Does the UK need or even want a 'Great British Firewall'?

September 20 2016, by Keith Martin

Credit: CC0 Public Domain

You've probably heard of the Great Firewall of China, the virtual fortification that allows the Chinese government to monitor and restrict internet traffic to and from the world's most populous nation. Well, the

cyber-security chief of the UK Government Communication Headquarters (GCHQ) has suggested early plans for what sounds rather like a "Great British Firewall". Privacy groups immediately sounded the alarm that it might pose a risk to freedom of speech, and offer the potential for Britain's secret services to get up to no good. So what exactly is GCHQ proposing and should we be worried?

Firewalls are standard tools for computer defence. They are essentially filters which can control what traffic enters and leaves a network. You are probably protected by a firewall right now, at your workplace or at home, that runs either on your computer's operating system or on the hardware that provides your connection to the internet.

A firewall can be configured to reject certain types of traffic deemed undesirable or potentially harmful. This might be a connection request from an untrustworthy source, such as a web address known to harbour hackers or spammers, for example. Or it could block a file that looks like it might contain a computer virus or other malware. While deflecting this sort of undesirable traffic the firewall allows standard traffic such as web browsing and email to pass through.

Who decides what gets in and what doesn't? This is normally the job of whoever manages the network, be that an IT professional working at a company, or you (or your ISP) at home. The policy this manager applies determines what is accepted and what is rejected, so anyone relying on the firewall to be effective needs to trust that this policy is acting in their best interest.

What GCHQ seems to be proposing is a large-scale, nationwide firewall behind which any UK organisation could sit. The intention appears to be that organisations that are central to Britain's national security would be required to operate behind this firewall, while other organisations big and small could opt-in.

There are too few details at the moment, but this seems like a classic case of who watches the watchman?. If GCHQ is to be the guard that chooses what is deemed "good" or "bad", then the debate about the merits of a Great British Firewall is really a debate about whether there is trust in GCHQ.

Wearing two hats

GCHQ has two roles that don't always sit particularly comfortably together. Most fundamentally it leads Britain's signals intelligence, which means essentially that GCHQ eavesdrops on communications for the UK government and the armed forces. Few would argue with the value of spying on enemies during wartime. What has proved much more controversial is GCHQ's capabilities and activities revealed by former National Security Agency contractor Edward Snowden, including the bulk collection of communication data relating to everyone's online activities. GCHQ has been accused of conducting mass surveillance, and there is no doubt that these revelations have damaged the reputation of it and the security services among some in the UK and worldwide.

However, GCHQ's other important role is as a source of cyber-security expertise. It helped develop the National Cyber Security Strategy and has been working hard to implement it alongside the UK government, industry and academia. In October 2016, the National Cyber Security Centre will open and will oversee many of these activities. GCHQ employs many cyber-security specialists and is supporting the training of even more. Put simply, there is a lot of cyber-security expertise in GCHQ.

So if there is to be a Great British Firewall, GCHQ seems like the logical organisation to provide it. Private companies will be given the opportunity to choose whether to trust GCHQ as their firewall guard. So long as they are genuinely free to make this decision for themselves, and

their customers are aware of this relationship, then this might well be workable. Achieving security in cyberspace inevitably requires placing faith in some organisations – why not trust one that knows a great deal about cyber-security?

Of course there is a precedent: the use of the Great Firewall of China by the Chinese government to censor internet content is infamous. Through constant tight monitoring of internet traffic the government blocks access to websites, filters or blocks searches for keywords, and monitors the population's interactions in cyberspace. There is no doubt that the Great Firewall of China stifles freedom of speech and is used in an authoritarian, anti-democratic fashion. Other nations are also known to interfere with the global Domain Name System (DNS) that links domain names (such as theconversation.com) to the actual internet addresses used by the web servers for those sites. Filtering out DNS requests for certain domains and dropping them essentially prevents those domains from being accessed – certainly not in the spirit of the global open internet that many desire.

Is GCHQ proposing something equivalent? I suspect not, as the UK has a very different view of human rights and internet governance than in China. But there is a fine line between having the power to censor the internet, and choosing to implement that power. Returning to GCHQ's two functions, while I suspect the security function of GCHQ has good intentions, the intelligence function of GCHQ does not have an unblemished record in this area. Something to think about before choosing to hide behind the Great British Firewall.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation