UK’s GCHQ spy centre seeks new powers to circumvent encryption

Thomas Scripps
6 July 2019

The Government Communications Headquarters (GCHQ) has proposed that tech companies allow state spies into encrypted chats and calls. The new surveillance measures, known as a “ghost protocol,” would allow a government agent to “sit in” on ostensibly secure private conversations without the knowledge of other participants.

This news comes just days after MI5 and GCHQ’s admission that they are acting illegally in their use of bulk data, gathered by intruding into the lives of millions of innocent people.

GCHQ spokesmen defended the demand for a ghost protocol with the Orwellian argument that such a method would maintain the security and privacy of encrypted communication, because the encryption itself would not be broken—just made irrelevant. Ian Levy, technical director of the UK’s national cyber security centre, and Crispin Robinson, head of cryptanalysis, said preposterously that the proposal was “no more intrusive than the virtual crocodile clips” used to wiretap non-encrypted communications.

Over 50 companies, organisations and security experts have signed an open letter to the UK government condemning GCHQ’s plans as a “serious threat” to digital security and human rights. The letter, co-authored by Google, Apple, WhatsApp, Microsoft, Liberty, Privacy International and others, explains that “to achieve this result, their proposal requires two changes to systems that would seriously undermine user security and trust.

“First, it would require service providers to surreptitiously inject a new public key into a conversation in response to a government demand. This would turn a two-way conversation into a group chat where the government is the additional participant, or add a secret government participant to an existing group chat.

“Second, in order to ensure the government is added to the conversation in secret, GCHQ’s proposal would require messaging apps, service providers, and operating systems to change their software so that it would 1) change the encryption schemes used, and/or 2) mislead users by suppressing the notifications that routinely appear when a new communicant joins a chat.”

Levy could barely contain his frustration with this criticism, writing with disdain, “We welcome this response to our request for thoughts on exceptional access to data—for example to stop terrorists.”

The reference to terrorism is a fraud. GCHQ’s ever-expanding arsenal of surveillance techniques is not fundamentally a response to the extremist networks that are often political instruments of Western imperialism and its allies. It is the ruling class’ answer to immense social discontent and unrest across the globe, which communication via the internet helps to give international unity and political direction.

GCHQ’s in-house historian Tony Comer explained in a recent interview with the *Financial Times*, “the arrival of the public internet was the bigger event” for GCHQ than the end of the Cold War.

He did not explain the reason for this was that the invention and expansion of the internet had a great democratising effect. It undermined the stranglehold on news held by the rich and enabled the world’s population to talk to one another. Above all, these developments benefited the international working class, whose common struggle against inequality, dictatorship and war could now be discussed and organised across countries and continents vastly more easily than ever before.

Intelligence agencies like GCHQ and the US National

Security Agency (NSA) are growing to monstrous proportions to counteract these developments.

The UK spy station will expand its 6,000-strong staff by 600 to 800 people this year and will open a new base in Manchester. The government has committed £22 million to supporting the £650 million development of a "Cyber Park," occupying 326 acres to the immediate west of GCHQ. The Park, which is set to create 7,000 new jobs and 1,200 new homes, will be based around the intelligence organisation's newly created Innovation Centre.

GCHQ's field of potential targets expands well beyond the domestic population. In the next few months, Britain will establish a 2,000-strong offensive cyber force, designed to attack foreign populations.

Just last year, according to Reuters, hackers using software called Regin linked to the "Five Eyes" intelligence alliance—made up of the United States, Britain, Australia, New Zealand and Canada—attacked the Russian internet search company, Yandex. Yandex serves approximately 75 percent of the Russian population. Sources told Reuters that the hackers appeared to be searching for technical information explaining how Yandex authenticates user accounts. This would help a spy agency impersonate a Yandex user and access their private messages.

The *Intercept* previously identified Regin as the software used during an attack on the Belgian communications company, Belgacom, in the early 2010s, carried out by GCHQ and the NSA.

The ultimate goal of the Five Eyes is to turn the internet into a giant surveillance network. Any lack of compliance, however slight, is denounced. Mozilla's plans for an encrypted web browser—which would bypass the government's method of blocking websites through Internet Service Providers—and declaration that it would list blocked sites was deemed "completely unacceptable" by GCHQ.

Labour's deputy leader Tom Watson wrote to Conservative Culture Secretary Jeremy Wright saying browsers like Mozilla's "threaten to unravel the Government's plans to protect the public from online harms… the Government have been slow to wake up to the threat [of encrypted browsers]. I am deeply troubled that is further evidence that tech giants continue to see themselves as above the law."

These conflicts do not alter the fact that the billionaire owners of the big tech companies do not care one iota for their users' democratic rights. Their only concern is that the undisguised authoritarianism of state intelligence agencies will exacerbate the growing distrust of the world's population for corporate news and communication platforms. Having witnessed the collapse of public trust in the traditional mainstream media, they are eager to more carefully manage their reputations—the better to enable government censorship and surveillance.

A passage from the open letter against the "ghost protocol" signed by Google, Apple et al. reads, "The overwhelming majority of users rely on their confidence in reputable providers to perform authentication functions and verify that the participants in a conversation are the people they think they are, and only those people. The GCHQ's ghost proposal completely undermines this trust relationship."

As government partnerships with Google, Facebook and Amazon make clear, imperialist states and Silicon Valley executives are working with the same dictatorial objectives in mind. GCHQ's illegal operations against the world's population can only be defeated as part of a broader movement in defence of democratic rights, based on a global struggle of workers and youth fighting for socialism.