

GCHQ DDOS HACKERS HANG OUT WITH NSA'S AUDIT-FREE TECHIES

Yesterday, I noted NBC's report that GCHQ conducted a DDoS attack against Anonymous IRC chat.

There's a subtle point that deserves more attention: GCHQ presented the underlying Powerpoint to NSA's SIGDEV conference.

The documents, from a PowerPoint presentation prepared for a 2012 NSA conference called SIGDEV, show that the unit known as the Joint Threat Research Intelligence Group, or JTRIG, boasted of using the DDoS attack – which it dubbed Rolling Thunder – and other techniques to scare away 80 percent of the users of Anonymous internet chat rooms.

[snip]

In the presentation on hacktivism that was prepared for the 2012 SIGDEV conference, one official working for JTRIG described the techniques the unit used to disrupt the communications of Anonymous and identify individual hacktivists, including some involved in Operation Payback. Called "Pushing the Boundaries and Action Against Hacktivism," the presentation lists Anonymous, Lulzsec and the Syrian Cyber Army among "Hacktivist Groups," says the hacktivists' targets include corporations and governments, and says their techniques include DDoS and data theft.

SIGDEV is NSA's term for the agency's efforts to develop new signals intelligence techniques and sources. Thus, GCHQ presented the attack as the cutting edge of what NSA does.

Goodie.

But remember: NSA's SIGDEV analysts have access to raw data outside of normal channels. This shows up repeatedly in the primary orders for the dragnet. And, as Bart Gellman noted (and I elaborated on here), Obama specifically exempted these folks from his Presidential Policy Directive limiting our spying (though his PPD did say foreigners could be spied on for cybersecurity reasons).

In other words, the people GCHQ boasted of their attack on Anonymous to are the people who have some of the least oversight within NSA.