IF CYBERCOM CAN'T BEAT RESERVISTS, WHY NOT SPLIT NSA?

ArmyTimes has a story about how CyberCommand service members took on a team of civilian reservists in a cyber war game last year, the civilians handed the active duty team their ass.

> When the military's top cyberwarriors gathered last year inside a secretive compound at Fort Meade, Maryland, for a classified war game exercise, a team of active-duty troops faced off against several teams of reservists.
>
> And the active-duty team apparently took a beating.
>
> "They were pretty much obliterated," said one Capitol Hill staffer who attended the exercise. "The active-duty team didn't even know how they'd been attacked."

ArmyTimes uses the shellacking to raise questions about the mix between active duty and reservists CyberCommand should be using.

But it seems the exercise ought to also undermine one justification for keeping NSA's Information Assurance Division, its spying, and CyberCommand unified.

One argument behind doing so is that's the only way to make the appropriate measure of which vulnerabilities the government should sit on and exploit for their own spying and offensive capabilities, and which they should disclose and patch. The unified CyberCommander — first Keith Alexander and now Admiral Mike Rogers — are the only ones who can appropriately measure the trade-offs.

If the military hierarchy — and the article suggests the hierarchy is part of the problem —

doesn’t serve the understanding of cyberwar very well, then how is the guy at the top of the hierarchy going to be best able to understand the trade-offs? If his subordinates don’t “even know they’d been attacked,” then how are they able to judge what exploits might be attackable?

Everything about this article, particularly the complementarity of the civilian and military skills it describes, suggests we’d be better served by having some who recognizes an attack as an attack in charge of keeping our networks safe.