BRIEF ISSUE

2
2015

Cyber jihadists and their web

by Beatrice Berton and Patryk Pawlak

Jihadist militants have long operated in the pockets of instability which stretch from Bamako to Bagdad. However, they have also been making the most of governance problems in the world's biggest open space: the internet.

Forced to confront this fact, the governments of France, the UK and the US, among others, have already announced their intention to reinforce the powers of their intelligence agencies and strengthen cooperation with the private sector in a joint effort to spot and eradicate online extremist safe havens.

New means to an old end

After most of al-Qaeda's top leaders were killed between 2010 and 2012, the organisation's splinters in the Arabian Peninsula (AQAP) and its regional allies in Somalia (al-Shabaab) abandoned the traditional top-down model of communication based on production, dissemination and reception. The groups then adopted (deceased) US citizen Anwar al-Awlaki's idea to promote a global jihadist message via social networks instead.

As the mastermind of the operation, the so-called 'bin Laden of the internet' had reached out to his followers through a blog, a Facebook page, YouTube videos and the online magazine *Inspire*. His strategy was intended to promote 'creative' terrorism based on the assumption that, if it is possible to bake a cake by watching videos or reading a cookbook, it is also possible to orchestrate a terrorist attack in the same way.

The conflicts in Syria and Iraq provided a fresh opportunity to leverage the power of social media among Western populations. Twitter and Facebook accounts have become online diaries from the battlefield, offering near live coverage of the swift advances made by the Islamic State of Iraq and the Levant (ISIL) and Jabhat al-Nusrah.

Online services such as Kik or Skype also allow for direct, real-time communication between 'e-hadists' – jihadist sympathisers active on the internet worldwide – and those fighting on the ground.

Ultimately, ISIL's strategy paid off, with thousands flocking from all over the world to join its ranks. Recent figures indicate that over 20,000 people from more than 80 countries have travelled to Syria and Iraq to fight under its banners, 3,000 of which come from Europe.

Virtual supporters...

The internet not only helps to spread information about the jihadists and their goal – toppling regimes in the region and establishing a state according to what they believe to be Islamic principles. It has also increasingly become a tool to recruit new members, raise funds, and conduct new types of attacks which do not involve explosives or bullets.

#Inspire

Even in its early days, al-Qaeda consistently demonstrated a clear interest in making use of the internet for propaganda purposes. Its first website, Azzam.com, was created twenty years ago. Ever since, the level of sophistication in the use of online tools for jihadist propaganda has grown significantly.

A study by the International Centre for the Study of Radicalisation and Political Violence – on the social media profiles of 190 European fighters in Syria – confirms that jihadists document the conflict in real-time by posting videos and pictures on social media, thereby rendering the tools an essential aspect of the war effort.

> 'The risk now is that ISIL's successful cyber campaign might encourage others to follow in its footsteps.'

In addition, online sources like *Technical Mujahid Magazine*, the *Cyber Jihadist's Encyclopedia* and *Inspire* all provide motivational material that is designed to fuel support. A detailed content analysis of *Inspire* carried out by researchers at the University of Maryland suggests that the magazine uses religious arguments and provocative quotes from prominent American figures to radicalise potential recruits based in the West. Its featured articles – such as *Make a bomb in your mum's kitchen* – provide guidance on how to turn easily available objects such as pressure cookers (as used in the terrorist attack at the Boston marathon in 2013) into deadly weapons. Al-Qaeda's media outlet, As-Sahab Media, also recently announced the release of a new English-language jihadist publication called *Resurgence*.

#JihadiPosterGirl

Social media accounts deliver constant updates on the state of the conflict(s) and help establish connections between foreign fighters in the field and potential new recruits. Women and young girls, in particular, are increasingly being targeted. The dream of becoming a 'jihadi poster girl' has prompted some teenagers from Western countries – including Nora el-Bathy, a 15-year-old French girl who left her home and travelled to Syria – to join ISIL. They are often lured by pictures posted online which seek to depict an ideal life within the areas under the group's control.

...to laptop warriors

To finance themselves, cyber-jihadists resort to the same tactics as cyber-criminals, conducting phishing attacks or purchasing online details of stolen credit cards. This is, for example, how UK-born Younis Tsouli – also know online as 'Irhabi 007' – and his affiliates generated some £2.5 million. The monies are used primarily to cover the costs of propaganda or recruitment operations, as well as paying internet providers.

In addition, cyber-jihadists use the internet to raise funds directly. Al-Qaeda's global fundraising network, for instance, is built on charities and NGOs that largely communicate with their donors through social media and online fora. ISIL has reached a new level by designing the mobile application *Dawn of Glad Tidings*, which provides users with regular updates and automatically tweets through their own personal accounts, helping the group reach more supporters, including potential donors.

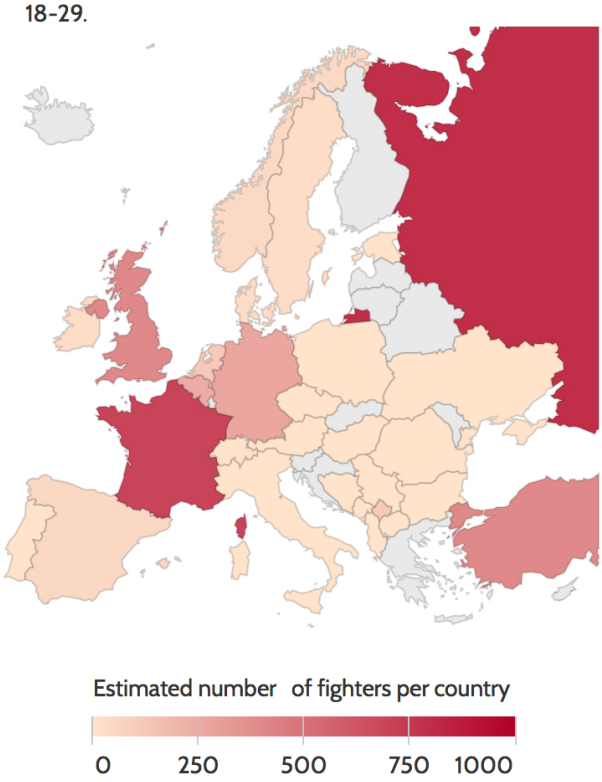
#CyberCaliphate

Cyber-jihadists have also expanded their use of the internet to mount attacks on Western governments and institutions. Al-Qaeda, for example, openly encourages its followers to hack Western websites and 'morally corrupt' pages: cyber jihad was also explicitly mentioned as a sacred duty for every Muslim in one of its documents entitled 'The 39 Principles of Jihad'.

Recent cases prove that the jihadist cyber army is growing in both numbers and sophistication. The ISIL-affiliated group *Cyber Caliphate* – allegedly led by a British hacker known as Abu Hussain Al Britani, who left Birmingham for Syria – has recently hacked and taken over control of both the Twitter and YouTube accounts of the US Central Command. Moreover, about 20,000 websites have been attacked in France in the aftermath of the terrorist acts in early January.

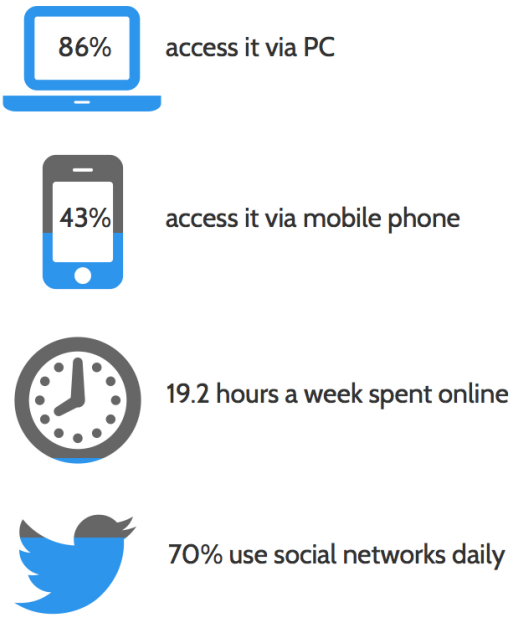
Demographics of foreign fighters

- The typical age range of individuals who are known - or claim - to have travelled to Syria as foreign fighters is 18-29.



Internet use by 'digital natives'

- 89% of a similarly aged group of 'digital natives' (16-24 year olds) in the EU are active online. This equates to some 85.5 million people.



Sources: R. Barrett, Foreign Fighters in Syria (2014); IAB Europe, Mediascope Europe (2013).

From cyber-jihadism to cyber-terrorism

There is no doubt that the internet helps shorten the distance between those engaged in combat abroad and followers worldwide, including in the West. The risk now is that ISIL's successful cyber campaign might encourage others to follow in its footsteps. Some have already tried: in April 2013 a group calling itself the *Syrian Electronic Army*, believed to be close to Assad's regime, gained control of the Associated Press Twitter account and published a hoax message announcing an attack on the White House. As a consequence, the Dow Jones stock exchange index fell by 1% and $200 billion was wiped off the market. The same group recently hacked the Twitter accounts of *Le Monde* and posted a message to the newspaper's 3.3 million followers.

As part of #OpBlackSummer – an online campaign against US companies and government websites – lesser-known groups like the *Al-Qaeda Electronic Army* and the *Tunisian Cyber Army* have attacked the US Customs and Border Protection and the US Office of Personnel Management. On 30 August 2012, the records of Nigeria's secret service were hacked by an individual claiming to be affiliated to Boko Haram, with the personal information of 60 Nigerian state security operatives subsequently being published on a local news site.

So far, only individual groups have managed to take control of Twitter accounts or deface the websites of governmental organisations – through parallel, but mostly uncoordinated initiatives. The virtual consolidation of several groups in a single cyber-hydra, however, could pose a serious challenge to global security and stability.

Leviathan's mission impossible...

In the real (and realist) world, the state exercises a monopoly over law making, law enforcement and, ultimately, power and the use of force. But this is not the case in cyberspace, where power is diffused among governments, private companies and individual users.

It appears therefore somewhat unreasonable that, when faced with cyber jihadism, citizens tend to place full responsibility for tackling the threat in the hands of the government. In any case, even when governments have the required legal and

operational tools – takedowns, domain name de-registration or filtering – to fight content that may constitute a threat to public order or national security (e.g. child pornography or hate speech), their use has always been politically sensitive due to the potential for the state to abuse its power(s).

Recent proposals to allow law enforcement agencies to break into encrypted communications or to ban these technologies altogether have already been criticised as posing a threat to civil liberties – even though al-Qaeda is encrypting online communications with its own products (*Tashfeer al-Jawwal* and *Amn al-Mujahid*) in order to evade intelligence organisations.

...and possible action

Even if governments cannot fix the problem alone, they do, however, have the responsibility to provide leadership and bring together other stakeholders around a common narrative. An explicit and unquestioned commitment to keeping the internet open, safe and secure – as stated in the Cybersecurity Strategy of the European Union – could be just (part of) the solution.

Keeping the internet open

When facing any new wave of terrorism, governments tend to follow their natural instinct: introduce new legislation and promise more resources for law enforcement and intelligence agencies. Such steps, however, do not always resonate well with citizens, as many are already worried about the extent to which the state can infringe on daily life. For example, Russia's ill-concealed attempts to throttle the free media or the Twitter ban imposed during the recent presidential elections in Turkey smack more of authoritarianism rather than attempts to foster security.

Governments will never have enough resources or gain citizens' unconditional acceptance for totally controlling cyberspace. It takes a network to beat a network: therefore, refocusing efforts on engaging with citizens might be the only solution. This will require, however, an unwavering commitment to the freedom of expression and the openness of the internet – and governments should learn to make better use of existing technologies like crowdsourcing or big data intelligence. Help in the fight against online jihadism may come from unexpected places. The 'hacktivist' collective known as *Anonymous* – whose actions in the past havealso included taking down the website of the CIA – has defaced several jihadist websites, including the French *ansar-alhaqq.net*, in retaliation for the *Charlie Hebdo* attacks.

Keeping the internet safe

The average age of those joining the jihadist ranks on the battlefield suggests that a better understanding of the use of various forms of media is a matter of priority in order to protect the youth. In this regard, interaction with internet providers and social network companies is a necessity. In the UK, for instance, such cooperation between the Counter-Terrorism Internet Referral Unit (CTIRU) and social media platforms has resulted in the voluntary removal of 72,000 pieces of terrorist and extremist content that was in breach of the companies' own terms and conditions. The experience of the Global Alliance against Child Sexual Abuse Online – a coalition of 54 countries launched by EU and US in 2012 – might also offer some useful lessons. In October 2013, several European and Arab countries (including Egypt, France, Saudi Arabia, the UK, and the UAE) joined forces with the US to establish an information coalition that compliments the military action being undertaken against ISIL.

Keeping the internet secure

The transnational nature of cyber-jihadist actions requires international cooperation between law enforcement agencies and courts that are often located in different jurisdictions. However, as it is often the case with the fight against terrorism and organised crime, effective collaboration is often hampered by lengthy procedures (i.e. mutual legal assistance), inadequate legislation (i.e. trans-border transfer of personal data), lack of experience (i.e. only a few countries are truly familiar with how to process electronic evidence) or, simply, limited trust. In order to ensure that the rule of law is not sacrificed on the altar of security, it is essential that police officers, prosecutors and judges receive appropriate training. This means learning not only how to detect and prosecute cybercriminals and terrorists, but also how to protect the rights of victims and people still only suspected of committing crime.

Finally, with a dynamic uptake of new technologies in developing countries, attempts to keep the internet secure will also depend on the capacity of those countries to detect phishing attempts, resist cyber attacks on their infrastructure, and prosecute criminals.

Beatrice Berton is a Junior Analyst and Patryk Pawlak is a Senior Analyst at the EUISS.

 | QN-AK-15-002-2A-N | ISBN 978-92-9198-258-5 | ISSN 2315-1110 | DOI 10.2815/77528