CONGRESS TO DOD: YOU MUST START BRIEFING US ON (SOME) CYBERWAR NOW

Robert Chesney notes that the HASC Mark on the Defense Authorization bill includes a section on cyberwar. Here's the entire section:

> This section would affirm that the Secretary of Defense has the authority to conduct military activities in cyberspace. The committee recognizes that because of the evolving nature of cyber warfare, there is a lack of historical precedent for what constitutes traditional military activities in cyberspace.
>
> In particular, this section would clarify that the Secretary of Defense has the authority to conduct clandestine cyberspace activities in support of military operations pursuant to the Authorization for the Use of Military Force (Public Law 107-40; 50 U.S.C. 1541 note) outside of the United States or to defend against a cyber attack on an asset of the Department of Defense.
>
> The committee notes that al Qaeda, the Taliban, and associated forces are increasingly using the internet to exercise command and control as well as to spread technical information enabling attacks on U.S. and coalition forces in areas of ongoing hostilities.
>
> While these terrorist actions often lead to increased danger for U.S. and coalition forces in areas of ongoing hostilities, terrorists often rely on the global reach of the internet to communicate and plan from distributed sanctuaries throughout the world. As a

> result, military activities may not be confined to a physical battlefield, and the use of military cyber activities has become a critical part of the effort to protect U.S. and coalition forces and combat terrorism globally.
>
> In certain instances, the most effective way to neutralize threats and protect U.S. and coalition forces is to undertake military cyber activities in a clandestine manner. **While this section is not meant to identify all or in any way limit other possible military activities in cyberspace**, the Secretary of Defense's authority includes the authority to conduct clandestine military activities in cyberspace in support of military operations pursuant to an armed conflict for which Congress has authorized the use of all necessary and appropriate force **or to defend against a cyber attack on a Department of Defense asset**.
>
> Because of the sensitivities associated with such military activities and the need for more rigorous oversight, **this section would require quarterly briefings to the congressional defense committees on covered military activities in cyberspace**.

While Chesney focuses on the use of "clandestine" in this passage (which I'll return to), I think one of the key phrases is simply the requirement that DOD brief the Armed Services Committees quarterly on what it's doing in cyberspace. As the AP reported in January, the SASC complained during the confirmation hearings of Michael Vickers that they weren't getting briefed on clandestine cyberwar activities. Vickers claimed in response that the law only required that DOD brief Congress on human 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.

So this section appears to close Vickers' loophole, now requiring that DOD brief Congress on its activities in its quarterly clandestine activities reports.

In addition to legally demanding briefings, the section appears to affirmatively approve—as clandestine activities—cyberattacks against an AUMF-authorized target (so, al Qaeda and people like Anwar al-Awlaki we claim to be included in AUMF), and cyberdefense against an attack on an asset of DOD.

By the way, anyone want to speculate whether a Specialist allegedly downloading several databases onto a Lady Gaga CD constitutes a cyberattack on a DOD asset? Because if this permission includes WikiLeaks, then this section might be retroactively authorize attacks—say, DNS attacks on US-based servers—on WikiLeaks (note that DOD can attack outside the US, but such geographical limits are not placed on defensive actions).

In any case, as Chesney emphasizes, this section specifically authorizes attacks on AUMF-authorized targets and defense against attacks on DOD targets. Chesney notes that by calling these activities "clandestine," it makes them a

Traditional Military Activity.

> That is to say, the language in § 962 refers to DOD authority to engage in cyber operations which are mean to go undiscovered but not meant to be denied. That alone would presumably keep them from being categorized as a "covert action" subject to presidential finding and SSCI/HPSCI notification requirements. Yet one can imagine that this does not quite suffice to solve the boundary dispute, insofar as it might not be clear on the front end that one would be willing to acknowledge sponsorship of an operation publicly if it becomes known…and indeed it might well be that the activity is very much meant to be both concealed and denied, making it hard at first blush to show that the activity is *not* a Title 50 covert action after all. But in at least some instances there is a separate reason it should not be deemed a covert action: i.e., when the action is best understood as a high-tech equivalent to a traditional military activity (the "TMA" category being an explicit exception to the T50 covert action definition). And that appears to be the case with the two categories explicitly described above, or at least arguably so.
>
> The explanatory statement accompanying § 962 supports this reading. It opens by stating that
>
> > [t]he committee recognizes that because of the evolving nature of cyber warfare, there is a lack of historical precedent for what constitutes traditional military activities in cyberspace.

So, to summarize, this section appears to affirmatively authorize two types of activities, defining them as clandestine operations, and mandating that Congress get quarterly briefings on them.

But note this clause: "this section is not meant to identify all or in any way limit other possible military activities in cyberspace."

So, it appears, there may be these two types of explicitly authorized clandestine operations, and then the stuff John Rizzo warned about.

> 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]

Now, maybe this section just politely puts the kibosh on all of this Title 50 masquerading as Title 10 stuff, stuff done under the auspices of DOD to avoid the oversight requirements that Title 10 intelligence operations would require.

Maybe this section limits DOD's activities to its two authorized clandestine activities.

But I doubt it. With the language about not limiting DOD to these two functions, you can pretty much assume there's some Special Access Programs (like the kind the Air Force refuses to talk to Congress about) not safe to be mentioned in public documents like laws.

Look on the bright side, though: Congress is at least requiring that DOD brief Congress on some of the secret stuff they're doing in cyberspace.

Update: Specialist corrected per Ralph.