ANTI-THESIS

‘Terrorist’ Use of the Internet: An Overblown Issue

Gilbert Ramsay

The role of the Internet in promoting transnational recruitment for armed groups, particularly “terrorist” organisations, is often taken for granted. In reality, the evidence is far from clear-cut. Research on how contemporary armed groups use the Internet suggests that they themselves view the Internet with considerable suspicion. Such accounts, however, fail to take account of an arguably more important question: whether those groups which make extensive use of the Internet have actually been more effective in causing violence than groups which have either chosen not to use it, or which were operating before it came into existence.

Keywords: Terrorism; Internet; Social Media; Political Violence

By virtue of inhabiting the same planet as the rest of us, some insurgents, guerrillas, political radicals and “terrorists” use the Internet. Since they use it for business as well as pleasure, their uses of the Internet are naturally of interest to the states against which their activities are directed. This would be nothing more than a statement of the obvious, were it not for the fact that, for many years—and to some extent even today—the mere fact of terrorists using the Internet has been presented as something remarkable, shocking, alarming and inherently transformative. Merely by using email, for example, or browsing publicly accessible websites, terrorists are, in the policy jargon, engaging in “misuse” or “abuse” of the Internet—as if the Internet were inherently reserved for morally sanctioned or legal practices, or as if escaping from a bank robbery in a getaway car represents a “misuse” or “abuse” of the roads.

In reality, while there is now some interesting research available exploring the specific online practices of “terrorists” (almost always Sunni jihadists and, at a distant second, far-right movements), there is very little systematic discussion of how much Internet use has fundamentally changed the nature of terrorism and political violence, let alone whether it has tilted things in the terrorists' favour.

In this article, I shall argue, both on the basis of what research *does* tell us, and what research has by and large failed to consider that there is little justification at present for believing that the Internet has profoundly reshaped the landscape of conflict in favour of insurgents and "terrorists." While terrorist groups undoubtedly use and therefore presumably gain some perceived advantage from using the Internet, it is by no means obvious that terrorist groups or terrorism more generally actually benefit from using the Internet, relatively or even absolutely.

For many years, armed rebels were seen more as a threat to information technology than as its potential beneficiaries. Steven Levy (132) records how bombproof plexiglass windows were installed to protect programmers at MIT's AI lab from possible attacks by the militant leftist splinter group, the Weather Underground. Nonetheless, as computer networks gradually became available to the general public, concerns quickly started to be raised about, for example, the use of early electronic bulletin boards to bring together American neo-Nazis (Hoffman).

By the end of the 1990s, it was beginning to be observed that some groups that appeared in some national lists of terrorist organisations were maintaining their own websites. This observation quickly fed into a broader discussion going on in Western and particularly American strategic thought about asymmetric threats and "information warfare." It also provided a new avenue for scholars of terrorism, who had long maintained that the phenomenon was best understood as "violence as communication" (Schmid and de Graaf). Early publications on the phenomenon of terrorist use of the Internet, as it tended to be called, to distinguish it from the more sensationalistic notion of cyberterrorism, were not immune to some hyperbole themselves. A typical discussion went something like this: First, based on examples of online content, or (usually anecdotal) reports of terrorists who had used the Internet in some way, it would be deduced that terrorists were systematically "exploiting" the Internet as a "tool" in order to achieve some quite clearly defined organisational outcome. For example, content identified as being produced either by terrorist organisations or by their apparent sympathizers would be taken to amount to a systematic propaganda strategy. Materials such as bomb-making recipes or small arms instruction manuals were presented as evidence for the existence of a "virtual training camp" (Weimann). Online calls for involvement would be treated as equivalent to recruitment and mobilization, and so on.

Second, the mere fact that apparent terrorists were apparently achieving such things online would be assumed—at least implicitly—to constitute a new and greater threat than had existed previously. Just as the Internet made everything more efficient, so the argument seemed to run, it would necessarily make terrorists more efficient. And furthermore, making terrorists more efficient necessarily must mean making them more efficient at causing carnage and mayhem—not, for example, at achieving political goals which might not be, in and of themselves, unjust or objectionable.

For substantive, relatively early work in this area we may look to scholars such as Gabriel Weimann, Maura Conway or Martin C. Libicki. But perhaps the clearest and most eloquent statement of the overall thrust of research in this area can be seen in Audrey Kurth Cronin's attempt to see deep historical parallels between "cyber-mobilisation" and the French revolutionary experience of *levée en masse*. As she argued:

> The means and ends of mass mobilization are changing, bypassing the traditional state-centered approach that was the hallmark of the French Revolution and leaving advanced Western democracies merely to react to the results. Today's dynamic social, economic, and political transitions are as important to war as were the changes at the end of the 18th century that Clausewitz observed. Most important is the twenty-first-century's levée en masse, a mass networked mobilization that emerges from cyber-space with a direct impact on physical reality. Individually accessible, ordinary networked communications such as personal computers, DVDs, videotapes, and cell phones are altering the nature of human social interaction, thus also affecting the shape and outcome of domestic and international conflict. (77)

At the heart of Cronin's argument lies an important paradox which seems at least to hover around what is now a generation's worth of attempts to understand the post-Cold War order and, in particular, the rise of militant Islamism: the question of whether we are witnessing, in essence, a postmodern or a modern phenomenon.

On the one hand, Cronin's article seeks to observe, in the ideological mobilisation of insurgents to battle the occupation of Iraq, a phenomenon closely akin to the raising of French citizens to defend and extend their revolution. (On this note, it is difficult to resist the temptation to compare the bloody, self-sacrificial ethic of a song like *Ummati Qad Lāḥ Fajr*, the informal anthem of IS, although of course this specific example postdates Cronin's article).

On the other hand, she seeks to present cyber-mobilization as something fundamentally alien to the centralized, hierarchical spirit of nationalism as it emerged in Hobsbawm's *Age of Revolution*—as something "individually accessible," spatially fragmented, "networked."

Behind this seeming tension in Cronin's argument lies another tension in another argument: the thesis that networked forms of organisation would increasingly dominate the landscape of conflict in the 21st century. Probably the leading exponents of this idea have been John Arquilla and David Ronfeldt, two analysts with RAND Corporation, who, through the 1990s, developed a theory of what they called "netwar." For Ronfeldt, the network represents the dominant organisational principle of the emerging epoch of human history, distinct from tribal, hierarchical, and market-based forms of organisation. Arquilla and Ronfeldt assumed that the US, in particular, would in future find its hierarchically organised institutions increasingly in conflict with networks which, by virtue of their greater adaptability and fluidity, would tend to outmaneuver conventionally organised forces. This in turn would require US forces to become more networked, on the grounds that "it takes a network to beat a network."

The central ambiguity in Arquilla and Ronfeldt's argument is this: On the one hand, they are keen to emphasize that networks obey a different logic than hierarchies, and therefore must be talked about in a new way. And yet, as military-strategic thinkers, they remain eager to retain at least one concept which seems quintessential to the old hierarchical order: the notion of war. To be sure, "netwar" is a mercurial kind of war. Many of its attributes more closely resemble what at first glance one might be tempted to call "peace." For example, the decision by the Zapatista movement in Chiapas, Mexico, to lay down arms in favor of transnational advocacy is closely analysed by Ronfeldt et al. in *The Zapatista Social Netwar in Mexico*, as a case of the adoption of a "netwar" strategy.

But the “war” in netwar is not, it seems, merely metaphorical. If nothing else, it invokes binary notions of us and them, of blue teams and red, where “red” may be a network but is still unmistakably an “adversary,” and where “us” is usually taken to mean not an equivalent network (such as the network of influential individuals underpinning a regime or a ruling class or a military-industrial complex or even a whole “civilisation”), but rather a set of clear institutions, such as a national military. In short, it conflates, in the helpful terminology of Internet governance expert Milton Mueller, two very different things: the “associative cluster” and the “network organisation.” The “network organisation” is what strategic thinkers like Arquilla and Ronfeldt presumably mean when they recommend more decentralization in the US military. The networks they see as the new enemies are sometimes presented as the same thing: for example, when groups like al-Qāʿida are presented as adopting a deliberate, top-down plan to reorganise into a “franchise” system. But often what is in fact being referred to—particularly online—looks more like the unbounded “associative cluster” consisting essentially of like-minded individuals who sometimes turn out to work in concert.

The issue of network organisations versus associative clusters is specifically important when we come to consider what we now know about how terrorist (for which we can usually read jihadi-Salafist) groups have used the Internet. Here, the broad lesson that seems to have been learned by terrorists and counter-terrorists alike is that the Internet is viewed as a boon to the extent that the online insurgents are prepared to use it as an open medium, and becomes a liability the moment there is any attempt to treat it as a secure environment appropriate for serious organisational activity.

Contrary to the idea of a “virtual safe haven” in which terrorists could freely plan, train, recruit, fundraise and case new operations, it has turned out that terrorists themselves view the Internet as a deeply problematic, often hostile medium to be treated with great caution (Torres Soriano; Hegghammer: ‘Interpersonal trust on jihadi forums’). Bomb-making instructions are often unreliable, and where good quality, vetted versions are to be found, it is difficult to translate theoretical learning into reality (Stenersen; Kenney). Trying to form conspiracies online to do illegal things in communities where the members have never met in person is an intelligence officer’s dream come true. Indeed, we now know that possibly al-Qāʿida’s single most important and trusted online forum in 2009 was a joint creation of Saudi intelligence and the CIA (Hegghammer). Even the authenticity of propaganda content can’t always be trusted. The website *tawhed.ws*, run by the most influential jihadist clerics in the worlds (Brachman and McCants; Wagemakers), was for a long time the single most trusted online resource for jihadi-Salafi literature on the web. Eventually, however, rumours began to circulate as to how the esteemed clerics were able to continue to produce authentic content while in jail, or under constant intelligence supervision. Jihadist advice for staying safe online—even in Western countries—has moved beyond the once universal advice not to try to “join the jihad” online, or to plot operations, to admonitions to not even publish or disseminate content which might openly violate anti-terrorism speech codes.

Moreover, the issue is not just one of operational security. It is also about the difficulty of message control. al-Qāʿida’s leadership turns out to have been deeply concerned about the risk of its message being distorted by its critics and its over-enthusiastic supporters online, striving instead, with little success, to get respectable mass media coverage on the anniversary of 9/11 (“Letters from Abbottabad”). Islamic State—widely hailed as an unassailable paragon of Internet “savviness”—would seem, in reality, to be little different. A leaked internal IS document called “Principles for the Management of the Islamic State” (*mubādāʾ fī idārat al-dawlat al-islamiyya*) reveals a rigidly hierarchical system for the administration of media activities based on a system of “foundations” (*muʾasasāt*), each of which is directly answerable to the governors of each province and, ultimately, to the caliphal *diwan*.

Despite all this, IS seems to be conflicted about its own message. The group is of course notorious for its “slick,” “sophisticated” propaganda videos which prominently feature the gory executions of the group’s many enemies. Off the bat, one might imagine that this approach would be a poor way to sell the group to idealistic young Muslims, either deeply affected by the human suffering of co-religionists, or aspiring to a utopian new society. But one also might imagine that IS had nonetheless thought through these problems and come to the conclusion that such gore was, in fact, effective. And yet, as turns out, it hadn’t. A report from ARA News Agency (Nasro) reveals internal concerns about image management as a result of execution videos, apparently coming from the very top of the organisation, which has since toned down its violent output and re-focused on presenting itself as administratively competent. By contrast, in its official English language magazine (al-Muhājira, “Slave Girls, or Prostitutes?”), IS picked a fight with its own online supporters for misleadingly trying to suggest that the group did not practice sex-slavery. Ultimately, the “netwar” lens through which so much analysis of “terrorist use of the Internet” is, explicitly or otherwise, presented misleads, because where informally bounded networks are in conflict, the size of the conflicting parties is in the eye of the beholder. For example, in the BBC World Service documentary “The Islamic State’s Social Media Machine,” the United States’ *Think Again, Turn Away*[1] counter-narrative program presents itself as “a rag tag guerrilla organisation waging a hit and run campaign […] the David against the ISIS Goliath.” This obviously absurd demarcation of the conflict illustrates how failing to think reflexively about the boundaries of competing networks can confuse. The centralized media apparatus of IS may indeed dwarf the resources of a tiny, experimental niche outfit within the Department of State. But for IS or al-Qāʿida, or indeed any insurgent group, violent or otherwise, the battle is not against some particular state “counter-narrative” program. It is against the massed influence of every satellite channel, every ISP, every cinematic film. In this case it is against Al Jazeera, Al Arabiya, the BBC, CNN, Buzzfeed, Rotana, Uturn Entertainment, Al-Manar, and Anonymous. It is against nearly every opinion leader in society. It is against countless individual Twitter, Facebook or YouTube users determined to expose or lampoon.

In sum, the idea that terrorist groups are formidable masters of the Internet is certainly overblown, and probably a myth. Terrorist groups (and terrorist sympathizers) use the Internet, to be sure. But they use it ambivalently, against opponents who, for all their complaints to the contrary, hold most of the cards. In using the Internet, terrorists are, at best, running faster to stay in the same place.

But are they even doing that? A major problem with research into terrorist use of the Internet is that there is very little systematic comparison between the outcomes for cases where the Internet was not used and cases where it was. And yet, *prima facie*, at least, it is by no means obvious that terrorist groups and other militants who have not had access to the Internet, or have made limited use of it, have been less effective on that account.

al-Qāʿida managed to simultaneously hijack four aircraft in an operation which made occasional and sometimes incidental use of email and web searches. But the absence of such things didn't prevent the PFLP from accomplishing much the same (albeit without the gory intent) in the 1970 Dawson's Field hijackings (Snow and Philips).

Measured solely by number and lethality of attacks, the Lord's Resistance Army managed to become one of the most notoriously lethal and persistent armed groups without apparently ever registering a single website. Much the same holds true for the Naxalites in India (Global Terrorism Database).[2] Even narrower comparisons seem possible, too. Consider, for example, two Iraqi groups: the Naqshbandi Army and the Islamic Army in Iraq. Both were Sunni insurgent militias incorporating significant numbers of former Baathists and of apparently roughly similar significance. But while the Naqshbandi Army has produced a clutch of videos and maintained a website, its material is distinctly pedestrian compared with the extraordinarily innovative campaigns of the Islamic Army in Iraq, as represented by multimedia campaigns such as the "Baghdad Sniper" videos or "Lee's Life for Lies." More research would be extremely valuable here, but it is far from obvious that this media imbalance was in any way replicated in the field.

Perhaps even more remarkably, it is not obvious that the Internet has made a significant difference even in the areas where it would seem almost impossible that it wouldn't—that is, in its ability to transnationalise conflict and radicalise a small but significant number of dispersed, marginal individuals into carrying out acts of violence at home. Media reports abound with tales of IS recruits (in particular) who underwent a mysterious transformation from ordinary sons or daughters to fanatical militants after forming relationships with online recruiters online, and no doubt online interactions have played a larger or smaller role in the recruitment of some of the 5,000 citizens of Western states to fight for jihadist groups in the Syrian civil war, as well as convincing a much smaller number to attempt bombings, stabbings or shootings at home (The Soufan Group). But Anarchist terrorism in the late 19th century, as chronicled by historians such as Richard Jensen (36), produced massacres and assassinations across Europe and North America which look strikingly similar in many ways (lethality, frequency, apparent lack of central organisation) to jihadist terrorism today.

Another obvious point of comparison for contemporary concerns about "foreign fighter" recruitment is the Spanish Civil War. What is striking here is not just that the patterns look similar, but that the numbers also look similar. Beevor (468, quoting Lefebvre and Skoutlsky) reports that the International Brigades recruited around 32,000 fighters over the three-year course of the war—almost exactly the same number as the upper estimate of the number of international fighters who have travelled to Syria and Iraq over the (so far) four-year duration of the Syrian Civil War, which The Soufan Group's most recent report puts at between 27,000 and 31,000.

But a still more focused comparison can be made. Proportionately, the two largest contributors of recruits to the Spanish Civil War were France and Belgium, each of which contributed just over 0.02% of their respective national populations as of 1933 to fight in the conflict.[3] Today these two countries are also Europe's most proportionately important recruitment grounds for the Syrian-Iraqi civil war. Taking into account only the *Muslim* populations of these two countries (which between them account for nearly two-fifths of all recruitment from Europe according to The Soufan Group), reasoning arithmetically, France's level of mobilization today stands

Gilbert Ramsay

is a lecturer in international relations at the Handa Centre for the Study of Terrorism and Political Violence (CSTPV) at the University of St Andrews. He works on media, mobilisation and political violence and is the author of *Jihadi Culture on the World Wide Web* (2013), a book based on his PhD thesis. He is co-editor of *State Terrorism and Human Rights: International Responses since the End of the Cold War* (2013) and *Globalizing Somalia: Multilateral, International and Transnational Repercussions of Conflict* (2013).
email: gawr2@st-andrews.ac.uk

at 0.03% of its Muslim population (based on Pew Research's estimate for the French Muslim population, 2015), Belgium's, at 0.08% of its Muslim population (also using the Pew figures). Even in the most extreme case, the proportion of the population mobilized remains firmly at the same order of magnitude. And this is without taking into account that presumably the entire population of France and Belgium was not realistically available to foreign fighter recruitment to the International Brigades, whereas some of the foreign fighter recruits to jihadist groups in Syria and Iraq are recent converts, meaning that the non-Muslim population of these countries is arguably a relevant recruitment reservoir in this case as well. It also overlooks the different timescales.

Indeed, the genuinely interesting question about "terrorist" use of the Internet is arguably not how or whether the Internet has transformed militancy, but why (so far) it apparently hasn't. Cronin was right to observe that the Internet has fundamentally changed the way that ordinary people communicate, across the entire world. Internet uptake statistics show that the age of the "digital divide" is rapidly coming to an end ("Internet Users in the World by Regions - 2015"). And yet the forms and methods of political violence we see today have not moved on. The basic practices of sub-state violence are the same as they were in the 1950s, and in many ways are closely reminiscent of what was happening (albeit in one small corner of the world) even in the 1890s. This may mean that what essentially causes political violence has little to do with how people communicate, but rather the fundamental nature of the relationships that this communication sustains. Or it may simply mean that, much as the political consequences of printing took a good century and a half to bear fruit in Europe, the implications of the Internet for how conflict happens, and what conflict is about, simply haven't borne fruit *yet*. But either way, it seems doubtful that the beneficiaries will be the "terrorists" of today who, while they may be drawing on transnational sentiment as a means, are still apparently trying, albeit not in conditions of their own choosing, to set up the orderly, hierarchical, territorially limited, and patriotic polities of yesterday.

Notes

[1] <http://thinkagainturnaway.tumblr.com>.

[2] Global Terrorism Database, <www.start.umd.edu/gtd/>. Search terms: "Lord's Resistance Army"; "Communist Party of India: Maoist". The Communist Party of India (Maoist), often (not wholly accurately) identified with "Naxalite" insurgents in India has now apparently established a Facebook page (<www.facebook.com/maoistindia>), and a collection of its press releases is available from < www.bannedthought.net/India/CPI-Maoist-Docs/>. But its online presence apparently remains limited.

[3] Absolute numbers of recruits from Beevor, population figures from <http://www.populstat.info/Europe/>.

Works Cited

Arquilla, John, and David Ronfeldt. *Networks and Netwars: The Future of Terrorism, Crime and Militancy*. Santa Monica: RAND, 2001. Print.

Beevor, Anthony. *The Battle for Spain: The Spanish Civil War 1936-1939.* New York: Penguin, 2006. Print.

Brachman, Jarret, and Will McCants. "The Militant Ideology Atlas: Executive Report." Westpoint: Combating Terrorism Centre, Nov. 2006. Web. 29 Mar. 2016.

Casciani, Dominic. "The Islamic State's Social Media Machine: The Documentary" 2 episodes. *bbc.co.uk*. BBC World Service, 5 and 17 May 2015. Web. 29 Mar. 2016.

Conway, Maura. "Terrorist 'Use' of the Internet and Fighting Back." *Information & Security: An International Journal* 19 (2006): 9-30. Web. 29 Mar. 2016.

Cronin, Audrey Kurth. "Cybermobilisation: The New 'Levée en Masse'?". *Parameters: United States Army War College Quarterly* 36.2 (2006): 77-87. Web. 29 Mar. 2016.

Hegghammer, Thomas. "Interpersonal Trust on Jihadi Forums." *hegghammer.com*. Draft chapter. *Fight, Flight, Mimic: Identity Signalling in Armed Conflicts.* Ed. Diego Gambetta. Oxford: Oxford UP, forthcoming. Web. 29 Mar. 2016.

---. "Spy Forums." Web Blog. *jihadica.com*. Jihadica, 19 Mar. 2010. Web.

Hobsbawm, Eric. *The Age of Revolution: Europe 1789-1848*. New York: Abacus, 1988. Print.

Hoffman, David S. *Web of Hate: Extremists Exploit the Internet. adl.com.* USA: Anti-Defamation League, 1996. ADL Research Report. Web. 29 Mar. 2016.

"Internet Users in the World by Regions – 2015." Chart. *internetworldstats.com.* Internet World Stats, Nov. 2015. Web. 29 Mar. 2016.

Jensen, Richard. *The Battle Against Anarchist Terrorism: An International History, 1878-1934*. Cambridge: Cambridge UP, 2014. Print.

Kenney, Michael. "Beyond the Internet: Mētis, Techne and the Limitations of Online Artefacts for Islamist Terrorists." *Terrorism and Political Violence* 22.2 (2013). 177-97. Web. 29 Mar. 2016.

Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. Santa Monica: Cambridge UP, 2007. Print.

Mueller, Milton. *Networks and States: The Global Politics of Internet Governance*. Cambridge, Massachusetts: MIT Press, 2013. Print.

Nasro, Jan. "Baghdadi Bans Broadcast of Slaughterscenes." *aranews.net.* ARA News Agency, 18 July 2015. Web. 29 Mar. 2016.

Snow, Peter, and David Philips. *Leila's Hijack War*. London: Macmillan, 1970. Print.

Pew-Templeton Global Religious Futures Project. *globalreligiousfutures.org*. Web. 29 Mar. 2016.

"Principles for the Administration of the Islamic State." [Original in Arabic]. Transl. Aymenn Jawad al-Tamimi. *meforum.org*. Middle East Forum, 7 Dec. 2015. Web. 30 Mar. 2016. Arabic original available on <fr.scribd.com/doc/292084330/Islamic-State-blueprint>. Web. 30 Mar. 2016.

Ronfeldt, David. "Tribes, Institutions, Markets, Networks: A Framework for Thinking About Societal Evolution." *RAND Paper* P-7967. Santa Monica, CA: RAND, 1996. Web. 30 Mar. 2016.

Ronfelt, David, et al. *The Zapatista "Social Netwar" in Mexico*. Santa Monica, CA: RAND, 1998. Web. 28 Mar. 2016.

Stenersen, Anne. "The Internet: A Terrorist Training Camp?" *Terrorism and Political Violence* 20.2 (2008): 215-33. Web. 30 Mar. 2016.

→

→ ---. "'Bomb Making for Beginners': Inside an Al-Qaeda e-Learning Course." *Perspectives on Terrorism* 7.1 (2013): 26-37. Web. 30 Mar. 2016

Schmid, Alex, and Janny de Graaf. *Violence as Communication: Insurgent Terrorism and the Western News Media*. Thousand Oaks, Calif.: Sage, 1982. Print.

The Soufan Group. "Foreign Fighters: An Updated Assessment of the Flow of Foreign Fighters into Syria and Iraq." *soufangroup.com*. NewYork: TSG, Dec. 2015. Web. 29 Mar. 2016.

Thomas, Hugh. *The Spanish Civil War*. London: Hamilton, 1977. Print.

Torres Soriano, Manuel R. "Vulnerabilities of Online Terrorism." *Studies in Conflict and Terrorism* 35.4 (2012): 263-77. Web. 30 Mar. 2016.

al-Muhājira, Umm Sumayyah. "Slave Girls, or Prostitutes?" *Dabiq* 9 (May 2015): 44-49. *pietervanostaeyen.wordpress.com*. Web. 29 Mar. 2016.

Wagemakers, Joas. *A Quietist Jihadi: The Ideology and Influence of Abu Muhammad al-Maqdisi*. Cambridge: Cambridge UP, 2013. Print.
Weimann, Gabriel. "A Virtual Training Camp: Terrorist Use of the Internet." *Teaching Terror: Strategic and Tactical Learning in the Terrorist World*. Ed. James J.F. Forest. Boulder, Colorado: Rowman & Littlefield, 2006. 110-32. Print.

---. *Terror on the Internet: The New Arena, the New Challenges*. Washington, DC: United States Institute of Peace Press, 2006. Print.

ISSN: 2196-629X
http://dx.doi.org/10.17192/meta.2015.6.5081