Q&A: Internet extremism and how to combat it

June 4 2017, by Dee-Ann Durbin

The Union flag flies at half mast in Whitehall, central London, Sunday June 4, 2017, after Saturday night's terrorist incident on London Bridge and at Borough Market. Several people were killed in the terror attack at the heart of London and dozens injured. Prime Minister Theresa May convened an emergency security cabinet session Sunday to deal with the crisis. (Stefan Rousseau/PA via AP)

In the wake of Britain's third major attack in three months, Prime

Minister Theresa May called on internet companies to do more to block extremist groups who use the web to recruit members and send coded messages.

Here's a look at terrorism on the web, what's being done to stop it and what could come next.

Q. What are technology companies doing to make sure extremist videos and other terrorist content doesn't spread across the internet?

A. Internet companies use technology plus teams of human reviewers to flag and remove posts from people who engage in terrorist activity or express support for terrorism. Google, for example, says it employs thousands of people to fight abuse on its platforms.

Facebook, Microsoft, Twitter and YouTube late last year teamed up to create a shared industry database of unique digital fingerprints for images and videos that are produced by or support terrorist organizations. Those fingerprints help the companies more quickly identify and remove terrorist content on the web. After the terror attack on Westminster Bridge in London in March, Google and other tech companies also agreed to form a joint group to accelerate anti-terrorism efforts.

Twitter says in the last six months of 2016, it suspended a total of 376,890 accounts for violations related to the promotion of terrorism. Three-quarters of those were found through Twitter's internal tools; just 2 percent were taken down because of government requests, the company says.

A person, centre, is led away at an address in Barking, east London, during a police operation Sunday June 4, 2017, following Saturday night's terrorist incident at London Bridge. Several people were killed in the terror attack at the heart of London and dozens injured. Prime Minister Theresa May convened an emergency security cabinet session Sunday to deal with the crisis. (Stefan Rousseau/PA via AP)

Facebook says it alerts law enforcement if it sees a threat of an imminent attack or harm to someone. It also seeks out potential terrorist accounts by tracing the "friends" of an account that has been removed for terrorism.

Q. What are technology companies refusing to do when it comes to terrorist content?

A. After the 2015 mass shooting in San Bernardino, California, and again after the Westminster Bridge attack, the U.S. and U.K.

governments sought access to encrypted—or password-protected—communication between the terrorists who carried out the attack. In both cases, the tech companies involved—Apple and WhatsApp—refused, although the governments eventually managed to go around the companies and get the information they wanted.

Tech companies say encryption is vital and compromising it won't just stop terrorists. Encryption also protects bank accounts, credit card transactions and all kinds of other information that people want to keep private. But others—including former FBI Director James Comey and Democratic Sen. Dianne Feinstein of California—have argued that the inability to access encrypted data is a threat to security. Feinstein has introduced a bill to give the government so-called "back door" access to encrypted data.

An armed Police officer looks through his weapon on London Bridge in London, Saturday, June 3, 2017. British police said they were dealing with "incidents" on London Bridge and nearby Borough Market in the heart of the British capital Saturday, as witnesses reported a vehicle veering off the road and hitting several pedestrians. (Dominic Lipinski/PA via AP)

Q. Shouldn't tech companies be forced to share encrypted information if it could protect national security?

A. Richard Forno, who directs the graduate cybersecurity program at the

University of Maryland, Baltimore County, said weakening encryption won't make people safer. Terrorists will simply take their communications deeper underground by developing their own cyber channels or even reverting to paper notes sent by couriers, he said.

"It's playing whack-a-mole," he said. "The bad guys are not constrained by the law. That's why they're bad guys."

But Erik Gordon, a professor of law and business at the University of Michigan, says society has sometimes determined that, in times of war, the government can intrude in ways it might not normally. He imagines a system where law enforcement would have to ask a judge for a warrant to retrieve encrypted information.

London Bridge, left, and The Shard are seen following an attack in central London, Saturday, June 3, 2017. Terrorism struck at the heart of London, police said Sunday, after a vehicle veered off the road and mowed down pedestrians on

London Bridge and gunshots rang out amid reports of knife attacks at nearby Borough Market. (Yui Mok/PA via AP)

"If we get to the point where we say, 'Privacy is not as important as staying alive,' I think there will be some setup which will allow the government to breach privacy," he said.

Q. Is it really the tech companies' job to police the internet and remove content?

A. Tech companies have accepted that this is part of their mission. In a Facebook post earlier this year, CEO Mark Zuckerberg said the company was developing artificial intelligence so its computers can tell the difference between news stories about terrorism and terrorist propaganda. "This is technically difficult as it requires building AI that can read and understand news, but we need to work on this to help fight terrorism worldwide," Zuckerberg said.

But Ross Anderson, a professor of security engineering at the University of Cambridge, says blaming Facebook or Google for the spread of terrorism is like blaming the mail system or the phone company for Irish Republican Army violence 30 years ago. Anderson says instead of working together to censor the internet, governments and companies should focus on working together to share information more quickly.

Police sniffer dogs on London Bridge after an incident in central London, Saturday, June 3, 2017. British police said they were dealing with "incidents" on London Bridge and nearby Borough Market in the heart of the British capital Saturday, as witnesses reported a vehicle veering off the road and hitting several pedestrians. (Dominic Lipinski/PA via AP)

Former Secretary of State John Kerry also worries about placing too much blame on the internet instead of the underlying causes of violence.

"The bottom line is that in too many places, in too many parts of the world, you've got a large gap between governance and people and between the opportunities those people have," Kerry said Sunday on NBC's "Meet the Press."

Armed police on St Thomas Street, London, Sunday June 4, 2017, near the scene of Saturday night's terrorist incident on London Bridge and at Borough Market. Several people were killed in the terror attack at the heart of London and dozens injured. Prime Minister Theresa May convened an emergency security cabinet session Sunday to deal with the crisis. (Dominic Lipinski/PA via AP)

© 2017 The Associated Press. All rights reserved.

Citation: Q&A: Internet extremism and how to combat it (2017, June 4) retrieved 25 April 2024 from https://phys.org/news/2017-06-qa-internet-extremism-combat.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.