Terrorists' use of messaging applications

Matthew Francis and Emma Barrett look at how emerging technologies have changed terrorist behaviour in the past and suggest that we should think about the implications of innovations in messaging applications.

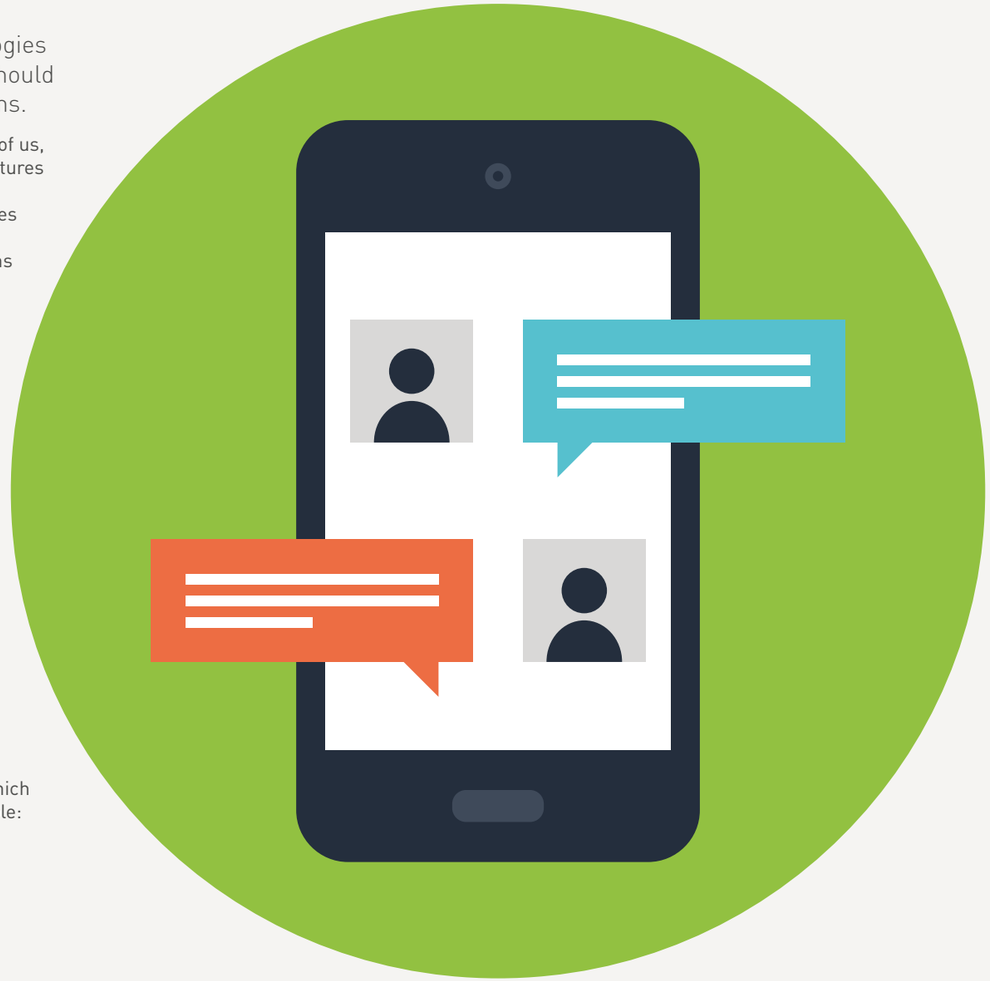
Terrorists and criminals, like the rest of us, need to communicate and, like the rest of us, they look out for ways of communicating that meet their particular needs. Some features of messaging applications may make them more attractive than others to terrorists when co-ordinating and planning their activities or distributing propaganda – features like encryption and anonymity, for example. As the current debate on encryption acknowledges, the use of apps for illicit communications has important ramifications for counter-terrorism, and not just in providing new ways to carry on old crimes.

People exploit emerging technologies for criminal or terrorist ends, but emerging technologies may also have qualities that enable or facilitate new types of criminal behaviour. There's nothing new about this. Consider the early adoption of the printing press by Pietro Aretino (1492-1556) to disseminate illicit pornographic material, and the way in which more recently the development of search engines aids the collection of illegal images of children.

In 1878, Russian revolutionary Vera Zasulich committed what has been described as the first act of non-state terrorism: the assassination of a city governor. This act of political violence was possible because of the development of the powerful British Bulldog revolver, which was compact enough to be hidden under her shawl. Until then her only choices had been bulky Smith & Wesson revolvers, meaning that her plans to carry out a political assassination had remained on the drawing board.

As these examples demonstrate, both how technology can be used for current purposes and what new uses it might facilitate are issues that need thinking through. So in the case of messaging applications what are some of their characteristics that might be attractive to criminals and terrorists, and what new forms of terrorist activity might they enable?

A guide produced by CREST assesses some of the key features, and applications, which are attractive to illicit use. Three categories of characteristics are particularly notable:



PRESENCE

This relates to the kind of information which tells users when someone was last online, their location and whether they have read messages. For example, with Telegram, users can control the timestamps of their messages, disabling them or replacing them with approximate times.

VERIFICATION

Using an email address or mobile number to validate identities are examples of the kind of processes that may, or may not be strictly enforced by some applications. Whether identities are verified or not can influence whether people trust those they communicate with. Twitter is a high-profile example of a networking service which supports messaging but which doesn't require verification.

ANONYMITY

Users may be able to conceal their identities by using pseudonyms or create accounts under different names that are not linked to their real contact details. The messaging application FireChat is one example of apps which allow messages to be sent from usernames as opposed to mobile numbers. FireChat users are not required to use real names so can send messages anonymously.

NOVEL FEATURES

Telegram's self-destructing messages and FireChat's Bluetooth connectivity (which circumvents telecom networks altogether) are of course intended by the manufacturers for benign use, although we need to consider how they might be used for malign purposes too. To be successful, terrorists and criminals need to keep their illicit activities secret, so it's no surprise that they are drawn to communication methods that offer the potential for encryption and anonymity.

But as well as thinking about how criminals and terrorists use such apps to carry out their 'usual' activities, we should also be aware of the new activities that innovation in messaging apps could trigger. Researchers have pointed out that terrorists' ability not just to reach out to a wide audience online but to engage that audience in two-way conversation has enabled the development of a virtual community – something that is difficult to achieve with traditional broadcast media. New messaging applications allow that communication to become ever more personalised and ever less detectable. Without the assurance of anonymity, the plans of someone interested in engaging with that virtual community might – like Zasulich's early assassination plans – remain on the drawing board. Encrypted apps thus reduce one barrier to engagement.

The CREST Introductory Guide: Messaging Applications, *is available to download for free at www.crestresearch.ac.uk/resources.*
This article originally appeared on the CREST website. You can read it and the research it is based on at https://crestresearch.ac.uk/comment/terrorists-use-of-messaging-applications/.