POLICY ESSAY

TERRORIST USE OF THE INTERNET

Same Kind of Different

Affordances, Terrorism, and the Internet

Paul J. Taylor

Donald Holbrook

Lancaster University

Adam Joinson

University of Bath

The rapid development of the Internet as a cornerstone of private and social life has provoked a growing effort by law enforcement and security agencies to understand what role the Internet plays in terrorism. Paul Gill, Emily Corner, Maura Conway, Amy Thornton, Mia Bloom, and John Horgan's (2017, this issue)~~<AUTHOR's>~~ effort to identify empirically when and how terrorists engage with the Internet is thus timely and important. Understanding *when* terrorists use the Internet is valuable for investigators who must evaluate the immediacy of the risk posed by a suspect or cell. Knowing the typical patterns of use (or lack of use) can facilitate inferences about a cell's preparedness, the nature of ~~their~~ its support, and even the goal of ~~their~~ its attack. Understanding *how* terrorists use the Internet is essential for policy makers who must construct legislation to deter citizens from terrorism while ~~at the same time~~ retaining their rights to freedom. This is arguably best accomplished by legislation targeted at

This work was part funded by the Centre for Research and Evidence on Security Threats (ESRC Award: ES/N009614/1). Direct correspondence to Paul J. Taylor, Department of Psychology, Lancaster University, Lancaster, U.K. LA1 4YF (e-mail p.j.taylor@lancaster.ac.uk).

Comment [SVV1]: AU: Please note that your article has been edited to be consistent with the style and preferences of CPP and the other articles included in this issue.

Will you please help us in maintaining this standard? We understand that might mean that some of our changes differ from individual preferences, but our goal is to set a standard for a more formal scientific style of writing.

Nevertheless, we do want to make sure that your intended meaning was not lost during editing, so please review the document carefully. In cases where we believe our edits might require explanation, we have included comments. Nevertheless, please feel free to ask about specific changes that were made.

NOTE: Your document has not yet been typeset, so page layout and formatting have yet to be set for publication.

Comment [SVV2]: AU: Please note that a "cell" is a collective "it" in this context.

a narrow set of Internet uses that are, as far as possible, exclusively associated with illegal actions.

In this policy essay, we focus on two of ~~<AUTHOR's>~~Gill et al.'s (2017) main contributions. We argue that, subject to robust independent replication, they encourage thought about the functions of the Internet for terrorists, which in turn may have implications that offer useful guidance for policy and practice. Alongside the article~~paper~~'s conceptual contributions, ~~the authors~~Gill et al. also assert to have resolved several~~a number of~~ pragmatic challenges and we suggest ways in which their solutions, if developed fully, could offer value to the security analyst community. Finally, we take stock of where ~~the~~ Gill et al.'s ~~<AUTHOR's>~~ contribution has left us and review the next steps.

Differences in Internet Use

A central finding of Gill et al. (2017)~~<AUTHOR>~~ is that terrorists' motivations and intentions make a significant difference to how and when they use the Internet. Their data reveal that a use of the Internet depends largely on the needs of the terrorist and on the opportunities afforded to him or her both offline and online. For example, Gill et al.~~<AUTHOR's>~~ show that terrorists who seek to undertake sophisticated attacks (e.g., IED attacks) tend to seek facts on how to conduct such attacks online~~, since~~ because presumably that knowledge is not so easily available offline. Similarly, Gill et al. ~~<AUTHOR>~~ find that terrorists engaging in a geographically distributed network are more likely to use the Internet for more interpersonal activities because~~, since~~ for these individuals, those opportunities are less available offline.

These differences, although descriptive rather than inferential, demonstrate for investigators the value that can come from systematically thinking about what a suspect or suspect cell needs, and where the opportunity might lie for those needs to be met. Identifying

needs (e.g., information~~,~~ ~~and~~or co-ideologues) and opportunity should allow inferences about how a suspect cell is likely to go about planning its~~their~~ attack or seeking additional information or input. Such inferences then allow the prioritization of investigative resource. For example, as part of a risk assessment, an investigator might consider~~:~~, "What's missing from a cell?" "Does that mean ~~they~~ it will need to look online?" "If ~~they~~ it does, then we should focus our online investigations on seeking evidence that the cell is pursuing such a resource. There may also be opportunity for secondary inferences. For example, perhaps there is an obvious affordance online. An investigator might ask, "W~~w~~hy hasn't the cell taken advantage of this?" "Is this non-use related to operational security or to ~~,~~ a lack of good investigative coverage, or does it mean that the cell is not a credible threat?" These kinds of inference may allow investigators to focus their work on credible threats and to identify appropriate interventions that dissuade the cell from progressing its~~their~~ attack.

The differences across groups observed by Gill et al. (2017) ~~<AUTHORS>~~ allow for similar inferences about what to expect and, thus, where to seek evidence to inform a risk assessment. The differences observed between far-right and Islamist extremist realms suggest that the militant opportunities and experiences embedded in each affect how those who identify with these realms use the Internet. For example, ~~the <AUTHOR's>~~Gill et al. observe that "extreme-right-wing offenders were significantly more likely to learn online than were Jihadist-inspired individuals~~"Extreme right-wing offenders were significantly more likely to learn online than Jihadist inspired individuals~~." As ~~the <AUTHOR's>~~Gill et al. argue, this is perhaps because there are and have been far fewer physical spaces for those identifying with the far-right to gain practical skills. The absence of opportunity for offline interaction ~~appears~~ seems to be leading extreme~~-~~right-wing offenders to ~~utilize~~ use the Internet for learning. Thus, as this example demonstrates, an investigative team can determine where ~~they~~ it might expect to find intelligence on a new threat based on what affordance the suspects have offline

Comment [SVV3]: AU: Please note that all direct quotes from Gill et al. were updated to reflect the copy-edited version.

and online. If it will be difficult for a cell to interact offline, then investigators might focus resources on online social media channels that provide an equivalent opportunity to interact. Investigators may also be able to extend such inferences to what might happen to the cell should some form of police intervention take place. The removal of an affordance will see it displaced elsewhere, from offline to online, from one forum to another, and so on.

Internet as Facilitator Not Instigator

A second argument ~~in the paper~~made by Gill et al. (2017), which has large implications for policy, is the observation that radicalization and attack planning are not dependent on the Internet, and that the Internet "is largely a facilitative tool that affords greater opportunities ~~(p. 23)~~." That is, the actor goes to the Internet as a resource for finding information once motivated to do so, and the Internet does not play a large role at pushing such information onto a vulnerable consumer. This finding is consequential because it contrasts findings from the last 20 years of general research on technology use that ~~argues for~~suggest a complex inter~~-~~play between technological innovation and social and economic factors (Williams ~~&~~and Edge, 1996). The results of r~~R~~esearch on the "~~"~~social ~~shaping'~~ shaping" of technology (e.g., MacKenzie ~~&~~and Wajcman, 1999) ~~suggests~~ reveal that we shape technology as much as we are in turn influenced by the decisions made by designers, or the content it provides (Williams ~~&~~and Edge, 1996). For practitioners, this means that use of the Internet needs to be considered ~~from~~ neither from a simple ~~'~~"~~"~~technologically ~~deterministic'~~ deterministic" standpoint (e.g., "Internet causes radicalization")~~,~~ nor as ~~simply as~~ a socially neutral "~~"~~tool~~'~~."

From the perspective of this past literature, ~~the <AUTHOR's>~~Gill et al.'s (2017) conclusion that the Internet is an enabler but not a cause is correct. ~~However~~Nevertheless, practitioners should be cautious not to interpret it in a manner that is overly deterministic. For example, the recent 2016 U.S. election has raised considerable discussion around the role of

technology (specifically social media) in propagating ‘‘-false ~~news’~~ news” and -‘‘filter ~~bubbles’~~ bubbles” (Isaac ~~*New York Times*~~, 2016). ~~While~~ Although there is still debate and analysis to be conducted, one lesson from the U.S. election is clear: Facebook was neither a cause, nor a simple ‘‘-enabler~~’~~,” but ~~rather~~ there was a complex interplay ~~between~~ among social validation, algorithmic filtering, and false news, whose impact is as yet uncertain. For policy makers and practitioners, the challenge is not one of treating the terrorists and their Internet use as separate entities~~,~~ but ~~rather~~ of treating them as two components of a single, complex socio-technical system. ~~<AUTHOR’s> paper~~Gill et al. sheds~~s~~ some light on that system.

The difference between Gill et al.’s (2017)~~the <AUTHOR’s>~~ findings and that of researchers in other disciplines highlights two further interrelated challenges that are faced when observing Internet behavior. First, what is the true effect of the material on presumed ‘‘-learning~~’~~?” Do crude open-~~-~~source searches that obfuscate more than clarify an issue constitute online learning? Might the vast volumes of data available online through, for instance, torrent downloads complicate the applicability of this learning in practice? The Internet does not necessarily provide targeted answers, and too much information can be just as unhelpful as no information at all. We might even argue that online ‘‘-engagement”~~’~~ offers parallels to engagement in the offline world and that, in doing so, the Internet disrupts or complicates pathways that lead to offline collaboration. Many prominent extremist texts that have been popular with convicted terrorists in the United Kingdom (e.g., the booklet ‘‘-39 Ways to Serve and Participate in ~~Jihad’~~Jihad”) emphasize precisely such an online-~~-~~offline dynamic. As Ramsay (2013: ~~, p.~~ 286) observed~~s~~, “it would seem, paradoxically, that the online violent radical milieu may actually generate its own *positive* reasons for non-engagement” by developing “a set of meaningful and, so it would seem, pleasurable practices of its own.”

Second, what are the secondary uses of online information? If one member of the cell downloads material and then shares it through offline means, the footprint of Internet use is less but the role of the Internet is equivalent. Given this, inferences such as "lone-actors require more online learning" made by Gill et al. (2017) ~~(p. 23)~~ are at risk of being misinterpretations of incomplete evidence. So how can we move from a snapshot of a behavior to a fuller understanding of the purpose of a behavior within the context of other actors and their behaviors? Fortunately, because investigators often have access to information not just on when something is used but also on what occurs after the points of use and the context in which such use occurs (Klein, Moon, ~~&~~and Hoffman, 2006), they can determine the qualitative value of each behavior and resolve some of these complications. At least they can up to a point.

One framework that may support investigator thinking about the opportunities offered by the Internet is the classic three-part classification of communication motivation. Within this framework, the Internet is ~~seen~~ perceived as affording a terrorist the opportunity to address instrumental (i.e., about substantive needs such as information), identity (i.e., about identity and ideological belief), and relational (i.e., about social affiliations and connections) goals (Taylor, 2014). This categorization has proven effective in understanding the purpose and construction of extremist and counter-extremist messaging (Prentice, Rayson, ~~&~~and Taylor, 2012; Prentice, Taylor, Rayson, Hoskins, ~~&~~and O'Loughlin, 2011), and so it may be valuable to untangling the facilitative versus~~s.~~ causal effects of the Internet. Table 1 presents ~~<AUTHOR's>~~Gill et al.'s (2017) findings as a function of communicative goals and whether the Internet was used by terrorists to instigate or facilitate involvement. In completing Table 1, we have inevitably simplified the intended purpose of different forms of engagement and a more critical analysis may reveal important nuances. Nevertheless, what begins to emerge from this kind of assessment is where the gaps in affordance appear to be. The Internet is

largely facilitative when it comes to instrumental goals, but it plays a more fundamental instigator role when it comes to relational goals.

A framework like that shown in Table 1 may allow an investigator to think critically about how a terrorist cell is addressing its various goals (if they are at all). Investigators are likely to have an advantage over ~~<AUTHOR>~~Gill et al. (2017) in completing such a table as they ~~are able to~~can layer on top of this initial picture two important facets of Internet use. First, investigators may have more information on day-to-day communicative uses by terrorist suspects of Internet-based platforms (e.g., Twitter or ~~,~~ WhatsApp; Charitonidis, Rashid, ~~&~~and Taylor, 2015) and they can glean a clearer picture of what relational needs and resources are being sought. Second, their fine-grained picture can help investigators determine ~~if~~ whether there are greater nuances in terms of how the nature of usage plays out. For example, ~~whilst~~ although it seems intuitive that those seeking to organize complex plots using IEDs are likely to "have learned online," ~~(p. 19),~~ as Gill et al. state, it is conceivable that the purpose of the Internet use in this instance was not to learn but to check on the authenticity of information provided offline.

Collaboration and Mechanisms as Next Steps

~~The <AUHTOR's>~~Gill et al.'s (2017) findings support the current investigative practice of considering offline and online behavior jointly when investigating terrorists (von Behr, Reding, Edwards, ~~&~~and Gribbon, 2013). Investigators tend to focus on considering different groups rather than people at different stages in their "~~"career'~~ career" or people in different contexts, and this approach fits nicely with ~~<AUTHOR's>~~Gill et al.'s suggestion of considering affordances. The proposal to not differentiate online and offline activity also provides timely support to government investment decisions in relation to security, at least in the United Kingdom. The 2016 National Cyber Security Strategy, which pledges to invest

£1.9 billion over the next ~~five~~ 5 years, distinguishes cyber-dependent and cyber-enabled offending, thereby recognizing the important offline element of many crimes and echoing the distinction between facilitator and cause.

~~<AUTHOR's>~~Gill et al.'s (2017) findings go beyond supporting current practice to highlight the value of increased collaboration. ~~While the <AUTHOR's>~~Although their statistical contribution helps prioritize what information should be used by investigators, investigators ~~are able to~~can say what information may be collected at low cost (e.g., low intrusion) and with more reliability. Collaboration will, therefore, help researchers avoid the challenges of exploring the connections between terrorist behavior and pre-arrest activities by using only open-source data. For example, the suggestion in ~~<AUTHOR>~~Gill et al. that "only a minority (44%) of cases actually included extremist (ideological) material" ~~(p. 14)~~ is significant because it raises fundamental questions about why these cases were defined as "~~'~~terroristic"~~'~~ to begin with. If ~~the majority of~~most convicted terrorists did not collect extremist material, how does this affect our understanding of the way in which political and ideological dimensions are used to label acts or attempted acts (and relevant support activity) as *terrorism*? The explanation might rest on the fact that the details of the material found are not necessarily presented at court, depending on the nature of the case, and then not necessarily reported fully in the press, depending on what was deemed relevant or interesting (cf. Sageman, 2014). The combination of researcher and investigator perspectives is thus a more holistic picture of what is known and what can be accomplished through criminological analyses.

In a search to understand affordance, researchers and investigators will need to ~~unpack~~discover~~??unpick~~ the mechanisms that underpin the behaviors observed by ~~<AUTHOR>~~Gill et al. (2017). This is essential if we are to move from description to inference and if we are to be confident in our inferences about

~~DISTINGUISNG??~~distinguishing new cases from ~~the~~ old ones. ~~<AUTHOR>~~Gill et al. lay out many predictions that researchers could explore in this regard. For example, they highlight the Internet as a potential place of learning, but precisely how terrorists go about consuming and consolidating any such online learning, and how that interfaces with the indirect learning that comes from social interaction, is not yet understood. They argue for choice when suggesting that the Internet is a ~~??facilitator~~facilitator. Understanding the mechanisms behind when and how such choices are made will offer researchers insights into the role of the Internet in terrorism and offer investigators insights into the efficacy of using Internet behavior as a marker of threat.

Conclusions

~~<AUTHOR>~~Gill et al. (2017) conducted ~~an~~ admirable data collection and analysis that give~~s~~ a compelling demonstration of the value of consider~~ing~~ the affordances that online, offline, and "~~"~~sub~~-~~contexts"~~"~~ in both of these environments bring to a terrorist. Their take~~-~~home message for investigators and policy makers, at least for us, is to (~~1~~a) continue to treat online and offline as two sides of the same coin, where one might compensate for a lack in the other, and vice ~~-~~versa; and to (b~~2~~) develop frameworks for systematically evaluating how a particular threat may make use of offline and online affordances~~,~~ by using such assessment to guide both risk assessment and intervention strategies.

References

Charitonidis, Christos, Awais Rashid, ~~Awais, &~~and Paul Taylor~~, Paul.~~ ~~(~~2015~~)~~. *Weak Signals a~~A~~s Predictors o~~O~~f Real-World Phenomena i~~I~~n Social Media*. ASONAM '15 Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015. New York : ACM, 2015. p. 864-871 (ASONAM '15).
~~Paper presented at the IEEE/ACM International Conference on Advances in Social Networks Analysis and Miningadvances in social networks analysis and mining (ASONAM), 864-871Paris, France.~~

Formatted: Highlight

Formatted: Highlight

Gill, Paul, Emily Corner, Maura Conway, Amy Thornton, Mia Bloom, and John Horgan. 2017. Terrorist use of the Internet by the numbers: Quantifying behaviors, patterns, and processes. *Criminology and Public Policy*. This issue.

Isaac, Mike. 2016. Facebook, in cross hairs after election, is said to question its influence. *The New York Times*. November 12. Retrieved November 27, 2016, from nytimes.com/2016/11/14/technology/facebook-is-said-to-question-its-influence-in-election.html.

Klein, Gary, Brian Moon, ~~Brian, &~~and Robert Hoffman~~, Robert.~~ ~~(~~2006~~)~~. Making sense of sensemaking 1: Alternative perspectives. *IEEE Intelligent Systems*, 21~~:~~ 70~~–~~73.

MacKenzie, Donald ~~, &~~and Judy Wajcman~~., Judy~~ ~~(~~1999~~)~~. *The ~~social~~ Social S~~s~~haping of T~~t~~echnology*. Milton Keynes, U.K.: Open University Press.

~~*New York Times* (2016). Facebook, in cross hairs after election, is said to question its influence. Downloaded on 27 November, 2016, from: http://www.nytimes.com/2016/11/14/technology/facebook-is-said-to-question-its-influence-in-election.html~~

Prentice, Sheryl, Paul Rayson, ~~Paul, &~~and Paul J. Taylor~~, Paul J~~. ~~(~~2012~~)~~. The language of Islamic extremism: Towards an automated identification of ideas, beliefs, motivations and justifications. *International Journal of Corpus Linguistics*, 17~~: ,~~ 259~~–~~286.

Prentice, Sheryl, Paul J. Taylor, Paul ~~J.,~~ Rayson, ~~Paul,~~Andrew Hoskins, ~~Andrew, &~~and Ben O'Loughlin~~, Ben.~~ ~~(~~2011~~)~~. Analyzing the semantic content and persuasive composition of extremist media: A case study of texts produced during the Gaza conflict. *Information Systems Frontiers*, 13~~: ,~~ 61~~–~~73.

Ramsay, Gilbert~~.~~ ~~(~~2013~~)~~. *Jihadi C~~e~~ulture on the World Wide Web*. New York: Bloomsbury.

Sageman, Marc. 2014. The stagnation in terrorism research. *Terrorism and Political Violence*, 26: 565–580.

Taylor, Paul J. ~~(~~2014~~)~~. The role of language in conflict and conflict resolution. In (Thomas M.~~,~~ Holtgraves~~,~~ e~~d~~ ~~(E~~d.), *The Oxford Handbook of Language and Social Psychology* ~~(pp. 459-470)~~. New York: Oxford University Press.

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.

Williams, Robin~~, &~~and David Edge~~, David.~~ ~~(~~1996~~)~~. The social shaping of technology. *Research Policy*, 25~~:~~ 865~~–~~899.

Table 1. Uses of the Internet as a Ffunction of Internet Rrole and Ccommunicative Ggoals

Internet Role	Communicative Goal		
	Instrumental	**Identity**	**Relational**
Instigator	Provide material support (6%)		Propaganda (15%) Recruit others (9%) Content radicalised radicalized to action (14%)
Facilitator	Learn about activity (54%) Attack preparation (32%) Overcome attack hurdle (10%)	Extremist media (44%) Ideological content (30%) Legitimization for future actions (5%) Signal plan prior to attack (5%)	Communicate w/-others (29%)

Paul J. Taylor is a professor of psychology at Lancaster University, United Kingdom, and a pProfessor of Human human Interaction interaction at the University of Twente, tThe Netherlands. He directs the U.K. Centre for Research and Evidence on Security Threats (CREST), an independent Centre commissioned by the Economic and Social Research Council with funding from the U.K. security and intelligence agencies.

Donald Holbrook is a lLecturer at in the Department of Politics, Philosophy and Religion, Lancaster University, and a vVisiting fFellow at the International Centre for Counter-terrorism at The Hague. He was formerly a sSenior rResearch fFellow at the Centre for the Study of Terrorism and Political Violence, University of St Andrews.

Adam Joinson is a pProfessor of iInformation sSystems at the University of Bath, and a programme lead on online behavior within CREST. His research examines the interaction of technology and behavior in areas that include communication patterns, influence, security and privacy, and how design can influence behavior.