Paul Stokes reviews the UK government's proposed counter-extremism bill and explains how advanced crime analytics can help in tackling the recruitment of foreign fighters via social media

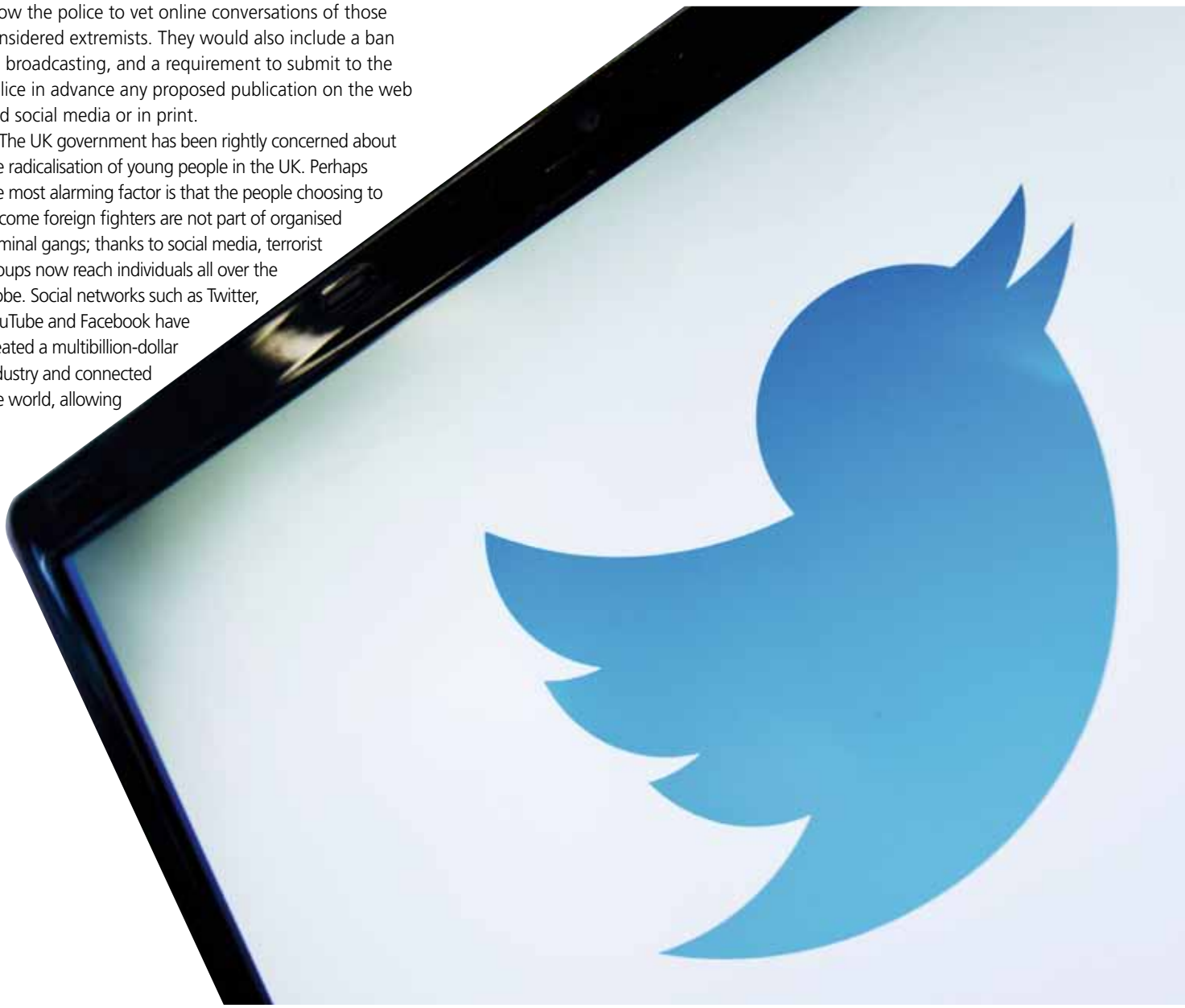
TERROR MEE

The recently elected UK Conservative government is to use its new unilateral power to push through anti-extremism laws. A revived counter-extremism bill was outlined in the Queen's Speech to Parliament on 27 May which reintroduced plans to tackle radicalisation and the rapid infiltration of terrorist recruitment into society. Prime Minister David Cameron stated that "for too long, the UK has been a passively tolerant society", and affirmed that those who seek to threaten the country's democracy will be confronted.

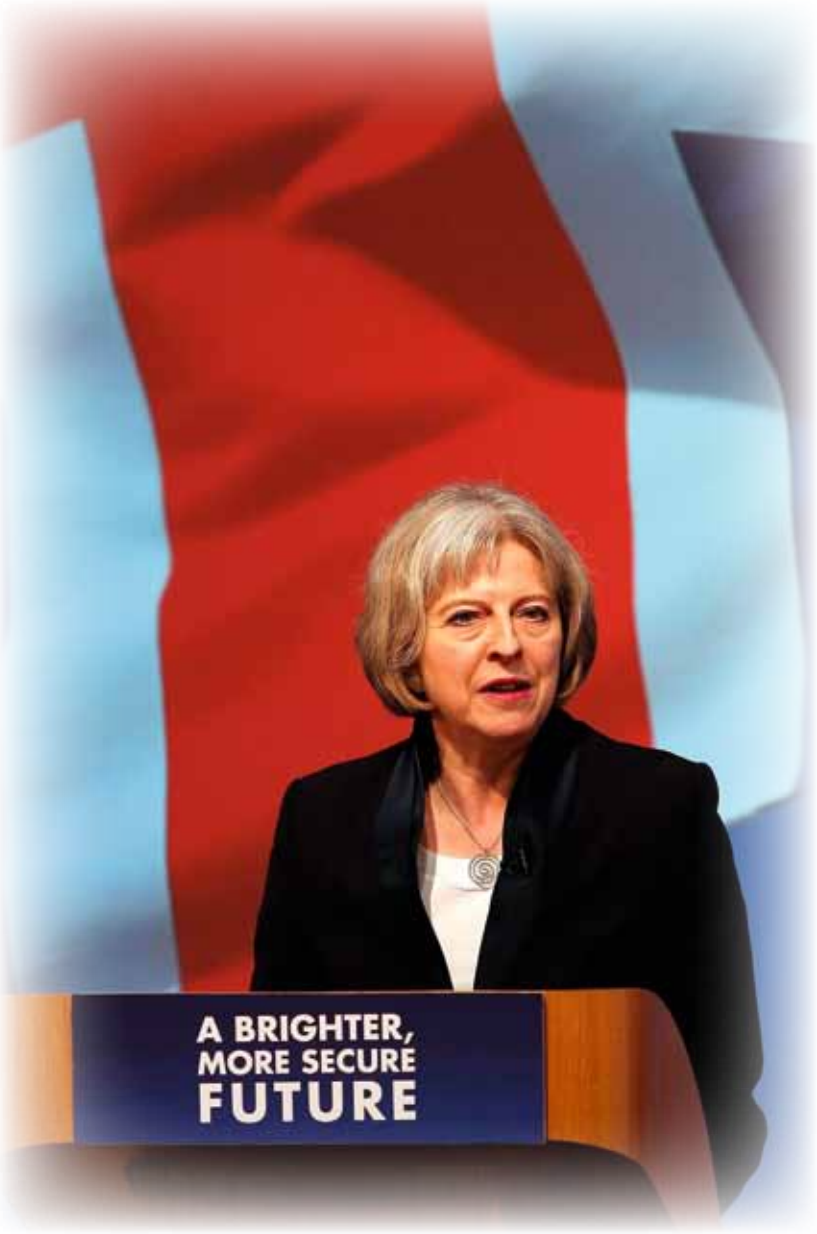
The new bill seeks to give enhanced powers to the police, enabling them to obtain court orders for public telecommunications providers to release Internet search records and other communications data on demand. These counter-extremism powers will allow the police to vet online conversations of those considered extremists. They would also include a ban on broadcasting, and a requirement to submit to the police in advance any proposed publication on the web and social media or in print.

The UK government has been rightly concerned about the radicalisation of young people in the UK. Perhaps the most alarming factor is that the people choosing to become foreign fighters are not part of organised criminal gangs; thanks to social media, terrorist groups now reach individuals all over the globe. Social networks such as Twitter, YouTube and Facebook have created a multibillion-dollar industry and connected the world, allowing

> "Thanks to social media, terrorist groups can now reach individuals all over the globe"



ETS TWITTER



©Getty Images

UK Home Secretary Theresa May hopes the new bill will prevent extremist groups from using social media to radicalise vulnerable youngsters

us to connect with friends, share our experiences and promote our business interests. Social networks, like every community, have a dark side, however. It is well publicised they are used as a communication vehicle for bullies, child sex abusers and, more recently, media savvy extremist groups which use them as command-and-control networks of choice.

Police have warned there is no end in sight to the numbers attracted and incited by jihadi propaganda spreading like wildfire via social media. Britain's counter-terror chief, Mark Rowley, recently highlighted the British threat, estimating that over half of 700 Britons who had travelled to Islamic State territory were now back in Britain.

The Metropolitan Police recently said potential recruits were being aggressively targeted through social media, particularly people with "violent backgrounds, the very young and those with mental health issues". In May a 19-year-old man was sentenced to eight years in a young offenders' institution for grooming a young man with learning difficulties to kill UK soldiers. Using BlackBerry Messenger and social media sites, the perpetrator encouraged the victim to change his name and attempted to radicalise him with stories of innocent children murdered by military forces. The judge condemned the recruiter's actions, stating: "you knew he [the victim] was an extremely vulnerable young man, your treatment of him was as callous as it was manipulative."

This example is just the tip of the iceberg: two teenagers from Coventry were recently arrested on suspicion of travelling to Syria for terrorism, and a British couple travelling with four children were arrested in Turkey for the same reason. The reach and radicalisation by ISIS is growing not just in the UK but across the globe – in fact, the total number of foreign fighters inside Syria and Iraq has now exceeded 20,000, according to the International Centre for the Study of Radicalisation (ICSR).

To give a sense of scale, it has recently been revealed that jihadis are sending up to 100,000 Twitter messages a day. In response to the threat, Europol director and ex-MI5 officer Rob Wainwright said that encrypted communications, often via social media, were the "most significant challenge" to tackling terrorism. As there is no one single entity controlling social media and no rule book, social media is the new Wild West.

Social networks are, albeit not willingly, increasingly hosting a virtual meeting place for those that threaten national security. And as we see a rapid shift from traditional warfare to cyber warfare, some governments risk sleepwalking their way through this problem. Fortunately, an increasing number are starting to recognise that the Internet has become "the fifth domain", after land, sea, air and space. The latter four are regulated because they can have a profound effect on the lives of citizens and need some controls to give order and protect. Governments across the world are starting to recognise that this fifth dimension, the Internet, while having much positive impact, also has the potential to undermine confidence in the state and commerce.

New measures to be introduced in the UK's counter-extremism bill offers a controlled approach and not a universal "right to know" for the police, which should provide some reassurance of its limitations in terms of surveillance while allowing police greater access to the data that will illuminate genuinely at-risk areas. As sophisticated recruitment via social media increases and becomes more trans-national in nature, law enforcement agencies need to be able to access online communications

TERROR MEETS TWITTER

to prevent those exploiting social media to recruit and radicalise youth. Doing this needs to be pursuant to the rule of law, with clear guidance and strict oversight.

The Counter-Terrorism Act includes provisions for making the availability of communications data easier for law enforcement agencies. The new law will require Internet service providers to keep a much better and more traceable log of individual user activity in case it is ever required in a criminal investigation. The Act also states that, where necessary, any required Internet and communications data should be "disclosed without delay" when it is "in the interests of national security or for the purpose of preventing crime".

Investigators already had the right to ask commercial providers such as Facebook, Microsoft and Google for communications data, but there was no legal obligation behind it and the sector has often been slow or reluctant to react to requests like this. The Act brought in new powers of enforcement in this regard. But, without the resources to analyse the data, little can change very quickly for investigators.

The volume and variety of data long ago reached such complexity and scale that only technology can truly handle it and maximise its value. As the volumes of data they have access to grow, the key challenge police forces face is about making sense of these data.

In fact, law enforcement and intelligence operations are, increasingly, a data analytics challenge. There is so much data from a vast array of different sources that it takes serious algorithmic smarts in order to make connections between seemingly unconnected pieces of data – or to detect anomalous relationships in a sea of mundane information.

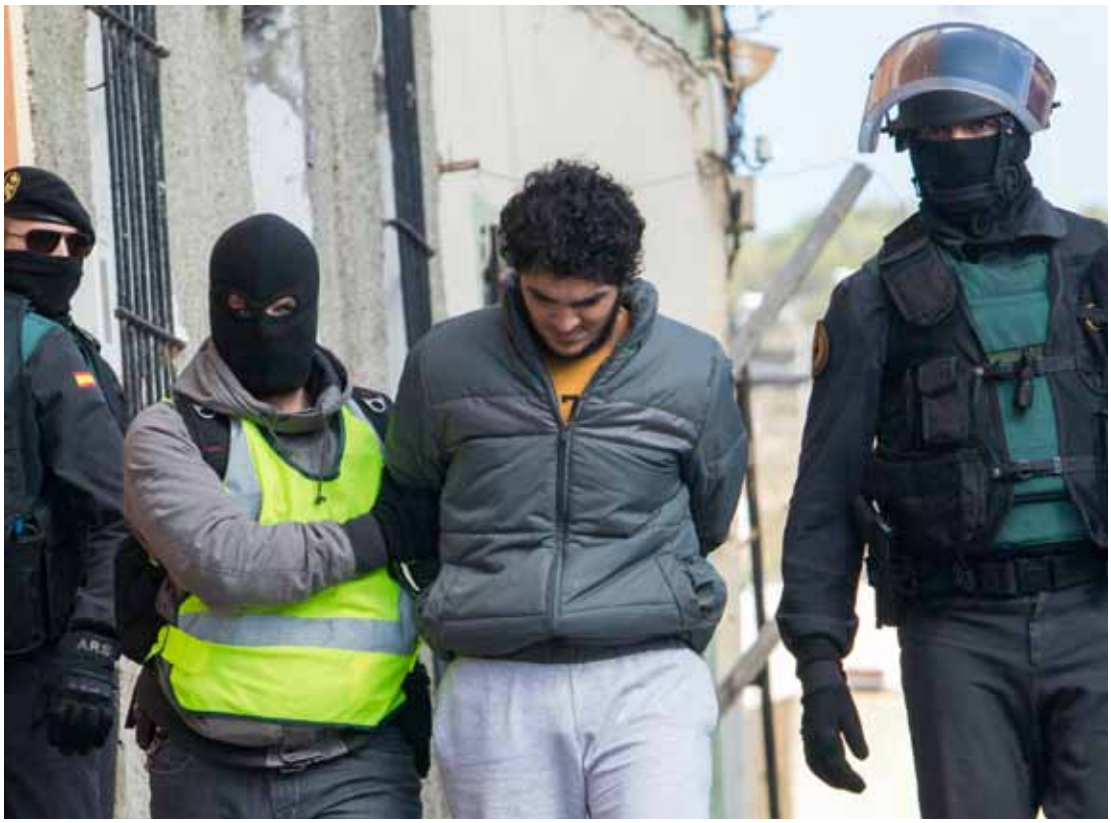
New advances in crime analytics solutions can connect different data types, discover links, and uncover people, entities, patterns, locations and relationships of interest. In addition, it can use unstructured data like text documents and social media posts, and recognise words and phrases as "entities" that can be analysed and linked automatically.

The latest crime analytics techniques such as link analysis, social network analysis and anomaly detection can help focus investigators' attention on potentially suspicious persons early on. This is critical in identifying at-risk young people before they leave home to train to fight – a decision that can have terrible consequences for them and their families once they leave the country.

These tools help law enforcement agents disrupt recruitment networks that target the vulnerable but, moreover, assist in eliminating from suspicion individuals who are not persons of interest. By working from known extremists, recruiters and financers out to a wider network, agencies can ensure they do not breach the privacy or civil liberties of citizens connected but not a threat or at risk. The focused nature of advanced crime analytics in targeting specific data sets and looking for distinct patterns or connections removes the need for the government to consider blanket surveillance and concentrates law enforcement resources on real at-risk areas.

Extremist groups use increasingly sophisticated technology to support their activities. Governments and law enforcement agencies must therefore constantly upgrade their own technical capability to meet this challenge. With the right technology support, the new legislation will lead to law enforcement agencies being able to legally access the right information at the right moment, saving valuable time and providing reliable results. This information could protect a child, save lives or defend a border.

Paul Stokes is COO of Wynyard Group, a market leader in serious crime fighting software used globally by intelligence, investigations and information security operations in justice and law enforcement, national security, financial services and critical national infrastructure.



Spanish police arrested several people in February suspected of spreading extremist propaganda through social media