GlobalResearch
Center for Research on Globalization

Hacking Online Polls and Other Ways British Spies Seek to Control the Internet

By Glenn Greenwald
Global Research, July 16, 2014
The Intercept 14 July 2014

Region: Europe
Theme: Intelligence

The secretive British spy agency GCHQ has developed covert tools to seed the internet with false information, including the ability to manipulate the results of online polls, artificially inflate pageview counts on web sites, "amplif[y]" sanctioned messages on YouTube, and censor video content judged to be "extremist." The capabilities, detailed in documents provided by NSA whistleblower Edward Snowden, even include an old standby for pre-adolescent prank callers everywhere: A way to connect two unsuspecting phone users together in a call.

The tools were created by GCHQ's Joint Threat Research Intelligence Group (JTRIG), and constitute some of the most startling methods of propaganda and internet deception contained within the Snowden archive. Previously disclosed documents have detailed JTRIG's use of "fake victim blog posts," "false flag operations," "honey traps" and psychological manipulation to target online activists, monitor visitors to WikiLeaks, and spy on YouTube and Facebook users.

But as the U.K. Parliament today debates a fast-tracked bill to provide the government with greater surveillance powers, one which Prime Minister David Cameron has justified as an "emergency" to "help keep us safe," a newly released top-secret GCHQ document called "JTRIG Tools and Techniques" provides a comprehensive, birds-eye view of just how underhanded and invasive this unit's operations are. The document—available in full here—is designed to notify other GCHQ units of JTRIG's "weaponised capability" when it comes to the dark internet arts, and serves as a sort of hacker's buffet for wreaking online havoc.

The "tools" have been assigned boastful code names. They include invasive methods for online surveillance, as well as some of the very techniques that the U.S. and U.K. have harshly prosecuted young online activists for employing, including "distributed denial of service" attacks and "call bombing." But they also describe previously unknown tactics for manipulating and distorting online political discourse and disseminating state propaganda, as well as the apparent ability to actively monitor Skype users in real-time—raising further questions aboutthe extent of Microsoft's cooperation with spy agencies or potential vulnerabilities in its Skype's encryption. Here's a list of how JTRIG describes its capabilities:

- "Change outcome of online polls" (UNDERPASS)
- "Mass delivery of email messaging to support an Information Operations campaign" (BADGER) and "mass delivery of SMS messages to support an

Information Operations campaign" (WARPARTH)

• "Disruption of video-based websites hosting extremist content through concerted target discovery and content removal." (SILVERLORD)

• "Active skype capability. Provision of real time call records (SkypeOut and SkypetoSkype) and bidirectional instant messaging. Also contact lists." (MINIATURE HERO)

• "Find private photographs of targets on Facebook" (SPRING BISHOP)

• "A tool that will permanently disable a target's account on their computer" (ANGRY PIRATE)

• "Ability to artificially increase traffic to a website" (GATEWAY) and "ability to inflate page views on websites" (SLIPSTREAM)

• "Amplification of a given message, normally video, on popular multimedia websites (Youtube)" (GESTATOR)

• "Targeted Denial Of Service against Web Servers" (PREDATORS FACE) and "Distributed denial of service using P2P. Built by ICTR, deployed by JTRIG" (ROLLING THUNDER)

• "A suite of tools for monitoring target use of the UK auction site eBay (www.ebay.co.uk)" (ELATE)

• "Ability to spoof any email address and send email under that identity" (CHANGELING)

• "For connecting two target phone together in a call" (IMPERIAL BARGE)

While some of the tactics are described as "in development," JTRIG touts "most" of them as "fully operational, tested and reliable." It adds: "We only advertise tools here that are either ready to fire or very close to being ready."

And JTRIG urges its GCHQ colleagues to think big when it comes to internet deception: "Don't treat this like a catalogue. If you don't see it here, it doesn't mean we can't build it."

The document appears in a massive Wikipedia-style archive used by GCHQ to internally discuss its surveillance and online deception activities. The page indicates that it was last modified in July 2012, and had been accessed almost 20,000 times.

GCHQ refused to provide any comment on the record beyond its standard boilerplate, in which it claims that it acts "in accordance with a strict legal and policy framework" and is subject to "rigorous oversight." But both claims are questionable.

British watchdog Privacy International has filed pending legal action against GCHQ over the agency's use of malware to spy on internet and mobile phone users. Several GCHQ memos published last fall by *The Guardian* revealed that the agency was eager to keep its activities secret not to protect national security, but because "our main concern is that references to agency practices (ie, the scale of interception and deletion) could lead to damaging public debate which might lead to legal challenges against the current regime." And an EU parliamentary inquiry earlier this year concluded that GCHQ activities were likely illegal.

As for oversight, serious questions have been raised about whether top national security officials even know what GCHQ is doing. Chris Huhne, a former cabinet minister and member of the national security council until 2012, insisted that ministers were in "utter ignorance" about even the largest GCHQ spying program, known as Tempora—not to mention "their extraordinary capability to hoover up and store personal emails, voice contact, social networking activity and even internet searches." In an October *Guardian* op-ed, Huhne wrote that "when it comes to the secret world of GCHQ and the [NSA], the depth of my 'privileged information' has been dwarfed by the information provided by Edward Snowden to *The Guardian*."
