Terrorist Use of the Internet by the Numbers

Quantifying Behaviors, Patterns, and Processes

Paul Gill
Emily Corner
University College London

Maura Conway
Dublin City University

Amy Thornton
University College London

Mia Bloom
John Horgan
Georgia State University

Research Summary

Public interest and policy debates surrounding the role of the Internet in terrorist activities is increasing. Criminology has said very little on the matter. By using a unique data set of 223 convicted United Kingdom–based terrorists, this article focuses on how they used the Internet in the commission of their crimes. As most samples of terrorist offenders vary in terms of capabilities (lone-actor vs. group offenders) and criminal sophistication (improvised explosive devices vs. stabbings), we tested whether the affordances they sought from the Internet significantly differed. The results suggest that extreme-right-wing individuals, those who planned an attack (as opposed to merely providing material support), conducted a lethal attack, committed an improvised explosive device (IED) attack, committed an armed assault, acted within a cell, attempted to recruit others, and engaged in nonvirtual network activities and nonvirtual place interactions were significantly more likely to learn online compared with those who did not engage

The research leading to these results has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 312827 under project name VOX-POL. Direct correspondence to Paul Gill, University College London, 35 Tavistock Square, London, WC1H 9EZ, United Kingdom (e-mail: paul.gill@ucl.ac.uk).

DOI:10.1111/1745-9133.12249

in these behaviors. Those undertaking unarmed assaults were significantly less likely to display online learning. The results also suggested that extreme-right-wing individuals who perpetrated an IED attack, associated with a wider network, attempted to recruit others, and engaged in nonvirtual network activities and nonvirtual place interactions were significantly more likely to communicate online with co-ideologues.

Policy Implications

Collectively the results provide insight into violent radicalization as a whole and not just into violent online radicalization. The results also largely confirm the results found in von Behr, Reding, Edwards, and Gribbon (2013) and in Gill and Corner (2015). The current study and the two previous studies have tackled these questions by using numerous methodological approaches and data sources and have arrived at similar conclusions. The Internet is largely a facilitative tool that affords greater opportunities for violent radicalization and attack planning. Nevertheless, radicalization and attack planning are not dependent on the Internet, and policy needs to look at behavior, intentions, and capabilities and not just at beliefs. From a risk assessment perspective, the study also highlights the fact that there is no easy offline versus online violent radicalization dichotomy to be drawn. It may be a false dichotomy. Plotters regularly engage in activities in both domains. Often their behaviors are compartmentalized across these two domains. Threat management policies would do well to understand the individuals' breadth of interactions rather than relying on a dichotomous understanding of offline versus online, which represent two extremes of a spectrum that regularly provide prototypical examples in reality. A preoccupation with only checking online behaviors may lead an intelligence analyst to miss crucial face-to-face components of a plot's technical development or a perpetrator's motivation. Policy and practice may benefit from adopting insights from emerging research arguing in favor of disaggregating our conception of the "terrorist" into discrete groups (e.g., foreign fighters vs. homegrown fighters, bomb-makers vs. bomb-planters, and group-actors vs. lone-actors; Gill and Corner, 2013; LaFree, 2013) rather than disaggregating the radicalization process into discrete groups (e.g., online radicalization and prison radicalization). We need to understand the drives, needs, and forms of behavior that led to the radicalization and attack planning and why the offender chose that environment rather than purely looking at the affordances the environment produced. By looking at the Internet as an affordance opportunity that some forms of terrorist or terrorist violence require more than others do, the focus is shifted from the radicalization process toward an understanding of how crimes are committed. In other words, we are looking at crime events rather than at the underlying dispositions behind the criminality.

Keywords

terrorist behavior, Internet, affordance, radicalization, situational crime prevention

Public interest and policy debates surrounding the role of the Internet in terrorist activities is increasing. Yet, rigorous, criminologically informed research has said very little on the matter. Of the largely theoretical and anecdotal literature on terrorist use of the Internet, studies generally have presented accounts on the affordances[1] offered by the Internet to terrorist groups, including virtual community building, mobilization, information provision, virtual training, propaganda dissemination, recruitment, financing, and risk mitigation (Holt, Freilich, Chermak, and McCauley, 2015; Rudner, 2016; Tsfati and Weimann, 2002; Weimann, 2006). Such accounts implicitly have viewed the interaction between the Internet and the user as unidirectional; exposure to Internet content may cause behavior change.

These accounts, however, have lacked an acknowledgment that not every potential user will make use of the affordance, nor will they use it in the same way. The degree to which an individual makes use of the affordance is modulated based on their goals, plans, values, beliefs, and experiences (Norman, 1988). For example, one may be aware of the affordances provided by Internet-based retailers when buying books but rarely use it, preferring the bookstore next door for a variety of practical and personal reasons. This shifts the focus from the Internet as a potentially causal factor to a focus on how individuals use the Internet based on their motivations, needs, expectations, and histories. As such, it embodies situational crime prevention (SCP) perspectives that presume rational terrorists actively scan, consume, and process information that they need to commit an offense. The real-world absence of these factors drives the need to seek such information online. The interaction between the Internet and the user is a two-way, person–situation interactive process in which the offender leads the way. Whereas affordances are concerned with what the environment offers the person, SCP is more concerned with what the person draws from the environment (Wortley, 2012).

As most samples of terrorist offenders vary in terms of capabilities (lone-actor vs. group-actors) and criminal sophistication (improvised explosive devices vs. stabbings), their constituent needs and preferences may differ with regard to the affordances they seek from the Internet. We would therefore expect to see significant differences in the Internet affordances used by distinct subsets of terrorist offenders. This focus on distinct subsets of terrorist offenders also adheres to traditional criminological approaches that split the outcome variable across crime types, or offender types (e.g., violent vs. nonviolent), rather than treating all terrorists in an aggregated manner as is typical within terrorism studies (Monahan, 2012).

In the absence of empirical data, we cannot begin to disaggregate the complexity of terrorist use of the Internet in a scientifically rigorous way. By using a unique data set of

[1] As regularly mentioned within Internet studies, and more recently in crime (Garwood, 2011) and terrorism-oriented publications (Taylor and Currie, 2012), an affordance provides opportunities to potential users.

223 convicted United Kingdom–based terrorists, this article addresses the lacuna in the existing literature. We first outline with descriptive statistics the degree to which various online activities related to radicalization and attack planning were present. We then report on a series of bivariate and multivariate analyses examining whether those interacting virtually with like-minded individuals or learning online exhibit markedly different experiences (e.g., radicalization, event preparation, and attack outcomes) than those who do not. The next section positions our article within the few existing empirically driven studies on this topic.

Existing Literature

An exhaustive search using dedicated academic research databases produced only three data-driven studies about how convicted terrorists made use of the Internet. Von Behr et al. (2013) examined 15 radicalized individuals, 9 of whom were convicted under U.K. terrorism legislation, which drew on interviews (with police and the individuals), trial records, and computer registries.[2] Their analysis suggested the Internet affords more prospects for radicalization in terms of being a "key source of information, communication and of propaganda for their extremist beliefs" and provides a "greater opportunity than offline interactions to confirm existing beliefs." They depicted the Internet as "not a substitute for in-person meetings but, rather, complements in-person communication" (2013: xi). They concluded that interactions with others, be they physical or virtual, are still crucial for radicalization.

Gill, Horgan, and Deckert (2014) measured the degree to which lone-actor terrorists engaged in online activities. Of 119 individuals, 35% interacted virtually with a wider network of political activists, while 46% learned aspects of their attack method by using virtual sources. Comparative analyses, which use inferential statistical methods, showed al-Qaeda–inspired lone-actors were significantly more likely to learn through virtual sources than were right-wing–inspired counterparts (65% vs. 37%). Isolated dyads were also significantly more likely to interact online with co-ideologues than were those who committed their attacks alone.

By using a similar range of inferential statistical techniques, Gill and Corner (2015) compared the behaviors and traits of lone-actor terrorists who either learned or interacted with co-ideologues online with lone-actor terrorists who engaged in neither activity. They found a growing trend among lone-actors to make use of the Internet. In other words, although the Internet had not caused a growth in numbers of lone-actor terrorists, it altered their means of radicalization and learning. The Internet, therefore, acts as a substitute for other forms of communication but not necessarily as a force enabler. They also found several variations in Internet behavior across subsets of terrorists. Younger offenders were significantly more likely to engage in both virtual learning and virtual interaction than were older offenders. Non–U.S.-based offenders were significantly more likely to learn through

[2] Computer registries essentially log all activities conducted on a computer.

virtual sources, which may be a function of U.S. offenders having greater access to firearms and, therefore, not needing to go online to source these. They also found a significant positive correlation existed between those who virtually interacted with co-ideologues and those who interacted with co-ideologues face to face. Lone-actor radicalization is not, therefore, a dichotomy of either offline or online but a dichotomy of interaction with others versus no interaction with others.

Data and Methods

Violent Online Political Extremism Database

Data-driven studies on online radicalization have been rare. Even for a field as bereft of empiricism as terrorism studies, the striking lack of data is surprising. As an illustration, the first 200 abstracts from a Google Scholar search of "online radicalization OR online radicalisation" shows only 6.5% used some form of data. Primary data existed in 2% of the studies. These mostly focused on extremist forums and social media and, therefore, captured radicalized individuals (and not necessarily individuals prepared to engage in terrorist acts).[3]

For this article, we set out to develop a database of terrorist offenders focused on their online behaviors. To maximize the potential utility of this endeavor and its scientific rigor, we considered several potential pitfalls. First, the initial goal of our study was to examine those individuals who radicalized online. Nevertheless, if our study focused only on individuals reportedly radicalized via the Internet, we could not look at the correlates of terrorists' decisions to use the Internet because the data would exclude cases in which the perpetrator did not use the Internet. In other words, we would be unable to falsify our claims or test hypotheses based on the arguments of the wider literature. Therefore, we decided to build a database of terrorist actors and code for numerous Internet-related activities and their presence or absence. By doing so, we could capture a continuum of Internet-inspired actors from those who were completely uninspired to those who were fully inspired and plot intervening positions.

This decision had implications for how far we could realistically spread our scope geographically and ideologically. Including those who radicalized offline necessitated tightening the search in other areas to allow for the data collection needed to conduct this study. We required our observation pool to be sufficiently large to allow for the application of inferential statistical methods. We also decided the actor dictionary should be limited to a single country to minimize potential open-source reporting bias and the need for cross-national data. In other words, some countries may report (online) radicalization in different ways; to avoid the vagaries of culturally distinct reporting methods, then, we settled on a single-country focus. A single country with a sufficient number of terrorism cases was, therefore,

[3] This search was conducted in May 2015.

deemed the most appropriate choice. Access to open sources is the key to building such a database, so English-language texts were crucial. This left us with two countries, the United Kingdom and the United States. We chose the United Kingdom for two reasons: (1) prior research by Gill and Corner (2015) showed higher levels of online behaviors in the U.K. sample versus the U.S. sample of lone-actor terrorists and (b) terrorism actor dictionaries were more available.

Individuals were identified through several preexisting actor dictionaries. Simcox, Stuart, and Ahmed's (2010) study listed all al-Qaeda–inspired individuals convicted in the United Kingdom. We updated this list to the end of 2014 and widened the scope to reflect very early Islamic State of Iraq and Syria (ISIS)-related activities. The data do not account for the large wave of activities from 2014 to date connected with ISIS and its social media activity. Because of the addition of some early ISIS-related activity, we collapsed both al-Qaeda- and ISIS-related actors into one Jihadist-inspired actor category for the analyses that follow. We added additional extreme-right-wing names through tailored search strings developed and applied to the LexisNexis "All English News" option. Although aggregated to the single category of "extreme right wing," these offenders are stratified across numerous grievances, including anti-immigration, anti-government, anti-Muslim, and anti-Jewish. Additional individuals were identified through the U.S. National Consortium for the Study of Terrorism and Responses to Terrorism's (START) Global Terrorism Database (GTD). Various publications on right-wing extremism in the United Kingdom and lone-actors identified through previous studies (Gill et al., 2014) were also included. We decided to limit the population to post-1990 events because large portions of our data were sourced from the LexisNexis[4] archive, which remains limited before 1990. Irish Republican actors were also omitted from data collection as their online activities were rarely, if ever, mentioned in open-source reporting. Left-wing extremists were next to impossible to identify in a rigorous manner because of the lack of existing research on this phenomenon and because U.K. legislation tends to treat these offenders under criminal damage statutes. They are, therefore, subsumed under a wider category of nonpolitically oriented offenders. We restricted our scope to those who were either convicted in the United Kingdom or died in the commission of a terrorist act in the United Kingdom. Foreign fighters in Syria and elsewhere were therefore omitted.

In total, 223 offenders fit the geographical, temporal, and operational criteria for our study. The variables spanned sociodemographic information (e.g., age, gender, occupation, family characteristics, relationship status, occupation, and employment), network behaviors (e.g., number of co-offenders and training location), event-specific behaviors (e.g., attack method(s), target(s)), and post-event behaviors and experiences (e.g., claim(s) of responsibility and arrest/conviction details). Data were collected on demographic and background

[4] LexisNexis currently provides an electronic online archive from more than 20,000 global news sources.

characteristics and radicalization-linked behaviors by examining and coding information contained in open-source news reports, sworn affidavits, and when possible, publically available first-hand accounts. Most data were collected from press reports via tailored LexisNexis searches. Additional information was gathered from online public record depositories (e.g., documentcloud.org), terrorist biographies, and relevant scholarly articles.

The variables related to online activities were developed in two stages. The first stage emerged from Gill and colleagues' previous lone-actor terrorism research (Gill and Corner, 2015; Gill et al., 2014). Gill et al. (2014) addressed two questions related to online behavior: Did the individual learn about the attack plans from virtual sources? Did the individual interact with co-ideologues online? Gill and Corner (2015) unpacked these two questions further and outlined a series of illustrative examples to show that the types of learning and interaction differed from case to case. The second stage involved an iterative coding process that developed new questions as the data were collected and reviewed.

Two coders examined all available open-source information on each individual. In cases where coders could not agree on the correct values for particular variables (e.g., one coder marked it as a "yes" and one marked it as a "no"), differences were resolved based on examination of the original sources that the coders relied on to make their assessments. Such decisions factored into the comparative reliability and quality of the sources and the sources cited in the report. To aid these decisions, each source was plotted on a continuum of reliability. Court transcripts and associated documents were deemed most reliable as these documents recorded final judicial decisions. Competency evaluations, sworn affidavits, and indictments were deemed reliable as these were carried out after arrest and before trial when initial investigations had been made. Statements (verbal or written) by the terrorist/affiliated group were deemed only somewhat reliable as there may be a drive for dishonesty. Warrants and expert witness reports (in the context of trials) were also reasoned to be somewhat reliable as warrants are produced prior to arrest and like expert witness reports are subject to unreliability and bias. Media articles were then placed on a separate continuum within the less reliable end of the spectrum, with personal opinion blogs at the least reliable end of the scale and nontabloid newspapers at the most reliable.

Some limitations exist in the sources used. First, the sample only includes information on individuals who planned or conducted attacks that led to convictions or death in the perpetration of the attack. It does not include plots intercepted or disrupted by security forces without a conviction. Second, data collection was limited to what could be collected from open sources for each terrorist offender; police, intelligence, classified, and/or closed-source files were unavailable to the researchers.

Third, it is often difficult to distinguish between missing data and variables that should be coded as "no" or "not present." Given the nature of newspaper and open-source reporting, it is unrealistic to expect each biographically oriented story to contain lengthy passages that list behaviors the offender did not engage in (e.g., the offender was *not* a substance abuser, a former convict, or recently exposed to new media). Definitive "no" answers were a rarity (less than 5%) within the data collection process. This percentage was generally uniform across most variables. Usually these "no" answers only occurred in response to incorrect reporting earlier in the news cycle about a particular offender. If definitive "no" answers were more prevalent, it would have been possible to consider using multiple missing data imputation methods (Scheffer, 2002). Current research by the first two authors in collaboration with the Greater Manchester Police has suggested that regularly finding definitive "no" answers necessitates access to closed-source data. Therefore, each variable in the analysis is treated dichotomously (e.g., the response is either a "yes" or not enough information to suggest a "yes" and, thus, a "no"). Unless otherwise stated, each percentage reported is of the whole sample ($N = 223$). There is precedent for this in previous research on attempted assassinations of public figures, fatal school shootings, and targeted violence affecting higher education institutions and terrorism (Fein and Vossekuil, 1999; Gill et al., 2014; Gruenewald, Chermak, and Freilich, 2014; Vossekuil, 2002).

Fourth, it was difficult to get consistently complete data on the temporal ordering of the variables. This is usually because the behaviors are not reported in this manner within our data sources (instead they are usually listed as present). Where possible, illustrative examples of what these orderings looked like in various cases are presented.

Finally, although the level of available granular behavioral data were greater than for some other types of issues that could be equally important (such as family upbringing or other factors associated with exposure to extremist narratives), this granularity does not go so far as to outline consistently the online spaces (e.g., websites, forums, and social media platforms) relied on, exact information gathered online, or frequency of Internet activity.

Despite these limitations, open-source accounts can provide rich data. This has been validated in other studies focusing on the sociodemographic characteristics, operational behaviors, and developmental pathways of members of formal terrorist organizations and lone-actor terrorists (Gill and Horgan, 2013; Gill et al., 2014). Reporting (and, hence, data availability) also tends to be richer when terrorism incidents are rare. For example, Gill et al.'s (2014) study of lone-actor terrorists ($N = 119$ over a 22-year period) obtained educational data on 65% of the sample, whereas in Gill and Horgan's (2013) study of provisional IRA members ($N = 1{,}240$ over a 29-year period), similar data were obtained on less than 10% of the sample. Analogous research also has indicated accessible information is more readily available in rare violent events (Duwe, 2000, 2005).

Methods

To compare those actors who engaged in online activities with those who did not, we followed the procedures in Gruenewald et al. (2013). We first conducted a series of bivariate tests such as chi-square analyses and, where appropriate, Fisher's exact tests. The significant differences between these subsets are discussed as follows. A series of odds ratios were then calculated.

Results

Descriptive Findings

The offenders captured in this database were overwhelmingly male (96%). They ranged in age from 16 to 58 years old with a median age of 27, a mode of 22, and a mean of 28. One third were unemployed at the time of their arrest/attack, a further one third worked in the service or administrative sectors, and 14% were students. Twenty-two percent had some university education. Half of the convictions were related to a planned attack, whereas the other half were related to facilitative behaviors (e.g., financing or distributing propaganda). Only 14% of the convictions were related to a completed attack. A total of 62% were associated with a wider network of co-ideologues, 83% were associated with an attack cell, 22% attended a terrorist training site, and 9% had front-line experience in foreign insurgencies.

When turning attention to online activities, in 61% of cases, there was evidence of online activity related to their radicalization and/or attack planning. As mentioned, we disaggregated these behavior types, which are rank ordered by prevalence in the following discussion.

Slightly more than half (54%) of all actors used the Internet to learn about some aspect of their intended activity. Since 2012, this figure has increased to 76%, indicating it is becoming more prevalent (even if the number of offenders year on year has not risen substantially). This finding is perhaps unsurprising given the ubiquity of Internet usage in most benevolent activities across wider society.

Extremist media were found or downloaded and subsequently reported on in open sources for 44% of the perpetrators. In half of these cases (21%), the content was reportedly videos with a smaller percentage reported for audio lectures (7%) and photographs (6%). The content itself ranged broadly and included extremist-produced video montages of 9/11 and attacks on Western coalition forces in Iraq; beheadings and executions; crimes against Muslims in Chechnya, Afghanistan, and Iraq; news footage of bombings; interviews with and speeches by Anwar al-Awlaki, Osama bin Laden, Abu Hamza, and radical preachers; pro-Jihad rallies; Jihadist texts; bomb-making instruction videos; and terrorist training videos.

A third (32%) prepared for their attacks by using online resources. These included bomb-making instruction videos; poison manuals; downloaded copies of *Inspire* magazine; surveillance advice; an assassination guidebook; torture techniques; suicide vest production; body disposal; plans for the London Underground, Buckingham Palace, and other symbolic landmarks; military police voting records; and terrorist training manuals.

At least 30% accessed extremist ideological content online. In many cases, arguably too much material was downloaded for any one individual to consume and understand thoroughly. One perpetrator had 17,779 computer files of ideological material, 1,152 of which contained extremist content. This may be typical for those individuals that download materials in large volumes via BitTorrents.[5]

Slightly less than a third (29%) of actors communicated with other radicals virtually, half of whom did so via e-mail (15%). Fewer actors communicated with others via online discussion forums (8%) and chat rooms (9%). Some of these interactions circled around the legitimacy of target selection. In one case, the interactions involved discussion of the comparative legitimacy of targeting civilians as opposed to civil servants or the police. In other cases, the interactions involved discussion of the intricacies of carrying out an attack. For example, one case involved a detailed discussion around the making of the highly explosive organic compound hexamethylene triperoxide diamine (HMTD)and how to develop the correct concentration of hydrogen peroxide.

Fifteen percent of actors disseminated propaganda online. This content was usually created by others and recirculated by the actors in our sample. Some of these individuals set up specific websites for this purpose. For example, the administrators of the Aryan Strike Force website are included in the offender data set. Others attempted to publish manuals concerning firearms and explosives on the Internet to incite others.

Our results suggest that 14% of offenders opted to engage in violence after witnessing something online. For example, on May 14, 2010, Roshonara Choudhry stabbed Stephen Timms, a Labour Party Member of Parliament, causing him serious bodily injury. During her police interview, Choudhry referred to a specific YouTube (YouTube, LLC, San Bruno, CA) video of Sheikh Abdullah Azzam that made her understand that "even women are supposed to fight" and that she had an obligation to engage in violence. According to police interviews, Choudhry made this realization at some point in April and soon after began her preparations for the attack. Unfortunately, data were sparse for the whole sample in terms of measuring (a) the time between witnessing these videos and individuals' decisions to take action and (b) whether this was the first example of extremist content individuals witnessed or the latest/most extreme in a long line of content.

One in ten of the sample used online resources to help overcome a hurdle they faced in the actual planning of an attack. In June 2007, two individuals conducted coordinated car bomb attacks in London and a follow-up attack at Glasgow International Airport when they drove their Jeep Cherokee (a brand owned by Fiat Chrysler Automobiles, Auburn Hills, MI) loaded with propane canisters into the terminal doors. They researched bomb-making techniques online, including how to set off a bomb with a mobile phone, and later bought some components online.

A small minority of individuals (9%) sought to recruit others online. Although a third of the sample prepared for some aspect of their attacks online, 9% specifically chose their target after conducting some online research. The analysis undertaken by police on one

[5] A protocol that allows for transferring large amounts of data via peer-to-peer file sharing.

TABLE 1

Observed Percentages for Individuals Who Used Online Learning (All Cases)

Variable	X^2 Value	Sig.	%	Odds
Online Learning (Extreme Right Wing)	5.952	0.015	78.3	3.390
Planned Attack	4.180	0.041	60.9	1.739
Government Target	4.319	0.038	83.3	4.505
Killed Others in Event	7.906	0.005	100.0	—
IED Attack	16.724	0.000	72.5	3.348
Armed Assault	5.995	0.015	85.7	5.505
Unarmed Assault	4.832	0.028	0.0	—
Acted Within a Cell	6.259	0.012	50.5	0.378
Attempts to Recruit Others	7.507	0.006	84.2	5.029
Nonvirtual Network Activity	17.487	0.000	79.2	4.398
Nonvirtual Place Interaction	13.747	0.000	73.1	3.176

Note. — = No odds calculated because of complete lack of variance.

Jihadist-inspired plot showed that the plotters had used the Internet to research the English Defence League (EDL), their activists, and the locations of its leader for up to a month prior to the day of their planned bombing attack.

Six percent of perpetrators provided material support to others online, by asking others to donate money to their cause or by selling *The Anarchist Cookbook* online, for example. A very few (5%) sought legitimization for future actions from religious, social, or political authority figures online; others did this indirectly by searching for fatwas and other legitimating texts. One individual conducted the following Google searches: "three places were [sic] you can kill someone in Islam" and "three place [sic] were [sic] you can kill someone in Islam in punishment."

Five percent also signaled online their plans to engage in attacks prior to the attack itself. In most cases, it was only possible to identify whether the Internet was used. The number of times actors used Internet sources or the hours spent online were impossible to determine. Isolated cases do provide some insight, but this is variable and not generalizable. One actor began researching bomb-making techniques weeks before engaging in his attack, whereas others reportedly spent months on Internet research, with one actor spending possibly 6 hours a day watching extremist footage and videos. In most plots, we see many of these outlined activities occurring at the same time.

Bivariate Analysis

First, we examined the differences between those who learned online and those who did not. Table 1 outlines these results.

The bivariate results suggest that extreme-right-wing individuals, those who planned an attack (as opposed to merely providing material support), conducted a lethal attack, committed an improvised explosive device (IED) attack, committed an armed assault, acted within a cell, attempted to recruit others, and engaged in nonvirtual network activities and nonvirtual place interactions were significantly more likely to learn online compared with those who did not engage in these behaviors. Those undertaking unarmed assaults were significantly less likely to display online learning. Odds ratios[6] indicate extreme-right-wing offenders were 3.39 times more likely to learn online than were Jihadist-inspired individuals. This finding may be a function of the differing circumstances these ideological movements experience in the United Kingdom. The United Kingdom's violent extreme-right movement tends to use the Internet for recruitment, communication, and information dissemination (Thornton, 2015), and compared with Jihadist-inspired lone-actors, extreme-right-wing terrorist activity is more likely to be conducted online in the United Kingdom (Gill, 2015).

The bivariate results showed some interesting findings with regard to target choice. Those who plotted to attack a government target (as opposed to the civilian population) were 4.50 times more likely to learn online. Indeed 83% of those who plotted to attack a government target displayed online learning traits. Given the additional security around government targets (compared with civilian ones), it is a riskier and more arduous practice. The need to go online and learn, therefore, is consistent with our thinking around how different subsets of offenders use Internet affordances differently.

We also found evidence of differing utilization of affordances with regard to attack type. Of all those who actually plotted an attack, those who used/planned to use an IED were 3.34 times more likely to have learned online. This reflects both the greater complexity in IED manufacturing compared with other weapons coupled with the relative ease of availability of online bomb-making manuals and YouTube videos that provide helpful demonstrations. On the other hand, those who used more primitive attack types, like arson or unarmed assaults, were significantly less likely to have learned online.

The bivariate analyses likewise found differing utilization of affordances with regard to the offender's immediate co-offending network. Lone-actors were 2.64 times more likely to learn online than were members of a cell. This may be a reflection of the fact that within a cell, there is a likely pooling of human, social, technical, and financial capital, the absence of which leads individuals to go online to learn how to conduct attacks and for other purposes. The corresponding finding that lone-actors who tried to recruit others (and failed) were 5.00 times more likely to have learned online also lends credence to this interpretation.

The evidence suggests that online learning was strongly correlated with face-to-face interactions with co-ideologues. Those who learned online were 4.39 times more likely to have experienced nonvirtual network activity and 3.17 times more likely to have experienced nonvirtual place interaction. Of those who plotted an attack, the individuals who attended training camps were also significantly more likely to have learned online. This finding

[6] OR = ($a \times d$) / ($b \times c$), where a, b, c, and d are elements from the 2 × 2 chi-square contingency table.

TABLE 2

Observed Percentages for Individuals Who Used Online Communication Across Ideologies

Variable	X^2 Value	Sig.	%	Odds
Communication Online (Extreme Right)	4.090	0.043	47.8	2.417
Military Target	5.479	0.019	10.7	0.251
IED Attack	3.740	0.053	37.5	1.783
Knife Attack	5.331	0.021	0.0	—
Association With a Network	4.315	0.038	72.7	1.934
Attempts to Recruit Others	42.296	0.000	94.7	58.500
Nonvirtual Network Activity	18.011	0.000	58.2	3.891
Nonvirtual Place Interaction	12.776	0.000	46.3	2.997

Note. — = No odds calculated because of complete lack of variance.

confirms the earlier research of von Behr et al. (2013) and Gill and Corner (2015) and may be a result of the compartmentalization of tasks noted by Gill (2015). For example, individuals tend to learn about a specific necessary task online (e.g., bomb-making), but then they find a different instrumentalization in their offline interactions with co-ideologues (e.g., the justification of bombing a particular target).

Next, we examined the differences between those who communicated online and those who did not. Table 2 outlines our results.

The bivariate results suggest that extreme-right-wing individuals who perpetrated an IED attack, associated with a wider network, attempted to recruit others, and engaged in nonvirtual network activities and nonvirtual place interactions were significantly more likely to communicate online. In comparison, those targeting the military and using knife attacks were significantly less likely to communicate online. This indicates a high level of overlap between the online learning and online communication bivariate results.

Extreme-right-wing offenders were 2.41 times more likely to have communicated online with co-ideologues than Jihadist-inspired individuals were. Again, this may be a function of the differing circumstances of these ideological movements, as noted earlier.

Those who targeted the military were significantly less likely to have communicated online. Only 7.4% of those who plotted against the military communicated online with co-ideologues. This may run counter to our expectations regarding affordances. It is probably a marker of greater operational security among these offenders.

The evidence also suggests that communicating with co-ideologues online was significantly more likely to have been accompanied by face-to-face interactions with nonviolent co-ideologues. Those who communicated online were 3.89 times more likely to have experienced nonvirtual network activity and 3.17 times more likely to have experienced nonvirtual place interaction. Of those who plotted an attack, the individuals who attended training camps were also significantly more likely to have communicated online.

TABLE 3

Comparisons of Instrumentality of Online Learning Across Ideologies

Variable	*B*(SE)	*df*	Sig.	Exp(*B*)
Accessing Ideological Content	0.505 (0.470)	1	0.282	1.658
Opting for Violence	−1.089 (0.801)	1	0.174	0.337
Choosing Targets	−0.316 (0.836)	1	0.705	0.729
Preparing an Attack	1.433 (0.496)	1	0.004***	4.193
Overcoming Hurdles	−0.916 (0.846)	1	0.279	0.400
Constant	−2.715 (0.365)	1	0.000	0.066

Notes. +*B* value = extreme right wing more likely to demonstrate. –*B* value = Islamist more likely to demonstrate.
***$p < .001$.

Multivariate Analysis

The bivariate results highlighted that extreme-right-wing offenders were significantly more likely to learn online than were Jihadist-inspired individuals. We hypothesized that the lack of collective action within the extreme-right-wing movement in the United Kingdom may lead individuals to seek answers online because they are not available offline. We therefore conducted binary logistic regression analyses for the five different types of learning outlined in the Data and Methods section to see which could significantly predict individuals as right-wing extremists (Table 3). The results illustrate that the sole difference in terms of the instrumentality of the learning was in attack preparation. Extreme-right-wing offenders were 4.19 times more likely to use online learning for attack preparation. There was no significant difference in terms of opting for violence, target choice, or overcoming hurdles.

Binary logistic regression analysis indicated that this disparity in online communications across ideologies was largely accounted for by extreme-right-wing offenders' greater propensity to use extremist online forums (Table 4). There was no difference in terms of e-mail or chat room usage. The latter forms of communication were more likely to be used for communication with (a) nonviolent radicals and (b) nonradicals. There was also no difference in terms of extreme-right-wing actors' propensity to communicate online with other cell members or other terrorists. A final predictor of this disparity was extreme-right offenders' greater likelihood of having used the Internet to disseminate propaganda compared with radical Jihadists. There was no significant difference in terms of reinforcing prior beliefs, seeking legitimization for future actions, disseminating propaganda, providing material support to others, or attack signaling.

Discussion and Conclusion

Collectively the results provide insight into violent radicalization as a whole and not just into violent online radicalization. The results also largely confirm the results found in von Behr et al. (2013) and in Gill and Corner (2015). The current study and the two previous studies

TABLE 4

Comparisons of Online Communication Across Ideologies

	B (SE)	*df*	Sig.	Exp(*B*)
Communication Methods				
E-mail	−0.544 (0.808)	1	0.501	0.580
Forum	1.345 (0.701)	1	0.055*	3.839
Chatroom	−0.296 (0.924)	1	0.748	0.744
Other	0.748 (0.614)	1	0.223	2.112
Constant	−2.327 (0.281)	1	0.000	0.098
Communication Outlet				
Cell	0.090 (0.713)	1	0.900	1.094
Other terrorists	0.013 (0.674)	1	0.985	1.013
Other radicals	−1.205 (0.594)	1	0.043**	0.300
Other nonradicals	−1.286 (0.731)	1	0.083*	0.281
Constant	−0.155 (0.968)	1	0.873	0.857
Instrumentality of Communication				
Cell preparation	−0.150 (0.642)	1	0.815	0.861
Reinforcing prior beliefs	−0.883 (1.337)	1	0.509	0.414
Seeking legitimization for actions	0.645 (1.040)	1	0.535	1.906
Disseminating propaganda	−1.881 (0.552)	1	0.001***	0.152
Providing material support	20.369 (10702.953)	1	0.998	—
Attack signaling	−0.557 (0.865)	1	0.519	0.573
Constant	−20.087 (10702.953)	1	0.999	0.000

Notes. +*B* value = extreme right wing more likely to demonstrate. –*B* value = Islamist more likely to demonstrate. — = Exp(*B*) not computed because of size.
**p* < .05. ***p* < .01. ****p* < .001.

have tackled these questions by using numerous methodological approaches and data sources and have arrived at similar conclusions. The Internet is largely a facilitative tool that affords greater opportunities for violent radicalization and attack planning. Nevertheless, radicalization and attack planning are not dependent on the Internet and researchers need to look at behaviors, intentions, and capabilities. Offenders hampered by their co-offending environment or the ambitions of their plot are afforded opportunities online. We found significant differences across targeting strategies, ideologies, network forms, and actors' propensity to engage in online learning and communication. Selection of harder targets was strongly associated with online learning. Technically more difficult attacks such as IEDs led to more online searching compared with primitive or simpler attacks. Lone-actors required more online learning because they lacked the pooled human talent typically associated with an attack cell. Extreme-right-wing offenders were more likely than Jihadist-inspired offenders in the United Kingdom to learn and communicate online. This may be a result of geography and the structural unavailability of co-offenders in their local area, as well as of their increased likelihood of being "lone-actors."

This study also highlights the fact that there is no easy offline versus online violent radicalization dichotomy to be drawn. It may be a false dichotomy. Plotters regularly engage in activities in both domains. Often their behaviors are compartmentalized across these two domains. For example, plotters may engage in face-to-face interaction regarding the ideological legitimacy of their actions while engaging in virtual communication regarding the technical specificity of bomb-making. Threat management policies would do well to understand the individuals' breadth of interactions rather than to rely on a dichotomous understanding of offline versus online, which represent two extremes of a spectrum that regularly provide prototypical examples in reality. A preoccupation with only checking online behaviors may lead an intelligence analyst to miss crucial face-to-face components of a plot's technical development or a perpetrator's motivation.

Perhaps policy debates in this area have been focused on the wrong things and in the wrong place. Policy seems fixated on the location in which the radicalization played out. We regularly see new proposals focused on different radicalization locales (e.g., online, prison, university, school, or place of worship). Our results suggest that often online and offline interactions go hand in hand. Policy and practice may benefit from adopting insights from emerging research arguing in favor of disaggregating our conception of the "terrorist" into discrete groups (e.g., foreign fighters vs. homegrown fighters, bomb-makers vs. bomb-planters, and group-actors vs. lone-actors; Gill and Corner, 2013; LaFree, 2013) rather than of disaggregating the radicalization process into discrete groups (e.g., online radicalization and prison radicalization). We need to understand the drives, needs, and forms of behavior that led to the radicalization and attack planning and why the offender chose that environment rather than purely looking at the affordances the environment produced.

As illustrated throughout, cases in which all transactions were conducted online are rare. Face-to-face interactions were still the key to the process for most actors even if they were aware of, and made use of, the bounty of ideological and training material available online. Indeed, much recent investigative reporting of ISIS recruitment of Western individuals has highlighted the importance of face-to-face interactions via Skype (Microsoft Corporation, Redmond, WA) and other online platforms (Callimachi, 2015; Erelle, 2015). Violent radicalization should therefore be framed as cyber-enabled rather than as cyber-dependent while underlining that enabling factors differ from case to case depending on need (i.e., who or what to attack and what tactic to use) and circumstance (i.e., availability of co-offenders, expertise, and ideology). The use of the Internet was largely for instrumental purposes whether it was pre-attack (e.g., surveillance, learning, practice, or communication) or post-attack (e.g., disseminating propaganda). There is little evidence to suggest that the Internet was the sole explanation prompting actors to decide to engage in a violent act. Instead, it was just one factor among many that helped crystallize motivation, intent, and capability at the same time and place. Our results further suggest that many went online not to have their beliefs changed but rather to have them reinforced. This falls in line with von Behr et al.'s (2013) previously cited research. Take, for example, Ian Davison who in 2010 was the first Briton to be convicted for producing a chemical weapon (ricin). In the aftermath of his trial (in which his son was also convicted on other offenses), police sources noted that Davison's "views developed over time. After going online he accessed websites and started to look at places where those kinds of views were shared with other people."

By looking at the Internet as an affordance opportunity that some forms of terrorist or terrorist violence require more so than others, the focus is shifted from the radicalization process toward an understanding of how crimes are committed. In other words, we are looking at crime events rather than at the underlying dispositions behind the criminality. This, of course, is the main thinking behind situational crime prevention approaches (Clarke, 1980; Clarke and Newman, 2006). Not all situational crime prevention approaches are easy to implement within the virtual realm where large social media organizations have displayed resistance or apathy, until recently, to increase the effort and risk of radicalizers and the radicalized to operate freely on their platforms. For example, see Twitter's (Twitter, Inc., San Francisco, CA) ongoing battle with ISIS-related accounts (Berger and Perez, 2016). Cooperation between these organizations and state bodies is crucial in combatting the affordances provided to would-be terrorists. State policies may potentially need to reframe this cooperation as a battle against opportunities for violence rather than as a battle against expressions of radical ideas and thoughts, which has recently dominated discourse on both sides of the Atlantic.

References

Berger, J. M. and Heather Perez. 2016. The Islamic States diminishing returns on Twitter. *GW Program on Extremism*, 2: 16.

Callimachi, Rukmini. 2015. ISIS and the lonely young American. *The New York Times*. June 27.

Clarke, Ronald V. 1980. Situational crime prevention: Theory and practice. *The British Journal of Criminology*, 20: 136–147.

Clarke, Ronald V. and Graeme R. Newman. 2006. *Outsmarting the Terrorists*. New York: Greenwood Press.

Duwe, Grant. 2000. Body-count journalism: The presentation of mass murder in the news media. *Homicide Studies*, 4: 364–399.

Duwe, Grant. 2005. A circle of distortion: The social construction of mass murder in the United States. *Western Criminology Review*, 6: 59–78.

Erelle, Anna. 2015. Skyping with the enemy: I went undercover as a jihadi girlfriend. *The Guardian*. May 26.

Fein, Robert A. and Bryan Vossekuil. 1999. Assassination in the United States: An operational study of recent assassins, attackers, and near-lethal approachers. *Journal of Forensic Sciences*, 44: 321–333.

Garwood, Jeanette. 2011. A quasi-experimental investigation of self-reported offending and perception of criminal opportunity in undergraduate students. *Security Journal*, 24: 37–51.

Gill, Paul. 2015. *Lone-Actor Terrorists: A Behavioural Analysis*. London, U.K.: Routledge.

Gill, Paul and Emily Corner. 2013. Disaggregating terrorist offenders: Implications for research and practice. *Criminology & Public Policy*, 12: 93–101.

Gill, Paul and Emily Corner. 2015. Lone-actor terrorist use of the Internet and behavioural correlates. In (Lee Jarvis, Stuart Macdonald, and Thomas M. Chen, eds.), *Terrorism Online: Politics, Law, Technology and Unconventional Violence*. London, U.K.: Routledge.

Gill, Paul and John Horgan. 2013. Who were the volunteers? The shifting sociological and operational profile of 1240 Provisional Irish Republican Army members. *Terrorism and Political Violence*, 25: 435–456.

Gill, Paul, John Horgan, and Paige Deckert. 2014. Bombing alone: Tracing the motivations and antecedent behaviors of lone-actor terrorists. *Journal of Forensic Sciences*, 59: 425–435.

Gruenewald, Jeff, Steven Chermak, and Joshua D. Freilich. 2013. Distinguishing "loner" attacks from other domestic extremist violence. *Criminology & Public Policy*, 12: 65–91.

Holt, Tom, Joshua D. Freilich, Steven Chermak, and Clark McCauley. 2015. Political radicalization on the Internet: Extremist content, government control, and the power of victim and jihad videos. *Dynamics of Asymmetric Conflict*, 8: 107–120.

LaFree, Gary. 2013. Lone-offender terrorists. *Criminology & Public Policy*, 12: 59–62.

Monahan, John. 2012. The individual risk assessment of terrorism. *Psychology, Public Policy, and Law*, 18: 167.

Norman, Don A. 1988. *The Design of Everyday Things*. New York: Basic Books.

Rudner, Martin. 2016. "Electronic Jihad": The Internet as Al Qaeda's catalyst for global terror. *Studies in Conflict and Terrorism*. Retrieved from dx.doi.org/10.1080/1057610X.2016.1157403.

Scheffer, Judy. 2002. Dealing with missing data. *Research Letters in the Information and Mathematical Sciences*, 3: 153–160.

Simcox, Robin, Hannah Stuart, and Houriya Ahmed. 2010. *Islamist Terrorism: The British Connections*. London, U.K.: Center for Social Cohesion.

Taylor, Max and P. M. Currie (eds.). 2012. *Terrorism and Affordance*. London, U.K.: Routledge.

Thornton, Amy. 2015. Understanding radicalization. Ph.D. Dissertation. University College London, U.K.

Tsfati, Yariv and Gabriel Weimann. 2002. www.terrorism.com: Terror on the Internet. *Studies in Conflict and Terrorism*, 25: 317–332.

von Behr, Ines, Anais Reding, Charles Edwards, and Luke Gribbon. 2013. *Radicalization in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism*. Santa Monica, CA: RAND. Retrieved from rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf.

Vossekuil, B. (2002). *The final report and findings of the Safe School Initiative: Implications for the prevention of school attacks in the United States*. Collingdale, PA: DIANE Publishing.

Weimann, Gabriel. 2006. Virtual disputes: The use of the Internet for terrorist debates. *Studies in Conflict and Terrorism*, 29: 623–639.

Wortley, Richard K. 2012. Affordance and situational crime prevention: Implications for counter-terrorism. In (Max Taylor and P. M. Currie, eds.), *Terrorism and Affordance*. New York: Continuum.

Paul Gill is a senior lecturer in the Department of Security and Crime Science at University College London. His research focuses on the behavioral underpinnings of terrorism and terrorist attacks. Much of his recent work has centered on lone-actor terrorism, and his book on this topic was recently published by Routledge.

Emily Corner is a Ph.D. student in the Department of Security and Crime Science at University College London. Her research focuses on mental illness and terrorist engagement. Her paper, “False Dichotomy,” was recently published in *Law and Human Behavior* and compared the prevalence of mental disorders among a sample of lone and group terrorist actors.

Maura Conway is a senior lecturer at the Department of Law and Government at Dublin City University. Her research focuses on terrorist use of the internet. She is the principal investigator on the European Union–funded network of excellence in “Violent Online Political Extremism” (voxpol.eu).

Amy Thornton is a postdoctoral research fellow at the Department of Security and Crime Science at University College London. She is currently working on the “What Works in Crime Reduction” project funded by the ESRC. Her Ph.D. focused on radicalization processes.

Mia Bloom is a professor of communication at Georgia State University. Her past research has examined suicide terrorism and the role of women in terrorist groups. Her previously published books include *Dying to Kill: The Allure of Suicide Terror* and *Bombshell: Women and Terrorism.* Her book on children in terrorism is forthcoming with Cornell University Press.

John Horgan is a professor of global studies and psychology at Georgia State University. An applied psychologist by training, his research focuses on terrorist behavior. He has more than 70 publications on terrorism and political violence, and his books include *The Psychology of Terrorism, Walking Away from Terrorism,* and *Divided We Stand: The Strategy and Psychology of Ireland’s Dissident Terrorists.*