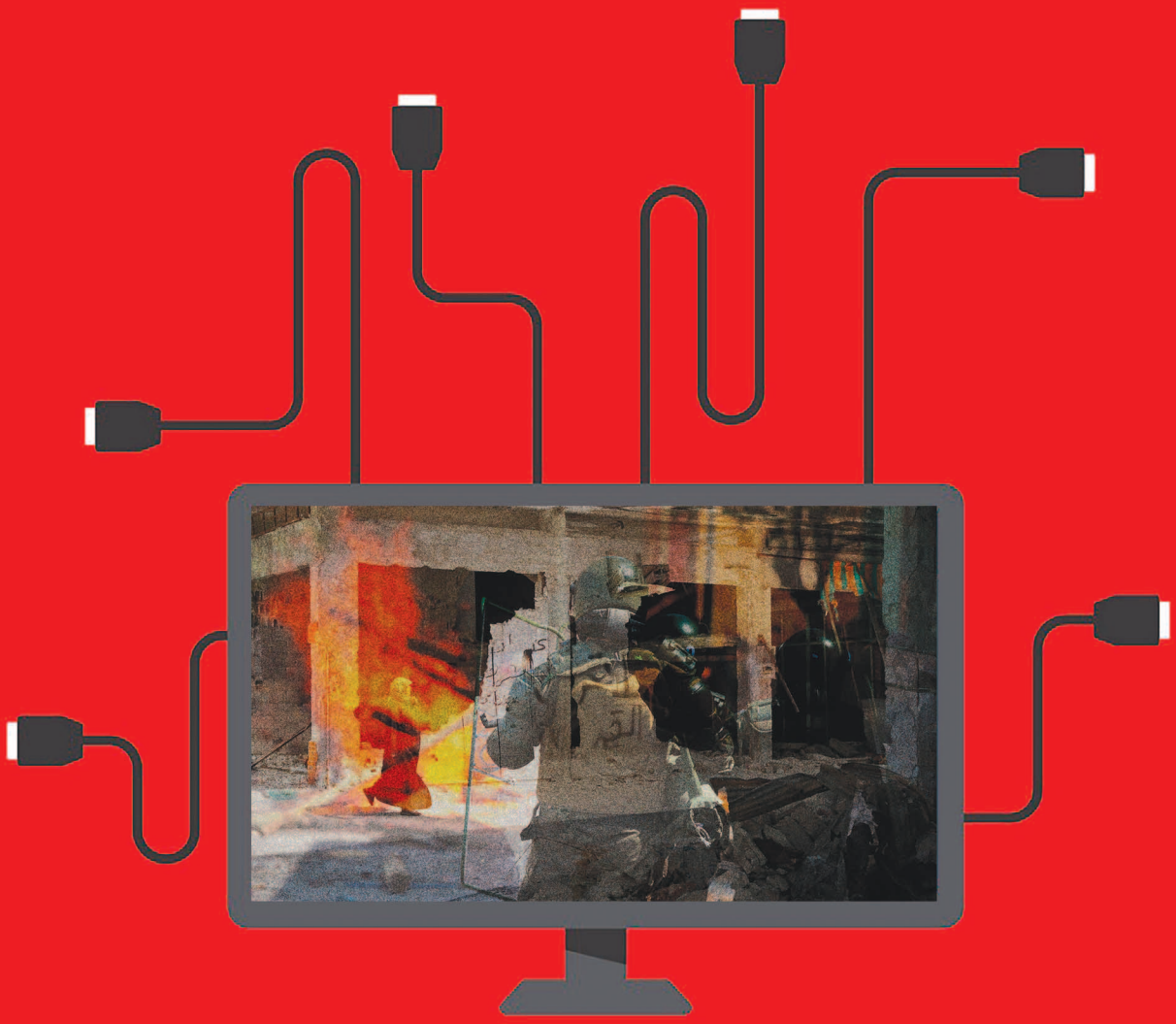

Terrorists' Use of Tradecraft

by Dr David Lowe

In our current lifestyle there is a heavy reliance in various forms of electronic communication. For example, using mobile phones we can bank or shop online while on the go, listen to the radio or watch television, keep in touch with friends and colleagues on various social media platforms and communicate via email, text or on various apps. Less we forget, we can also make calls on the mobile phone! The mobile phone is in addition to the personal computer, laptop and tablet we use to access the various forms of electronic communication. Lewis and Callahan's 2018 study of the digital world found that 4.3 billion people use the internet, 3.9 billion people use a mobile internet and 3.4 billion people use various forms of social media.

Their study found that every 60 seconds:
1. One million people log into Facebook;
2. 3.7 million Google search enquiries are made;
3. 4.3 million videos are viewed on YouTube;
4. 18 million text messages are sent;
5. 38 million WhatsApp messages are sent;
6. 187 million emails are sent.

This study did not include Twitter, Instagram, Snapchat, Skype and other social media use, but it does reveal how widespread global electronic digital communication use is. In addition to innocent, everyday usage, terrorists and criminals also take advantage of current methods of electronic communication and as the figures above reveal the enormity of the task facing security service and policing agencies in monitoring communication between terrorists. This article will provide an illustration of activities that amount to tradecraft, mainly those carried out by state agencies. This is followed by looking at how terrorists exploit the various electronic communications via their own methods of tradecraft, which in essence are methods of counter-surveillance techniques.

What is Tradecraft?
Tradecraft use is not exclusive to terrorists and criminals, it is used by state agencies such as the security services and specialist police departments within the intelligence community. Tradecraft refers to the techniques, methods and technologies used in modern espionage and generally, as part of the activity of intelligence. There is a wide range of tradecraft activity used by state agencies including:

1. Agent/Informant Handling – this is where persons

already operating within terrorist organisations are recruited to pass on intelligence on their peers;

2. Black Bag Operations – these are covert entries into buildings and locations to obtain information on targets during human intelligence operation, such as placing covert listening devices in rooms and vehicles;

3. Use of Legends – this where mainly trained state agency officers are given a well-prepared and credible made-up identity with the aim of infiltrating a target organisation;

4. Surveillance – this activity includes physical static and mobile surveillance operations to surveillance of targets' electronic communications.

Because tradecraft is intrusive into the lives of targets (and potentially their family members), state agency tradecraft activity is not arbitrary, they are strictly controlled powers granted under statutory authorities/warrants issued either by the judiciary or a secretary of state (with subsequent judicial examination). Factors considered when issuing these authorities and warrants are the legal issues of necessity and proportionality. Necessity is where due to the circumstances in which the target is operating, obtaining evidence using conventional investigative methods are ineffective and these powers are needed. Proportionality is balancing the reasons for the requirement of this power with human rights provisions such as right to privacy and data protection. The main legislation covering these powers in the UK are the Regulation of Investigatory Powers Act 2000 regarding use of informants (referred to as covert human information sources in the Act) and applying static and mobile observation. The Investigatory Powers Act 2016 provides authorisations for various forms of surveillance of electronic communications, with other powers being granted under terrorism statues introduced from the Terrorism 2000 Act to the Terrorism and Border Security Act 2019. In Ireland the Communications (Retention fo Data) Act 2011, the Criminal Justice (Surveillance) Act 2009 and Criminal Justice (Terrorist Offences) Act 2005 provides authorisations for state agency tradecraft that is predominantly carried out by An Garda Siochana (the Irish police).

Terrorists' Counter-Surveillance Tradecraft Methods

Knowing or expecting to be under state agency surveillance, terrorists also use tradecraft techniques as counter-surveillance methods. In his book, 'On Guerrilla Warfare', Mao Tse-Tung stated that the guerrilla must move among the people as the fish swims in the sea and it is the same for the terrorist that in order not to bring attention to themselves, they must act as normal as possible in their day-to-day activities. In order to do so, terrorists must be conscious of how and what content they communicate or promote using open sources, such as social media sites like Twitter, YouTube or Facebook and, potentially to be careful in their use of more deeply encrypted sites like WhatsApp.

In order to prevent state agencies from monitoring their activity there are two distinct methods of tradecraft deployed by terrorists. Firstly, those active within a terrorist group know it is highly likely their movements and use of electronic devices are being monitored by states' counter-terrorism agencies and therefore must be extremely mindful who they associate with and how they communicate. Most terrorist groups give advice on counter-surveillance tradecraft to group members and followers, an example of which is the group Islamic State (IS) who in issue 2 of their online magazine Rumiyah published an article regarding the use of electronic communications. It informs its members and followers to be aware of the various malware methods adopted by state agencies to gain access to electronic communication used by the group, along with how to counter the impact of the malware. The final piece of advice IS provide is, if all else fails return the device to factory settings thereby wiping off all communications data. Although returning a device to factory settings can frustrate investigations into terrorist activity, such a move is not a total failsafe move as forensic examination can still detect images and, albeit broken communication, some relevant information related to terrorist activity. When this is added to other evidence, it can still provide an overall pattern of activity revealing terrorists' use of tradecraft.

Being aware their communications is being monitored, be it far-right, nationalist or Islamist terrorist groups, they are now regularly using more deeply encrypted sites to communicate through the likes of Telegram, GAB (mainly by far-right groups and followers) or WhatsApp and darknet sites. In order to attract custom, darknet sites promote a world of complete freedom and anonymity, claiming users can say and do what they like uncensored, unregulated and outside society's norms. This has resulted in terrorist groups increasingly moving to the darknet to communicate. For example, Islamic State use the darknet marketplace Silk Road to raise funds, sell books on how to carry out jihad, make bombs and homemade firearms, as well as purchasing weaponry. A popular darknet site used by terrorists to communicate with each other is Tor. Tor is a virtual private network that protects the identity of the user by wrapping layers around the communication, a process referred to as 'onion rooting'. As such, Tor hides the location and identity of its users allowing terrorists and extremists to have various forums and to communicate relatively freely without detection. However, most state agencies, including the UK and Ireland, have malware technology to infiltrate and monitor most terrorists' darknet usage.

The second method of tradecraft deployed by terrorists is in their handling of cleanskins. Cleanskins are people who do not have an existing criminal record or who have not attracted the attention of police or security services, or, occasionally, those who may be on the periphery of intelligence systems that are not regarded as a great risk. As such, cleanskins imbued with an extremist ideology are a valuable

commodity to terrorist groups. Once directed to a more deeply encrypted site, or ideally though clandestine meetings, advice is passed onto cleanskins on how to apply counter-surveillance tradecraft, including how to create a legend to portray what appears to be innocent, normal day-to-day activity.

An example where I provided expert witness evidence on terrorists' use of tradecraft concerned an individual who became imbued with the Islamist ideology. His electronic footprint and activity over a two-year period was submitted at his trial by England's Crown Prosecution Service as evidence for the offence of engaging in the preparation of committing acts of terrorism under section 5 Terrorism Act 2006. After watching online YouTube videos of radical Muslim preachers, he became influenced by the Islamist ideology. Following certain terrorist attacks this individual emailed/messaged politicians and journalists who were critical of Al Qaeda and IS activity. None of these messages contained a violent threat, but they were extremely critical of violence against Muslims in the Middle East by Western states' military action in the region.

At this stage this individual's actions are not illegal, but it is a pattern that an individual is at a stage of being vulnerable of being drawn towards terrorism. If such behaviour is exhibited by persons in Britain today, especially for staff in specified British authorities (health, education and criminal justice system) who have the statutory responsibility under section 26 Counter-Terrorism and Security Act 2015 in having due regard to the need to prevent people from being drawn into terrorism, this is a stage where individuals can be referred to agencies involved in the Prevent strategy. Even though his extremist behaviour was prior to the introduction of the 2015 Act, even without the statutory responsibility, the Prevent strategy was still in place and he could still have been referred to Prevent agencies, but he was not given this opportunity (The Prevent strategy does not apply to Northern Ireland). In the autumn of 2015, following a visit to his extended family in Bangladesh, his actions went beyond simply expressing extremist commentary.

In 2016 IS still controlled large areas of Syria and the group were actively recruiting foreign fighters, which included males from the UK, most of whom travelled to Turkey, then onto the Turkish border with Syria. In January 2016 this individual planned to travel to Syria to join IS, but prior to doing so he created his own legend. He booked online a return flight to Istanbul, the e-visa for Turkey and four-night hotel accommodation in Istanbul via his credit card. In addition to this he purchased Turkish Lire to the amount that would reasonably be expected to cover costs of a four-night stay in Istanbul. A few weeks prior to his departure he joined an online dating site and made connection with a female from Istanbul, stating he would meet her on his arrival. Should he be challenged by the police prior to his departure, this online activity was his cover story for travelling to the region.

On the day of his departure he checked-in at the airport and prior to boarding the flight, at the airport ATM he withdrew all the money he had in his bank account. On arrival at Istanbul he checked into the Istanbul hotel, and, as is normal practice, he presented his credit card to cover any extra hotel costs to the reception staff. Evidence revealed that after checking in, this individual did not stay at the hotel, instead he returned to Ataturk Airport and purchased with cash a single air flight ticket to Gaziantep. From there he boarded a bus from Gaziantep to Kilis, close to the Turkish/Syrian border. At the border this individual was stopped by Turkish border authorities who searched his property and found camouflage fatigues, military style boots and a black IS shahada flag. As a result, they contacted the UK's counter-terrorism police and sent him back to the UK. On his return he was stopped by the police at the airport under Schedule 7 Terrorism Act 2000 who examined the sites he was looking at and the communications he made on his electronic devices. A sim card linked to a pay-as-you go mobile phone was also found. He was arrested under section 5 Terrorism Act 2006, for the offence of engaging in the preparation of committing acts of terrorism. Following his subsequent police interviews and forensic examination of his electronic devices it revealed the sim card was from a pay-as you-go phone used during his time in Bangladesh, and later the UK, where he was in communication with IS members. It was found that they groomed and instructed him in relation to creating a legend prior to joining the group as a foreign fighter in Syria. During the forensic examination of cell site data that provides geographical locations, it revealed the individual's use of his i-phone and the pay-as -you-go phone were in the same location, thereby proving his use of both phones.

Conclusion

In this summary of terrorists' use of tradecraft, what can be provided by expert witnesses who research and have practiced in this area is:

1. Showing patterns of behaviour linked to internet and communications use revealing a progression from interest in extremist/terrorist sites to becoming vulnerable to being drawn towards terrorist activity. This is linked to Britain's Prevent strategy and the statutory responsibility of specified authorities under section 26 Counter-Terrorism and Security Act 2015;

2. Identifying methods and rationale behind terrorists' tradecraft through their use of more deeply encrypted communications sites;

3. Identifying and revealing terrorists' tradecraft in their use of internet and electronic communications in creating a legend;

4. Associating investigations into terrorists' use of internet and communications sites with the relevant law and practice by state agencies. This includes the relevant state statutes granting these agencies powers to intercept and carry out surveillance as mentioned above, data protection law including the EU's Directive on the protection of personal data processed for

the purposes of preventing, investigating, detecting or prosecuting criminal matters and human rights legal provisions such as the European Convention on Human Rights and updates in courts' decisions in interpreting the statutes be it from domestic courts, the Court of Justice of the European Union or the European Court of Human Rights.

As communication technology advances, so do terrorists use and application of that technology. As such a 'cat and mouse' game between state agencies investigating terrorists' activity develops with continuous changes of behaviour and practice by terrorists use of electronic communication that investigators must monitor, and with-it legislative provisions introduced to keep pace with technological advances, ensuring that state agencies investigatory methods remain within the rule of law.

About the Author
Dr David Lowe is a retired police officer and is currently a senior research fellow at Leeds Beckett University Law School researching terrorism & security, policing and criminal law. He has many publications in this area including his recent books 'Terrorism and State Surveillance of Communication' and 'Terrorism: Law and Policy', both published by Routledge. David is regularly requested to provide expert commentary to UK national and international mainstream media on issues related to his research areas.