November 3, 2014 6:03 pm

FT.com

The web is a terrorist's command-and-control network of choice

Robert Hannigan

The Islamic State of Iraq and the Levant (Isis) is the first terrorist group whose members have grown up on the internet. They are exploiting the power of the web to create a jihadi threat with near-global reach. The challenge to governments and their intelligence agencies is huge -- and it can only be met with greater co-operation from technology companies.

Terrorists have long made use of the internet. But Isis's approach is different in two important areas. Where al-Qaeda and its affiliates saw the internet as a place to disseminate material anonymously or meet in "dark spaces", Isis has embraced the web as a noisy channel in which to promote itself, intimidate people, and radicalise new recruits.

extremists of Isis use messaging and social media services such as Twitter, Facebook and WhatsApp, and a language their peers understand. The videos they post of themselves attacking towns, firing weapons or detonating explosives have a self-conscious online gaming quality. Their use of the World Cup and Ebola hashtags to insert the Isis message into a wider news feed, and their ability to send 40,000 tweets a day during the advance on Mosul without triggering spam controls, illustrates their ease with new media. There is no need for today's would-be jihadis to seek out restricted websites with secret passwords: they can follow other young people posting their adventures in Syria as they would anywhere else.

The Isis leadership understands the power this gives them with a new generation. The grotesque videos of beheadings were remarkable not just for their merciless brutality, which we have seen before from al-Qaeda in Iraq, but for what Isis has learnt from that experience. This time the "production values" were high and the videos stopped short of showing the actual beheading. They have realised that too much graphic violence can be counter-productive in their target audience and that by self-censoring they can stay just the right side of the rules of social media sites, capitalising on western freedom of expression.

Isis also differs from its predecessors in the security of its communications. This presents an even greater challenge to agencies such as GCHQ. Terrorists have always found ways of hiding their operations. But today mobile technology and smartphones have increased the options available exponentially. Techniques for encrypting messages or making them anonymous which were once the preserve of the most sophisticated criminals or nation states now come as standard. These are supplemented by freely available programs and apps adding extra layers of security, many of them proudly advertising that they are "Snowden approved". There is no doubt that young foreign fighters have learnt and benefited from the leaks of the past two years.

GCHQ and its sister agencies, MI5 and the Secret Intelligence Service, cannot tackle these challenges at scale without greater support from the private sector, including the largest US technology companies which dominate the web. I understand why they have an uneasy relationship with governments. They aspire to be neutral conduits of data and to sit outside or above politics. But

increasingly their services not only host the material of violent extremism or child exploitation, but are the routes for the facilitation of crime and terrorism. However much they may dislike it, they have become the command-and-control networks of choice for terrorists and criminals, who find their services as transformational as the rest of us. If they are to meet this challenge, it means coming up with better arrangements for facilitating lawful investigation by security and law enforcement agencies than we have now.

For our part, intelligence agencies such as GCHQ need to enter the public debate about privacy. I think we have a good story to tell. We need to show how we are accountable for the data we use to protect people, just as the private sector is increasingly under pressure to show how it filters and sells its customers' data. GCHQ is happy to be part of a mature debate on privacy in the digital age. But privacy has never been an absolute right and the debate about this should not become a reason for postponing urgent and difficult decisions.

To those of us who have to tackle the depressing end of human behaviour on the internet, it can seem that some technology companies are in denial about its misuse. I suspect most ordinary users of the internet are ahead of them: they have strong views on the ethics of companies, whether on taxation, child protection or privacy; they do not want the media platforms they use with their friends and families to facilitate murder or child abuse. They know the internet grew out of the values of western democracy, not vice versa. I think those customers would be comfortable with a better, more sustainable relationship between the agencies and the technology companies. As we celebrate the 25th anniversary of the spectacular creation that is the world wide web, we need a new deal between democratic governments and the technology companies in the area of protecting our citizens. It should be a deal rooted in the democratic values we share. That means addressing some uncomfortable truths. Better to do it now than in the aftermath of greater violence.

The writer is the director of GCHQ, a UK government intelligence and security organisation.