INSTITUTE *for* STRATEGIC DIALOGUE

POLICY BRIEFING:

RADICALISATION, THE ROLE OF THE INTERNET

Rachel Briggs

With the financial support from the Prevention of and
Fight against Crime Programme of the European Union
European Commission - Directorate-General Home Affairs

About this paper

This paper has been prepared by the Institute for Strategic Dialogue as a background briefing for the European Policy Planners' Network on Countering Polarisation and Radicalisation (PPN). It aims to provide an overview of recent developments in far-right extremism across Europe, highlight case studies of projects seeking to combat this threat, and offer practical lessons learned for policy makers and frontline workers.

About the authors

Rachel Briggs OBE is Research and Policy Director at the Institute for Strategic Dialogue, where her research focuses on security, violent extremism and conflict, with a growing emphasis on the ways in which technology can be used to tackle these problems. She regularly advises governments, companies and non-governmental organisations, has published widely on these issues and comments in the international media. She is co-chair of the European Commission's Radicalisation Awareness Network's working group on the Internet and social media, is an advisory board member of Wilton Park (executive agency of the Foreign Office), and is Associate Editor of Renewal. She holds a senior research post at Warwick University. Rachel is also Director of Hostage UK, a charity that supports hostages and their families, and was awarded an OBE in the 2014 Honours list for her work with hostages.

Cover photo

The cover image on this report was uploaded to Flicker on December 6, 2008 by eGuidry , accessible here: http://www.flickr.com/photos/eguidry/4010965162/

This project has been funded with support from the European Commission. This publication reflects the views only of the authors, and the European Commission cannot be held responsible for any use which may be made of the information contained therein.

Introduction

It has become a truism to say that the Internet has revolutionised our lives. It has changed so many aspects of how we live, work, shop, conduct our hobbies, and the ways we form and maintain our relationships. Most profoundly, **the internet has transformed the way we communicate**; it has dramatically reduced the cost of communication; it has enabled unlimited access to much of the world's knowledge and begun to organise it in a way that makes it more searchable; it has made it easier to find people and create networks among like-minded individuals, across great distances and beyond national borders; and it has lowered the threshold for engaging in 'risky' or 'embarrassing' behaviour because users can interact anonymously. **It is not surprising that terrorists and extremists have adopted it as one of the tools of their trade.**

This paper provides a broad summary of our current understanding of the role of the Internet in relation to extremist and terrorist networks. It covers **the role of the Internet in radicalisation**; **the use of new technologies by extremists looking to organise and/or use violence, whether in a group or alone** (including how this is changing the presence of women online); **the ways in which the internet has been used as an operation tool by terrorists** (to recruit, train, coordinate and communicate); and the **range of policy responses**, including the emerging priority area of counter-narratives to take on the dominant messages of extremists and challenge their legitimacy.

It is fair to say that our knowledge base is low, still fairly anecdotal, and lacking a strong empirical underpinning. But we know enough to make some general conclusions, and do not have the luxury of delaying policy responses until we have all the evidence. The paper finds that:

- The Internet is important in the radicalisation process;
- There are few examples of individuals radicalising entirely online, but there are signs that this could increase over time;
- There is less evidence of the Internet's role in recruitment to terrorist networks or the use of violence – offline socialisation remains important. But there is evidence of Al Qaeda placing growing emphasis on individual jihad;
- Al Qaeda has a sophisticated online set up, comprising of online media organisations, mother sites feeding content to others, and a large number of other websites and forums maintained by the wider network. It is also reaching out more to western audiences through these means. These tools are essential for their propaganda;
- Extremists are making more use of social media, and its importance is likely to grow. It is especially important in allow women to play a larger role in jihadist networks;
- It is clear that extremists use the Internet for operational purposes, including communication and the

coordination of attacks. They are even shown to have used it during an attack;

- European governments are developing a range of policy responses, including negative measures and the development of counter-narratives, but these efforts are at an early stage of development.

The paper sets out a sample of existing knowledge and provides examples of policy, practice and activities where they are available. Further information about some case studies is provided in the PPN dossier where it has been made available by PPN members. It focuses almost exclusively on the use of the Internet by individuals, groups and networks linked to and inspired by Al Qaeda.

This paper has been prepared by the Institute for Strategic Dialogue (ISD) on behalf of the European Policy Planners Network on Countering Radicalisation and Polarisation (PPN). The PPN is an intergovernmental network of eight EU countries: Belgium, Denmark, France, Germany, the Netherlands, Spain, Sweden and the UK. It brings together policy planners from both security and integration ministries, taking a comprehensive approach to the dual challenges of radicalisation and social polarisation. The network provides a systematised, informal and closed forum in which policy makers can look in depth at good and bad practices in specific policy areas with the aim of sharing and transferring experiences, developing joint initiatives where desirable, and upgrading policy approaches and strategies over the longer term. It also provides a comprehensive logging of policy developments in PPN countries and has to date covered areas such as religious institution building and religious education, de-radicalisation strategies and approaches, government engagement with Muslim communities, communications and responding to crises, government crisis management, evaluation, and engagement with non-EU countries.

The Role of the Internet in the Radicalisation and Recruitment Processes

There have been growing concerns that the Internet could increase both radicalisation and recruitment to terrorist organisations or activities. These fears are due to the fact that the **Internet allows individuals to 'self-radicalise'** without input or encouragement from individuals in an off-line setting (so-called 'lone wolves'); it makes available to these or networked individuals **information about bombing making** to allow them to mount an attack without the normal infrastructure of a formal terrorist group around them; and **allows determined individuals to communicate more easily and find like-minded individuals** some distance away.

Table One outlines some examples of individuals who are thought to have radicalised wholly or partly online.

Table One: Individuals radicalised wholly or partly through the Internet

Individual	Details
Younis Tsouli (Irhabi007)	Tsouli joined a number of popular web forums in early 2004 and quickly emerged as the undisputed superstar of 'jihadism online'. Tsouli and Ifran Rafa spent hundreds of hours downloading videos, posting email messages, and chatting on web forums. As a result of these activities, and without any prior involvement with extremist groups, both concluded that they wanted to participate in a terrorist attack. They were joined by others online to create a 'virtual' terrorist cell. Both men were arrested by British authorities.
Ifran Rafa	See above.
Hamaad Munshi	Hamaad Munshi was 16 years old when he was found guilty of possessing materials that were likely to be used in acts of terrorism in the UK. He collected instructions for making napalm, high explosives and suicide vests, and was a member of a British group of 'online jihadists' who regularly shared extremist videos and spent hours discussing their plans to travel to Pakistan and die as 'martyrs'. Much of his extremist activism took place online, but was also developed through an offline contact, Aabid Khan, who had attended a terrorist training camp in Pakistan and was a local recruiter.
Abdul Basheer	Abdul Basheer, a Singaporean law graduate, was arrested by Singapore's Internal Security Department in February 2007 for attempting to join the Taliban in Afghanistan. He had turned to the internet for answers to his questions on religion and chanced upon radical explanations that resonated with him.
Abdul Benbrika	The Australian Benbrika group downloaded, collated and distributed extremist material, including videos of hostage beheadings and documents entitled *The terrorist's handbook* and *White resistance manual* that contained recipes for the manufacture of explosives.
Human al-Balawi	Human al-Balawi, a Jordanian doctor, started out as an eager online 'jihobbyist' and later switched his keyboard for a suicide bomb belt at a CIA base in Afghanistan.
Arid U. (also known as Abu Reyyan)	Arid U. killed and attacked US servicemen at Frankfurt airport February 2011. He appears to have been radicalised online, telling police that the spark that led to his actions was seeing a video online the night before the attack in which US soldiers were apparently raping a Muslim girl. He also had a history of playing violent video games online. For weeks for the attack, he had developed a web of digital acquaintances in the Islamist community. Within this network, he wrote about jihad and listened to lectures at Dawa FFM, a Facebook group he joined.
Hussain Osman	Hussain Osman, one of the London bombers, claimed to have been influenced by watching Internet video footage of the Iraq conflict and reading about jihad online.
Various	Perpetrators of the 2005 Khan al-Khalili bombing in Cairo downloaded bomb-making instructions from a jihadist website.
Aabid Hussein Khan	Aabid Hussein Khan, a 22-year-old British Muslim, founded a terrorist cell in the UK. From the age of 12, he had become an avid fan of anything he could find on the Internet relating to jihad and the mujahideen. He discussed these issues in newsgroups and discussion forums. He created an online network of supporters in Europe, Canada, and the United States, who formed a tightly-knit circle. The cell was broken by British officials in June 2006.

As Raffaello Pantucci has argued, "The increasing prevalence of the Internet and the easy availability of extremist material online have fostered the growth of the autodidactic extremist." In his 2011 paper, he outlines a **typology of lone wolves**: **the loner** (an individual who plans or attempts to carry out an act of terrorism using the cover of extreme Islamist ideology but with no connection or contact with extremists); **the lone wolf** (individuals who, while appearing to carry out their actions alone and without any physical outside instigation, in fact demonstrate some level of contact with operational extremists); **the lone wolf pack** (a group of individuals who have self-radicalised using the Al Qaeda narrative but do not make contact with operational extremists); and **lone attackers** (individuals who operate alone but demonstrate clear command and control links with actual Al Qaeda core or affiliated groups).

The Internet is an important part of the radicalisation process in most cases, intensifying and accelerating radicalisation. It can provide the user with the **information** they are looking for to **confirm their beliefs**. Especially important in this regard are **videos and images** which reinforce a particular world view and can be powerful sparks for the radicalisation process. It allows individuals to **find like-minded people** where they are not able to do this offline, creating an online community. And in doing so, it **normalises abnormal views and behaviours**, such as extreme ideological views or the use of violence to solve problems and address grievances. Head of US Intelligence at Central Command General John Custer is quoted as saying that on many sites, terrorists can "download scripted talking points that validate you have religious justification for mass murder." (cited in O'Rourke, 2007) Some have talked of it acting as an **'echo chamber'** for extremists who can find others to reflect back their views and further amplify them; even the most extreme ideas and suggestions receive the most encouragement and support.

There is less evidence about the role of the Internet in recruitment for the purpose of violent activity. In the majority of cases to date, the Internet tends to be complemented by offline contacts and influences. Social network theorists, such as Marc Sageman, argue that **real world relationships are a necessary part of the radicalisation process**. In his book, *Leaderless Jihad*, he observes, "...most online participants also have friends who share their views and desires but do not spend so much time on the internet. Terror networks consist of a mixture of online and offline elements, and their respective in-person and virtual discussions mutually influence each other." (pg 121)

Quintan Wiktorowicz has argued that "exceptionally 'risky' behaviours, such as engaging in violence or crime, always require social networks in order for the perceived cost/benefit calculation to tip in their favour. **Involvement in violence needs to be preceded by a prolonged process of 'socialisation'** in which perceptions of self-interest diminish and the value of group loyalties and personal ties increase." (cited in ICSR 2009) The ICSR study also cites research by Hoskins et al that found that much of the jihadist web

presence was about 'preaching to the choir'; "While the internet provides a convenient platform for activists to renew their commitment and reach out to like-minded individuals elsewhere, it is largely ineffective when it comes to drawing in new recruits."

Looking to the future, consideration must be given to the notion that the Internet will play an increasingly important role in recruitment and coordination, as well as radicalisation. Jytte Klausen's 2010 study for the Institute for Strategic Dialogue highlighted the **growing trend for Al Qaeda to seek out individuals precisely because of their lack of prior connections to the jihadist network** in response to the improving intelligence and policing response. Pantucci highlights the fact that **influential ideologues**, such as Abu Musab al-Suri and Anwar al-Awlaki, are **placing a growing emphasis on individual jihad and small cells taking up action wherever they are able to in furtherance of Al Qaeda's more general global ambitions**. Adam Gadahn (Al Qaeda's spokesman in the US) has openly praised Nidal Hassan Malik and called upon other Muslims to follow his lead. And the January 2011 edition of *Inspire* magazine, Al Qaeda in the Arabian Peninsula published an article that praised Roshonara Choudhry, the British woman who tried to kill Stephen Timms MP, and Taimour Abdulwahab al-Abdaly, an Iraqi-Swede who blew himself up outside a shopping mall in Stockholm in December 2010 (see Pantucci, 2011, for further information)

The Use of New Online Technologies by Extremists for Operational Purposes

New evidence is emerging all the time of the ways in which extremists and terrorists use the Internet as an operational tool, including recruitment, training, coordination and communication as well as wider propaganda efforts which feed into all of the above. This section provides an overview of what we know, with a special focus on the use of new and emerging technologies. It also considers the impact these trends are having on the role of women and the ability of these networks to reach a much wider western or even global audience. However, it should be stressed that **online activities need to be understood in conjunction with offline events**; the Internet on the whole has added to what was there already rather than replaced it entirely. **Its impact is quantitative rather than qualitative**; it has increased reaction time, provided greater scale and interactivity, and made communication easier and more seamless.

There are a handful of virtual media organisations that play an important role in creating jihadist publications and audio-visual materials, which can then be picked up and passed on via a multitude of websites and forums. The most important one are: As-Sahab ('Al Sahab Institute for Media Production'), Global Islamic Media Front (GIMF), and Al-Fajr (Media Centre). They are relatively autonomous and have various levels of organisational links with jihadist groups, and the

nature and quality of their work differs. More information can be found in the referenced report from the NCTb. There are also a number of small-scale virtual media organisations, such as 'Al-Furqan Foundation for Media Production'.

Table Two below provides an overview of the three main organisations listed above.

Table Two: Key Virtual Jihadist Media Organisations

Virtual Media Organisation	Description
As-Sahab ('The Clouds')	This acts as the media organisation for AQ core. Messages are produced in various languages (including English) and versions, and are aimed at a wide audience. It is the only and exclusive organisation which maintains physical contact with the AQ leadership. It is thought to have been run out of Pakistan, although its current physical base is unclear.
Global Islamic Media Front (GIMF)	This is one of the largest and longest-running media organisations, but has not had direct links with AQ leadership. It is a European propaganda arm in support of Al Qaeda, run by Muslims based in Europe, especially Germany and Austria. It operates in an open way, and its content focuses more on the conflict on the ground than AQ leaders. It also acts as a publisher of digital books and magazines and has made video training courses on how to handle weapons, ammunition and explosives. It is thought to be run by amateurs.
Al-Fajr ('The Daybreak')	This focuses on jihadist groups in Iraq, North Africa and the Arabian Peninsula, and was responsible for a number of AQ websites, such as al-Falluja and Shumukh al-Islam. It also produces publications (including 'The Technical Mujahid' which focuses on ICT methods and techniques) and media products, supports the 'al-Malahem Foundation' (the Al Qaeda media organisation in the Arabian Peninsula), and reproduces the media productions of as-Sahab and Labbayk, the Taliban's media organisation. It was established in 2006.

Online media units are beginning to transform from information centres to online news agencies that function very much the same way as Reuters, Bloomberg, or the Associated Press, reporting on group activities and providing up to the minute news updates. They also produce pictures, interviews, and propaganda material and offer newsfeed services direct from website to desktop. By emulating established media news outlets, they are beginning to narrow the credibility gap between themselves and the established news media, so that more people will tune into their radical Islamist version of world affairs. It is also worth noting the existence of a **small number of 'mother sites' which are the source of information and content for other second or third tier sites**. For example, Al-Fajr controlled and ran a number of (former) mother sites such as al-Ekhlaas, al-Boraq, al-Firdaws and al-Hesbah. They are thought to number just 5-10 at any one time, but their reach is considerable. They have a large number of registered users, and their messages are quickly adopted and passed on to second and third tier websites and forums.

There has been much speculation about whether online spaces could replace physical training camps by providing information, coaching and guidance to recruits on tactics and skills such as bomb making. However, **while the destruction of training camps at certain points in time has hurt terrorist networks, they do not seem to rely on online alternatives.** There is an abundance of military and tactical training handbooks on jihadist websites, but most are poor quality. Instead, the Internet appears to act as a library or classroom for jihad, but not an interactive training forum.

One of the most interesting new trends is the **increasing use of new social media by extremists and terrorist networks.** Some have argued that this has come about as a result of government strategies to ban jihadist websites, which has pushed their members onto other forums, like YouTube and Facebook and other local equivalents. These platforms have lower technical and financial barriers to entry, and have the added bonus of **reaching much wider constituencies than is likely via a dedicated website**. Facebook offers a new type of mass interpersonal persuasion and YouTube motivates individuals to contribute by uploading videos or commenting on others'. These forums also have the added bonus of **making users harder to identify**; their real IP addresses are not compromised, as they are not required to fill in verifiable personal details. There is **some evidence to show that jihadists are now adopting this approach as part of a formal and identifiable strategy,** and there have been examples of websites providing detailed instructions on how to use Facebook and YouTube for these purposes. One jihadist site contains a detailed invitation to use popular American web forums to distribute jihadist films and disinformation about the war. The invitation is accompanied by tips on how to present yourself, which parts of the forum to use, what type of discussions to look for or initiate and what topics to avoid. As part of this strategy, jihadists are urged to:

- 'Invade' social network sites such as Facebook by setting up groups with

radical views and to seek to gather users with the 'right' attitude;

- 'Invade' file-sharing sites like YouTube by placing various clips with extreme content;
- Infiltrate popular Islamist websites in order to attempt to convert them into militant sites in line with the closed websites by spreading extremist contents on the discussion forums of these sites

There are some examples of this wider approach in action. A content analysis study conducted by Conway and McInerney at Dublin City University traced the viewing activities of a small group of individuals who posted and discussed material concerning the conflict in Iraq. The results showed how **individuals browsing generic websites could be integrated into a specific network**. In one example, a young male who identified himself as an 'Irish rugby fan' posted a comment citing his admiration for Islam and his wish to convert after seeing a martyrdom video. Within weeks of posting this message, he was targeted by several heavy users with radical links, whose aim at a minimal was religious conversion. There are also examples of **networks using social media to aid their operations**; for example, it is thought that the gang who perpetrated the 2008 attack in Mumbai were able to follow the movements of the police and security forces via eye witness Twitter updates.

This is perhaps part of **wider attempts to reach out to broader western audience**. As a report from the NCTb outlines, this can be observed through the emergence of three trends. Firstly, speeches by the leaders of Al Qaeda and video productions about terrorist activities are often accompanied by proper **subtitles in Western languages, particularly in English**. Secondly, there is a marked **improvement in the quality of translations and use of language**. Some publications such as 'Jihad Recollections' have been written or narrated in perfect American English. Thirdly, **influential jihadist sites are being expanded to include English, French and German sections**, which contain news, communiqués, bulletins and videos about the jihadist conflict.

One of the main limitations of these kinds of social media is their openness and transparency. Extremists therefore still rely on more closed 'forums' for communication and coordination of a more advanced nature. These forums reinforce the views of their members, create virtual communities, reinforce norms and normalise behaviour. They are also an important space for making connections and passing on knowledge, although this would tend to be done behind several layers of passwords and security. A report by the Quilliam Foundation reviewed a large number of Arabic-language jihadist and militant forums and provided a number of observations:

- Their primary concern is attacking other Muslims – identifying traitors and enemies to the jihadist cause.
- They attempt to recruit Salafists – pro-jihadist forum users clearly think that

Salafists and Wahhabis are susceptible to being recruited and the regularly conduct 'raids' onto Salafist forums and websites to post Jihadist material.

- There is an absence of real debate – compared to general English-language web forums; Arabic-language Jihadist forums are notable for their lack of real debate. There is a deliberate attempt to create an impression of unity.
- There is a lack of scriptural knowledge – most users appear to lack any depth of understanding, and instead tend to paste the rulings of clerics and fall back on platitudes.
- There is unity of dislike for Hamas among forum users.
- They continue to use the works of 're-canted' jihadist – something which is perhaps surprising.
- London continues to be an important hub for jihadists' forums.

It is worth noting that **some of the most popular Islamist militant web forums are easily rivalled in popularity by white supremacist websites such as Stormfront.** This was founded in 1995 by ex-Grand Wizard of the Ku Klux Klan, Don Black. As of January 2009, its forum had over 150,000 members, of whom 31,000 were noted as 'active'. Single issue groups such as environmentalist extremists and radical animal rights activists also have a strong web presence. Despite the use of these public or semi-public forums, **extremists still need secure and private places to meet, communicate and coordinate their activities.** In this regard, **their use of the so-called 'deep' or 'dark' web is likely to increase considerably**, and this is one of the most difficult areas to monitor. It is likely that there will be increased use of hidden internet architecture, such as file repositories and storage sites. These hidden layers remain unknown to the general public and are difficult for intelligence and

law enforcement agencies to detect. It is also likely that terrorist cells and groups will adopt greater vigilance against the activities of law enforcement agencies and develop more innovative information security measures to protect their communications from infiltration and monitoring. Extremists are known to use satellite imagery to help them plan their attacks.

There is growing evidence to suggest that the anonymity of the Internet offers greater opportunity for women to become active within extremist and jihadist circles in a way that isn't generally the case offline. A study by Bermingham et al conducted social network and sentiment analysis on a group of YouTube users and found more extreme views among women; they were more positive towards the topic of Al Qaeda and the use of political violence, and were more negative towards the topic of Judaism. Unlike the men, they seemed unwilling to distinguish between the Israeli state and the Jewish religion, and they also had more negative views towards Christianity, suggesting a greater lack of tolerance of other religions. Interestingly, females scored higher both in terms of network density and average communications speed, which indicates a

potentially increased leadership role for women online than they would generally be held to have within jihadi circles in the real world.

Finally, there are many possibilities for fundraising by and for jihadists on the Internet, whether through direct and open fundraising initiatives on websites or through e-commerce and online fraud. But as yet, **there is little evidence of fundraising happening online in practice.**

Policy Responses to Extremists' Use of the internet

Policy responses to the use of the internet by extremists and terrorists are still in their infancy as we learn more about how and why they use the online space and build abetter understanding about the tools we can use to disrupt and deter. Some countries are more developed in their responses than others, but all still have gaps and potential to share ideas and lessons with others. There are also dilemmas regarding when, how and to what extent to intervene, and in relation to the balance between Internet freedoms and national security.

The European legal framework is covered by two Council of Europe (CoE) conventions that contribute to preventing terrorists' use of the Internet: the Convention on the Prevention of Terrorism (2005) and the Convention on Cybercrime (2001). Both are open to signature by non-EU states. They are outlined in Table Three below.

Table Three: Council of Europe conventions covering terrorists' use of the Internet

The Convention on Cybercrime is the only international treaty dealing specifically with substantive and procedural criminal laws in the area of cyber-related crime, including the use of the Internet for terrorist purposes, and which facilitates international cooperation in the investigation and prosecution of computer crimes. The convention opened for signature in November 2001 and entered into force on 1 July 2004. Of non CoE states, only the US has both signed and ratified the convention. It requires states that sign and ratify to ensure that specific cybercrime offences are incorporated into their domestic law, and to establish specific law enforcement powers to enable the investigation and prosecution of offences committed by means of a computer system. The convention also aims to establish a fast and effective regime of international cooperation for investigating and prosecuting cybercrime offences, and for gathering evidence electronic form, including the expedited preservation, disclosure, search, seizure and real-time collection of data.

The CoE Convention on the Prevention of Terrorism also contains provisions that are relevant in the fight against terrorists' use of the Internet. It aims to strengthen efforts to prevent terrorism by establishing as criminal offences acts such as public provocation to commit a terrorist offence, recruitment for terrorism, and training for terrorism. Complicity in the commission of these offences is also a crime, which has implications for anyone helping terrorists to create or maintain websites.

The ICSR report describes **three types of 'negative' measures** that governments and law enforcement agencies can adopt to counter terrorists' use of the Internet: **removing content** from the web; **filtering** – restricting users' access and controlling the exchange of information; and **hiding** – manipulating search engine results, so that undesirable content becomes more difficult to find. An assessment of the strengths and limitations of each approach is outlined in the Table Four below which is re-produced exactly from the ICSR report (p.22).

Table Four: 'Negative' measures to counter terrorists' use of the Internet (from ICSR report, p.22)

Type of measure	Measure	Method	Assessment
Removing	Take downs	Government tells hosting company to 'take down' content of website.	Hosting company needs to be located in same jurisdiction.
	Domain names de-registration	Government tells domain name provider to deregister domain name.	Top-level domain (e.g. '.uk') needs to be operated by national registry.
	Denial of service attack	Overloading servers or networks with communication requests.	Illegal and, at best, a temporary means of disruption.
Filtering	IP filtering	Requests for blacklisted IP addresses are intentionally dropped.	Cheap, but blocks all services hosted by a web host ('over-blocking').
	Content filtering	Filtering software 'sniffs' all information packets for blacklisted keywords.	Expensive. Also requires 'white listing' of permitted websites.
	Domain name tampering	During IP 'look-up', requests for banned domain names are dropped.	Cheap, but problems with Over-blocking. Also, easy to circumvent.
	Proxy filtering	Proxy filters decide whether to allow requests for individual web pages.	Expensive. May slow down traffic unless substantial investments are made.
	Hybrid IP and proxy filtering	Combines IP and proxy filtering: proxy filtering only for blacklisted IP addresses.	Technically effective. But, like other methods, relies on blacklisting and fails to capture dynamic content.
Hiding	Search engine filtering	Search engines drop requests for certain web pages and keywords.	Requires active collaboration of search engine provider.
	'Black hat' search engine optimisation	Manipulating search engines to boost or reduce websites' page rank.	Widely frowned upon. Utility may be limited.

In broad policy terms, this can translate into **three broad approaches**: a **hard strategy of zero tolerance** – using the types of tools outlined in the box above, combined with legal actions; a **softer strategy of encouraging internet end users to directly challenge the extremist narrative and report offensive or illegal material**; and an **intelligence-led strategy of monitoring leading to targeting, investigation, disruption and arrest.** Most countries adopted a mixed approach, using a combination of all three depending on the nature of the content, the identity of its creators or hosts, and the tools at their disposal.

There are also **cautions about over-using 'negative' tools**, partly on practical grounds because law enforcement will never be able to keep pace with new material, and because targeting can raise the profile and kudos of these sites and forums. There are also of course **ethical dilemmas about how to balance the need to intervene with the need to preserve civil liberties**. When, where and how the balance should be struck between these competing priorities is still a matter for much discussion between governments, including with private sector and community/civilian groups. These debates are only likely to increase in volume as the challenge from cyber security grows and moves centre stage within the security community. Finally, there are **difficult judgements to be made about where harm lies and therefore when to intervene**. For example, some governments place a great emphasis on ideology in radicalisation towards violence, and might as a result take a harsher line on the removal of content non-violent in nature but linked to or stemming from an ideology believed to drive radicalisation. Others focus less on ideology and take a more pragmatic approach, allowing more content to stay up and focusing instead on the point at which radicalisation tips into recruitment and incitement.

The UN Taskforce Inventory of Practices report outlines emerging projects and practices of UN member states in relation to efforts to counter the use of the Internet by terrorists. Some of these practices and examples found during the compilation of this report are outlined briefly in Table Five below. This excludes practices in the area of counter-narratives, which is dealt with later in this section.

Table Five: Policies and practices to counter the use of the Internet by terrorists

The UK Counter-Terrorism Internet Referral Unit provides citizens with an easy to use interface for reporting content which is extremist or illegal, and the unit where appropriate works to get the content removed.

Nigeria has organized several seminars on combating terrorism through the Internet, including the organization of capacity building and training/workshops on law enforcement and digital technologies for all agencies involved in countering radicalisation, as well as the initiation of online projects aimed at undermining the capacity of violent extremists to propagate violent ideologies through the Internet.

In the Netherlands, webmasters of sites that attract large numbers of Muslim youths have installed systems whereby radical expressions are countered by a message stating alternative views.

A regional Dutch police force has developed IRN, an Internet investigations network. It is a framework that facilitates anonymous investigations by police officers. It is an open source piece of software, so has been easy and cheap to create, there are no updating costs, and it can be improved by its users. They are now developing an alert system that is key word driven.

The Dutch government has produced a new code of conduct for 'Notice and Take Down' with the internet sector.

The Belgian authorities have put in place mechanisms that systematically investigate all Internet sites that encourage and facilitate violent extremism and recruitment. This is reflected in the "Internet Open Source Platform," which is administered by the Federal Police with representation from the Intelligence Services and the Counterterrorist Joint Unit. This includes measures to encourage individuals to report sites that host illegal material through a point of contact within the Federal Police.

In Singapore, authorities have encouraged a group of volunteer religious scholars and teachers to launch a website which carries arguments that rebut violent extremist teachings and beliefs.

The European Commission backed "Check the Web" project, launched during the German Presidency of the European Union in May 2007, proposes a common European approach to Internet monitoring based on strengthened cooperation and coordinated monitoring and evaluation of open Internet sources. Based on a web portal, it acts as a repository for information, materials, risk assessments, etc, to avoid member states duplicating costs and resources.

The European Commission is funding a research project mapping the tools and technology available to detect radicalisation on the Internet. One of its outcomes will be advice to the Commission on ways to aid law enforcement officials in this area.

The European Commission is about to launch the 'Clean IT' programme to exchange and promote best practice among EU members states.

The United Arab Emirates has subjected all media forms to monitoring, and is using them, including TV channels, to teach the "right Islam" and rebut distorted violent ideology.

One of the most important areas of debate in relation to the response to terrorists' use of the Internet relates to the **development and spread of counter-narratives online**. These broadly take **three forms**: **messages that pick apart the terrorists' ideology**; **messages that seek to mock, ridicule or somehow undermine their credibility**; and those that **promote a positive alternative**. A number of meetings and conferences have been held on this theme since the start of the year, so discussions are moving forward with some pace and new practical projects are being agreed and developed currently. **This is potentially one of the most effective areas to counter terrorists' use of the Internet, but arguably the most difficult for governments to get right.**

There are two approaches to critiquing terrorists online. The first relates to attempts to counter their ideology by offering alternative interpretations of key texts and speeches and showing how the methods and means they adopt are inconsistent with their own beliefs. This might involve better use and dissemination of religious edicts that counter jihadist narratives. In this regard, the identity of the messenger is critical as they must have the credibility to deliver such detailed and evidenced answers. However, some have argued that the importance of the messenger is over-emphasised, especially in relation to social media online where messages spread in a different way to previous generations of technology and seem to undermine the importance of creator in favour of the carrier. **Former extremists can be especially powerful in delivering these kinds of messages** although it has already been noted that jihadist forums often still use the messages of these individuals even after they have re-canted.

The second type of negative counter-narrative is an attempt to undermine jihadists, not in terms of the credibility and authenticity of their ideology and motivations, but in terms of their effectiveness. These kinds of counter-narratives point out when extremists get things wrong and make mistakes, they stress the counter-productive consequences of their actions for the communities that they claim to defend, and they point out that violence does not achieve the desired effects. **They can also take a more personal approach, seeking to undermine the 'Jihadi cool' brand, mocking them as groups and/or individuals, and using humour to de-humanise them.** One of the most powerful and important messengers in this respect are the **victims of terrorism**, whose voices are consistently silent and ignored but who have a strong and compelling story to tell about the futility of terrorism. They also undermine jihadists' talk of being 'at war' by communicating the ordinary lives of the people they have killed. There has been **interest in creating a database of the victims of terrorism**, able to provide comment and analysis.

One of the areas with considerable potential for future development relates to the promotion of a positive and credible alternative, including through the use of online social media combined with offline campaigning and community organising techniques. Such attempts would aim to create

not just a community of interest, but a **movement for change** that would by its nature need to be bottom up and organic (or appear to be) for it to be credible and taken seriously. They would need to be built from the interests of the target audience, their content needs to be compelling, and there need to be feedback loops to the narratives can be responsive to changing events and feedback. The most effective campaigns use multiple effects, messages, and media/platforms to change attitude and behaviour.

The challenges of making this approach work in practice are considerable, not least for governments in finding the right balance between facilitating and supporting while stepping back, not seeking to control, and not reigning things in when messengers use anti-government rhetoric. When these projects are close to government or seen to be close to government, they lose their credibility and become ineffective. In many ways, **the ideal carriers for counter-narrative messages are part of the audience itself.** Governments need creative approaches to funding, capacity building, facilitation and political risk management. **Governments will also need to deal with potential inconsistencies in what they say and do domestically and their approach to foreign policy**, which could be used against them by extremists in response to their counter-narratives.

A number of suggestions have been made about **potential projects and activities** in relation to counter-narratives:

- Increased government support for the translation and dissemination of messages by repentant former radicals;
- Search engine optimisation to bring counter-narratives to the top of search engine results;
- A one-stop-shop or repository for counter-narratives, building up a library of texts and other material rebutting extremists' views, promoting alternatives, victims' statements and exposés of false statements;
- Use of the gaming environment and virtual worlds;
- Capacity building with a range of community and civilian individuals and groups, through technical support, training, and networking;
- Developing a database of the victims of terrorism, as outlined previously;
- The deployment of experienced individuals to counter arguments made on both specialist jihadist forums, but also increasingly on more open forums such as Facebook and YouTube.

Conclusions

The Internet is an important tool for terrorists and extremists – it is a tool for propaganda, it is involved in the radicalisation process, it can contribute towards recruitment, and it is undoubtedly an operational aide in terms of communication and cooperation. **Our knowledge base is still somewhat limited, but we do not have the luxury of pausing our response efforts until we have a full picture.** Besides, the speed of online developments mean the picture is constantly evolving anyway. This paper has provided an overview of current knowledge and a fragmentary picture of policy responses (more case studies and further information are available in the background dossier).

In policy response terms, **it is vital that governments share information on projects, activities and develop a rolling list of 'lessons learned' to ensure they are not reinventing the wheel. Within and between PPN members, this will be possible through the Policy Exchange Portal** which will provide an online repository for these materials. These efforts must **also involve the private sector and civil society groups**, as a whole society response is the only one that will be comprehensively successful. **There are further opportunities for international collaboration** on projects, with some efforts already underway. It is also important for governments to continue to reflect on some of the ethical dilemmas as well as the practical ones – when to intervene, how to balance security and civil liberty imperatives, and understanding where harm lies.

References

- Ali Musawi, M (2010) *Cheering for Osama: How jihadists use internet discussion forums* Quilliam
- Bergin, A et al (2009) *Countering Internet Radicalisation in Southeast Asia: ASPI Special Report* RSIS and ASPI
- Bermingham, A et al 'Combining Social Network Analysis and Sentiment Analysis to Explore the Potential for Online Radicalisation [available at http://doras.dcu.ie/4554/3/DCU_asonam09.pdf]
- Centre for Terroranalysis (CTA) (2010) *Youtube.com and Facebook.com – the new radicalisation tools?* PET
- Change Institute (2008) *Studies into Violent Radicalisation: Beliefs, Ideologies and Narratives of Violent Radicalisation* Change Institute
- Conway, M and McInerney, L (2008) 'Jihadi video and auto-radicalisation: evidence from an exploratory YouTube study' in *EuroISI 2008 – First European Conference on Intelligent and Security Informatics* 3-5 December 2008, Esbjerg, Denmark
- Counter-Terrorism Implementation Task Force (CTITF) (2011) *Riyadh Conference on "Use of the Internet to Counter the Appeal of Extremist Violence"*
- Europol (2011) *TE-SAT 2011: EU Terrorism Situation and Trend Report* Europol
- Gerdes, A 'Online Radicalisation on YouTube and Facebook [available at http://www.ccsr.cse.dmu.ac.uk/conferences/ethicomp/ethicomp2011/abstracts/ethicomp2011_40.php]
- Homeland Security Institute (2009) *The Internet as a Terrorist Tool for Recruitment and Radicalisation of Youth* Homeland Security Institute
- Hoskins, A. et al (2009) *Legitimising the discourses of radicalisation: Political violence in the new media ecology: Full Research Report*
- *ESRC End of Award Report*, RES-181-25-0041 ESRC
- Klausen, J. (2010) *Al Qaeda-Affiliated and 'Homegrown' Jihadism in the UK: 1999-2010* Institute for Strategic Dialogue
- Martsch, M and Stark, H (2011) 'Can Radicalisation via Facebook be Stopped?' *Der Spiegel* [accessed 10 May 2011]
- Mostarom, TR (2009) 'Al Qaeda's female jihadists: The islamist ideological view' *RSIS Commentaries*
- National Coordinator for Counterterrorism (2009) *Jihadists and the Internet*
- O'Rourke, S (2007) 'Virtual Radicalisation: Challenges for Police' *Australian Information Warfare and Security Conference* [available at http://ro.ecu.edu.au/isw/42]
- Pantucci, R. (2011) *A Typology of Lone Wolves: Preliminary analysis of lone Islamist terrorists* The International Centre for the Study of Radicalisation and Political Violence
- Sageman, M (2008) *Leaderless Jihad: Terrorist networks in the twenty-first century* University of Pennsylvania Press
- Sinai, J. (2011 forthcoming) 'How Terrorists Exploit the Internet and Effective Countermeasures' *The Journal of Counter-terrorism & Homeland Security International* (forthcoming)
- Stevens, T and Neuman, P (2009) *Countering Online Radicalisation: A strategy for action* The International Centre for the Study of Radicalisation and Political Violence
- Sutton, M and Wright, C (2009) 'Finding the Far Right Online: An exploratory study of white supremacist websites' *Internet Journal of Criminology*
- Thomas, T (2009) 'Countering Internet Extremism' *IOSphere Journal*
- United National Counter-Terrorism Implementation Taskforce (2009) *First Report of the Working Group on Radicalisation and Extremism that Lead to Terrorism: Inventory of State Programmes* United Nations
- United States Senate Committee on Homeland Security and Governmental Affairs (2008) *Violent Islamist Extremism, The Internet, and the Homegrown Terrorist Threat*
- Wilton Park (2011) *Tackling Online Jihad: Understanding the issues and how to respond?* Wilton Park Conference Report WP1082 (unpublished)

Institute for Strategic Dialogue
48 Charles Street, London W1J 5EN
T: +44 (0)20 7493 9333
info@strategicdialogue.org

INSTITUTE *for*
STRATEGIC DIALOGUE