THE CONVERSATION
Academic rigor, journalistic flair

‘Burner’ phones, social media and online magazines: understanding the technology of terrorism

Prepaid cellphones are just one of many technological tools used by criminals and terrorists. flip phone image via shutterstock.com

Amid the global threat of terrorism, the actual attacks that occur can vary widely. Terrorists aim at different targets in different locations, and tend to be either shooting or bombing or both. There is, however, a central point of connection linking all these events: the use of technology to coordinate and organize the incident.

Recent reporting suggests that terrorists used “burner” phones, prepaid disposable mobile phones, to coordinate their actions during last year’s Paris terror attacks. This is not a new or innovative tactic. Drug dealers, street prostitutes and other criminal groups in the U.S. regularly use these devices for communication: they are cheap, plentiful and difficult to link to a real identity. Their value lies in real-time communication, via text or voice call, that needs no software nor even a computer to connect.

Having researched cybercrime and technology use among criminal populations for more than a decade, I have seen firsthand that throwaway phones are just one piece of the ever-widening technological arsenal of extremists and terror groups of all kinds. Computers, smartphones and tablets also draw people into a movement, indoctrinate them and coordinate various parts of an attack, making technology a fundamental component of modern terrorism.

Attracting attention

Different resources and applications are pivotal at different phases in the process of radicalization to violence, and for good reason. For instance, social media platforms like Facebook, Twitter, Instagram and Periscope give extremist groups a venue to attract individuals to join their movements.

Social media is especially effective for terrorist groups because it allows people to share and spread short messages, including text and images, in rapid bursts. With access from nearly any device, such

Author

Thomas Holt

Associate Professor of Criminal Justice, Michigan State University

as desktop or laptop computers and mobile phones – including burners – individuals can connect to larger networks of members around the world. Those communities can then reinforce ideological beliefs and spin messages.

The Islamic State group has a significant presence on Twitter. It uses hundreds of thousands of user accounts to broadcast information about its activities on the ground in real time, as well as to attract individuals to the movement. There have been several examples over the last few years of young people being recruited into the Islamic State group via social media and encouraged to travel to join the fight.

Since social media posts are shared in near-real time, terror groups can also post messages to claim responsibility for a terror attack or act of violence. People who see it can share it with others, drawing attention to this news and giving these groups additional attention from people who might join their cause.

Engaging in discussion

Web forums are another important venue for information sharing, radicalization and recruitment. Forums are asynchronous, meaning posts made can be seen at any time – seconds, minutes or even days after being made. Forums also let individuals post lengthy messages with images, hyperlinks and text that may take more time to read and interpret. As a result, they are more conversational and lead people to participate over long periods of time.

Forums are essential for long-term construction of shared cultures underlying extremist movements. They let people debate at length topics and minutiae of belief systems beyond what is possible on social media. In fact, one of the oldest web forums used by members of neo-Nazi and other radical far-right extremist groups in the U.S., called Stormfront, has been in operation since 1996.

Individual websites also play an important role in the spread of information and radicalization because creators can tailor specific messages to audiences in ways that may not be readily

contradicted. For instance, the racist group Stormwatch operates a website about civil rights leader Dr. Martin Luther King Jr. The site (martinlutherking.org) appears to be filled with biographical information, but in reality attacks King, questioning his motives and his morals. It also takes facts about his life and quotes from speeches out of context in an attempt to undermine his role in the American civil rights movement.

In addition, websites allow groups to publish highly stylized media materials to support and promote their agendas. For example, *Inspire* magazine appears to be a lifestyle publication published in multiple languages, but is published by al-Qaida in the Arabian Peninsula to promote a jihadist agenda. Evidence suggests that the perpetrator of the San Bernardino terror attacks of 2015, Syed Rizwan Farook, and his neighbor would regularly consume radical jihadist media including Inspire magazine and online videos produced by al-Qaida's Somalian branch, Al-Shabaab.

Planning and acting

Extremist groups can also use online information to plan their attacks. For instance, al-Qaida-linked actors allegedly used Google Earth in the run-up to their eventually failed attack against oil processing facilities in Yemen in 2006. Similarly, Google Earth maps were used by terrorists to navigate during the 2008 Mumbai attacks.

Once someone is radicalized and expresses willingness to travel to engage in foreign training or an actual attack, the use of burner phones becomes essential to reduce detection by law enforcement. It does take more work than regular use of a mobile phone: to sustain communications over time, users must share and keep track of often-changing phone numbers.

Privacy advocates suggest that burner phone users never actually store contacts' numbers on the device itself, which would save them on the phone's SIM card. That could let police use that data during an investigation. So users must write down or memorize phone numbers, which keeps the information available but easily abandoned in case of emergency.

Burner phones can also be used to activate bombs, since only the maker may know the phone number and call it to activate the device. After they are used, burner phones can be destroyed to further reduce the likelihood of identification and forensic evidence collection.

Taken as a whole, we must recognize that technology use by extremist groups extends well beyond any one type of device, across the continuum of both hardware and software communication platforms. As technologies continue to evolve, extremists will continue to stay on the cutting edge of communications, whether they are encrypted or completely open. Law enforcement and intelligence agencies must be able to adapt investigative resources to these various platforms and do so quickly in order to better respond to these threats. Otherwise, gaps in collection and analysis may lead to intelligence failures and successful attacks.

Social media **Terrorism** **mobile phone** **Al-Qaeda** **Internet forum** **Islamic State** **Terrorist** **cellphone** **Paris Attacks 2015**