CYBERCOMMAND TURNS ITS “CYBERBOMBS” FROM ASSAD TO ISIS

David Sanger has a long piece on how CyberCom is – for the first time, he says! – launching cyberattacks on ISIS.

> The United States has opened a new line of combat against the Islamic State, directing the military’s six-year-old Cyber Command for the first time to mount computer-network attacks that are now being used alongside more traditional weapons.
>
> The effort reflects President Obama’s desire to bring many of the secret American cyberweapons that have been aimed elsewhere, notably at Iran, into the fight against the Islamic State — which has proved effective in using modern communications and encryption to recruit and carry out operations.
>
> The National Security Agency, which specializes in electronic surveillance, has for years listened intensely to the militants of the Islamic State, and those reports are often part of the president’s daily intelligence briefing. But the N.S.A.’s military counterpart, Cyber Command, was focused largely on Russia, China, Iran and North Korea — where cyberattacks on the United States most frequently originate — and had run virtually no operations against what has become the most dangerous terrorist organization in the world.
>
> [snip]
>
> The goal of the new campaign is to disrupt the ability of the Islamic State to spread its message, attract new adherents, circulate orders from

> commanders and carry out day-to-day functions, like paying its fighters. A benefit of the administration's exceedingly rare public discussion of the campaign, officials said, is to rattle the Islamic State's commanders, who have begun to realize that sophisticated hacking efforts are manipulating their data. Potential recruits may also be deterred if they come to worry about the security of their communications with the militant group.
>
> [snip]
>
> "We are dropping cyberbombs," Mr. Work said. "We have never done that before."
>
> The campaign has been conducted by a small number of "national mission teams," newly created cyberunits loosely modeled on Special Operations forces.

Golly, what a novel idea, hacking an adversary that relies on the Internet for its external strength? Imagine how many people we could have saved if we had done that a few years ago? And all this time CyberCom has just been sitting on its thumbs?

Sanger suggests, of course, that CyberCom has been otherwise focused on Russia, China, Iran, and North Korea, which (post-StuxNet) would be significantly an active defense. He pretends that cyber attacks have not been used in the ISIS theater at all.

Of course they have. They've been going on so long they even made the Snowden leaks (as when NSA "accidentally" caused a blackout in Syria).

But it would be inconvenient to mention attacks on Syria (as distinct from its ally Iran), I guess, because it might raise even more questions about why we'd let ISIS get strong enough, largely using the Internet, to hit two European capitals without undercutting them in the most obvious way. It all makes a lot of sense if you realize we have, at the same time, been directing those resources instead at Bashar al-Assad.