GlobalResearch
Center for Research on Globalization

What Exactly Are the Spy Agencies Doing with their Bag of Dirty Tricks?

Specific Examples of what they May Be Doing

By Washington's Blog
Global Research, July 16, 2014
Washington's Blog 15 July 2014

Region: Europe
Theme: Intelligence, Law and Justice, Police State & Civil Rights

Newly-released documents from Edward Snowden show that the British spy agency GCHQ has developed numerous offensive digital tools.

But what exactly are they doing with these dirty tricks?

We think it's important to think through the specific possibilities, in order to gain an understanding of how pernicious these manipulations can be.

We quote verbatim (in black) the names and descriptions of some of these tools – some of which Glenn Greenwald didn't highlight in his report. We then provide descriptions in blue of potential misuses of such tools.

Then we discuss how likely such misuses really are.

Tools and potential misuses

Here are the actual dirty tricks in the British spy agencies toolkit, with hypothetical examples of potential misuses ...

CHANGELING: Ability to spoof any email address and send email under that identity. *Fake an email from a privacy advocate to make it look like he's proposing terrorism.*

SCRAPHEAP CHALLENGE: Perfect spoofing of emails from Blackberry targets. *Fake an email from an opponent of bank bailouts to make it look like she's proposing bombing a bank.*

BURLESQUE: The capacity to send spoofed SMS messages. *Fake a message from an an anti-war pacifist to make it look like he's advocating sabotage of a military base.*

IMPERIAL BARGE : For connecting two target phone together in a call. *Fake a telephone connection to make it look like an opponent of genetically modified foods spoke with a leader of Al Qaeda.*

BADGER : Mass delivery of email messaging to support an Information Operations campaign. *Send out a fake, mass email pretending to be from a whistleblower "admitting" that he's mentally unstable, disgruntled, dishonest and vindictive.*

WARPATH: Mass delivery of SMS messages to support an Information Operations campaign. *Send out a fake, mass message pretending to be from a whistleblower "admitting" he's a*

Russian spy.

SPACE ROCKET: A programme covering insertion of media into target networks. *Insert a fake video calling for jihad on a the website of a moderate American Muslim lawyer.*

CLEAN SWEEP Masquerade Facebook Wall Posts for individuals or entire countries. *Put up a bunch of fake wall posts praising the Islamic State on the Facebook page of a reporter giving first-hand reports of what's really happening in a country that the U.S. has targeted for regime change.*

HAVOK Real-time website cloning technique allowing on-the-fly alterations. *Hack the website of a state politician critical of those who ignore the Constitution and post fake calls for terrorism against Washington, D.C.*

SILVERLORD: Disruption of video-based websites hosting extremist content through concerted target discovery and content removal. *Disrupt websites hosting videos espousing libertarian views.*

SUNBLOCK: Ability to deny functionality to send/receive email or view material online. *Block the emails and web functionality of a government insider who is about to go public on wrongdoing.*

ANGRY PIRATE: A tool that will permanently disable a target's account on their computer. *Disable the accounts of an activist working for clean food and water.*

PREDATORS FACE: Targeted Denial Of Service against Web Servers. *Take down a website which is disclosing hard-hitting information on illegal government actions.*

UNDERPASS: Change outcome of online polls. *Change the results of an online poll from one showing that the American people overwhelmingly oppose a new war which is unnecessary for the defense of America's national security to showing support for it.*

GATEWAY: Ability to artificially increase traffic to a website. *Make a website calling for more surveillance against the American people appear hugely popular.*

BOMB BAY: The capacity to increase website hits, rankings. *Make it look like a hate site is popular among a targeted local population which actually despises its views.*

SLIPSTREAM: Ability to inflate page views on websites. *Make it appear that an article saying that the Constitution is "outdated" and "unrealistic in the post-9/11 world" is widely popular.*

GESTATOR: Amplification of a given message, normally video, on popular multimedia websites (Youtube). *Make a propaganda video – saying that we should just relax and trust Big Brother – go viral.*

What is the likelihood of misuse?

We don't know which of the above hypothetically forms of misuse are actually occurring. However, as we wrote in February:

> We've warned since 2009 (and see this) that the government could be launching cyber "false flag attacks" in order to justify a crackdown on the

Internet and discredit web activists.

A new report from NBC News – based on documents leaked by Edward Snowden – appear to confirm our fears, documenting that Britain's GCHQ spy agency has carried out cyber false flag attacks:

> In another document taken from the NSA by Snowden and obtained by NBC News, a JTRIG official said the unit's mission included computer network attacks, disruption, "Active Covert Internet Operations," and "Covert Technical Operations." Among the methods listed in the document were jamming phones, computers and email accounts and masquerading as an enemy in a "false flag" operation. The same document said GCHQ was increasing its emphasis on using cyber tools to attack adversaries.

Later that month, we noted:

> A new report from NBC News shows that the British spy agency used "false flag attacks" and other dirty tricks:
>
> > 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."
> >
> > ***
> >
> > The agency's goal was to "destroy, deny, degrade [and] disrupt" enemies by "discrediting" them, planting misinformation and shutting down their communications.
>
> Sound familiar? It should:
>
> > Between 1956 and 1971, the FBI operated a program known as COINTELPRO, for Counter Intelligence Program. Its purpose was to interfere with the activities of the organizations and individuals who were its targets or, in the words of long-time FBI Director J. Edgar Hoover, to "expose, disrupt, misdirect, discredit or otherwise neutralize" them.
>
> NBC continues:
>
> > [The agency] 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.
> >
> > ***
> >
> > JTRIG used negative information to attack private companies, sour business relationships and ruin deals.

> ***
>
> Changing photos on social media sites and emailing and texting colleagues and neighbors unsavory information.

And reporter Glenn Greenwald noted that Snowden documents showed:

> Western intelligence agencies are attempting to manipulate and control online discourse with extreme tactics of deception and reputation-destruction.
>
> ***
>
> These agencies are attempting to control, infiltrate, manipulate, and warp online discourse …. Among the core self-identified purposes … are two tactics: (1) to inject all sorts of false material onto the internet in order to destroy the reputation of its targets; and (2) to use social sciences and other techniques to manipulate online discourse and activism to generate outcomes it considers desirable. To see how extremist these programs are, just consider the tactics they boast of using to achieve those ends: "false flag operations" (posting material to the internet and falsely attributing it to someone else), fake victim blog posts (pretending to be a victim of the individual whose reputation they want to destroy), and posting "negative information" on various forums.
>
> ***
>
> The discussion of many of these techniques occurs in the context of using them in lieu of "traditional law enforcement" against people suspected (but not charged or convicted) of ordinary crimes or, more broadly still, "hacktivism", meaning those who use online protest activity for political ends.
>
> The title page of one of these documents reflects the agency's own awareness that it is "pushing the boundaries" by using "cyber offensive" techniques against people who have nothing to do with terrorism or national security threats, and indeed, centrally involves law enforcement agents who investigate ordinary crimes…. no conceivable connection to terrorism or even national security threats.
>
> ***
>
> Then there is the use of psychology and other social sciences to not only understand, but shape and control, how online activism and discourse unfolds. Today's newly published document touts the work of GCHQ's "Human Science Operations Cell", devoted to "online human intelligence" and "strategic influence and disruption"….***
>
> Under the title "Online Covert Action", the document details a variety of means to engage in "influence and info ops" as well as "disruption and computer net attack", while dissecting how human beings can be manipulated using "leaders", "trust, "obedience" and "compliance":

The U.S. government is also spending millions to figure out how to manipulate social media to promote propaganda and stifle dissenting opinions.

And *any* criticism of government policies is now considered "extremist" and potential terrorism. The government also considers anyone who tries to protect himself from government oppression and to claim his Constitutional rights a "extremist". This is not

entirely new ... the CIA director relabeled "dissidents" as "terrorists" so he could continue spying on them in 1972. Indeed – for 5,000 years straight – mass surveillance of one's own people has *always* been used to crush dissent.

The NSA is now also collecting and retaining the most intimate personal details of Americans, including nude and suggestive pictures and medical and financial records ... even though they admittedly have *no conceivable* security value.

You may think you have "nothing to hide", but you're breaking the law numerous times every day ... without even knowing it (update).

Indeed, top NSA whistleblowers say that the NSA is blackmailing and harassing opponents with information that it has gathered – potentially even high-level politicians – just like FBI head J. Edgar Hoover blackmailed presidents and Congressmen.

Moreover, if the NSA takes a dislike to someone, it can *frame* them. This has been CONFIRMED by top NSA whistleblowers.

And the following facts make it likely that British and U.S. spy agencies are misusing their powers:

- The government and big banks joined forces to violently beat up peaceful protesters speaking out against bank corruption. Organizers of the protests say that their emails were blocked

- The NSA engages in offensive attacks ("we hack everyone everywhere"). And private corporations – big banks – will likely get the power to declare cyber war. Similarly, the largest German newspaper alleges that the U.S. government helped Monsanto attack the computers of activists opposed to genetically modified food

- The U.S. government at times uses national security powers to protect things *other* than the interests of the American people – such as globalism or global corporations (and may be putting foreign countries' needs over our own) – and relies on countries which don't even *have* a Constitution to justify unconstitutional acts. NSA's recent actions are motivated by a power grab, not fighting terrorism

- Top NSA whistleblowers Bill Binney and Thomas Drake both say that the U.S. has become a *police state.* They say that the U.S. government has become like the Stasis or Soviets, Binney says that the NSA has become like "J. Edgar Hoover on super steroids" and that "the ultimate goal of the NSA is total population control"

Postscript: We don't know whether or not the spy agencies are misusing their bag of tricks in the *specific* ways discussed above (in blue). The whole point is that they have been caught lying time and again about what they're doing, they're running amok with no oversight, and the fact that they *could* be targeting government critics shows how bad things have become.
