This is an author produced version of a paper published in:
*Studies in Conflict & Terrorism*

Cronfa URL for this paper:
http://cronfa.swan.ac.uk/Record/cronfa35706

**Paper:**
http://dx.doi.org/10.1080/1057610X.2016.1157402

This item is brought to you by Swansea University. Any person downloading material is agreeing to abide by the terms of the repository licence. Copies of full text items may be used or reproduced in any format or medium, without prior permission for personal research or study, educational or non-commercial purposes only. The copyright for any work remains with the original author unless otherwise specified. The full-text must not be sold in any format or medium without the formal permission of the copyright holder.

Permission for multiple reproductions should be obtained from the original author.

Authors are personally responsible for adhering to copyright and publisher restrictions when uploading content to the repository.

http://www.swansea.ac.uk/library/researchsupport/ris-support/
Introduction to the Special Issue:
Terrorist Online Propaganda and Radicalization

Anne Aly
Edith Cowan University, Perth, Australia
Email address for correspondence: a.aly@ecu.edu.au

Stuart Macdonald
College of Law & Criminology, Swansea University, Singleton Park, Swansea, UK
Email address for correspondence: s.macdonald@swansea.ac.uk

Lee Jarvis
School of Politics, Philosophy, Language and Communication Studies, University of East Anglia,
Norwich, UK
Email address for correspondence: l.jarvis@uea.ac.uk

Thomas M. Chen
School of Mathematics, Computer Science & Engineering, City University London, UK
Email address for correspondence: tom.chen.1@city.ac.uk

Abstract: The Internet is a transformative technology that terrorists are exploiting for the spread of propaganda and radicalizing new recruits. While al-Qaeda has a longer history, Islamic State is conducting a modern and sophisticated media campaign centered around online social networking. This article introduces and contextualizes the contributions to this Special Issue by examining some of the ways in which terrorists make use of the Internet as part of their broader media strategies.
In October 2014, three teenage girls from Denver, Colorado, were noticed missing from high school. German authorities intercepted them at the Frankfurt airport and sent them back to the U.S. where they were questioned by FBI agents. The girls were suspected of heading to Turkey then Syria to join Islamic extremists although details of the case were sealed because of their ages (15 to 17). All three had browsed extremist websites to research how to get to Syria. Earlier that year, in January, 19 year old Shannon Conley was arrested at Denver International Airport en route to Syria via Frankfurt and Turkey. Charged with conspiracy to help the Islamic State (IS, formerly ISIS - Islamic State of Iraq and al Sham, also known as Daesh) in Syria, she admitted to ‘radicalization’ by a Tunisian militant who she had met online and intended to marry. Conley said that her knowledge of Islam was based solely on her own online research.

Similarly alarming stories of radicalization are repeated regularly in the news media and beyond. Indeed, according to some of the more hysterical reports, more British citizens joined IS in Iraq and Syria than enlisted in the UK Army Reserve in 2013 (several hundred compared to 170). Reports such as these are invariably accompanied by two types of causal question. First is a question of direct causation: Why do young men and women want to leave often comfortable lives in order to join violent extremists in distant countries? Second, is a question of enabling causes: How important is the influence of the Internet in this process? What role does it play in encouraging or facilitating efforts to participate in campaigns such as those waged by al-Qaeda or IS?

**Terrorism, Technology and the Internet**

The types of violence now typically described as terrorism, of course, existed long before the Internet but, as everyone is aware, the Internet has been an enormously transformative technology. Digital divides notwithstanding, it is literally at our fingertips; about one in four people on Earth today carries a smartphone that allows instant connection to the Internet. Facebook counts close to 1.5 billion active users, almost 20 percent of the world population. Unsurprisingly, the Internet has been embraced by terrorists for the same reasons as it has by other organizations, including its capacity to expand reach and influence. If terrorism is understood as a form of communicative violence, and
spreading propaganda and attracting attention are therefore central to it, then an online presence is logically even more vital to terrorists than it is many other organizations. Recent studies have identified thousands of overtly jihadi websites operating on the Internet today.\(^8\) IS has been particularly active and successful in recruiting foreign fighters, notably from Europe and America, using Twitter, Youtube, Diaspora, and other online social networks.

The Internet offers obvious and unique advantages over older media such as radio and television. Virtually anyone can set up a website easily and inexpensively to publish literature, images, videos, and software. The message can be completely controlled by the author-publisher and is not dependent on news reporters or government approval or mediation (television stations are state operated in many countries). More important, though, is the opportunity presented by new media technologies for two-way interactivity through forums, chat rooms, email, texts. Terrorists can connect directly with various audiences, and those audiences, in turn, can become active participants in an unfolding conversation. A sense of virtual community can therefore be fostered, which is often not possible with more traditional forms of broadcast media like radio and television.

Terrorists recognize that the Internet is a powerful tool to utilize deliberately and tactically to advance their strategic objectives. In order to properly understand online propaganda and radicalization – the theme of this special issue of *Studies in Conflict & Terrorism* – the Internet should be examined within the broader context of other tools in terrorists' media strategies.

**Online Propaganda Strategies**

Ayman al-Zawahiri, current head of al-Qaeda and former deputy to Osama bin Laden once said, “We [al-Qaeda] are in a battle, and more than half of this battle is taking place in the battlefield of the media. And that we are in a media battle in a race for the hearts and minds of our people”.\(^9\) Al-Qaeda has been able to adapt its media strategy to changing circumstances and technologies over the years. Initially al-Qaeda concentrated on aiming propaganda, mostly videos and pamphlets, internally to its own members, contributing to the construction of something of a personality cult around Osama bin Laden.\(^10\) Through the 1990s, al-Qaeda began expanding its reach throughout the West with interviews
of bin Laden being given to prominent Western journalists such as Robert Fisk. At the same time, al-Qaeda strived to build support in the Muslim world, including through the Al-Jazeera television network, mainly via interviews of bin Laden or his deputy, Ayman al-Zawahiri.

In 2001, the focus of al-Qaeda’s media strategy turned toward attacks and kidnappings, starting with a long video recording of the attack on the USS Cole destroyer in October 2000. With attention from the 9/11 attack, al-Qaeda shifted their propaganda internationally. An example of its new focus was the filming of the kidnapping and assassination of American journalist Daniel Pearl in 2002. Before 9/11, al-Qaeda had one website which was only in Arabic. Post 9/11, al-Qaeda expanded its propaganda campaign through its website (al_nida.com) establishing a special media production division, al-Sahab, for audiovisual tapes and CDs for distribution through Arab television channels and a growing number of jihadist websites in different languages.

Much of the propaganda was aimed at the Muslim mainstream because a central objective of al-Qaeda’s propaganda strategy was winning the support of the Muslim ummah. However, al-Qaeda recognized the necessity to engage its enemy on several fronts simultaneously. Its propaganda was therefore also aimed at maximizing the impact of terrorism to inflict damage upon the ‘far enemy’ of the US and its allies, and mobilizing Western Muslims against their own governments. The Internet served as the prime channel for distributing propagandist materials, complemented by radio and satellite TV channels and print media. In turn, al-Qaeda relied increasingly on young adults with technology skills to improve the quality of propaganda materials distributed on the Internet and social networking sites, and expanded media production outlets such as Al-Furquan, As-Sahab Media, Media Commission, and Sawt al-Jihad.

Although IS traces its origins to bin Laden, it split decisively from al-Qaeda in February 2014 and its current leader is Abu Bakr al-Baghdadi. The ideology and propaganda strategy of IS differ from those of al-Qaeda. Although the relationship between politics and religion is always a complex one, IS has articulated a desire for returning to a particular reading of early Islam and the "Prophetic methodology" referring to the prophecy and example of Muhammad. Following takfiri doctrine, it is committed to purifying the world by killing vast numbers of people. Unlike al-Qaeda’s focus on the
Western enemy, IS is more concerned with the application of Sharia in the caliphate and expansion of local territory, although the recent 13 November 2015 coordinated attacks in Paris suggest an expansion of their agenda to the international stage.

IS’s propaganda strategy is modern and sophisticated, which includes not only extensive use of online social networking but also high quality video production and publications. A highly publicized instance was a slickly produced video of the beheading of American journalist James Foley in August 2014. The New York Post published a graphic image on its front page, and screenshots from the video spread widely on Twitter. Most media outlets and journalists declined to share the graphic video or photos, but IS was aware that social media was an easy way to bypass the checks used by media organizations to stop the spread of propaganda.

IS publishes annual reports on its progress complete with high quality illustrations and infographics. Reports are filled with attack metrics, an approach emulating modern metrics-oriented corporations. The effect is to “communicate organizational efficacy to outside parties, such as donors, al-Qaeda groups, and adversaries,” according to a report by the Institute for the Study of War.14

IS’s sophisticated propaganda campaign depends prominently on social networking. Thousands of IS’s Twitter followers installed a custom-developed app called Dawn of Glad Tidings that allows IS to send out centrally written tweets through their accounts. Released simultaneously, the messages swamp social media and extend IS’s online presence much further than normal. In addition to centralized Twitter accounts, provincial accounts publish live feeds about local IS operations. Also, an online fan club of thousands of IS supporters retweets its hashtags and translates messages from Arabic to Western languages.

Everything done in IS’s propaganda strategy has a combined effect to build the "brand". IS has additional advantages over al-Qaeda: more money; weapons and battle experience; and help from a growing number of Western recruits who bring technology skills and English skills. IS also appears deliberately to use English in posts and some videos, including in execution of James Foley in the above-noted video.
While the news media tend to focus on IS's barbarism, its propaganda strategy has been described as much broader, encompassing five additional narratives: (1) mercy (as opposed to brutality); (2) victimhood, e.g., collateral damage blamed on the enemy; (3) war or military gains; (4) belonging (appealing to especially foreign recruits with friendship, security, and a sense of belonging); and (5) utopianism, i.e., not just talking about the caliphate but enacting it. In other words, IS's propaganda is intended to appeal to a broad audience, not only bloodthirsty fighters, which helps to explain its recruitment success.

**Online Radicalization Strategies**

A US Senate Committee on Homeland Security and Governmental Affairs report on violent Islamist extremism and the internet argued that the Internet campaign by al-Qaeda affects a viewer in different ways across discrete stages of radicalization. During the first stage of pre-radicalization and self-identification, an individual may be interested in learning more about the ideology. Websites will lead them directly to the group’s enlistment pages with articles about religious beliefs and core ideologies. The next stage is one of indoctrination when individuals, having accepted the core ideologies and beliefs, seek ways to participate and further the goals of the organization. In the subsequent stage of jihadization, the Internet allows individuals to connect with other recruits and organization members in order to plan and carry out their own attacks.

In the movement toward that which has been termed al-Qaeda 2.0, it may be that al-Qaeda does not depend on the Internet for recruitment as much as it relies on the tendency of individuals to seek out the websites and contact the organization, or in other words, radicalize and indoctrinate themselves. Al-Qaeda's recruitment process via the Internet follows a bottom-up strategy in which sympathizers, who are predisposed to be affected by propaganda, and perhaps indoctrinate themselves by repeatedly exposing themselves to these sites and videos.

IS is believed to operate one of the most sophisticated social media campaigns. It is highly visible and well funded. Reportedly, IS also benefits from its considerable wealth, earning £3 million a day through oil smuggling, extortion, theft and human trafficking. It is deliberately slanted toward
foreigners, both in its content and its target audience. For instance, IS produced a 20-minute video at the end of Ramadan in August 2014 that highlighted shots of the Mujahideen repeating variations of the same message — British, Finnish, Indonesian, Moroccan, Belgian, American, and South African. Important IS messages are commonly released simultaneously in English, French, and German, then later translated into other languages, such as Russian, Indonesian, and Urdu. According to Thomas Hegghammer in an interview with BillMoyers.com, “Foreign fighters are overrepresented, it seems, among the perpetrators of the Islamic State’s worst acts. So they help kind of radicalize the conflict — make it more brutal. They probably also make the conflict more intractable, because the people who come as foreign fighters are, on average, more ideological than the typical Syrian rebel.”

Doctrine requires believers to reside in the caliphate if it is at all possible for them to do so. An exact number of foreign fighters is almost impossible to estimate due to the dangers for journalists and intelligence operatives. Open-source estimates have varied widely. The majority of fighters have come from the Middle East and North Africa, especially Tunisia and Saudi Arabia. The rest have come from other places including former Soviet republics, the Americas, and Australia. Government estimates on the number of Americans joining IS have varied around the range of approximately 30 to 100. Estimates for UK are similarly difficult but usually higher, e.g., news reports have cited 500 British citizens affiliated with IS in Syria and Iraq. French and German fighters have also been observed in large numbers on social media, suggesting perhaps more than 550 fighters from Germany and more than 1,000 from France.

A typical jihadi foreign fighter is a male between 18 to 29 years old, according to the Soufan Group, although there are many exceptions both younger and older. Beyond age and gender, there is no reliable profile of who is most likely to become a foreign fighter. After four decades of research on radicalization, no common socio-economic or religious pathway toward violence has been found, and the term itself is characterized by considerable contestability.

Radicalization has not been limited to men. IS has featured women among their most vocal and visible supporters online. Aqsa Mahmood was one of the many women working to recruit foreigners to join IS. She chose to leave a typical, seemingly happy teenage life in Glasgow, Scotland. She documented her transformation and attraction to radicalism on Tumblr. From Syria, she continued
using Twitter and Tumblr to encourage others to follow her example. The same propaganda and extremist narratives luring male foreign fighters have also been tailored for female audiences, highlighting the "Muslim" cause, a new "utopian" state, and jihadists who are willing to become martyrs in their duty to God. Some women are attracted to a romanticized vision of becoming the wife of a jihadist fighting for the ultimate cause (the caliphate), and many foreign girls will be married off to foreign fighters upon their arrival.

IS's strategy has been innovative. IS has seemingly learned from earlier ultraviolent terrorist groups who ended up alienating supporters. IS has crafted a novel media campaign mixing narratives of brutal violence and utopian idealism. Also, IS's recruitment strategy has differed from al-Qaeda's approach of attracting fighters first and radicalizing them later. IS seeks recruits who are further down the path toward ideological radicalization or more inclined by personal disposition toward violence. When these pre-radicalized fighters and their families arrive in Iraq and Syria, they are exposed to an environment filled with violence and death.

**Terrorists’ Use of the Internet Symposium 2014**

The papers in this special issue were selected from a multidisciplinary symposium held on the 5th and 6th June 2014 on the theme of "Terrorists’ Use of the Internet” organized by the Cyberterrorism Project and hosted at Swansea University. Speakers came from the UK, Republic of Ireland, France, the Netherlands, Norway, Turkey, Canada and Australia. Sixteen papers spanning a range of different disciplines were presented to an audience of academic researchers as well as practitioner representatives from policing and policy circles including the UK Home Office, South Wales Constabulary and the Scottish Organised Crime and Counterterrorism Police Unit.

Across the diverse topics presented, several themes appeared to emerge across the event:

- **Definition:** There were different perspectives on key terms related to cyberterrorism, including definition of cyberterrorism itself. Some debate may be healthy but disagreement on basic definitions also have the potential to impede discussion. Moreover, different definitions may have important practical ramifications (for example, in developing models of risk
management). Deconstructing different understandings of cyberterrorism has the potential to open up a range of other important research questions and create space for dissident voices.

- Transnational: Many online terrorist activities - publicity, propaganda, radicalization, finance - now transcend national boundaries. As a result, international law has a significant role to play, and international cooperation is essential. At the same time, it is important to recognize that many terrorist groups have a specific geographical focus.

- Decentralization: Terrorist activities are increasingly decentralized. Examples include the outsourcing of propaganda production, bottom-up radicalization and the growing number of self-funded terrorist cells.

- Vulnerability: Computer networks enable cyber attacks to reach any connected targets, exposing vulnerable systems to remote attackers. A particular concern in cyberterrorism is national critical infrastructures that are both vulnerable and likely to attract terrorist attention. Attacks on critical infrastructures could endanger large populations. Vulnerability has another meaning as well; citizens are often portrayed as possibly vulnerable to online radicalization.

- Credibility: The credibility of terroristic narratives and counter narratives is important. So too is the credibility of governments’ counterterrorism laws and policies, and the discourse surrounding these. This is particularly apparent in the case of cyber surveillance.

- Power: Terrorist groups employ both hard and soft power in pursuit of their objectives. Whilst counterterrorism frequently employs hard forms of response, there are concerns about the extent to which soft countermeasures are used and their effectiveness.

- Evidence: Areas where understanding is currently lacking and further research is required include: terrorists’ cyber capabilities and the materials they place online; the consumers of extremist online content; the relationship between the Internet and the offline world; the effectiveness of counterterrorism laws and policies, including accountability mechanisms and how to assess effectiveness; how counterterrorism policies are produced; and, how cooperation can be engendered between the private and public sectors and within the international community.
Special Issue

The papers collected in this special issue of Studies in Conflict & Terrorism are organized around the theme of online propaganda, publicity and radicalization. It is intended that this collection will provide a critical portrayal of current thinking on a subject that is increasingly prominent, seemingly straightforward, and yet also controversial. Terrorists do not hide their uses of the Internet for spreading their message and propaganda materials, fund raising, and fostering a sense of community. These uses of the Internet are clearly evident. Among the less understood and more controversial issues is the significance of the Internet in radicalization, which is explored by three of the articles in this special issue.

The introductory article by Martin Rudner sets the general scene examining al-Qaeda's open embrace of the Internet as a tool for "electronic jihad." First establishing that al-Qaeda's strategy documents call for any and all means including electronic communications to ensure eventual victory, the article proceeds to detail how terrorists take advantage of the Internet to: incite fervor and activism by spreading their messages and propaganda, particularly importantly reaching the West; recruit new members including so-called lone wolf terrorists and foreign jihadists from outside the Muslim world; deliver training and indoctrination particularly in weaponry, explosives, and tactics; solicit funds; disseminate tactical instructions for planning and carrying out specific attacks, with some examples cited; and perpetrate cyber attacks, though cyber terrorism to date has been limited to website defacements rather than serious damage to critical infrastructures.

In the second article, David Mair investigates the real-time use of Twitter by Somalia-based group al Shabaab during a 2013 attack on the Westgate shopping mall in Nairobi, Kenya. This was a rare instance of a group producing a live feed through a social network of an ongoing attack. Over the four days of the Westgate attack, 556 tweets from eight al Shabaab affiliated Twitter accounts were analysed in terms of their composition, content, and intended audience. Mair's investigation asks: what was the purpose of tweeting about the attack, and to whom were the tweets directed? The article
presents a number of breakdowns of these messages and discusses their implications for counter terrorism.

The role of the Internet in radicalization is a crucial and controversial issue. The third article by Angela Gendron examines how charismatic preachers utilize the Internet to promote violent radicalization. According to Gendron, al-Qaeda and IS use social networks and websites to appeal to susceptible young Muslims in the West. Relationships are built to groom susceptible individuals based on the religious teachings of charismatic preachers and other information and propaganda materials. Charismatic preachers operate at the global level acting as "mediators" between the dense ideological pronouncements of the movement’s leaders and particular target audiences. Interactive sites with online sermons and militant Salafist materials help to bring together like-minded second and third generation radicalized Muslims living in the West and reinforce their new found beliefs through the relationships they forge online.

In the Issue’s fourth article, Anne Aly challenges the assumption of causality linking online narratives and radicalization to violent extremism. It is often argued that extremist propaganda on the Internet transforms individuals who are somehow susceptible to ‘grooming’, inciting them to violence on behalf of a cause. This presumption of a vulnerable and passive audience is challenged by Aly. To address it, her article proposes a new framework drawing on media theory through which researchers might study the audiences who receive and internalize terrorist narratives. The approach studies the audience from three levels of analysis focusing on the message, its producers and its consumers as well as the relationships between these three. Potentially this framework could contribute to understanding how the terrorist message becomes meaningful to certain people and how online leaders can mobilize audiences in ways that matter offline.

In the concluding article, Maura Conway reviews the state of research produced to date on the role of the Internet in violent extremism and terrorism. This establishes context for a variety of arguments that have been made for and against the significance of the Internet's role. The discussion leads to two basic questions regarding the issue of online radicalization: whether it is a real phenomenon, and the nature of the process. From these questions, six suggestions are offered by Conway through which future research might progress on violent online extremism.
Finally, a word about terrorists’ use of the Internet would be incomplete without pointing out the downside for terrorists. The Internet is a valuable source of intelligence for law enforcement and intelligence organizations, and even journalists who can easily keep an eye on known social media accounts.\(^2\) Although some forums may be vetted and password protected, there is no doubt that law enforcement prefers the status quo over possible alternatives where terrorists turn to more stealthy and covert technologies. Perhaps that explains why the US government has shown surprisingly little effort to formulate a clear strategy to counter IS’s online recruitment campaign.\(^2\) For those involved in law enforcement, an enemy in plain sight is better than one who is unseen.


\(^3\) The limited religious literacy of many individuals drawn to the Islamic State is also evidenced in the case of Mohammed Ahmed and Yusuf Sarwar. As Akil Awan notes, these: “young British men from Birmingham who were jailed for travelling to Syria to join and fight alongside a jihadist group in 2013, in response to what they saw as their religious duty. But it was the reading material they purchased to accompany them on their trip, the books, Islam for Dummies and The Koran for Dummies, which are most revealing about their lack of religious literacy and motivation.” See Akil Awan, “The Charlie Hebdo Attack: The Double Alienation Dilemma”, The National Interest, January 13, 2015, accessed September 7, 2015, http://nationalinterest.org/feature/the-charlie-hebdo-attack-the-double-alienation-dilemma-12021.


16 Lieberman and Collins, *Violent Islamist extremism*.


19 Ibid.

20 For more information on the Cyberterrorism Project, please see: http://www.cyberterrorism-project.org (accessed September 7, 2015).

