http://www.nbcnews.com/news/investigations/snowden-docs-british-spies-used-sex-dirty-tricks-n23091

# Snowden Docs: British Spies Used Sex and 'Dirty Tricks'

By Matthew Cole, Richard Esposito, Mark Schone and Glenn Greenwald, Special Contributor

2/7/2014

British spies have developed “dirty tricks” for use against nations, hackers, terror groups, suspected criminals and arms dealers that include releasing computer viruses, spying on journalists and diplomats, jamming phones and computers, and using sex to lure targets into “honey traps.”

Documents taken from the National Security Agency by Edward Snowden and exclusively obtained by NBC News describe techniques developed by a secret British spy unit called the Joint Threat Research and Intelligence Group (JTRIG) as part of a growing mission to go on offense and attack adversaries ranging from Iran to the hacktivists of Anonymous. According to the documents, which come from presentations prepped in 2010 and 2012 for NSA cyber spy conferences, the agency’s goal was to “destroy, deny, degrade [and] disrupt” enemies by “discrediting” them, planting misinformation and shutting down their communications.

Both PowerPoint presentations describe “Effects” campaigns that are broadly divided into two categories: cyber attacks and propaganda operations. The propaganda campaigns use deception, mass messaging and “pushing stories” via Twitter, Flickr, Facebook and YouTube. JTRIG also uses “false flag” operations, in which British agents carry out online actions that are designed to look like they were performed by one of Britain’s adversaries.

The spy unit’s cyber attack methods include the same “denial of service” or DDOS tactic used by computer hackers to shut down government and corporate websites.

Other documents taken from the NSA by Snowden and previously published by NBC News show that JTRIG, which is part of the NSA's British counterpart, the cyber spy agency known as GCHQ, used a DDOS attack to shut down Internet chat rooms used by members of the hacktivist group known as Anonymous.

Civil libertarians said that in using a DDOS attack against hackers the British government also infringed free speech by individuals not involved in any illegal hacking, and may have blocked other websites with no connection to Anonymous. While GCHQ defends the legality of its actions, critics question whether the agency is too aggressive and its mission too broad.

Eric King, a lawyer who teaches IT law at the London School of Economics and is head of research at Privacy International, a British civil liberties advocacy group, said it was "remarkable" that the British government thought it had the right to hack computers, since none of the U.K.'s intelligence agencies has a "clear lawful authority" to launch their own attacks.

"GCHQ has no clear authority to send a virus or conduct cyber attacks," said King. "Hacking is one of the most invasive methods of surveillance." King said British cyber spies had gone on offense with "no legal safeguards" and without any public debate, even though the British government has criticized other nations, like Russia, for allegedly engaging in cyber warfare.

But intelligence officials defended the British government's actions as appropriate responses to illegal acts. One intelligence official also said that the newest set of Snowden documents published by NBC News that describe "Effects" campaigns show that British cyber spies were "slightly ahead" of U.S. spies in going on offense against adversaries, whether those adversaries are hackers or nation states. The documents also show that a one-time signals surveillance agency, GCHQ, is now conducting the kinds of active espionage operations that were once exclusively the realm of the better-known British spy agencies MI5 and MI6.

Intelligence officials defended the British government's actions as appropriate responses to illegal acts.

According to notes on the 2012 documents, a computer virus called Ambassadors Reception was "used in a variety of different areas" and was "very effective." When sent to adversaries, says the presentation, the virus will "encrypt itself, delete all emails, encrypt all files, make [the] screen shake" and block the computer user from logging on.

But the British cyber spies' operations do not always remain entirely online. Spies have long used sexual "honey traps" to snare, blackmail and influence targets. Most often, a male target is led to believe he has an opportunity for a romantic relationship or a sexual liaison with a woman, only to find that the woman is actually an intelligence operative. The Israeli government, for example, used a "honey trap" to lure nuclear technician Mordechai Vanunu from London to Rome. He expected an assignation with a woman, but instead was kidnapped by Israel agents and taken back to Israel to stand trial for leaking nuclear secrets to the media.

The version of a "honey trap" described by British cyber spies in the 2012 PowerPoint presentation sounds like a version of Internet dating, but includes physical encounters.

The version of a "honey trap" described by British cyber spies in the 2012 PowerPoint presentation sounds like a version of Internet dating, but includes physical encounters. The target is lured "to go somewhere on the Internet, or a physical location" to be met by "a friendly face." The goal, according to the presentation, is to discredit the target.

A "honey trap," says the presentation, is "very successful when it works." But the documents do not give a specific example of when the British government might have employed a honey trap.

An operation described in the 2010 presentation also involves in-person surveillance. "Royal Concierge" exploits hotel reservations to track the whereabouts of foreign diplomats and send out "daily alerts to analysts working on governmental hard targets." The British government uses the program to try to steer its quarry to "SIGINT friendly" hotels, according to the presentation, where the targets can be monitored electronically – or in person by British operatives.

A slide from the documents taken from the NSA by Edward Snowden and obtained by NBC News.

The existence of the Royal Concierge program was first reported by the German magazine Der Spiegel in 2013, which said that Snowden documents showed that British spies had monitored bookings of at least 350 upscale hotels around the world for more than three years "to target, search and analyze reservations to detect diplomats and government officials."

According to the documents obtained by NBC News, the intelligence agency uses the information to spy on human targets through "close access technical operations," which can include listening in on telephone calls and tapping hotel computers as well as sending intelligence officers to observe the targets in person at the hotels. The documents ask, "Can we influence hotel choice? Can we cancel their visits?"

The 2010 presentation also describes another potential operation that would utilize a technique called "credential harvesting" to select journalists who could be used to spread information. According to intelligence sources, spies considered using electronic snooping to identify non-British journalists who would then be manipulated to feed information to the target of a covert campaign. Apparently, the journalist's job would provide access to the targeted individual, perhaps for an interview. The documents do not specify whether the journalists would be aware or unaware that they were being used to funnel information.

The executive director of the Committee to Protect Journalists, Joel Simon, said that the revelation about "credential harvesting" should serve as a "wake up call" to journalists that intelligence agencies can monitor their communications. Simon also said that governments put all journalists at risk when they use even one for an intelligence operation.

"All journalists generally are then vulnerable to the charge that they work at the behest of an intelligence agency," said Simon.

The journalist operation was never put into action, according to sources, but other techniques described in the documents, like the Ambassadors Reception computer virus and the jamming of phones and computers, have definitely been used to attack adversaries.

In Afghanistan, according to the 2012 presentation, the British used a blizzard of text messages, phone calls and faxes to "significantly disrupt" Taliban communications, with texts and calls programmed to arrive every minute.

In a set of operations that intelligence sources say were designed to stop weapons transactions and nuclear proliferation, JTRIG used negative information to attack private companies, sour business relationships and ruin deals.

The British cyber spies also used blog posts and information spread via blogs in an operation against Iran.

Other effective methods of cyber attack listed in the documents include changing photos on social media sites and emailing and texting colleagues and neighbors unsavory information. The documents do not give examples of when these techniques were used, but intelligence sources say that some of the methods described have been used by British intelligence to help British police agencies catch suspected criminals.

The documents from 2010 note that "Effects" operations, GCHQ's offensive push against Britain's enemies, had become a "major part" of the spy agency's business.

The presentation from 2012 illustrates that two years later GCHQ had continued to shift its workload from defending U.K. cyber networks to going on offense -- targeting specific people or governments. The British government's intelligence apparatus, which also includes MI5 and MI6, had a role in the 2010 Stuxnet computer virus attack on Iran's nuclear facilities, according to sources at two intelligence agencies.

GCHQ would not comment on the newly published documents or on JTRIG's "Effects" operations. It would neither confirm nor deny any element of this report, which is the agency's standard policy. In a statement, a GCHQ spokesperson emphasized that the agency operated within the law.

"All of GCHQ's work is carried out in accordance with a strict legal and policy framework," said the statement, "which ensure[s] that our activities are authorized, necessary and proportionate, and that there is rigorous oversight, including from the Secretary of State, the Interception and Intelligence Services Commissioners and the Parliamentary Intelligence and Security Committee. All of our operational processes rigorously support this position."