I will kill people this month’.⁸ In 88.5% of the cases, the lone actors leaked support. As one example, in case 31, the lone actor pledged support to ISIS and its leader in a Facebook post that stated, ‘I support the brother Abu al-baghdadi. I support ISIS’.⁹ In addition, 76.9% of the sample leaked specifics regarding the details of

Table 3. Number of lone actors who initiated their attack within each leakage group.

Leakage group	Number of attacks initiated (%)	<i>N</i>
Leakage	2 (7.7)	26
No Leakage	3 (60)	5

their plans/plot. For example, case 25 expressed his specific desire to conduct attacks on police stations using triacetone triperoxide.¹⁰ Figure 3 shows that there was some variation between what sort of leakage was leaked depending on the type of lone actor in question. For instance, all lone actors operating as facilitators leaked both support and specifics, but no individuals acting as facilitators (only) leaked intent. All lone actors operating as attackers, however, leaked intent, with the majority also leaking support and specifics. Furthermore, those acting as both a facilitator and an attacker leaked support and intent, with a smaller majority leaking specifics.

The leakage of support and intent occurred in the build-up to all planned stabbing attacks, and 50% of the time in the build-up to attacks planning on using a vehicle. Leakage of plot specifics occurred 66.7% of the time prior to planned shootings and bombings, and 50% of the time prior to planned stabbings and vehicle attacks. The raw numbers of lone actors exhibiting each subgroup of leakage before the specified attacks are summarized in Table 4.

Figure 4 shows that intent and specifics were leaked to other perceived ISIS sympathizers in the majority of leakage cases, and considerably less frequently to all other recipients. Support was leaked most frequently to the public, moderately to other perceived ISIS sympathizers, even less frequently to family and friends, and never to known law enforcement. This suggests that more 'important' information regarding an attack tends to be leaked to those closest to the lone actors and withheld from members of the public.

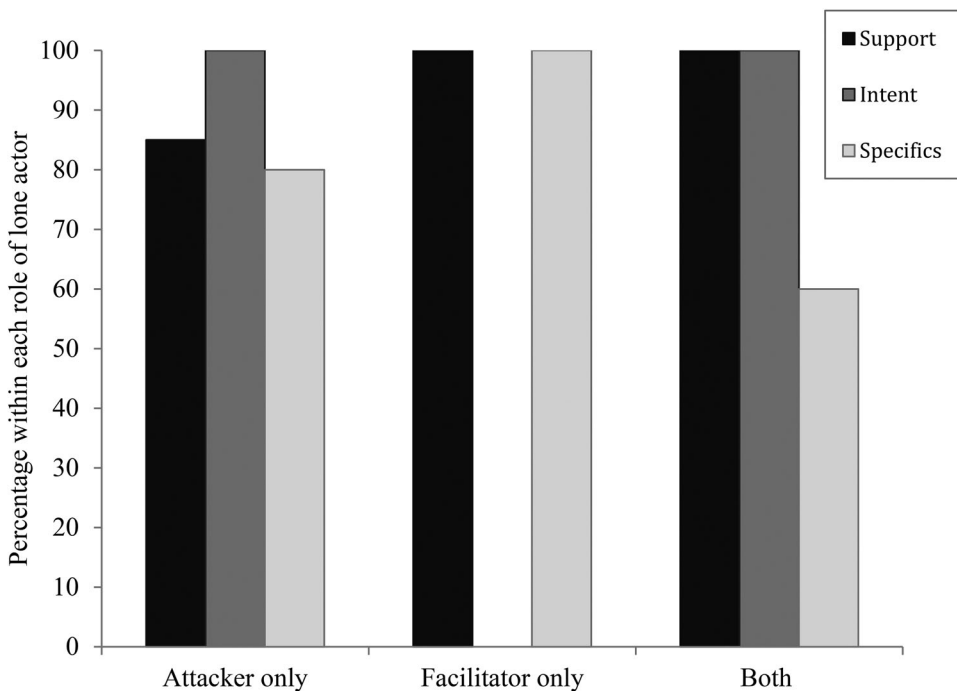


Figure 3. The percentages of those leaking support, intent and specifics within each role of lone actor.

Table 4. Number of lone actors leaking support, intent or specifics in the buildup to the four types of planned attacks.

	Support <i>n</i> (%)	Intent <i>n</i> (%)	Specifics <i>n</i> (%)	Total leakage <i>N</i>
Shooting	14 (77.8)	16 (88.9)	12 (66.7)	18
Bombing	8 (66.7)	10 (83.3)	8 (66.7)	12
Stabbing	2 (100)	2 (100)	1 (50)	2
Vehicle	1 (50)	1 (50)	1 (50)	2

Figure 5 shows that both Intent and Specifics were leaked more frequently through verbal communication, whilst support was leaked most frequently through written text (written online or via messenger applications). This might have important implications for law enforcement as in some instances verbal communication is less easily intercepted.

Support was leaked most frequently on the Internet (78.3% of cases) in comparison to the other forms of leakage. Intent was leaked online in 44%, and specifics in a lesser 35% of leakage cases. Figure 6 shows that when online leakage did occur, support was most frequently leaked on Facebook, whilst both intentions and specifics were most frequently leaked on online instant messaging apps. To note, intentions were never leaked on Twitter, and one might infer this is due to the publicity of this platform.

Finally, a significant relationship was found between leakage warning behavior and fixation warning behavior (Fisher's test $p = .02$). There was also a significant relationship

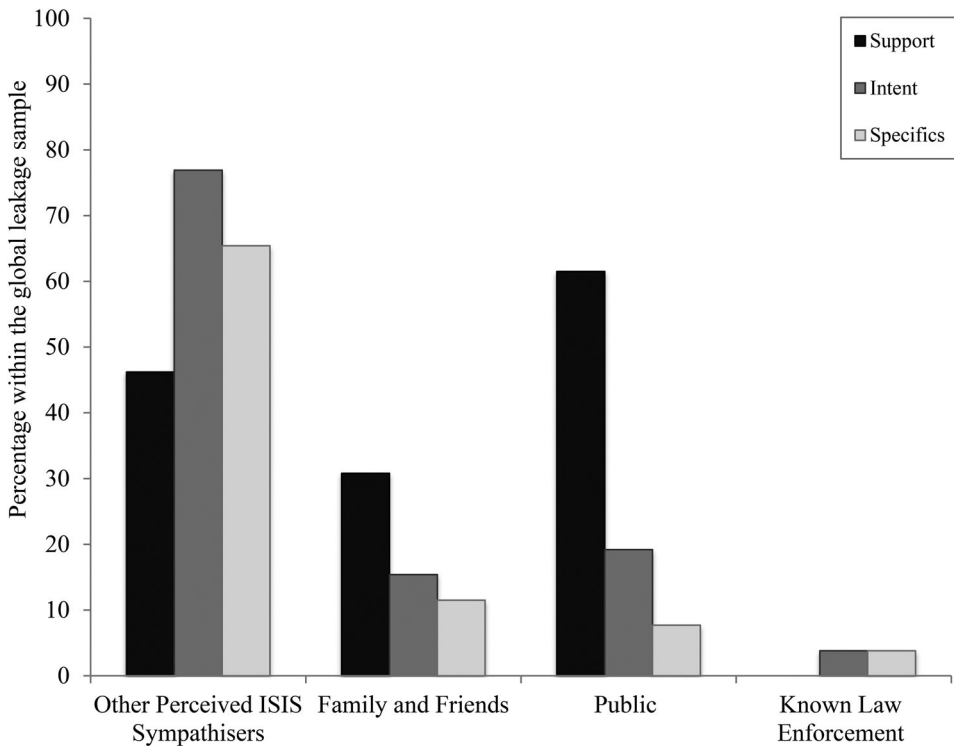


Figure 4. The percentages of those who did leak, leaking either support, intent or specifics to the four specified groups of recipients.

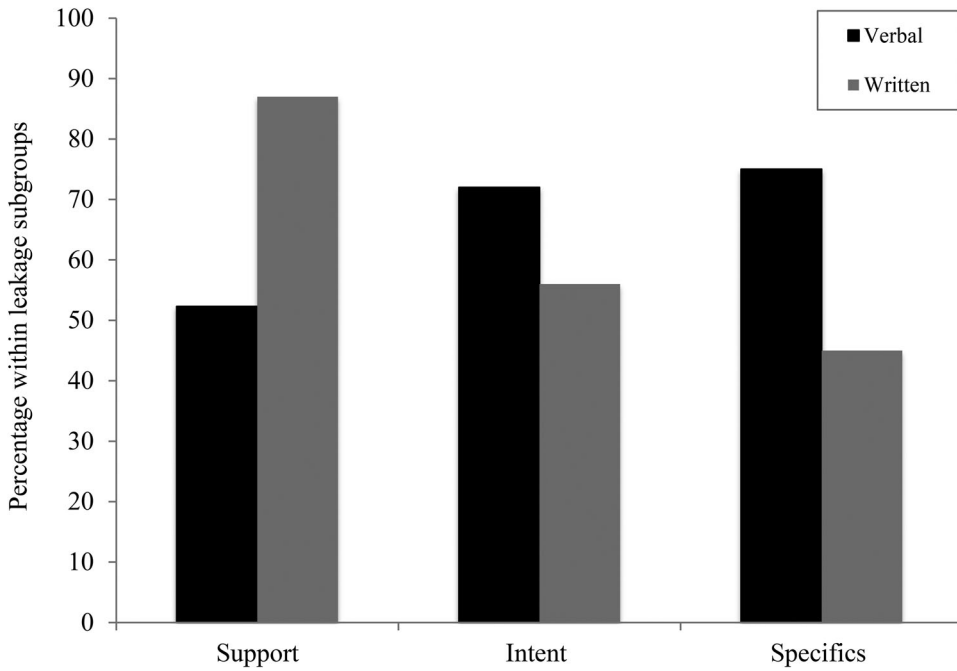


Figure 5. The percentages of those within each leakage subgroup leaking verbally or through written text.

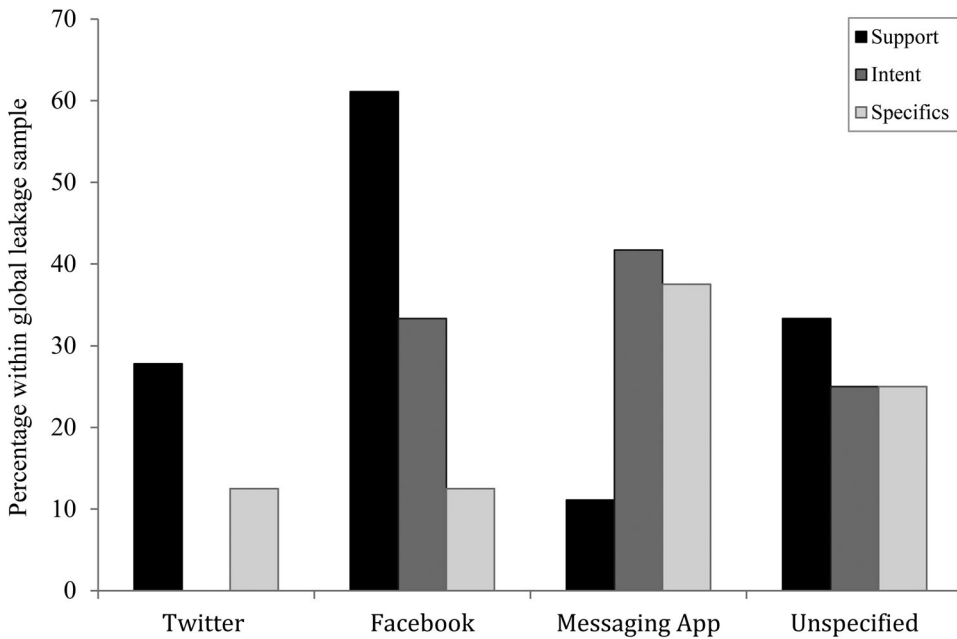


Figure 6. The percentages of those who did demonstrate leakage ($n = 26$) leaking support, intent and specifics on the four specified online platforms.

between fixation warning behavior and the leakage of support (Fisher's test; $p = .009$), but no significant relationship was found between leakage and identification warning behavior (Fisher's test; $p = .06$).

Discussion

In line with previous research, such as that conducted by Meloy and Gill (2016) and Schuurman, Bakker, et al. (2018), this study found that a large majority (83.9%) of the lone-actor sample demonstrated leakage warning behavior in the build up to their planned attacks. This finding, therefore, reiterates that there is a considerable prevalence of leakage warning behavior in lone-actor terrorists. This section will now critically discuss the results with the aim of breaking down the concept of leakage and further develop our understanding of this behavior.

Recipients

This study found that the prevalence of leakage disclosed to the four specified recipient groups varied to a noteworthy extent. In the highest majority (76.9%) of leakage cases information was leaked to other perceived ISIS sympathizers; in a slightly smaller majority (65.4%) information was leaked to the public, and in a moderate minority (38.5%) of the sample information was leaked to family and close friends. When considering these findings, it is necessary to emphasize a few key points.

Firstly, it is important to consider the possibility that the psychology and motivation driving leakage behavior towards the various recipients is likely to vary. For instance, leaking to the public might be driven by a longing to frighten or intimidate the community, or by a desire for infamy (Schuurman, Bakker, et al. 2018). In contrast, it might be the case that leaking to other perceived ISIS sympathizers is driven by existing anxieties regarding the details of a particular plan or is simply viewed as a necessary means of communication to proceed with the preparations for an attack. Interestingly, whilst most of these ideas do not appear to have been discussed in the existing literature, they are, to some extent, supported by the results of this study when we consider the three different subgroups of leakage. For instance, it was found that 'intentions' and plot 'specifics' were leaked to other perceived ISIS sympathizers more frequently than any other recipient, whilst 'support' for violent extremism etc. was leaked most frequently to the public. These findings do carry some importance because it also shows that some of the most informative content regarding intent and plot specifics is more likely to be leaked to other perceived ISIS sympathizers and could therefore be less readily identified by counterterrorism organizations. With this in mind, it is also important to consider whether leaking to other perceived ISIS sympathizers is actually a true form of leakage. Is it not instead attack planning? If this were deemed to be the case, one might argue that those lone actors leaking to other perceived ISIS sympathizers should be removed from the sample altogether. Importantly, however, Schuurman and Eijkman (2015) specify that 'unfocused attack planning' might involve an individual expressing their desire to commit an unspecified attack. 'They may, for instance, let slip that they desire to "do something" or kill "someone"' (p.13). Thus, one could argue that in some instances attack planning might in fact mimic the leakage of intent. Furthermore,

in this study, in the majority of the cases where leakage to other perceived ISIS sympathizers appears to be similar to that of attack planning, the same lone actors also leaked to the public, family and friends and/or law enforcement. Thus, should it still be argued that those leaking to other perceived ISIS sympathizers should be removed from the sample, the total number of leakage cases identified in this study would be reduced by just four as seventeen out of the 21 lone actors that did leak to other perceived ISIS sympathizers also leaked to one or more other groups of recipients.

Secondly, given that a majority of those that did leak did so to the public, it does seem important to highlight that the link between leakage and any subsequent involvement of counter-terrorism organizations is likely to depend on the individual (or member of the public) that sees, reads, or hears about it (Meloy & O'Toole, 2011). This is because if a witness lacks the motivation or appropriate knowledge to report an incident of leakage, counter-terrorism organizations will remain unaware of its existence (Borum, 2013; Gill et al., 2017). Importantly, in society this issue might also be augmented due to the bystander effect. This effect has long been examined in social psychology, and refers to the idea that '... an individual's likelihood of helping decreases when passive bystanders are also present in a critical situation' (taken from Fischer et al., 2011, p. 517; Darley & Latane, 1968; Latane & Darley, 1968; 1970; Latané & Nida, 1981). Crucially, this concept might apply to anticipated targeted violent events, such as terrorist attacks, when a third party knows or assumes that other people know of the threat, believes that they are better equipped to report the threat, and therefore does nothing about it (Meloy & O'Toole, 2011). Interestingly, however, some research has found that the bystander effect can be weakened when situations are perceived as dangerous (Fischer et al., 2011); and thus with this research in mind, educating the public about the significance of leakage behavior and the potential dangerousness of the individual behind it should be deemed a priority.

Mediums and the internet

This study also found that leakage was communicated both verbally and through written text. While the overall prevalence of verbal versus written leakage did not vary significantly, a noteworthy pattern did emerge when these two mediums were considered in relation to the leakage of support, intent or specifics. While intent and specifics were leaked most often through verbal communication, support was leaked more regularly through written text. Interestingly, this elevated prevalence of written support does seem fitting when one also considers the fact that 78.3% of those leaking support did so online. Some research suggests that this latter finding might be explained by the relative anonymity of the Internet (Bargh & McKenna, 2004), which is thought to reduce feelings of responsibility for one's online behaviors (Dutton, 2007), to diminish the negative emotional consequences of one's actions (Meloy & Yakeley, 2014), and to subsequently intensify the lone-actor's willingness to express their radical views online. In contrast, this study found that the leakage of more important information, such as intent and specifics, was done most frequently offline – a finding that is also consistent with previous research. For example, Mueller and Stewart (2015) analyzed 61 cases of Islamic terrorism in the US from September 11th 2011 to 2015, and also found that some of the most important information was communicated with greater secrecy face-to-face (Zeman et al., 2017).

At first, when considering the overall high prevalence of leakage found online, one might argue that stringently analyzing all skeptical Internet activity would be a particularly informative and efficient exercise for counterterrorism, especially given that intercepting electronic leakage would be far easier than intercepting non-electronic communications, such as paper letters (Mueller & Stewart, 2015). However, manually searching online for all potential terrorist communications is virtually impossible (Zeman et al., 2017), and this study even shows that the most informative forms of leakage cannot always be found online in the first place. One must also note that even if we did stringently search and find leakage online, not all those who have leaked will go on to commit acts of terrorism (Holt et al., 2015; Khalil, 2014; Schuurman & Eijkman, 2015; Zeman et al., 2017) – an observation further discussed later in this discussion. Furthermore, it should be noted that, in this sample, when support was shared online it was most commonly done so on Facebook – an online platform that is deemed more private and less open to the public in comparison to others such as Twitter (Kwon et al., 2014). It is important that when we assess online interaction we do not consider it to be homogenous. There must be a respect for the variety of platforms, and even the variety of forms of communication within an individual platform. One must also consider the nature of the pre-existing online and offline relationships between the communicators. With a larger dataset of actors and interactions a more nuanced analysis reflecting this heterogeneity could be plausible.

Unsurprisingly, even when lone actors do share their thoughts, feelings, and occasionally their plans, online, they appear to refrain from doing so on the most public and readily accessible platforms. It does, therefore, seem important to suggest that counterterrorism organizations should not rely on the Internet as the *main* tool for identifying and retrieving information about particular terrorist cases, but rather use it as a supplementary source. In support of this suggestion, researchers such as Zeman et al. (2017) have argued that the Internet might play a more significant role in providing insight into the process of radicalization rather than the preparations of an attack.

Mental health

This study also found that 38.7% of the sample was reported as having a mental illness of some sort. This is similar to that previously found by Gill et al. (2014), who reported that 31.9% of their sample had a history of mental illness or personality disorder. In addition, and of more interest for this particular study, no significant interaction between leakage and mental health was found. This finding challenges previous ideas that offenders with mental illness ‘... might plausibly be less able to regulate their communication and more likely to leak their intentions to commit acts of violence’ (Silver et al., 2018, p. 98), and instead supports the literature that suggests that there is an incorrect conflation of mental disorder with irrationality (Fein & Vossekuil, 1999). For example, it has been found that lone-actors with mental illness are just as capable of displaying rational motives (Gill et al., 2014), engaging in rational and sophisticated attack planning behaviors (Borum, 2013; Corner & Gill, 2015) and successfully executing attacks (Fein & Vossekuil, 1999). Our finding adds to this research and suggests that lone-actor terrorists with mental illness are just as likely as those without mental illness to engage in leakage warning behavior. The existence of any relationship between different mental illnesses

and different patterns of leakage, however, is not clear due to the small sample size of this study and further research is required.

Limitations and future research

Some of the findings discussed thus far have given us valuable further insight into leakage warning behavior. However, it is also important to raise awareness about the limitations of this research, and to discuss the consequential areas for development in future studies.

Firstly, the sample size of this study was small ($n = 31$). Whilst this is a shared limitation with previous lone-actor research (e.g. Schuurman, Bakker, et al. 2018 similarly analyzed only 55 lone-actor terrorists), and inevitable in this study given the limited population of ISIS inspired lone-actor terrorists based in the US, it is necessary to treat all findings discussed so far as preliminary and with caution. Furthermore, it is important to highlight that having such a small sample size did mean that the researcher was unable to draw any inferences about the types of mental illnesses evident in the sample. Similarly, it was deemed inappropriate to infer anything about the relationship between leakage and attack type. This is due to the finite number of leakage cases that ended up occurring before particular types of attacks. For instance, whilst 18 individuals in this sample planned shooting attacks, only two individuals planned to execute both stabbing and vehicle attacks. Therefore, drawing any conclusions about the percentages of those who leaked within these different attack types could lead to premature and misleading conclusions about the likelihood of leakage prior to particular types of attack. Nevertheless, understanding whether a relationship between leakage and attack type does exist could be of great utility for counterterrorism, and therefore this should be an area to target in future research.

When considering the methodology of this study, five key limitations arise. Firstly, not all relevant information sought after in this study was necessarily reported in the court documents analyzed. Secondly, in the instances where additional open sources were required to identify missing information, the amount of data available for certain lone actors varied in a systematic way that could undermine the validity of our findings. For example, high profile lone actor attacks were given more attention and coverage in the media in comparison to those deemed to be lower profile, and yet our data collection was limited to what could be reasonably collected for each case. Whilst this methodological issue is perhaps unavoidable, it is worth keeping in mind when considering that some cases in this dataset are missing data. It is also plausible that the results of this study have been prone to both hindsight and confirmatory bias. This is because it is much easier to identify warning behaviors retrospectively than it would be to identify them prospectively (Meloy & Gill, 2016); and it is possible that marginal evidence in support of leakage and other warning behaviors was searched for and too readily included in this study due to the knowledge of the previously found existence of these behaviors in lone-actor terrorists. Whilst this limitation was hard to overcome in this study due to the inability to blind the researcher to the subject matter etc., simply being mindful of this issue has hopefully lessened its impact. In future studies, however, it is worth ensuring multiple coders of the court reports in order to minimize the subjectivity and potential bias in the findings, and to maximize the inter-rater reliability. This study, like many others in terrorism research, did not include a control-group. Unfortunately, this shortcoming does mean that this

study is at risk of overlooking the simple facts that, in the wider population of lone-actor terrorists, not all those who demonstrate leakage behavior go on to perform terrorist attacks (Holt et al., 2015; Khalil, 2014; Schuurman & Eijkman, 2015; Zeman et al., 2017), and not all those who commit acts of terrorism leak (Schuurman, Bakker, et al. 2018). Including these types of lone actors within their own control groups in future studies would, firstly, enable research to examine whether there are any notable characteristics or behaviors that could help distinguish true warning signals from the 'noise' of those who don't follow through (Meloy et al., 2015), and secondly, enable research to examine whether there are any significant behaviors that are most likely to be present in the absence of leakage altogether. Finally, it is important to highlight that by heavily relying on court documents, this research does not capture the lone-actor terrorists who successfully carry out their attacks and die during the course of doing so. Is it possible that these individuals' success might be due to the fact that they leak less? Further research is required to explore these sorts of questions.

Whilst implementing stringent inclusion/exclusion criteria was both fundamental and effective in producing a manageable and focused piece of exploratory research, we must highlight that these criteria do restrict our knowledge in a few ways. Perhaps most notably, this sample included lone actors who had been inspired by ISIS only, and who planned to attack in the US. However, whilst ISIS does present as one of the most threatening terrorist organizations of this present day, society is also seeing an increase in other terrorist typologies, such as right-wing extremism (Koehler, 2016; Meloy & Gill, 2016). Furthermore, whilst lone-actor terrorism is a particular concerning phenomenon in the US, it is also evolving in Europe (Schuurman, Lindekilde, et al., 2018) and elsewhere. It is, therefore, crucial that future research considers leakage behavior in those with alternative typologies, and in those plotting attacks in different countries. This would then enable us to understand whether identified patterns of leakage warning behaviors are apparent within lone-actor terrorism as a whole, rather than remaining only inherent to those included within this sample.

Whilst this study did aim to assess the relationship between leakage and other warning behaviors, the nature of the court reports used in this study did mean that no reliable evaluation of these relationships could be made. This was primarily because during data collection it did become apparent that in written text, fixation, identification and leakage warning behaviors coincided with each other to a considerable extent. For example, whilst the results of the analysis do suggest that the prevalence of fixation warning behavior significantly increases in the presence of leakage behavior, one argues that this might be due to the fact that, during coding, evidence for one warning behavior was often also perceived to be indicative of another. In order to alleviate this shortcoming, future methodologies might also need to include psychological assessments for certain warning behaviors in replacement of, or in addition to, examining their presence in written text. Importantly, this is an area that does demand further attention because assessing leakage in the context of other behaviors is essential in order to determine its dangerousness and predictive value (O'Toole, 2000).

The final limitation of this study comes to light when one considers the significant relationships found between leakage and FBI interaction, and leakage and attack initiation. Specifically, it was found that, in the presence of leakage warning behavior,

the cases of FBI interaction significantly increased, and, therefore perhaps unsurprisingly, the chances of attack initiation notably decreased. These results alone do beg the question – why, when it appears so counterproductive, do lone actors leak at all? However, what this study does fail to consider is the timing of both leakage and FBI involvement. This means that one is actually unable to conclude whether FBI involvement was a result of the leakage, or in actual fact, if it was the cause. This apparent issue has briefly been mentioned in the literature (Spalek & O’Rawe, 2014), and heavily in the media – where a number of friends and family of those found guilty of terrorist charges have argued that the lone actors in question have been set up by the FBI and tricked into disclosing their thoughts, feelings and plans that they would have otherwise not alluded to (Associated Press 11 December 2019). For example, in one case, the friends and family of a lone actor included in this sample said that the FBI was responsible for manipulating him into actually thinking and expressing that he could commit an act of terrorism. Future research should therefore strive to more closely examine leakage and FBI involvement – then, the counter-productivity of leakage could be more reliably affirmed, and its true prevalence more definitely understood.

Conclusion

With the key limitations of this study highlighted, it is of course important to recall its strengths, and to recapitulate what this research does have to offer. Importantly this study set out to develop our understanding of leakage warning behavior, and it did so in a small yet focused sample of lone-actor terrorists, using some novel and more accurate open-source research methods. Crucially the findings have highlighted that leakage is by no means a uniform concept, and it is now more apparent that certain types of leakage tend to be leaked to particular individuals, and through certain types of mediums. For example, whilst support for extremist ideology was leaked most frequently to the public via written text and on the Internet, intent and specifics appeared to be more regularly leaked to other perceived ISIS sympathizers through verbal communication that avoided the online world. Whilst some of these findings are novel and important, it is, of course, necessary to recognize that they only scratch the surface of what there is to know about leakage and other warning behaviors in lone-actor terrorists. For this reason, it is imperative that this research is viewed as exploratory and preliminary, and that its potential is also recognized and subsequently built upon in ways that will benefit our understanding of what is a deeply complex, unfolding and contemporary phenomenon.

Notes

1. Case 9 – United States District Court for the Western District of New York. Application for a Search Warrant: Case No. 14-MJ-635: 6 August 2014. Available online: <https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Elfgeeh%20Affidavit.PDF> (Last Accessed 25 February 2021).
2. Case 10 – United States of America v Daniel Seth Franey, United States District Court for the Western District of Washington at Tacoma. Available online <https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Franey%20Complaint.pdf> (Last Accessed 25 February 2021).

3. Case 6 – United States of America v Miguel Moran Diaz, United States District Court for the Southern District of Florida, 2 April 2015. Available online: <https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Diaz%20Criminal%20Complaint.pdf> (Last Accessed 25 February 2021).
4. Case 31 – United States of America v Clark Calloway, United States District Court for the District of Columbia, 5 May 2017. Available online: https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Calloway_criminal%20complaint.pdf (Last Accessed 25 February 2021).
5. Case 2 – United States of America v Christopher Lee Cornell, United States District Court for the Southern District of Ohio, 14 January 2015. Available online: <https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Cornell%20Criminal%20Complaint.pdf> (Last Accessed 25 February 2021).
6. Case 3 – Affidavit for Arrest Warrant in the name and by the Authority of the State of Texas. CS No. 18045858. Available online: <https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/AziziYarandAffidavitforArrestWarrant.pdf> (Last Accessed 25 February 2021).
7. Case 6 – United States of America v Miguel Moran Diaz, United States District Court for the Southern District of Florida, 2 April 2015. Available online: <https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Diaz%20Criminal%20Complaint.pdf> (Last Accessed 25 February 2021).
8. Case 26 – United States of America v Justin Nojan Sullivan, 22 June 2015. Available online: <https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Sullivan%20Criminal%20Complaint.pdf> (Last Accessed 25 February 2021).
9. Case 31 – United States of America v Clark Calloway, United States District Court for the District of Columbia, 5 May 2017. Available online: https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Calloway_criminal%20complaint.pdf (Last Accessed 25 February 2021).
10. Case 25 – United States of America v Aziz Ihab Sayyed, United States District Court Northern District of Alabama Northeastern Division, Available online <https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Sayyed%20Information.pdf> (Last Accessed 25 February 2021).

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributor

Menna Rose is a Forensic Psychology MSc student at Royal Holloway, University of London at time of writing. Now pursuing a Professional Doctorate in Counselling Psychology at City, University of London. **John Morrison**: A senior lecturer in Criminology at Royal Holloway, University of London.

ORCID

John Morrison  <http://orcid.org/0000-0003-1548-6392>

References

- Associated Press. (2019, December 11). Terror convict: I was mentally incompetent, entrapped by FBI. *Cincinnati.com*. Retrieved July 13, 2020, from <https://eu.cincinnati.com/story/news/2017/11/21/terror-convict-mentally-incompetent-entrapped-fbi/887772001/>
- Bargh, J. A., & McKenna, K. Y. (2004). The internet and social life. *Annual Review of Psychology*, 55(1), 573–590. <https://doi.org/10.1146/annurev.psych.55.090902.141922>
- Billig, O. (1985). The lawyer terrorist and his comrades. *Political Psychology*, 29–46. <https://doi.org/10.2307/3791269>
- Borum, R. (2004). *Psychology of terrorism*. University of South Florida. <http://scholarcommons.usf.edu/cgi/viewcontent.cgi>
- Borum, R. (2013). Informing lone-offender investigations. *Criminology & Public Policy*, 12(1), 103. <https://doi.org/10.1111/1745-9133.12016>

- Borum, R., Fein, R., & Vossekuil, B. (2012). A dimensional approach to analyzing lone offender terrorism. *Aggression and Violent Behavior, 17*(5), 389–396. <https://doi.org/10.1016/j.avb.2012.04.003>
- Böllinger, L. (1985). Terrorist conduct as a result of a psychosocial process. In P. Pichot, P. Berner, R. Wolf & K. Thau (Eds.), *Psychiatry* (pp. 387–389). Springer.
- Brynielsson, J., Horndahl, A., Johansson, F., Kaati, L., Mårtensson, C., & Svenson, P. (2013). Harvesting and analysis of weak signals for detecting lone wolf terrorists. *Security Informatics, 2*(1), 11. <https://doi.org/10.1186/2190-8532-2-11>
- Cohen, K., Johansson, F., Kaati, L., & Mork, J. C. (2014). Detecting linguistic markers for radical violence in social media. *Terrorism and Political Violence, 26*(1), 246–256. <https://doi.org/10.1080/09546553.2014.849948>
- Cooper, H. H. A. (1977). What is a terrorist: A psychological perspective. *Legal Medical Quarterly, 1*, 16.
- Corner, E., & Gill, P. (2015). A false dichotomy? Mental illness and lone-actor terrorism. *Law and Human Behavior, 39*(1), 23. <https://doi.org/10.1037/lhb0000102>
- Darley, J. M., & Latane, B. (1968). Bystander intervention in emergencies: Diffusion of responsibility. *Journal of Personality and Social Psychology, 8*(4, Pt.1), 377–383. <https://doi.org/10.1037/h0025589>
- Dutton, D. G. (2007). *The psychology of genocide, massacres, and extreme violence: Why normal people come to commit atrocities: Why normal people come to commit atrocities*. ABC-CLIO.
- Fein, R. A., & Vossekuil, B. (1999). Assassination in the United States: An operational study of recent assassins, attackers, and near-lethal approachers. *Journal of Forensic Science, 44*(2), 321–333. <https://doi.org/10.1520/JFS14457J>
- Fischer, P., Krueger, J. I., Greitemeyer, T., Vogrincic, C., Kastenmüller, A., Frey, D., Heene, M., Wicher, M., & Kainbacher, M. (2011). The bystander-effect: A meta-analytic review on bystander intervention in dangerous and non-dangerous emergencies. *Psychological Bulletin, 137*(4), 517. <https://doi.org/10.1037/a0023304>
- Gill, P. (2015). *Lone-actor terrorists: A behavioural analysis*. Routledge
- Gill, P., & Corner, E. (2017). There and back again: The study of mental disorder and terrorist involvement. *American Psychologist, 72*(3), 231. <https://doi.org/10.1037/amp0000090>
- 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 & Public Policy, 16*(1), 99–117. <https://doi.org/10.1111/1745-9133.12249>
- 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>
- Gruenewald, J., Chermak, S., & Freilich, J. D. (2013). Overview of: Distinguishing ‘loner’ attacks from other domestic extremist violence: A comparison of Far-right homicide incident and offender characteristics. *Criminology & Public Policy, 12*(1), 63–64. <https://doi.org/10.1111/1745-9133.12009>
- Hacker, F. J., & Hacker, F. (1976). *Crusaders, criminals, crazies: Terror and terrorism in our time*. Norton.
- Hoffmann, J., Meloy, J. R., Guldemann, A., & Ermer, A. (2011). Attacks on German public figures, 1968–2004: Warning behaviors, potentially lethal and non-lethal acts, psychiatric status, and motivations. *Behavioral Sciences & the Law, 29*(2), 155. <https://doi.org/10.1002/bsl.979>
- Holt, T., Freilich, J. D., Chermak, S., & McCauley, C. (2015). Political radicalization on the internet: Extremist content, government control, and the power of victim and jihad videos. *Dynamics of Asymmetric Conflict, 8*(2), 107–120. <https://doi.org/10.1080/17467586.2015.1065101>
- Horgan, J. (2003). The search for the terrorist personality. In A. Silke (Eds.), *Terrorists, victims and society: Psychological perspectives on terrorism and its consequences* (Vol. 3, pp. 3–27). Wiley.
- Khalil, J. (2014). Radical beliefs and violent actions are not synonymous: How to place the key disjuncture between attitudes and behaviors at the heart of our research into political violence. *Studies in Conflict & Terrorism, 37*(2), 198–211. <https://doi.org/10.1080/1057610X.2014.862902>
- Koehler, D. (2016). Right-wing extremism and terrorism in Europe. *Prism, 6*(2), 84–105. <https://www.jstor.org/stable/26470450>
- Kwon, S. J., Park, E., & Kim, K. J. (2014). What drives successful social networking services? A comparative analysis of user acceptance of Facebook and Twitter. *The Social Science Journal, 51*(4), 534–544. <https://doi.org/10.1016/j.soscij.2014.04.005>

- Latane, B., & Darley, J. M. (1968). Group inhibition of bystander intervention in emergencies. *Journal of Personality and Social Psychology*, 10(3), 215. <https://doi.org/10.1037/h0026570>
- Latané, B., & Darley, J. M. (1970). *The unresponsive bystander: Why doesn't he help?* Appleton-Century-Crofts.
- Latané, B., & Nida, S. (1981). Ten years of research on group size and helping. *Psychological Bulletin*, 89(2), 308. <https://doi.org/10.1037/0033-2909.89.2.308>
- Meloy, J. R., & Gill, P. (2016). The lone-actor terrorist and the TRAP-18. *Journal of Threat Assessment and Management*, 3(1), 37. <https://doi.org/10.1037/tam0000061>
- Meloy, J. R., Habermeyer, E., & Guldemann, A. (2015). The warning behaviors of Anders Breivik. *Journal of Threat Assessment and Management*, 2(3–4), 164. <https://doi.org/10.1037/tam0000037>
- Meloy, J. R., Hoffmann, J., Guldemann, A., & James, D. (2012). The role of warning behaviors in threat assessment: An exploration and suggested typology. *Behavioral Sciences & the Law*, 30(3), 256–279. <https://doi.org/10.1002/bsl.999>
- Meloy, J. R., Hoffmann, J., Roshdi, K., & Guldemann, A. (2014). Some warning behaviors discriminate between school shooters and other students of concern. *Journal of Threat Assessment and Management*, 1(3), 203. <https://doi.org/10.1037/tam0000020>
- Meloy, J. R., & O'Toole, M. E. (2011). The concept of leakage in threat assessment.
- Meloy, J. R., & Yakeley, J. (2014). The violent true believer as a “lone wolf”—psychoanalytic perspectives on terrorism.
- Mueller, J., & Stewart, M. G. (2015). Terrorism, counterterrorism, and the internet: The American cases. *Dynamics of Asymmetric Conflict*, 8(2), 176–190. <https://doi.org/10.1080/17467586.2015.1065077>
- O'Toole, M. E. (2000). *The school shooter: A threat assessment perspective*. DIANE Publishing.
- Pearce, K. I., & Macmillan, H. (1977). Police negotiations: A new role for the community psychiatrist. *Canadian Psychiatric Association Journal*, 22(4), 171–175. <https://doi.org/10.1177/070674377702200405>
- 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. <https://doi.org/10.1111/1556-4029.13676>
- Schuurman, B., & Eijkman, Q. (2015). Indicators of terrorist intent and capability: Tools for threat assessment. *Dynamics of Asymmetric Conflict*, 8(3), 215–231. <https://doi.org/10.1080/17467586.2015.1040426>
- Schuurman, B., Lindekilde, L., Malthaner, S., O'Connor, F., Gill, P., & Bouhana, N. (2018). End of the lone wolf: The typology that should not have been. *Studies in Conflict & Terrorism*, 42(8), 771–778. <https://doi.org/10.1080/1057610X.2017.1419554>
- Silke, A. (1998). Cheshire-cat logic: The recurring theme of terrorist abnormality in psychological research. *Psychology, Crime and Law*, 4(1), 51–69. <https://doi.org/10.1080/10683169808401747>
- Silke, A. (2003). Terrorists, victims and society. In *Terrorists, victims and society: Psychological perspectives on terrorism and its consequences* (pp. 29–53). <https://doi.org/10.1002/9780470713600.ch2>
- Silver, J., Horgan, J., & Gill, P. (2018). Foreshadowing targeted violence: Assessing leakage of intent by public mass murderers. *Aggression and Violent Behavior*, 38, 94–100. <https://doi.org/10.1016/j.avb.2017.12.002>
- Spaaij, R. (2011). *Understanding lone wolf terrorism: Global patterns, motivations and prevention*. Springer Science & Business Media.
- Spalek, B., & O'Rawe, M. (2014). Researching counterterrorism: A critical perspective from the field in the light of allegations and findings of covert activities by undercover police officers. *Critical Studies on Terrorism*, 7(1), 150–164. <https://doi.org/10.1080/17539153.2013.847264>
- United States v Abidin. (2017). *Affidavit in support of an application for a criminal complaint and arrest warrant: 2:17-mj-00081-MCRI*. Retrieved July 13, 2020, from <https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Abidin%20affidavit%20in%20support%20of%20an%20application%20for%20a%20criminal%20complaint%20and%20arrest%20warrant.pdf>
- Victoroff, J. (2005). The mind of the terrorist: A review and critique of psychological approaches. *Journal of Conflict Resolution*, 49(1), 3–42. <https://doi.org/10.1177/0022002704272040>

Zeman, T., Břeň, J., & Urban, R. (2017). Role of internet in lone wolf terrorism. *Journal of Security & Sustainability Issues*, 7(2), 2. [https://doi.org/10.9770/jssi.2017.7.2\(1\)](https://doi.org/10.9770/jssi.2017.7.2(1))

Appendices

Appendix 1 – table

Date of attack		
Attack type		
Cell number		
Target		
Inspired by		
Attack initiated		
Un-initiated attack		
Attack as planned		
Date of arrest		
Number of fatalities		
Gender		
Mental health		
Mental health diagnosis		
Age		
Interaction with undercover FBI?		
Type of terrorist		
Fixation		
Identification		
Leakage		
Support	Intent	Specifics
Verbal	Verbal	Verbal
Written	Written	Written
Both	Both	Both
Other perceived ISIS sympathizers	Other perceived ISIS sympathizers	Other perceived ISIS sympathizers
Friends and family	Friends and family	Friends and family
Public	Public	Public
Internet	Internet	Internet
Twitter	Twitter	Twitter
Facebook	Facebook	Facebook
Unspecified	Unspecified	Unspecified
Messaging application	Messaging application	Messaging application
<i>Other comments</i>		
<i>Sources</i>		

Appendix 2 – codebook

Inclusion criteria

In order to be eligible for inclusion, each individual must meet one of the following criteria:

1. The individual was arrested
2. The individual was killed as a result of his or her ideological activities – this includes being killed during the commission of an attack, including suicide or being killed during an attempted arrest/acquisition by security forces.

In addition, the individual must:

1. Have planned to, or have successfully, committed or facilitated an attack without any external commands or control links
2. Have planned to, or have successfully, committed or facilitated an attack alone, in pairs (dyads) or in small groups of threes (triads).
3. Have planned to, or have successfully, committed or facilitated a lone-actor terrorist attack in the United States

4. Have planned to, or have successfully, committed or facilitated a lone-actor terrorist attack between 31st January 2014 and 31st January 2019.
5. Have been inspired by the Islamic State of Iraq and Syria (ISIS)

Definitions of key terms

Leakage warning behavior – the behavior of a (would be) lone-actor terrorist who intentionally or unintentionally divulges their motivation or capability to commit acts of violence

Support – a type of leakage warning behavior that indicates ones support for radicalized violence, ISIS and/or previous attacks and attackers.

Intent – a type of leakage warning behavior that indicates an individual’s violent intent

Specifics – a type of leakage warning behavior that gives an indication towards the details of the research, plans and preparations of a particular event

Fixation – any behavior that indicates an increasingly pathological preoccupation with a person or cause

Identification – any behavior that indicates a psychological desire to be a ‘pseudo-commando’, have a ‘warrior mentality’, closely associate with weapons or other military or law enforcement paraphernalia, identify with previous attackers or assassins, or identify oneself as an agent to advance a particular cause or belief system

Attacker – an individual who actively plans to, or succeeds in, carrying out a terrorist attack themselves

Facilitator – an individual who engages in nonviolent behaviors that facilitates or encourages others to carry out violent actions that intend to cause terror and do harm to others

Lone-actors – ‘operate autonomously and independently of a groups (in terms of training, preparation and target selection, etc. In some cases, the individual may have radicalized toward violence within a wider group but left and engaged in illicit behaviors outside of a formal command and control structure’ (Gill et al., 2014, p. 426)

Isolated dyads – ‘include pairs of individuals who operate independently of a group. They may have become radicalized to violence on their own (or one may have radicalized the other), and they conceive, develop and carry out activities without direct input from a wider network’ (Gill et al., 2014, p. 426)

Isolated triads – include small groups of three individuals who operate independently of a group. Again, they may have become radicalized to violence on their own, or have all radicalized one another, and they must still conceive, develop and carry out activities without direct input from a wider network.

Other perceived ISIS sympathizers – other individuals or strangers who are perceived to have similar views and ideas with regards to the Islamic State.

Recipients – those individuals on the receiving end of leakage.

FBI interaction – the engagement in conversation, either virtual or face-to-face, between an undercover FBI agent and a lone-actor terrorist.

Variables

1. Field name: Subject ID

Variable Type: Numerical

Description: Unique 2-digit numerical identifier for each individual in the dataset.

1. Field name: Gender

Variable type: Dichotomous

Description: What is the individual's gender?

0 = Female

1 = Male

1. Field name: Date_attack

Variable type: Date

Description: Enter the data (using the format dd.mm.yyyy) at which the individual's attack took place. If attack did not take place, list -88. If date of attack is unknown, list -99.

1. Field name: Date_arrest

Variable type: Date

Description: Enter the date (using the format dd.mm.yyyy) at which the individual was arrested. If arrest did not take place, list -88. If date of arrest is unknown, list -99.

1. Field name: Age

Variable type: Numerical

Description: What was the age of the individual at the date of the arrest? If the individual died during the attack, list their age at this time.

1. Field name: Attack_type

Variable type: Categorical

Description: What type of attack was planned or executed? If unknown, list -99.

1 = Shooting

2 = Bombing

3 = Stabbing

4 = Vehicle

1. Field name: Attack_Initiated

Variable type: Dichotomous

Description: Was the attack executed?

0 = No

1 = Yes

If the answer to variable 7 is no, proceed with variable 8. If the answer is yes, proceed to variable 9.

1. Field name: Uninitiated_Attack

Variable type: Categorical

Description: For what reason was the attack not executed?

- 1 = Thwarted
- 2 = Malfunction
- 3 = Change of mind

1. *Field name:* Attack_As_Planned

Variable type: Categorical

Description: Was the executed attack the one planned by the lone-actor(s)?

- 0 = No
- 1 = Yes

1. *Field name:* Fatalities

Variable type: Numerical

Description: If attack was executed, how many fatalities were there? If attack thwarted, list –88. If number of fatalities unknown, list –99.

1. *Field name:* Target1

Variable type: Categorical

Description: Who was the target of the attack, or the planned attack? If unknown, list –99.

- 1 = Civilians
- 2 = Specified individual
- 3 = Military personnel
- 4 = Law enforcement
- 5 = Government officials

1. *Field name:* Target2

Variable type: Categorical

Description: Who was the second target of the attack, or the planned attack? If there was no second target, list –88.

- 1 = Civilians
- 2 = Specified individual
- 3 = Military personnel
- 4 = Law enforcement
- 5 = Government officials

1. *Field name:* Target3

Variable type: Categorical

Description: Who was the third target of the attack, or the planned attack? If there was no third target, list -88.

- 1 = Civilians
- 2 = Specified individual
- 3 = Military personnel
- 4 = Law enforcement
- 5 = Government officials

1. *Field name:* Role

Variable type: Categorical

Description: What specific role did the individual have in the attack/planned attack?

- 1 = Attacker

- 2 = Facilitator
- 3 = Both

1. *Field name:* Cell_number

Variable type: Categorical

Description: Was the individual operating alone or in a cell (of up to three members)? If unknown, list -99.

- 1 = Lone-actor
- 2 = Dyad
- 3 = Triad

1. *Field name:* FBI_interaction

Variable type: Dichotomous

Description: Was the FBI in contact with this individual prior to the arrest or attack?

- 0 = No
- 1 = Yes

If the answer to variable 16 is yes, proceed with 17. If the answer is no, proceed to variable 18.

1. *Field name:* Understanding_of_FBI

Variable type: Categorical

Description: Who did the individual believe the undercover agent to be?

- 1 = Other perceived ISIS sympathizer
- 2 = Unsure

1. *Field name:* Mental_Health

Variable type: Categorical

Description: Is there reportedly a history of mental illness for this individual? If there is no information assume 0 for no.

- 0 = No
- 1 = Yes – through speculation
- 2 = Yes – professionally diagnosed

If the answer to variable 18 is no, proceed to variable 25. If the answer to variable 18 is 'yes – through speculation', proceed with variables 19–21. If the answer to variable 18 is 'yes – professionally diagnosed', proceed with variables 22–24.

1. *Field name:* Speculation_Diagnosis1

Variable type: Categorical

Description: Was the individual diagnosed (through speculation) with one of the following?

- 1 = Unspecified
- 2 = Schizophrenia
- 3 = Substance abuse
- 4 = Alcoholism
- 5 = Bipolar Disorder
- 6 = Obsessive Compulsive Disorder
- 7 = Psychosis

1. *Field name:* Speculation_Diagnosis2

Variable type: Categorical

Description: Was the individual diagnosed (through speculation) with one of the following?

- 1 = Unspecified
- 2 = Schizophrenia
- 3 = Substance abuse
- 4 = Alcoholism
- 5 = Bipolar Disorder
- 6 = Obsessive compulsive Disorder
- 7 = Psychosis

1. *Field name:* Speculation_Diagnosis3

Variable type: Categorical

Description: Was the individual diagnosed (through speculation) with one of the following?

- 1 = Unspecified
- 2 = Schizophrenia
- 3 = Substance abuse
- 4 = Alcoholism
- 5 = Bipolar Disorder
- 6 = Obsessive compulsive Disorder
- 7 = Psychosis

1. *Field name:* Professional_Diagnosis1

Variable type: Categorical

Description: Was the individual professionally diagnosed with one of the following?

- 1 = Unspecified
- 2 = Schizophrenia
- 3 = Substance abuse
- 4 = Alcoholism
- 5 = Bipolar Disorder
- 6 = Obsessive compulsive Disorder
- 7 = Psychosis

1. *Field name:* Professional_Diagnosis2

Variable type: Categorical

Description: Was the individual professionally diagnosed with one of the following?

- 1 = Unspecified
- 2 = Schizophrenia
- 3 = Substance abuse
- 4 = Alcoholism
- 5 = Bipolar Disorder
- 6 = Obsessive compulsive Disorder
- 7 = Psychosis

1. *Field name:* Professional_Diagnosis3

Variable type: Categorical

Description: Was the individual professionally diagnosed with one of the following?

- 1 = Unspecified
- 2 = Schizophrenia
- 3 = Substance abuse
- 4 = Alcoholism
- 5 = Bipolar Disorder

6 = Obsessive compulsive Disorder
7 = Psychosis

Leakage

1. Field name: Leakage

Variable type: Dichotomous

Description: Was there any evidence of leakage warning behavior prior to the attack/arrest?

0 = No

1 = Yes

If the answer to variable 25 is no, proceed to variable 71. If the answer is yes, proceed with variable 26.

1. *Field name:* Other perceived ISIS sympathizer

Variable type: Dichotomous

Description: Did this individual leak to other perceived ISIS sympathizers?

0 = No

1 = Yes

1. *Field name:* Family_friends

Variable type: Dichotomous

Description: Did this individual leak to close family or friends?

0 = No

1 = Yes

1. Field name: Public

Variable type: Dichotomous

Description: Did this individual leak to members of the public or close friends?

0 = No

1 = Yes

1. *Field name:* Known_Law_Enforcement

Variable type: Dichotomous

Description: Did this individual leak to known members of law enforcement?

0 = No

1 = Yes

1. *Field name:* Verbal

Variable type: Dichotomous

Description: Did this individual leak through verbal communication?

0 = No

1 = Yes

1. *Field name:* Written

Variable type: Dichotomous

Description: Did this individual leak through written text?

1. *Field name:* Both

Variable type: Dichotomous

Description: Did this individual leak through both verbal communication and written text?

0 = No

1 = Yes

1. *Field name:* Internet

Variable type: Dichotomous

Description: Did this individual leak online?

0 = No

1 = Yes

1. *Field name:* Twitter

Variable type: Dichotomous

Description: Did this individual leak on Twitter?

0 = No

1 = Yes

1. *Field name:* Facebook

Variable type: Dichotomous

Description: Did this individual leak on Facebook?

0 = No

1 = Yes

1. *Field name:* Unspecified

Variable type: Dichotomous

Description: Did this individual leak on an unspecified online platform?

0 = No

1 = Yes

1. *Field name:* Messaging_App

Variable type: Dichotomous

Description: Did this individual leak on a messaging application?

0 = No

1 = Yes

Support

1. *Field name:* Support

Variable type: Categorical

Description: Did the individual leak support for ISIS?

0 = No

1 = Yes

If the answer to variable 38 is yes, proceed with variable 39. If the answer is no, proceed to variable 49.

1. *Field name:* Support_Medium

Variable type: Categorical

Description: Was information leaked verbally?

1 = Verbal

2 = Written

3 = Both

1. *Field name:* Support_Internet

Variable type: Categorical

Description: Did any leakage take place online?

0 = No

1 = Yes

If the answer to variable 40 is yes, proceed to variable 41. If the answer was no, proceed with variable 45.

1. *Field name:* Support_Twitter

Variable type: Dichotomous

Description: Was support for ISIS leaked on Twitter?

0 = No

1 = Yes

1. *Field name:* Support_Facebook

Variable type: Dichotomous

Description: Was support for ISIS leaked on Facebook?

0 = No

1 = Yes

1. *Field name:* Support_Unspecified

Variable type: Dichotomous

Description: Was support for ISIS leaked on an unspecified online platform?

0 = No

1 = Yes

1. *Field name:* Support_Messaging_App

Variable type: Dichotomous

Description: Was support for ISIS leaked on an unspecified online platform?

0 = No

1 = Yes

1. *Field name:* Support_Coconspirators

Variable type: Dichotomous

Description: Was support for ISIS leaked to coconspirators?

0 = No

1 = Yes

1. *Field name:* Support_Family

Variable type: Dichotomous

Description: Was support for ISIS leaked to family members, or close friends.

0 = No

1 = Yes

1. *Field name:* Support_Public

Variable type: Dichotomous

Description: Was support for ISIS leaked to members of the public?

0 = No

1 = Yes

1. *Field name:* Support_Law_Enforcement

Variable type: Dichotomous

Description: Was support for ISIS leaked to law enforcement?

0 = No

1 = Yes

Intentions

1. *Field name:* Intentions

Variable type: Dichotomous

Description: Did the individual leak information about his or her intentions to commit a lone-actor terrorist attack?

0 = No

1 = Yes

If answer to variable 49 is no, proceed to variable 60. If answer is yes, proceed with variable 50.

1. *Field name:* Intent_Medium

Variable type: Dichotomous

Description: How did the individual leak specific information about the plot, plans and/or preparations?

1 = Verbal

2 = Written

3 = Both

1. *Field name:* Intent_Internet

Variable type: Dichotomous

Description: Did the individual leak any intentions online?

0 = No

1 = Yes

If answer to variable 51 is yes, proceed with variable 52. If the answer is no, skip to variable 56.

1. *Field name:* Intent_Twitter

Variable type: Dichotomous

Description: Was intent to commit a lone-actor terrorist attack leaked on Twitter?

0 = No

1 = Yes

1. *Field name:* Intent_Facebook

Variable type: Dichotomous

Description: Was intent to commit a lone-actor terrorist attack leaked on Facebook?

0 = No

1 = Yes

1. *Field name:* Intent_Unspecified

Variable type: Dichotomous

Description: Was intent to commit a lone-actor terrorist attack leaked on an unspecified social media platform?

0 = No

1 = Yes

1. *Field name:* Intent_Messaging_App

Variable type: Dichotomous

Description: Was intent to commit a lone-actor terrorist attack leaked on a messaging app?

0 = No

1 = Yes

1. *Field name:* Intent_coconspirators

Variable type: Dichotomous

Description: Was intent to commit a lone-actor terrorist attack leaked to other perceived ISIS sympathizers?

0 = No

1 = Yes

1. *Field name:* Intent_Family

Variable type: Dichotomous

Description: Was intent to commit a lone-actor terrorist attack leaked to family members?

0 = No

1 = Yes

1. *Field name:* Intent_Public

Variable type: Dichotomous

Description: Was intent to commit a lone-actor terrorist attack leaked to members of the public?

0 = No

1 = Yes

1. *Field name:* Intent_Law_Enforcement

Variable type: Dichotomous

Description: Was intent to commit a lone-actor terrorist attack leaked to law enforcement?

0 = No

1 = Yes

Specifics

1. Field name: Specifics

Variable type: Dichotomous

Description: Did the individual leak specific information about the details of the plot, plans and/or preparations?

0 = No

1 = Yes

If answer to variable 60 is no, proceed to variable 59. If answer is yes, proceed with variable 49.

1. Field name: Specifics_Medium

Variable type: Dichotomous

Description: How did the individual leak specific information about the plot, plans and/or preparations?

1 = Verbally

2 = Written text

3 = Both

1. Field name: Specifics_Internet

Variable type: Dichotomous

Description: Was specific information about the plot, plans and/or preparations leaked online?

0 = No

1 = Yes

1. Field name: Specifics_Twitter

Variable type: Dichotomous

Description: Was specific information about the plot, plans and/or preparations leaked on Twitter?

0 = No

1 = Yes

1. Field name: Specifics_Facebook

Variable type: Dichotomous

Description: Was specific information about the plot, plans and/or preparations leaked on Facebook?

0 = No

1 = Yes

1. Field name: Specifics_Unspecified

Variable type: Dichotomous

Description: Was specific information about the plot, plans and/or preparations leaked on an unspecified online platform?

0 = No

1 = Yes

1. Field name: Specifics_Messaging_App

Variable type: Dichotomous

Description: Was specific information about the plot, plans and/or preparations leaked on a messaging app?

1. *Field name:* Specifics_Coconspirators

Variable type: Dichotomous

Description: Did the individual leak specific information about the plots, plans and/or preparations to coconspirators and believers?

0 = No

1 = Yes

1. *Field name:* Specifics_Family

Variable type: Dichotomous

Description: Did the individual leak specific information about the plots, plans and/or preparations to family members and close friends?

0 = No

1 = Yes

1. *Field name:* Specifics_Public

Variable type: Dichotomous

Description: Did the individual leak specific information about the plot, plans and/or preparations to members of the public?

0 = No

1 = Yes

1. *Field name:* Specifics_Law_Enforcement

Variable type: Dichotomous

Description: Did the individual leak specific information about the plot, plans and/or preparations to any member(s) of law enforcement?

0 = No

1 = Yes

Other warning behaviors

1. *Field name:* Fixation

Variable type: Dichotomous

Description: Did the individual demonstrate any fixation warning behavior in the run up to the attack / planned attack?

0 = No

1 = Yes

1. *Field name:* Identification

Variable type: Categorical

Description: Did the individual demonstrate any identification warning behavior in the run up to the attack / planned attack?

0 = No

1 = Yes