ONLINE PERSONAS AND CONGRESS

I've been meaning to return to our government's contracting for persona software for a while. Last week RawStory had a good story providing details of the persona management contract the Air Force put out for bid. RS reveals that the contract was awarded to Ntrepid, a firm in LA with the kind of website that screams "cover." And it has this from CENTCOM's digital media engagement team.

> According to Commander Bill Speaks, the chief media officer of CENTCOM's digital engagement team, the public cannot know what the military wants with such technology because its applications are secret.
>
> "This contract," he wrote in reference to the Air Force's June 22, 2010 filing, "supports classified social media activities outside the U.S., intended to counter violent extremist ideology and enemy propaganda."
>
> Speaks insisted that he was speaking only on behalf of CENTCOM, not the Air Force "or other branches of the military."
>
> While he did reveal who was awarded the contract in question, he added that the Air Force, which helps CENTCOM's contracting process out of MacDill, has even other uses for social media that he could not address.

It's secret, Sparks says, even the stuff that gets contracted openly.

In a post that looks like pushback against the concerns raised in the RS story, Jeff Stein has the same spokesperson reassuring us that these Cyberwar tactics won't be directed against us.

> Centcom spokesman Cmdr. Bill Speaks acknowledged in an interview last week that the Air Force had a contract for the Persona Management Software, but denied it would be deployed against domestic online protesters.
>
> "The contract, and the Persona management technology itself, supports classified blogging activities on foreign-language Web sites to enable CENTCOM to counter violent extremist and enemy propaganda outside the U.S.," Speaks told SpyTalk. "The contract would more accurately be described as supporting U.S. Central Command, rather than the Air Force – the Wing here at MacDill provides contracting support for us – efforts."
>
> Speaks said the software would "absolutely" not be used against law-abiding Americans.

Only, it looks like Stein asked the obvious follow-up question and got something less reassuring.

> *Update*: Speaks adds, "The phrase [law-abiding] suggests that we might use it against Americans who are not law-abiding. The truth is that these activities are not directed towards Americans, without qualification."

And how do they know that? Do they refuse to interact online with anyone whose IP address shows them to be in the US? Our Cyberwar folks do know that the InterToobz are global, don't they? I feel like this gets us back to the old reverse targeting problems with the government's replacement to FISA, with a very easy loophole to not "direct" fake personas at US persons, but to influence them with fake personas nevertheless.

Which brings me back to the point I always

return to in these discussions: to the evidence that DOD generally is hiding its Cyberwar programs from Congress, and the Air Force in particular has issued strict guidelines prohibiting its people from telling Congress about AF Special Access Programs.

> The AP noticed something troubling in Michael Vickers' response to the Senate Armed Services Committee questions on his nomination to be Undersecretary of Defense for Intelligence: the government did not include descriptions of its cyberwar activities in the quarterly report on clandestine activities.
>
> > The Senate Armed Services Committee voiced concerns that cyber activities were not included in the quarterly report on clandestine activities. But Vickers, in his answer, suggested that such emerging high-tech operations are not specifically listed in the law — a further indication that cyber oversight is still a murky work in progress for the Obama administration.
> >
> > Vickers told the committee that the requirement specifically calls for clandestine human intelligence activity. But if confirmed, he said, he would review the reporting requirements and support expanding the information included in the report.
>
> Now, Vickers apparently portrays this as a matter of legal hair-splitting: since the law doesn't explicitly require information on cyberwar activities, DOD didn't give it.
>
> But the story reminded me of something

> Steven Aftergood reported last month: the Air Force has explicitly prohibited anyone cleared into Air Force Special Access Programs from sharing any information on those programs with Congress.
>
> > The Air Force issued updated guidance (pdf) last week concerning its highly classified special access programs, including new language prohibiting unauthorized communications with Congress.
> >
> > [snip]
> >
> > "It is strictly forbidden for any employee of the Air Force or any appropriately accessed organization or company to brief or provide SAP material to any Congressional Member or staff without DoD SAPCO [Special Access Program Central Office] approval. Additionally, the Director, SAF/AAZ will be kept informed of any interaction with Congress." See Air Force Policy Directive 16-7, "Special Access Programs," December 29, 2010.

Even if Congress had issued clear guidelines for limits on Cyberwar to protect Americans—which they haven't—there would still be huge technical problems with those guidelines. But Congress can't impose limits on activities they know nothing about. And it sure looks like our military has carved out an area that could very well hide its Cyberwar programs from the people who could try to limit them.

Until DOD ends this policy of secrecy, I think it much safer to assume that all of Commander Speaks' reassurances ring hollow.