HIDING OUR CYBERWAR FROM CONGRESS

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.

Mind you, nothing says the SAPs the Air Force wants to hide from Congress pertain to cyberwar; after all, they might just be hiding our latest and greatest drone programs. Likewise, there's no reason to believe that the cyberwar activities DOD didn't describe to Congress are Air Force activities.

But there seems to be some interesting carving out of programs to hide from Congress.

Update: One more point on this: Every time Keith Alexander, in his function as the head of CyberCommand, talks about the legal authority for CyberCommand, he focuses on Title 10. That reminded me of John Rizzo's warning about the minimal oversight of Title 10 cyber-operations activities last year:

> I did want to mention—cause I find this interesting—cyberwarfare, on the issue of cyberwarfare. Again, increasing discussion there clearly is an active arena, will continue to be active. For us lawyers, certainly for the lawyers in the intelligence community, I've always found fascinating and personally I think it's a key to understanding many of the legal and political complexities of so-called cyberlaw and cyberwarfare is the division between Title 10, Title 10

> operations and Title 50 operations. Title 10 operations of course being undertaken by the Pentagon pursuant to its war-making authority, Title 50 operations being covert action operations conducted by CIA.
>
> Why is that important and fascinating? Because, as many of you know being practitioners, how these cyber-operations are described will dictate how they are reviewed and approved in the executive branch, and how they will be reported to Congress, and how Congress will oversee these activities. When I say, "these activities," I'm talking about offensive operations—computer network attacks.
>
> This issue, this discussion, has been going on inside the executive branch for many years, actually. I mean I remember serious discussions during the Clinton Administration. So, again, this is not a post-9/11 phenomenon. Now, I'm speaking her from a CIA perspective, but I've always been envious of my colleagues at the Department of Defense because under the rubrik of Title 10, this rubrik of "preparing the battlefield." They have always been able to operate with a—to my mind [?] a much greater degree of discretion and autonomy than we lawyers at CIA have been, have had to operate under, because of the various restrictions and requirements of Title 50 operations. Covert actions require Presidential Findings, fairly explicit reports to the Intelligence Oversight Committees. We have a very, our Intelligence Committees are … rigorous, rigorous and thorough in their review. I've never gotten the impression that the Pentagon, the military, DOD is subject to the same degree of scrutiny for their information warfare operations as CIA. I'm actually very envious of the

> flexibility they've had, but it's critical—I mean I guess I could say interesting but critical how—I mean if there were operations that CIA was doing, they would be called covert actions, there's no getting around that. To the extent I've ever understood what DOD does in this arena, they certainly sound like covert actions to me but given that I've had more than my hands full over the years trying to keep track of what CIA's doing at any given time, I've never ventured deeply into that area. But I think it's fascinating. [my emphasis]

So John Rizzo—John Rizzo!!!—warned about how DOD's offensive cyber-operations were eluding oversight last year. And surprise, surprise? DOD specifically left such operations out of its report on clandestine activities?