PUTTING "REALLY MUSHY" FUNCTIONS IN A DEPARTMENT THAT REFUSES TO BE AUDITED

Noah Shachtman points to NextGov's unsuccessful attempt to define how much DOD plans to spend on cybersecurity next year. DOD or its components have offered three different versions:

- DOD's mid-February report it would spend $2.3 billion
- Air Force's mid-February report it, by itself, would spend $4.6 billion
- DOD's March 23 revised report it would spend $3.2 billion

Part of the problem, as Shachtman explains in the NextGov piece, is that the definition of what counts as cybersecurity is not yet well defined.

> "All of this stuff is still really mushy," Shachtman said. Further obscuring visibility into the budget is the fact that some cybersecurity funding is classified at Defense components such as the NSA. Meanwhile, Cyber Command presents a new spending variable, he noted.
>
> "Exactly where the NSA ends and the Cyber Command ends is a very open question," Shachtman said. "How the Cyber Command is supposed to interact with the services is still being worked out." He predicted it will take years to untangle the process of budgeting for federal computer security.

While you're trying to get your head around how the Air Force has a bigger budget than the whole DOD for cybersecurity, remember a couple of things.

First, both the Air Force and DOD generally have stated policies of not telling Congress about Special Access Programs (in the case of Air Force) or clandestine cyberops. So to the extent that this mushy budget is mixed in with cyberops (as distinct from cybersecurity), there's a decent chance Congress isn't seeing all of it.

But even if Congress decided to look, to the extent that NSA (or CyberCommand, which General Keith Alexander also commands) has a hand in it, Congress is almost guaranteed to be unable to track it closely. That's because NSA books can't be audited and apparently NSA doesn't intend to fix those problems.

Now all of would be pretty funny except that, insofar as the government can't distinguish between legitimate cybersecurity (you know, preventing hackers and leakers from using thumb drives to upload malware and download entire databases) and cyberwar financially, there's a decent chance they can't do so organizationally either.

Or to put it in more tangible terms, HB Gary's past governmental work has been about cybersecurity—assessing malware and finding intrusions. But they've been proposing collecting information about citizens' First Amendment activity to use to target those citizens. And the Air Force—that entity with a cybersecurity budget bigger than all of DOD's cybersecurity budget—is the service that was engaging cybersecurity firms to develop persona management software.

But aside from that, why should we be worried that such dangerous entities are organizationally such a clusterfuck?