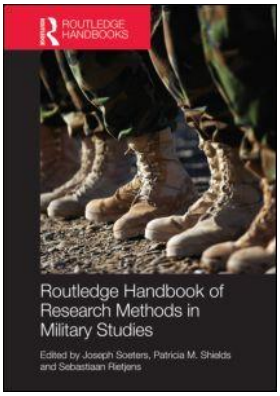

Routledge Handbook of Research Methods in Military Studies

Joseph Soeters, Patricia M. Shields, Sebastiaan Rietjens

Scrutinizing the Internet in Search of "Homegrown" Terrorism

Publication details
https://www.routledgehandbooks.com/doi/10.4324/9780203093801.ch15
Risa Brooks
Published online on: 09 Jun 2014

How to cite :- Risa Brooks. 09 Jun 2014, *Scrutinizing the Internet in Search of "Homegrown" Terrorism from:* Routledge Handbook of Research Methods in Military Studies Routledge
Accessed on: 02 Oct 2023
https://www.routledgehandbooks.com/doi/10.4324/9780203093801.ch15

15

SCRUTINIZING THE INTERNET IN SEARCH OF "HOMEGROWN" TERRORISM

Risa Brooks

R. Brooks (2011) "Muslim homegrown terrorism in the United States: How serious is the threat?" *International Security,* 36(2): 7–47.

This article evaluates the claim that homegrown Islamist terrorism is a growing threat in the United States. The "threat" of homegrown terrorism is defined as an increase in the number of deaths within the United States perpetrated by American citizens or residents inspired by Islamic militant jihadist ideologies, but acting independently from established terrorist organizations. The author identifies three conditions that could produce a growing threat of this kind. These include (1) an increased incidence of the number of American Muslims initiating terrorist plots in the United States; (2) an increase in the efficacy and skill of aspiring militants, such that even if more plots are not initiated, more Americans will be harmed by those that are attempted; (3) an increase in the ability of militants to hide or conceal their terrorist activities, such that the activities of aspiring terrorists are less likely to be detected and foiled by arrests, resulting in a greater number of successfully executed attacks. Evidence in support of any of these conditions suggests the threat of homegrown terrorism is indeed growing.

Online research is a principal method employed by the author. The article uses the Internet to search for resources to analyze the empirical record of terrorism in the United States. The diversity and accessibility of sources online is a principal advantage. The author also uses the Internet as a means for assessing conventional views and definitions of homegrown terrorism. This is facilitated by examining a wide sample of materials to identify trends in the reporting and descriptions of homegrown terrorism. Specifically, relying on Internet resources offered several benefits to the author's research.

(continued)

(continued)

First, through online research, the author was able to access court records and, especially affidavits by federal and local law enforcement officials involved in terrorism investigations. These revealed the expanded efforts and novel methods employed in monitoring and investigating terrorist activity in the United States. These records detail use of "informants" who monitor local communities and supply information to law enforcement. There was also evidence of extensive efforts by officials to covertly assist suspected militants in the advancement of their plans, in order to develop legal cases against them, in a process known as "sting operations." The use of such operations raised questions about whether the plots would have been pursued by militants without law enforcement influence.

Second, Internet research allowed for the investigation of factual details about when and how suspected militants first formulated and began to implement their plots. This research revealed that recent spikes in terrorist-related arrests are the result of a clustering of arrests of individuals who had become engaged in militancy at different times in the past. This finding suggests, contrary to conventional wisdom, that a spike in terrorism arrests is not evidence of a growing trend in the amount of terrorist activity occurring in the United States.

Third, the use of online research helped the study confirm the accuracy of data, such as about the number of terrorism related arrests in the United States. Online research allowed for cross-checking of information by making available different studies and data bases that use variable criteria or coding rules for identifying terrorist activity.

Fourth, online research provided a means for integrating factual details from diverse news and official sources to learn operational details about plots. This helped the author establish the pervasiveness of mistakes and errors in operational security perpetrated by the militants. These errors provide evidence of the limited capabilities of homegrown terrorists in the United States.

Fifth, online research revealed biases in how terrorism is reported, and drew attention to the different definitions of homegrown terrorism used by analysts. It highlighted the editorial approaches of media outlets in their reporting on acts of suspected terrorism. Recognizing such biases was crucial to the author's efforts to provide a more comprehensive view of domestic terrorism in the United States. A comprehensive survey reveals that Muslim originated terrorist activity has not been the sole or even primary source of threat in recent years. These characteristics of reporting on terrorist activity help explain the common mischaracterization of the homegrown terrorism threat.

The Internet represents a vast and evolving resource for researchers, with enormous potential to link scholars and analysts to primary and secondary information on an array of phenomena. Relying on the Internet as a tool or method for research, however, can expose scholarship to weaknesses and biased results if key problems and methodological issues are not explicitly recognized.

Both the promise and pitfalls of online research are illustrated by the effort to employ the Internet to study the incidence and nature of homegrown terrorism in the United States. Homegrown terrorism is defined as terrorism committed by American citizens or residents who are inspired by the propaganda of a militant jihadist group, but who operate independently from the organization (see e.g. Bjelopera and Randol 2010). The discussion that follows describes how online research can be a useful method for analyzing terrorism. The analysis also illuminates broader methodological issues that can arise in online research on military or security related issues.

As a method, online research involves employing a set of tools or strategies for searching the Internet in order to locate relevant and desired factual, analytical or opinion-laden information. A principal advantage of online research is the speed with which a researcher can access information from diverse sources. The web lacks inherent structure or administration, however, so that how and whether that information is accessed depends on the tools a researcher employs to search the Internet.

Search engines and directories structure how online information is conveyed to the user. The results yielded from a search reflect an imposed order and hierarchy that is otherwise absent on the web. How the hierarchy of results is determined and then displayed depends on the nature of the search engine chosen by a user. Searches are mediated by the algorithms and indexing of the search engine employed, or of the methodology of the directory that a researcher consults. The results of any given search reflect those rules and methods (Comer 2011).

To the extent it is possible, a working understanding of the methodology employed by search engines can increase the efficiency of using the Internet. This background information can help individuals anticipate what kinds of information and results are most likely to be captured by the search engines they use. The best search results come from using multiple search engines, and employing targeted terms and search techniques. Also valuable is learning how to access the vast amounts of materials not captured by the spiders that compile indexes from which search results are built, which is known as the invisible web. Generally, researchers using the Internet will benefit from a basic understanding of how the web works, and of the search engine services and directories on which they rely.

Benefits of online research

There are several ways that online research can benefit researchers.[1] By focusing on the specific example of researching homegrown terrorism, these advantages of online research are illustrated.[2]

First, the Internet expands the volume of open-source, or publicly available, information accessible about militant groups and their violent activities, which represents a critical resource to terrorism analysts. This information comes in the form of quantitative data located in large databases made available online, through free or paid access. Alternatively, it can come from coverage and analyses of events related to terrorist-related activities, from news media, social media, blogs, private think-tank reports and collections, and court and government documents accessed online.

Second, it can provide primary source information about militant groups' recruitment and operational activities. Researchers can study the militants' ideological doctrine through open-source reporting and by accessing propaganda available on extremist web sites. This includes audio and video files, training manuals, pamphlets and writings, and copies of speeches. They can monitor the debate and discussion that may occur on websites or in other online forums. This may reveal themes or narratives in the group's doctrine or guiding beliefs.[3]

Visiting militant groups' websites and monitoring communications is also a valuable intelligence tool for members of law enforcement or the intelligence community. Militants may use the Internet to facilitate their violent activities in a variety of areas, including training through the supply of instructional materials; planning by using the Internet to facilitate communications or undertake surveillance; recruitment and incitement with online propaganda; and fundraising and financing. Authorities therefore can use the Internet to enhance knowledge about the organization and operational methods of terrorist groups and individuals by studying these activities online. Researchers can also gain insight into these aspects of militant groups' operations and

organization by visiting relevant websites. Accessing these sites, however, can be difficult for lay people because many groups may restrict access to cyber forums, such as Internet chat groups, or employ platforms such as password protected websites.

Third, for researchers interested in learning about the scope and nature of terrorist-related activity, the Internet can provide a means of tracking or verifying under-reported events. Terrorist plots that are serious, or are executed successfully, will receive a great deal of media coverage. Assessing the nature and degree of terrorist activity in a country, and hence the quality of the threat it poses, however, requires that researchers also examine plots that do not result in actual attacks or injuries.

This subset of attacks includes, for example, those that fail due to a mistake in planning or in fabricating a weapon. It includes plots that are abandoned before execution, and those that end in the militants' arrest as the result of law enforcement's detection of a plot. By incorporating details about plots that are foiled or fail, researchers have a clearer picture of the actual operational skills of the pool of terrorists in a country. The analysis also reveals the ways in which law enforcement involvement can influence the development of a terrorist plot. Only focusing on plots that are executed and result in deaths could lead to a distorted understanding of who is engaging in home-grown terrorist activity, and risks overstating the efficacy and skill of the pool of aspiring militants (Dahl 2011). Online research can therefore provide an important methodological advantage to studies by allowing researchers to incorporate "non-events" into their studies of terrorist activity.

Fourth, Internet research can allow researchers to establish the accuracy of particular details and accounts of events that are otherwise difficult to confirm. Through triangulation of information and reporting available from different sites, researchers can confirm details about cases and events that are otherwise only available to intelligence and law enforcement authorities. Drawing from the Internet, for example, can help researchers parse otherwise scarcely reported operational details of attempted attacks or terrorist-related activities. When different sources report similar details, it provides some confidence in the accuracy of the information. Similarly, when a detail is reported in one source, but is not consistent with other accounts, it can alert the reader to potential factual errors.

This requires that the sites are consulting independent sources and are not relying on each other to confirm details. If apparently independent reports turn out to refer back to the same source, it can promote a circuitous, self-reinforcing chain of evidence that artificially lends credibility to a story. In particular, researchers should make sure factual details cited in online resources do not link back to the same source. This issue is also discussed below.

Fifth, the Internet provides novel methods for evaluating popular attitudes, reactions or beliefs about terrorist groups and activities within a larger public or subset of the population. This is afforded by the possibility of deploying online surveys and engaging in online interviews. There are many logistical and cost-saving benefits, as well as the possibility of reaching otherwise difficult to access populations. Researchers, however, should consider that there may be potential sources of bias in a sample or results that come with relying on Internet surveys over onsite methods (see Hooley et al. 2012). This can originate in the way that respondents react to Internet surveys, or differences in who is likely to respond to online solicitations, versus those contacted via other mediums. Generally, researchers should be attentive to issues of recruitment and how the use of online versus onsite methods may affect their research if relying on the Internet means some subgroups of the population are less apt to participate, and therefore that a population relevant to the study is systematically underrepresented in the sample (see Hooley et al. 2012: 66; Hamilton and Bowers 2006; Salmons 2009).

The emergence of reputable online companies and commercial entities that can be hired by researchers to conduct surveys, online interviews, and carry out experiments on their behalf has

expanded the use of these methods in some academic disciplines. These online companies facilitate research about political and social phenomena in foreign countries, in particular, where in the past language differences and logistical costs would pose obstacles to the researcher. In addition to evaluating the credentials of the site, analysts with funding who aim to employ such entities should look carefully at how the population to be sampled is compiled by the organization. This will help ensure that demographic or political differences in the sampled population that are important for the researcher's study are actually controlled in the random sample provided by the polling organization. For example, a survey of attitudes about terrorist groups active in a foreign country, such as Iraq or Lebanon, would likely need to control for the religious or ethnic differences of respondents, by providing a sample that encompasses individuals from different sects. These differences may not be captured in a random sample of individuals that varies primarily in age, education or other demographic variables.

Information about attitudes can also be developed through ethnographic methods, such as by observing virtual communities and reading participant contributions in opinion oriented forums, such as chat rooms, comments pages and the like. Scholars or analysts may read through participant contributions in order to gauge attitudes or reactions and get a sense of how consumers of the information and visitors to online sites understand and evaluate different events or phenomena. While, as I explain below, one must be careful not to assume these expressed views are representative of the patterns of opinion within a larger audience, they can reveal important themes or narratives, and illuminate more extreme or particular interpretations and reactions.

Potential methodological problems of online research

Clearly, there are benefits to online research. There are also problems that such methods can generate.

Definitional issues in online searches

One set of issues relates to how researchers choose the key words employed in searches. A problem occurs if the terms are likely to be used selectively by those authoring and supplying material on websites. This can occur if a term, like "terrorism," has political implications, or implies normative judgments about the validity of an act or actor. As a result, the term may not be applied consistently and its use in a story may correspond with the biases or perspective of those reporting an event (Silke 2004).

The terms used in keyword searches can also generate biased results because the terms themselves have no widely shared meaning, and are used arbitrarily to describe events. Consider the use of the term "homegrown." As stated above, homegrown terrorism is often used in reference to Islamist militants who are citizens of the United States (or Europe) and operate independently from organized militant groups. In this usage, analysts associate the word "homegrown" primarily with Islamist fundamentalist, or jihadist ideologies, thereby employing the term to designate acts of terrorism perpetrated by individuals inspired by that particular ideology. Analysts may conversely use the term "domestic" terrorism for acts inspired by other secular or religious-based ideologies, such as individuals pursuing extremist left- or right-wing causes. Hence, members of the Hutaree militia who were prosecuted in 2010 for an alleged terrorist plot involving the murder of a police officer and a follow-on attack on his funeral may be referred to as "domestic" rather than "homegrown" terrorists.

Other scholars, however, use the term homegrown to refer to all self-starters operating independently from large organizations, regardless of the particular ideology that inspires him. They

may refer to the 2011 shooting in Norway by Anders Breivik as an act of homegrown terrorism, despite the fact that he espoused right-wing ideology.

A third possible distinction involves discriminating terrorism that might be perpetrated by Muslims from that perpetrated by Islamist fundamentalists. Some analysts, for example, include in their studies of homegrown terrorism all Muslims perpetrating acts that could meet the criteria of terrorism, not just individuals inspired by a particular ideological doctrine associated with militant jihadism. Hence, the October 2002 Beltway or "D.C. Sniper" is included in these data bases, because the chief perpetrator, John Allen Mohammed, was a Muslim. He is rarely included in other data on homegrown terrorism because although he was a Muslim, his shootings were thought to be motivated by personal grievances, and not by jihadist ideology.

The importance of definitions can also be illustrated by considering the term "terrorism" in greater detail. The difficulty involved in deriving a shared definition of terrorism is well-known. Less appreciated is how that definitional problem can skew search results and, consequently, efforts to assess the nature and intensity of terrorist-related activity in a country, like the United States. These problems require vigilance in any terrorism related research online. Consider a researcher that is examining incidents of terrorist violence in the United States and using the following working definition: terrorism is violence aimed at individuals who are not implicated in the offending policies (civilians) to generate fear in a broader audience, in an effort to advance the militants' political goals. All of these are common elements in definitions of terrorism.

An online search of U.S. news reports in which the word "terrorist" is used would, however, yield incomplete results because of the reluctance of some editors, reporters, and government officials to apply the term consistently regardless of the alleged perpetrator's political viewpoint. For example, researchers might observe reluctance by some news outlets to use the term "terrorist" to describe those perpetrating violence for the sake of anti-government ideologies, in order to avoid the repercussions of being seen as questioning or delegitimizing causes sometimes associated with the political right in the United States. Hence, the 2010 attack by the long time anti-tax activist Joseph Stack on an I.R.S. building in Austin, Texas, which was accompanied by a detailed manifesto, often will not appear in searches of terrorist activity in the United States. Alternatively, it will appear relatively low in search results, because the term terrorism is not used in descriptions of his violent act. Fortunately, in that case, the researcher may stumble upon articles detailing the details of the attack, and correct his or her data so that the incident is included, in accordance with the aforementioned definition of terrorism.

More problematic are the cases that are not detected because the individual reporting or supplying information about the events chose to selectively avoid (consciously or not) the term terrorism in describing acts committed by one subsection of the population, regardless of whether or not those acts qualify as terrorism according to objective analytical criteria. Add to this the deeper problem that news organizations lack the economic incentive to invest the same resources monitoring and covering terrorist acts that originate in non-jihadist militants, compared with those that resonate with post 9–11 apprehensions about violence originating from Muslim fundamentalists. The result is that searches of terrorist attacks or acts in the United States will yield a biased sample in which Islamist oriented attacks may appear to occur in greater incidence or proportion to those perpetrated by others. In short, the use of different definitions of "homegrown terrorism" yields different quantitative and qualitative data, which affects assessments of the magnitude and nature of the problem. If right- and left-wing terrorists as well as Islamist extremists are included in the definition of homegrown terrorism employed in a researcher's online sources, quite a different picture emerges of the nature of the threat than a study based on sources that defines homegrown terrorism as a strictly Islamist phenomenon.

One lesson for researchers in this regard is that search terms that could potentially have varied interpretations or definitions must be parsed into constituent concepts, or the researcher must look closely at the definition of the term that informs the selection of cases or events in the source from which he or she is deriving data. Researchers may want to avoid terminology that is loaded, or ambiguous, and identify more concrete or fundamental aspects of the phenomenon studied and employ terms derived in that manner. While these dangers are not exclusive to online research, the variety of reports and data sources available from a simple keyword search can disarm the researcher and reduce the impulse to critically analyze those resources. Unlike a report that a researcher might solicit from a known scholar after learning of its content, a researcher may have little background on the methodology or definitions employed in online reports or databases and must remain vigilant in attending to these critical details.

Selection bias

A second set of lessons stems from the methodological bias that can be introduced into research when analysts rely on online sources. One can consider this a kind of "selection bias." The information found by a researcher is presumed to represent an unbiased subset of the knowledge available on a topic. In actuality, however, the information available is only partial and incomplete.

To see how information may be biased in this manner, a first step is to consider who has access to the Internet and what information they may and may not make available online. While it may seem limitless, the Internet does not capture the universe of information available on any given issue. It does not even capture a representative subset. Consider that, whether participating in an online discussion forum, or uploading reports, supplying information online requires investment in time and money, however nominal, by the person or entity involved. Therefore, that supply is inherently selective and partial. Information may be supplied by organizations and individuals who often have an editorial perspective, or a political, commercial or social motivation to provide it. In short, what is put online reflects the perspectives or interests of those able and willing to make available the information. This may seem a straightforward observation, but it has profound implications for those employing the Internet in their research.

For example, an individual researching the incidence of terrorism may be drawn to government reports and official data. Yet, information may be selectively provided by the government institution in question. Some data may be omitted in a document or resource online, or in the case of state censorship, as a result of the sensitivities of the authorities to the public availability of such information (Langford 2000). All of these factors affect the baseline pool of data available online. In the case of subject matter like terrorism, they can influence the information obtained through online research.

In general, analysts should regularly reflect on what is being offered online, and why. One set of issues relates to government interference. In the case of a government release of a report on terrorism, why has some information been made available and what might not be released? Is there an opaque agenda designed to influence assessments and understandings of terrorist activity occurring in the country? What data might the state have that is not being publicly offered? What are the boundaries of online monitoring or censorship in the state and how might that affect what opinions appear, or do not appear? In short researchers should be mindful of bias that comes from government selectivity, controls, or other forms of censorship.

Another factor that could influence what is available online is the commercial interests or organizational goals of those producing content on websites. Given the spread of online advertising and other commercial activities, what information is made available on websites could be influenced by economic pressures and forces. Given the non-hierarchical nature of the web, which suggests that information will flow unhindered by the interventions and control of large

institutions, users may neglect that those using the web must fund their activities and therefore may be influenced by commercial motives as well. This could shape reporting on issues and what is made available online by these websites. Analysts should in general bear in mind the interests and motives of institutions, both public and private, in supplying information on their websites, or in blocking or concealing other information.

Sample bias

Internet research can also be vulnerable to the methodological problem of sample bias. Consider the problems that can occur in efforts to monitor social media or opinion oriented websites or discussion forums. Analysts may look at chat rooms, discussion boards, listservs, blogs, and a variety of social networking sites, such as Twitter feeds and Facebook pages, to gauge popular reactions or opinions about an issue or event. A researcher may, for example, try to gauge sympathy for terrorism or how acts of terrorism are being received and interpreted in a local setting or community. In the case of social media or discussion forums, the ability of individuals or a subset of the population to access the Internet, technological and financial barriers to entry and the varying motivations to participate in online commentary and communications may affect who is participating in online discussions. If who is online is not a representative sample of the population of interest, then inferences about the attitudes exhibited in those online contributions will reflect that sample bias.

Consequently, analysts should consider who has access to the Internet and how the demographic or political backgrounds of those who are active online might affect what opinions are represented – and not represented. The absence of a set of opinions should not be taken as evidence that those opinions are not held in the wider population. Rather, the absence of such evidence may simply mean that subset of a population lacked the will or capacity to participate in online discussions or share their opinions online.

A related issue, especially relevant for researching the attitudes of participants in online forums, is the relationship between the online community and actual real-world lives of members of that community. Are the assessments about attitudes and behaviors toward extremist causes and terrorist activity gleaned through ethnographic research of online communities correlated with professed attitudes and observed behaviors offline? Put simply, is what people say online related to what they think and do offline, and therefore, can reliable inferences be drawn from observing online communities? Similarly, scholars should consider the significance of studying individuals that interact as a virtual "community" versus in-person social relationships. For example, scholars have debated whether the social bonds that emerge online in militant networks have the same resilience and depth as in-person social networks (Sageman 2008). In assessing sympathy for terrorism or propensity for extremism, the impact of the Internet as a medium on the content and expression of attitudes should be considered.[4]

In general, as scholars or analysts contemplate relying on online resources as a research method, they should consider how sample or selection bias can influence or skew their findings. The sheer volume of material available online generates the image that the Internet is a comprehensive and neutral source of information. Online information, however, is not inherently value neutral, representative or universal in its supply. How information becomes available, and who makes it available, can shape the results of Internet searches, introducing potential sources of bias.

Misinformation

An additional concern about online research relates to the validity of the information researchers find online. Information may not just be skewed by selection or sample bias. It may be factually

wrong or incomplete. This can be result of error or lack of experience among those supplying the information, or the deliberate efforts to manipulate content on websites.

Concerns about the veracity of information and data in research certainly are not exclusive to online sources. Yet, information online may be more vulnerable to inaccuracies, omissions and distortions (Vedder 2001). For those with interest and access to the web and a desire to contribute to public debate and discussion, the technological barriers to entry have fallen considerably. In the past, information about defense or military related topics, or terrorist activity, would often originate in print and broadcast media reports, government institutions and academic researchers. When information is reported by established institutions, assuming adherence to conventional standards of evidence in academic scholarship and journalism, it would be sourced and vetted. The advent of individuals and small groups providing news and commentary means that those standards or conventions of validating information may not be accepted or followed. Hence, with the supply of more information from more diverse sources, the relative reliability of the information has fallen.

Also relevant is the phenomenon of "citizen journalism." This refers to the opportunity for individuals with smartphones, or computers to act as de facto freelance journalists, supplying information to established news sources, to websites of their choice, or communicating it themselves via social media. This "democratization" of journalism has clear advantages in that it means more diverse and varied information may be available to the public. But it also means that information is circulating with few checks on its reliability.

Add to this the speed with which information spreads, and inaccuracies that might in the past have been detected before being introduced to the public, can be widely circulated and, through their very ubiquity, gain credibility. Misinformation, like accurate information, spreads quickly online. Such a phenomenon occurred in the aftermath of the May 2013 Boston Marathon bombings in Massachusetts, when an individual was identified by an onlooker as a potential perpetrator of the bombings. His picture was taken and then circulated widely on the web. Only subsequently did it become clear that the individual in question had nothing to do with plotting the attack.

Also relevant, is how stories and facts reported online often come to be seen as valid and reliable. Consider the algorithms employed by search engines and the indexes created from which search results are built. Well-known search engines rely on algorithms that order the results of searches according to what amounts to the popularity of websites; how many times the site is visited may affect where it appears in the hierarchy of results. Search engines may use links to webpages from other webpages in indexing, such that "popular" pages can move up the hierarchy of search results.

A source that, in turn, appears on the first page of search results may in turn seem to be more legitimate or credible than one buried in subsequent pages. Consequently, a website may appear credible because it is frequently accessed, independent of its actual accuracy and consistency with real events. In other words, the more people who visit a site, the more popular it becomes, and the more accepted and therefore reliable it may appear. Search engines, however, do little to evaluate the actual credibility or reliability of website content.

In general, the frequency that a report or fact appears online should not be taken as evidence of its accuracy. For example, a particular fact or event may be reported in stories on apparently unrelated websites. A reader may conclude that the widespread coverage means the information reported is accurate. Researchers, however, should always consider tracking back to original sources. At the least, it is useful to click through the links provided on a website to other sites to find where the relevant information originated. A danger is that each seemingly independent story may in fact all reference the same source. This does not mean the information is incorrect,

but it does suggest it has not been as widely validated as its appearance in stories on multiple sites suggests. Rather, the spread of the report reflects the non-hierarchical and unfettered flow of information online.

Researchers seeking to assess the accuracy of information provided on websites can examine a number of features of those sites. This evaluation can also reveal biases or editorial perspectives that could affect the content or presentation of information. A first step is to assess the identity and credentials of the author or organization that produced the website. Online sites can be evaluated in a manner similar to that of conventional print sources. A researcher may look at who funds the organization supporting the website, examine its mission statement and principal audience, and investigate the background and experience of the authors whose work appears on the site. Other steps involve looking at the text and linked reports. One should assess the evidence provided in support of an author's claims, and whether attributions to source material are appropriate and common; the most reliable sources will include references, citations and the like.

Other steps relevant to ascertaining the validity of online sources include looking for contact information of the authors or organizations publishing or sponsoring a site to see if it is provided. Generally, more reputable sources will provide a means for contacting those sponsoring the site, or publishing material that appears on it. The reliability of a website also depends on how current is the information, and whether it is frequently updated. Researchers should also look at the server hosting the site to see if it is reputable and consider the domain (e.g. ".edu"; ".gov"; ".com"). Looking to see what links connect the site to other sites is also useful in assessing the reliability and biases of a website.

Many of these steps are intuitive, and most Internet users will be accustomed to detecting sites that seem suspect. Yet, for those aiming to use online research in support of their work, it is worthwhile to be systematic in evaluating websites. In addition to the suggestions cited above, many government institutions and libraries also publish comprehensive guides for evaluating Internet resources.

Propaganda and the strategic use of the Internet

Mistakes and errors represent one potential source of misinformation. In these instances, the intent of those supplying the inaccurate information is not necessarily to deliberately mislead. Another set of problems, however, that could affect online research stems from efforts by individuals or institutions to deliberately mislead or provide false information online. This can come in the form of fabricating or embellishing information and stories on websites or in the form of a more concerted propaganda campaign aimed at influencing a particular audience.

The Internet, in fact, represents a tremendous resource to governments, organizations and individuals seeking to influence a designated target audience (Shah 2005). It provides opportunities to alter or control information and shape popular reactions and opinion. The motivation for such efforts can be political or commercial. For example, companies may deploy paid workers to surf the web and offer favorable reviews and contribute positive commentary about their products or services. Government authorities may covertly participate in cyber forums, or otherwise provide selective information targeted to shape debate on an issue of concern. For these reasons, it is essential to consider how the Internet can be used as a tool or instrument of influence by individuals and institutions. This will safeguard against researchers unwittingly reporting and using incomplete, skewed or false information and data.

Research on terrorism and militant groups once again illustrates these concerns. Assume a Western government is monitoring and covertly participating in discussion in Internet chatroom

forums on militant jihadist websites. That government in turn is aiming to undermine the organization and supplies stories and commentaries by its own agents posing as visitors to the sites. In an effort to sow divisions and provoke factionalism, for example, government employees might pose as participants who offer divisive opinions or information intended to strike discord in the organization. An outsider that monitors that website can come away with the impression that the fissure is real or originating within the movement's leadership. But it may be artificial and may not reflect any actual debate occurring in the group. Although not the intended audience, the researcher nonetheless will have an inaccurate understanding of the dynamics within the organization he or she is studying.

Similarly, a researcher seeking to analyze counterinsurgency operations in a country could experience related problems. With the emphasis in counterinsurgency doctrine on grassroots appeals to local populations, a government seeking to advance its goals could conceivably have incentives to control information or influence reporting about local military events or economic development efforts. While these tactics of shaping reporting and public information are certainly nothing new to the practices of military organizations, the Internet provides new and creative opportunities to disseminate stories and means for disguising their sources and authenticity. A researcher interested in how economic development efforts are proceeding or being received locally in a conflict zone might, consequently, be misled by positive reports disseminated as part of a larger public relations effort.

In summary, the Internet provides an opportunity for government entities to influence targeted audiences, by shaping information online, or through subterfuge and participation on relevant websites. Those with commercial interests, or those motivated by other political and social motivations, may also try and influence what does and does not appear online. For this reason, researchers need to be cautious and stay mindful that the information they might find on sites may be the result of third parties' efforts to manipulate data or otherwise to use the Internet to their advantage.

Conclusion

The Internet represents a vast and unharnessed resource and opportunity for researchers. Yet, even as scholars and analysts exploit these opportunities, it is essential that they remain mindful of potential pitfalls and dangers of using the Internet as a resource and method in their research. These include problems related to selection bias, sample bias, misinformation and propaganda, and problems with definitional and concept uniformity. Some of these issues are similar in kind to conventional research methods, but may be rendered more acute in online research, while others are problems that originate in the nature of the Internet itself. Regardless, just as researchers invest time and resources in learning to employ conventional methodologies in their research, they are wise to educate themselves about both the opportunities and potential risks of online research.

Notes

1 I focus here on the benefits and methodological considerations related to online research. The Internet is also an important resource for researchers in their efforts to enhance collaboration, share information, disseminate and market their research to academic and other audiences. See for example, "Social Media: A Guide for Researchers," Research Information Network, February 2011. Available at www.rin.ac.uk/our-work/communicating-and-disseminating-research/social-media-guide-researchers

2 For general overviews of online research across different disciplines see Johns et al. (2003), Hooley et al. (2012) and Hewson et al. (2003).

3 For an example of an online resource that focuses on monitoring jihadist websites see the SITE Intelligence Group, which provides, among other products, a subscription service for governments and corporations. Available at http://news.siteintelgroup.com/services.

4 For discussion of issues that arise in online ethnographic research see Hooley et al. (2012: pp. 73–89), Kozinets (2009) and Garcia et al. (2009).

References

Bjelopera, J.P. and M.A. Randol (2010). *American Jihadist Terrorism: Combating a Complex Threat*. Washington, D.C.: Congressional Research Service, Library of Congress.

Comer, D.E. (2011). *Computer Networks and Internets*. Upper Saddle River, NJ: Pearson Higher Education.

Dahl, E. (2011). "The Plots That Failed: Intelligence Lessons Learned from Unsuccessful Terrorist Attacks against the United States." *Studies in Conflict and Terrorism*, Vol. 34, No. 8: 621–648.

Garcia, A.C., A.I. Standlee, J.H. Bechkoff and Y. Cui (2009). "Ethnographic Approaches to the Internet and Computer-Mediated Communication." *Journal of Contemporary Ethnography*, Vol. 38, No. 1: 52–84.

Hamilton, R.J. and B.J. Bowers (2006). "Internet Recruitment and E-Mail Interviews in Qualitative Studies." *Qualitative Health Research*, Vol. 16, No. 6: 821–835.

Hewson, Y.C., P. Laurent and C. Vogel (2003). *Internet Research Methods*. London: Sage.

Hooley, T., J. Marriott and J. Wellens (2012). *What Is Online Research?* New York: Bloomsbury.

Johns, M., S.L. Chen and J. Hall (eds) (2003). *Online Social Research: Methods, Issues and Ethics*. New York: Peter Lang.

Kozinets, R.V. (2009). *Netnography: Doing Ethnographic Research Online*. Thousand Oaks, CA: Sage.

Langford, D. (2000). *Internet Ethics*. New York: St. Martin's Press.

Sageman, M. (2008). *Leaderless Jihad: Terror Networks in the Twenty-First Century*. Philadelphia, PA: University of Pennsylvania Press.

Salmons, J. (2009). *Online Interviews in Real Time*. London: Sage Publications.

Shah, A. (2005). "War, Propaganda and the Media." *Global Issues*, March 31, 2005. Available at http://www.globalissues.org/article/157/war-propaganda-and-the-media.

Silke, A. (ed.) (2004). *Research on Terrorism: Trends, Achievements and Failures*. London: Frank Cass.

Vedder, A. (2001). *Ethics and the Internet*. Oxford: Intersentia.