THE STATE MONOPOLY ON DDOS

One reason I harped on the way Ken Dilanian referred to the "official position" that hacking other governments was acceptable was because I suspected the government does what NBC just reported they do: engage in hacking against other targets, in this case, hackers like Anonymous.

> [A] division of Government Communications Headquarters Communications (GCHQ), the British counterpart of the NSA, shut down communications among Anonymous hacktivists by launching a "denial of service" (DDOS) attack — the same technique hackers use to take down bank, retail and government websites — making the British government the first Western government known to have conducted such an attack.

As I noted on Twitter, the report that GCHQ targeted Anonymous should raise questions (that have already been raised) whether either GCHQ or NSA was behind the DDoS attack on noted publishing site WikiLeaks in 2010.

So the NSA (and GCHQ) believe some hacks are legitimate and some are not. But in addition, both are effectively asserting that the state should have a monopoly on hacking, just as it asserts a monopoly on violence. As some of the people involved have been commenting on Twitter, they got charged for DDoSing, even as the Brits were engaging in precisely the same behavior. Particularly troubling, there's no indication NSA or GCHQ believe they need warrants to exercise their monopoly on hacks against their own citizens (FBI has in the past gotten a warrant to bring down a botnet, so there is precedent).

Of course, therein lies part of the problem:

that intelligence is bleeding into law enforcement, and the tools of inter-state spying are being wielded against criminals (and dissidents).

None of this is surprising. It arises directly out of the way the government has gone after terrorists, and this treatment of an IRC channel is directly parallel to the same kind of guilt by association used against terrorists.