NETWORK OF EXCELLENCE FOR RESEARCH
IN VIOLENT ONLINE POLITICAL EXTREMISM

ONLINE BEHAVIOURS OF CONVICTED TERRORISTS

Paul Gill
University College London

Email info@voxpol.eu
www.voxpol.eu

Executive Summary

Reported herein are two complementary pieces of research on online behaviours of convicted UK terrorists and attack plotters, one large scale and based on open source data (n=223) and another smaller scale and based on closed sources (n=49), that build significantly upon the current knowledge base.

Open Source Results

- In 61% of cases, there was evidence of online activity related to radicalisation and/or attack planning.
- Fifty four per cent used the Internet to learn about some aspect of their intended activity, with an increase to 76% from 2012 onwards.
- Extremist media was found or downloaded by 44% of perpetrators. Half of the content was reportedly videos, with smaller percentages reported for audio lectures and photographs.
- Thirty two per cent prepared for attacks by accessing online resources such as bomb-making and suicide vest instructions, maps of iconic sites, MP voting records, and terrorist training manuals.
- At least 30% accessed extremist ideological content online, with some collecting an excessive—even unmanageable—amount of such information.
- Fourteen per cent of offenders opted to engage in violence after witnessing something online.
- Twenty nine per cent of actors communicated with other radicals through email, discussion forums, or chat rooms. Interactions regarded matters such as the legitimacy of target selection and intricacies of carrying out an attack.
- Fifteen per cent of actors disseminated propaganda online, while others attempted to publish manuals concerning weapons in order to incite others.
- One in ten of the sample used online resources to overcome hurdles they faced in attack planning.
- While a third of the sample prepared for some aspect of their attacks online, 9% specifically chose their target after conducting online research.
- In the vast majority of cases, the number of times actors utilised Internet sources or exact hours spent online was impossible to determine.

Closed Source Results

- In 26.5% of cases, the offender produced letters or public statements prior to the event outlining his/her beliefs (but not necessarily his/her violent intent); extremist online forums were the most popular choice for such pronouncements.
- While just over half (51%) of those in this sample interacted face-to-face with members of a wider network, an even larger number (59.2%) did so virtually.
- Nearly 35% aspired, within their online postings, to copy other terrorists. In 87.8% of cases, there is evidence to suggest that the individual read or consumed literature or propaganda from a wider movement, including online.
- In fact, at times there appears to be direct knowledge diffusion amongst lone actors within our sample, with data suggesting that 28.6% read or consumed literature or propaganda concerning other lone-actor terrorists.
- Attack training occurred in a number of ways. While just over 16% received some form of hands-on training, 81.6% learned through virtual sources. In 71.4% of cases, investigators found evidence of bomb-making manuals in the offender's home or on his/her property.

Introduction

Previous research on terrorist use of the Internet generally discusses the opportunities offered by the Internet to terrorist groups (Tsfati & Weimann, 2002; Weimann, 2006; Holt et al., 2015; Rudner, 2016). Such accounts implicitly view the interaction between the Internet and the user as uni-directional (i.e. exposure to Internet content may cause behaviour change). This lacks an acknowledgement that not every potential user will make use available opportunities, nor use these in the same way. The degree to which an individual makes use of an opportunity is modulated based upon their goals, plans, values, beliefs, and experiences (Norman, 1988). At present, there are only three data-driven studies examining how convicted terrorists have used the Internet: Von Behr et al., 2013, Gill et al., 2014, and Gill and Corner 2015. These studies shift the focus from the Internet as a potentially causal factor to how individuals use the Internet based upon their motivations, needs, expectations, and histories. They acknowledge, in other words, the way in which the interaction between Internet and user is a two-way person-situation interactive process in which the individual leads the way. Reported herein are two complementary pieces of research, one large scale and based on open source data and another smaller scale and based on closed sources, that build significantly upon the above-described research.

Data and Methods

Open Source

For the purposes of this research, a database of 223 terrorist actors who were either convicted or died in the commission of a terrorist act in the UK between 1990 and 2014 was constructed and coded for the presence or absence of a number of Internet-related activities. Early IS-related activities and Simcox et al's (2011) list of al-Qaeda-inspired individuals were collapsed into one Jihadist-inspired actor category (updated to the end of 2014). Additional individuals were identified through tailored search strings in LexisNexis, the Global Terrorism Database (GTD), publications on UK right-wing extremism, and previous studies on lone-actors (Gill et al., 2014). The variables analysed span socio-demographics, network behaviours, event-specific behaviours, and post-event behaviours and experiences. Data were collected using open-source news reports, sworn affidavits, publicly available first-hand accounts, online public record depositories, terrorist biographies, and scholarly articles. The procedures in Gruenewald et al. (2013) were followed to compare actors who engaged in online activities with those who did not. Bivariate tests such as chi-square analyses and Fisher's exact tests were used.

Closed Source

Follow-up research on the antecedent behaviours, including online activities, of UK-based lone-actor terrorists leading up to their planning or conducting a terrorist event was subsequently undertaken. What sets this research apart from the above and the rest of the field is the privileged closed-source data that underpins the analysis. Analysts at the UK police's North-West Counter Terrorism Unit collected data on demographic and background characteristics and antecedent event behaviours by examining and coding information contained in police data files, psychological reports (when available),

interviews with case officers, intelligence reports, and open-sources for further context within each case. These data sources, unprecedented in the academic study of terrorism, were then de-identified and handed over to researchers at University College London for this analysis. The sample composed 49 individuals who engaged in or planned to engage in lone-actor terrorism within the UK between 1995 and 2015. Included were individual terrorists (with and without command and control links) and isolated dyads.[1]

Open Source Results

The sample consisted of both jihadists (89%) and right-wing extremists (11%). The offenders captured in this database were overwhelmingly male (96%), ranging in age from 16 to 58 (mean = 28). One third were unemployed at the time of their arrest/attack; one third worked in service or administrative sectors. Fourteen per cent were students, with 22% having a university education. Half of convictions related to a planned attack, half to facilitative behaviours (e.g. financing, distributing propaganda), and 14% to a completed attack. Sixty two per cent were associated with wider networks of co-ideologues, 83% with an attack cell. Twenty two per cent attended a terrorist training site, and 9% had front-line experience in foreign insurgencies.

In 61% of cases, there was evidence of online activity related to radicalisation and/or attack planning. Fifty four per cent used the Internet to learn about some aspect of their intended activity, with an increase to 76% from 2012 onwards. According to open-sources, extremist media was found or downloaded by 44% of perpetrators. Half of the content was reportedly videos, with smaller percentages reported for audio lectures and photographs. Content included montages of 9/11 and attacks on Western coalition forces; executions; crimes against Muslims; radical speeches; terrorist training videos, etc. Thirty two per cent prepared for attacks by accessing online resources such as bomb-making and suicide vest instructions, maps of iconic sites, MP voting records, and terrorist training manuals. At least 30% accessed extremist ideological content online, with some collecting an excessive—even unmanageable—amount of such information. Fourteen per cent of offenders opted to engage in violence after witnessing something online.

Twenty nine per cent of actors communicated with other radicals through email, discussion forums, or chat rooms. Interactions regarded matters such as the legitimacy of target

[1] *Individual terrorists* operate autonomously and independently of a group (in terms of training, preparation and target selection etc.). In some cases, the some cases, the individual may have radicalized towards violence within a wider group but left and engaged in illicit behaviours outside of a formal command and control structure. *Individual terrorists with command and control links*, on the other hand, are trained and equipped by a group – which may also choose their targets – but attempt to carry out their attacks autonomously. *Isolated dyads* include pairs of individuals who operate independently of a group. They may 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.

Although not technically 'lone' actors, we decided to include isolated dyads for a number of reasons. First, a key component of this project focuses upon the network qualities of terrorists who are not members of terrorist groups. Second, an initial review of our cases showed that isolated dyads often formed when one individual recruited the other specifically for the terrorist attack. The formation of a dyad, in some cases, may be a function of the type of terrorist attack planned. Finally, by including these cases, it added to our sample, making the types of inferential statistics used later more applicable.

selection and intricacies of carrying out an attack. Fifteen per cent of actors disseminated propaganda online, while others attempted to publish manuals concerning weapons in order to incite others. One in ten of the sample used online resources to overcome hurdles they faced in attack planning. While a third of the sample prepared for some aspect of their attacks online, 9% specifically chose their target after conducting online research. Six per cent of perpetrators provided material support (money donation, selling of material) to others online. Five per cent sought legitimization for future actions from religious, social, or political authority figures online. Five per cent signalled via the Internet plans to engage in attacks. In most plots, the above outlined activities were concurrent. In the vast majority of cases, the number of times actors utilised Internet sources or exact hours spent online was impossible to determine. Isolated cases do provide insight, but this is variable and not generalisable.

Those who planned an attack (as opposed to 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, or engaged in non-virtual network activities and place interactions were significantly more likely to learn online compared to those who did not engage in these behaviours. Extreme right-wing offenders were 3.39 times more likely to learn online than Jihadist inspired individuals. Those who plotted to attack a government target were 4.50 times more likely to learn online, and 83% of this subgroup displayed online learning traits. Those who used/planned to use an IED were 3.34 times more likely to have learned online, reflecting complexity in IED manufacturing and the availability of online bomb-making manuals / demonstrations. Those who used more primitive attack types, e.g. arson, were significantly less likely to have learned online. Lone actors were 2.64 times more likely to learn online than members of a cell and lone actors who tried to recruit others were 5 times more likely to have learned online. Those who learned online were 4.39 times more likely to have experienced non-virtual network activity and 3.17 times more likely to experience non-virtual place interaction. Of those who plotted an attack, the individuals who attended training camps were significantly more likely to have learned online.

Those targeting the military and using knife attacks were significantly less likely to communicate online. Extreme right-wing offenders were 2.41 times more likely to have communicated online with co-ideologues than Jihadist inspired individuals. Communicating with co-ideologues online was significantly more likely to have been accompanied by face-to-face interactions with non-violent co-ideologues. Those who communicated online were 3.89 times more likely to have experienced non-virtual network activity and 3.17 times more likely to experience non-virtual place interaction. Of those who plotted an attack, individuals who attended training camps were significantly more likely to have communicated online.

Violent extreme-right movements in the UK tend to use the Internet for recruitment, communication, and information dissemination (Thornton, 2015), which may explain the disparity in online communications across ideologies. Extreme-right wing offenders' had greater propensity to use extremist online forums. There was no difference in terms of email or chat room usage, or in extreme-right wing actors' propensity to communicate

online with other cell members or terrorists. A final predictor of this disparity was extreme right offenders' greater likelihood of having used the Internet to disseminate propaganda compared to radical Jihadists. There was no significant difference in terms of reinforcing prior beliefs, seeking legitimisation for future actions, disseminating propaganda, providing material support to others, or attack signalling.

Closed Source Results

The lone-actor terrorists in this sample, like the previous, subscribed to a range of ideologies. Religiously inspired lone actors constituted the largest set of actors at 51%. This is perhaps unsurprising given how loosely connected al-Qaeda's transnational network(s) became over time, coupled with the rise of IS and their focus on lone-actor attacks. Right wing extremists constituted the second largest group, representing 30.6% of the total sample. The third largest grouping was a clustering of individuals driven by nationalist ideas (unrelated to the extreme-right wing), left-wing, and other single issue causes. Our lone-actor terrorist sample was heavily male-oriented at 87.8%. As regards ideology, all six females were classified as jihadist-inspired.

With regard to online behaviours and activity, it was found that, in most cases, other people knew something concerning some aspect of the offender's grievance, intent, beliefs, or extremist ideology prior to the attack or planned attack. In 26.5% of cases, the offender produced letters or public statements prior to the event outlining his/her beliefs (but not necessarily his/her violent intent); extremist online forums were the most popular choice for such pronouncements. While just over half (51%) of those in this sample interacted face-to-face with members of a wider network, an even larger number (59.2%) did so virtually. Nearly 35% aspired, within their online postings, to copy other terrorists. In 87.8% of cases, there is evidence to suggest that the individual read or consumed literature or propaganda from a wider movement, including online. In fact, at times there appears to be direct knowledge diffusion amongst lone actors within our sample, with data suggesting that 28.6% read or consumed literature or propaganda concerning other lone-actor terrorists. Attack training occurred in a number of ways. While just over 16% received some form of hands-on training, 81.6% learned through virtual sources. In 71.4% of cases, investigators found evidence of bomb-making manuals in the offender's home or on his/her property.

Conclusions and Recommendations

Collectively, the results highlight the need to focus upon online behaviours linked to the demonstration of terrorist intent. Whilst engagement with radicalising materials and/or radicalisers is a prerequisite of radicalisation, it is perhaps a poor predictor to base disruption activities upon given the much larger volume of individuals exposed to these materials. The conclusions from this report have a number of implications for research, risk assessment, policy, and practice. In terms of research, the results illustrate the great degree of granularity possible from both open and closed sources. Rather than focusing on 'who' became radicalised, this is the first research of its type to instead focus upon the 'how' of online radicalisation and provided insight into the prevalence of various attack planning

behaviours in an online setting. The results also make clear that whilst analysing the opportunities afforded by the Internet is important, it is perhaps more instructive to view it in the context of how potential terrorists use the Internet based upon their motivations, needs, expectations, and histories. Online radicalisation is not a uniform process across or even within ideologies, for example, but there tends to be significantly different behaviours witnessed depending upon the needs of a potential attack/attacker.

The results largely confirm the conclusions of von Behr et al. (2013) and Gill and Corner (2015), whereby the Internet is largely a facilitative tool that affords greater opportunities for violent radicalisation and attack planning. Offenders hampered by their co-offending environment or plot ambitions are afforded opportunities to overcome these online. We found significant differences across targeting strategies, ideologies, network forms, and propensity to engage in online learning and communication. Our research highlights the fact that there is no easy offline versus online violent radicalisation dichotomy to be drawn, as plotters regularly engage in activities in both domains. Threat management policies would do well to understand individuals' breadth of interactions rather than relying upon 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 behaviours may lead to crucial components of a plot's technical development or a perpetrator's motivation being missed. Policy and practice may benefit from adopting insights from emerging research arguing in favour of disaggregating our conception of the 'terrorist' into discrete groups (LaFree, 2013; Gill & Corner, 2013) rather than disaggregating the radicalisation process.

Cases in which all transactions were conducted online were found to be rare. Face-to-face interactions were still key to the process for the vast majority of actors even if they were aware of, and made use of, the bounty of ideological and training material available online. Violent radicalisation should therefore be framed as cyber-enabled rather than cyber-dependent, while underlining that enabling factors differ from case to case depending upon need and circumstance. The use of the Internet was largely for instrumental purposes whether it was pre- or post-attack. There is little evidence to suggest that the Internet was the sole factor prompting actors to decide to engage in a violent act. Our results further suggest that many went online not to have their beliefs changed, but rather reinforced. This is in line with von Behr *et al.*'s (2013) previously cited research.

A number of significant challenges remain with regards to research and practice. First, the recent development of databases and larger datasets have led to the development of variables (e.g. demographic, behavioural, historical, social, and, to a lesser extent, biological) that co-vary significantly with radicalisation, recruitment, involvement in, and to a lesser extent, disengagement from violent extremism has accumulated. As datasets continue to expand—involving an ever-larger number of variables across an ever-larger number of cases—the list of significant statistical associations is likely to grow. It is now time to take stock of the evidence rather than endlessly developing new (and largely untested) risk factors. Second, base rates remain a continual problem. Quite simply, we have no grasp on the societal prevalence of the vast majority of online radicalisation indicators. In some cases, like issues surrounding mental disorders, it is easier because of

epidemiological studies (see Corner, Gill and Mason, 2016). Other behaviours, like making threats online, are a far more difficult task to quantify. Without a sense of base rate, we can't measure with any certainty how reliable any one indicator is, either in isolation or in combination with other indicators. Instead, we can only sample on the dependent variable, which is not good practice.

Third, there is a distinct lack of research concerning protective factors. The literature just does not account for them. We only look for 'risk factors', which may lead to a series of confirmation biases amongst intelligence analysts. Protective factors may come in many forms and include individual factors (e.g. attitudes, academic achievement, social orientation, self-control, personality factors), peer factors (e.g. close relationships with non-criminal peers, pro-social norms within peer group, number of affective relationships), family factors (e.g. highly connected to family, involvement in social activities).

The final problem is that of weighting. In most studies of radicalisation indicators, all indicators are treated equally. For example, the Safire Project[2] outlines 21 indicators, ranging from "lingering concerns with questions of meaning and identity" to "dependence on communication technology" to "associating with extremist groups" and "training travel," without prioritising any. Other risk assessment tools discriminate between indicators to a small extent (e.g. the Terrorist Radicalization Assessment Protocol or 'TRAP-18'). The argument for such discrimination is logical, interesting, and yet rarely made. Of course, in reality, not all indicators are equal. A part of the problem is that those developing indicators oftentimes try to do too much—from highlighting indicators of someone adopting an extremist ideology to highlighting indicators of someone planning an attack. These are very different processes, underpinned by very different behaviours and necessitating intervention by very different parts of the policing/intelligence/partner agency framework. Basically, the radicalisation literature lacks specificity in terms of what it is studying the indicators of. Exasperation at current attempts to counter online radicalisation is perhaps therefore understandable given the unclear parameters concerning what we are trying to, or even what we should, counter (e.g. do we counter ideological adoption, ideological radicalisation, attack planning, attack commissioning, or the variables and experiences that may make these phenomena more likely).

The research reported herein acts as a starting point in the scientific study of terrorist engagement via the Internet by providing a count of various online behaviours and how they co-vary with other attack-related variables. To advance the science further, it is important to utilise both open and closed sources, learn from the shortcomings outlined in the preceding paragraphs and importantly disaggregate online radicalisation into various discrete phenomena (e.g. ideological attainment, attack planning, attack commissioning) whilst also understanding that the importance of various factors may be modulated by ideology, the presence of co-offenders, and attack sophistication.

[2] See http://www.safire-project-results.eu/documents/focus/8.pdf.

References

Gill, Paul, and Corner, Emily. 2013. 'Disaggregating Terrorist Offenders: Implications for Research and Practice.' *Criminology & Public Policy* 12(1): 93-101.

Gill, Paul, and Horgan, John. 2013. 'Who Were the Volunteers? The Shifting Sociological and Operational Profile of 1240 Provisional Irish Republican Army Members.' *Terrorism and Political Violence* 25(3): 435-456.

Gill, Paul, Horgan, John, & Deckert, Paige. 2014. 'Bombing Alone: Tracing the Motivations and Antecedent Behaviors of Lone-Actor Terrorists.' *Journal of Forensic Sciences* 59(2): 425-435.

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

Gill, Paul, & Corner, Emily. 2015. 'Lone-Actor Terrorist Use of the Internet and Behavioural Correlates.' In L. Jarvis, S. Macdonald and T. Chen (eds.), *Terrorism Online: Politics, Law, Technology and Unconventional Violence* (London: Routledge).

Holt, Tom, Freilich, Joshua. D., Chermak, Steven, and McCauley, Clark. 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.

Gruenewald, Jeff, Chermak, Steven, and Freilich, Joshua. D. 2013. 'Distinguishing "Loner" Attacks from Other Domestic Extremist Violence.' *Criminology and Public Policy*, *12*(1), 65-91.

LaFree, Gary. 2013. 'Lone-Offender Terrorists.' *Criminology and Public Policy* 12(1): 59-62.

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 & Terrorism* 40(1): 1-14.

Simcox, Robin, Stuart, Hannah & Ahmed, Houriya. 2010. *Islamist Terrorism: The British connections* (London: Center for Social Cohesion).

Thornton, Amy. 2015. 'Understanding Radicalisation', PhD Thesis, University College London, UK.

Tsfati, Yariv and Weimann, Gabriel. 2002. "www.terrorism.com: Terror on the Internet". *Studies in Conflict and Terrorism* 25(5): 317-332.

von Behr, Ines, Reding, Anais, Edwards, Charle, and Gribbon, Luke. 2013. *Radicalization in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism* (Brussels: RAND Europe): http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf

Weimann, Gabriel. 2006. Virtual Disputes: The Use of the Internet for Terrorist debates. *Studies in Conflict & Terrorism* 29(7): 623-639.