At a glance
May 2015

Cybersecurity: Jihadism and the internet

Since the beginning of the conflict in Syria in March 2011, the numbers of European citizens supporting or joining the ranks of ISIL/Da'esh have been growing steadily, and may now be as high as 4 000 individuals. At the same time, the possible avenues for radicalisation are multiplying and the risks of domestic terrorism increasing. The proliferation of global jihadi messaging online and their reliance on social networks suggest that the internet is increasingly a tool for promoting jihadist ideology, collecting funds and mobilising their ranks.

Background

The use of the internet as a platform for terrorist propaganda is not new. The Al-Qaeda leadership has threatened to use cyber weapons almost since the very beginning of its activities. In 2005, Ayman al-Zawahiri referred to the media as 'one of the battlefields', and the US army expressed its concerns about the potential uses of internet-enabled mobile devices by terrorist organisations. Al Qaeda has openly encouraged cyber jihad as a sacred duty of every Muslim and called upon its followers to hack Western websites. The conflict in Syria – and now in Iraq – provided a fresh opportunity to leverage the power of social media and attract support. Even though most of that grassroots support is generated by a relatively small group of very active users, social media campaigns, like AllEyesOnISIS, have allowed jihadist groups to replace their online forums with more dynamic engagement. Twitter, Facebook and numerous chat-rooms have become online diaries from the battlefield, offering near live coverage of the territorial advances made by ISIL/Da'esh. The Syrian conflict has also produced a set of new spiritual leaders who use the internet to offer guidance and inspiration to Western foreign fighters.

Propaganda, training and recruitment

The most common use of the internet by jihadi groups has so far been to promote a better understanding of Islam (*da'wah)* and diffuse information about jihadism. Online magazines like *Technical Mujahid Magazine*, *Al-Battar*, *Cyber Jihadist's Encyclopedia* and *Inspire* all provide motivational material that is supposed to fuel sympathy towards jihad, and as a consequence gradual radicalisation. Analysis of the content of *Inspire* highlights that the magazine uses religious arguments and quotes from prominent American figures as tools to radicalise and recruit Western terrorists. For many foreign fighters, posting videos and pictures on Twitter becomes a way to engage with their sympathisers and *de facto* render social media an essential factor in the war. Women and young girls are also targeted and encouraged to run away from home and join the Caliphate proclaimed by ISIL/Da'esh.

The internet has not only altered traditional channels for radicalisation and facilitated a two-way communication between terrorist organisations and their supporters but also allowed for a change in planning, coordination and execution of attacks. Al Qaeda's splinter groups in the Arabian Peninsula (AQAP) and its regional allies in Somalia (al-Shabaab) have gradually supplemented traditional tactics and models of communication (i.e. websites and blogs) with more decentralised approaches. Anwar al-Awlaki – one of AQAP's key figures also known as the 'bin Laden of the Internet' – has used internet to promote a 'creative' terrorism and explain how to turn easily found objects into improvised explosive devices (IEDs). Spreading this new version of 'do-it-yourself' terrorism has also become possible thanks to the emergence of media outlets – like the al-Hayat Media Center – associated with the jihadi cause. Several terrorist attacks in recent years – including the one in Boston in 2013 – have derived their inspiration from such sources. As-Sahab Media – al Qaida's media outlet – has recently announced the release of a new English-language jihadist publication *Resurgence*.

EPRS | European Parliamentary Research Service
Author: Patryk Pawlak, **Members' Research Service**
PE 557.006

Funding and fundraising

Modern communication networks and crowdfunding have proven to be a cheap and efficient way of gathering funds for financing terrorist activities or managing the jihadi network. Using phishing attacks, identity theft or purchasing stolen credit cards details in online forums, terrorist groups are able to gather additional funds for their activities. Terrorist groups also use the internet to raise funds. Al Qaida's global fundraising network is built on donations to charities and NGOs, which communicate with donors through social media and online forums. Twitter accounts have also been used to ask supporters for donations to the cause of jihad. Dawn of Glad Tidings – a smartphone application developed by ISIL/Da'esh – was designed to maximise outreach, and encourage donations from supporters in Saudi Arabia, Kuwait and other Gulf countries, which is where most ISIL/Da'esh affiliated Twitter accounts are located. A growing sophistication in cyber-threats – including malware that encrypts files on the compromised computer and demands a ransom to decrypt them – could constitute an additional source of funding in the near future.

Cyber attacks

Cyber jihadists have gradually expanded their use of internet to conduct attacks on Western governments and institutions. In 2014, Cyber Caliphate – a jihadist online group affiliated to ISIL/Da'esh and allegedly led by a British hacker, Abu Hussain Al Britani – took over Twitter and YouTube accounts of the US Military Command. As part of the operation #OpBlackSummer against US websites, Al Qaeda Electronic Army and the Tunisian Cyber Army have performed coordinated attacks on the websites of US government agencies (including US Customs and Border Protection) and petroleum companies. Even though no significant attack against critical infrastructure has been reported, the FBI has predicted that terrorists and criminal organisations will develop their abilities or hire hackers to perform cyber-attacks or a combination of cyber and conventional attacks. Distributed-denial-of-service attacks such as the one in Estonia in 2007, deployment of sophisticated malicious software, like Stuxnet or Flame which caused substantial damage across the Gulf region, a breach of South Korea's nuclear plant operator KHNP in 2014, and the cyber-attack on the French public-service television network, TV5 Monde in April 2015, all demonstrate an increasing level of threat sophistication.

Policy responses

International response to cyber jihadism is organised around three main pillars: constraining the use of internet by jihadi organisations, strengthening de-radicalisation efforts (including by judicial response), and limiting access to funding. As part of its objective to defeat jihadi groups like ISIL/Da'esh, the EU intends to curb the use of the internet for terrorist recruitment and dissemination of terrorist practices. Whether this objective is achieved will partly depend on the outcome of the ongoing debate about the use of encryption tools. Al Qaeda and its affiliates have been encrypting their online communications and even provided a public encryption key for those wishing to establish contact via email. Nonetheless, the ban on encryption and its implications for the privacy of over 3 billion internet users worldwide have galvanised privacy advocates. Simultaneously, the EU's de-radicalisation efforts increasingly focus on strategic communications and counter-narrative policies. The aim of the Syria Strategic Communications Advisory Team (SSCAT) – operating with a €1 million budget from the Internal Security Fund – is to develop and exchange best practices with a view to prevent and counter terrorist crime and violent extremism. Similarly, the military campaign against ISIL/Da'esh has been supported since October 2014 by the online coalition including Egypt, France, Saudi Arabia, the UK, and the UAE. These actions could be futile if jihadi groups are not cut off effectively from fresh flows of cash. This in turn requires closer international cooperation between financial institutions, law enforcement and judicial bodies. Some of the key aspects of such cooperation (i.e. implementing appropriate preventive measures or actively involving the private sector) are also mentioned in the Manama Declaration on Combating the Financing of Terrorism and more recently in UN Resolution 2199 (2015).

At the informal EU Council meeting of Ministers of Justice and Home Affairs on 29 and 30 January 2015 in Riga, Member States reiterated that 'terrorism, radicalisation, recruitment and financing related to terrorism are main threats to the EU's internal security'. The European Parliament resolution of 12 March 2015 on recent attacks and abductions by ISIL/Da'esh in the Middle East mentions, among other things, the need 'to stop the spread of extremist and jihadist ideology worldwide'. On 16 March, the Member States adopted the EU Regional Strategy for Syria and Iraq as well as the ISIL/Da'esh threat.