NSA REORGANIZING IN MANNER THAT DIRECTLY CONFLICTS WITH PRESIDENT'S REVIEW GROUP RECOMMENDATION

Back in 2013, the President's Review Group recommended that NSA's defensive function — the Information Assurance Directorate — be removed from NSA. I've put the entirety of that recommendation below, but PRG recommended the change to:

- Eliminate the conflict of interest between NSA's offensive and defense functions
- Eliminate the asymmetry between the two functions, which can lead the defensive function to be less visible
- Rebuild trust with outside cybersecurity stakeholders

Not only didn't President Obama accept that recommendation, but he pre-empted it in several ways, before the PRG could publicly release their findings.

> [O]n Thursday night, the Wall Street Journal and New York Times published leaked details from the recommendations from the review group on intelligence and communications technologies, a panelPresident Obama set up in August to review the NSA's activities in response to theEdward Snowden leaks.
>
> The stories described what they said

> were recommendations in the report as presented in draft form to White House advisors; the final report was due to the White House on Sunday. There were discrepancies in the reporting, which may have signaled the leaks were a public airing of disputes surrounding the review group (both articles noted the results were "still being finalized"). The biggest news item were reports about a recommendation that the director of the NSA(Dirnsa) and Cyber Command positions be split, with a civilian leading the former agency.
>
> Before the final report was even delivered, the White House struck. On Friday, while insisting that the commission report was not yet final, national security council spokesperson Caitlin Hayden announced the White House had already decided the position would *not* be split. A dual-hatted general would continue to lead both.
>
> By all appearances, the White House moved to pre-empt the results of its own review group to squelch any recommendation that the position be split.

Today, Ellen Nakashima reports that NSA will go further still, and completely merge its offensive and defensive missions.

> In place of the Signals Intelligence and Information Assurance directorates, the organizations that historically have spied on foreign targets and defended classified networks against spying, the NSA is creating a Directorate of Operations that combines the operational elements of each.
>
> [snip]
>
> Some lawmakers who have been briefed on the broad parameters consider

> restructuring a smart thing to do because an increasing amount of intelligence and threat activity is coursing through global computer networks.
>
> "When it comes to cyber in particular, the line between collection capabilities and our own vulnerabilities — between the acquisition of signals intelligence and the assurance of our own information — is virtually nonexistent," said Rep. Adam B. Schiff (Calif.), the ranking Democrat on the House Intelligence Committee. "What is a vulnerability to be patched at home is often a potential collection opportunity abroad and vice versa."
>
> But there have been rumblings of discontent within the NSA, which is based at Fort Meade, Md., as some fear a loss of influence or stature.
>
> Some advocates for the comparatively small Information Assurance Directorate, which has about 3,000 people, fear that its ability to work with industry on cybersecurity issues will be undermined if it is viewed as part of the much larger "sigint" collection arm, which has about eight times as many personnel. The latter spies on overseas targets by hacking into computer networks, collecting satellite signals and capturing radio waves.

While Nakashima presents some conflicting views on whether IAD will be able to cooperate with industry, none of the comments she includes addresses the larger bureaucratic issue: that defense is already being shortchanged in favor of the glitzier offensive function.

But Edward Snowden did weigh in, in response to a comment I made on this onTwitter.

> When defense is an afterthought, it's not a National Security Agency. It's a National Spying Agency.

It strikes me this NSA reorganization commits the country to a particular approach to cybersecurity that will have significant ramifications for some time. It probably shouldn't be made with the exclusive review of the Intelligence Committees mostly in secret.

We recommend that the Information Assurance Directorate—a large component of the National Security Agency that is not engaged in activities related to foreign intelligence—should become a separate agency within the Department of Defense, reporting to the cyber policy element within the Office of the Secretary of Defense.

In keeping with the concept that NSA should be a foreign intelligence agency, the large and important Information Assurance Directorate (IAD) of NSA should be organizationally separate and have a different reporting structure. IAD's primary mission is to ensure the security of the DOD's communications systems. Over time, the importance has grown of its other missions and activities, such as providing support for the security of other US Government networks and making contributions to the overall field of cyber security, including for the vast bulk of US systems that are outside of the government. Those are not missions of a foreign intelligence agency. The historical mission of protecting the military's communications is today a diminishing subset of overall cyber security efforts.

We are concerned that having IAD embedded in a foreign intelligence organization creates potential conflicts of interest. A chief goal of NSA is to access and decrypt SIGINT, an offensive capability. By contrast, IAD's job is defense. When the offensive personnel find some way into a communications device, software

system, or network, they may be reluctant to have a patch that blocks their own access. This conflict of interest has been a prominent feature of recent writings by technologists about surveillance issues.

A related concern about keeping IAD in NSA is that there can be an asymmetry within a bureaucracy between offense and defense—a successful offensive effort provides new intelligence that is visible to senior management, while the steady day-to-day efforts on defense offer fewer opportunities for dramatic success.

Another reason to separate IAD from NSA is to foster better relations with the private sector, academic experts, and other cyber security stakeholders. Precisely because so much of cyber security exists in the private sector, including for critical infrastructure, it is vital to maintain public trust. Our discussions with a range of experts have highlighted a current lack of trust that NSA is committed to the defensive mission. Creating a new organizational structure would help rebuild that trust going forward.

There are, of course, strong technical reasons for information-sharing between the offense and defense for cyber security. Individual experts learn by having experience both in penetrating systems and in seeking to block penetration. Such collaboration could and must occur even if IAD is organizationally separate.

In an ideal world, IAD could form the core of the cyber capability of DHS. DHS has been designated as the lead cabinet department for cyber security defense. Any effort to transfer IAD out of the Defense Department budget, however, would likely meet with opposition in Congress. Thus, we suggest that IAD should become a Defense Agency, with status similar to that of the Defense Information Systems Agency (DISA) or the Defense Threat Reduction Agency (DTRA). Under this approach, the new and separate Defense Information Assurance Agency (DIAA) would no longer report through

intelligence channels, but would be subject to oversight by the cyber security policy arm of the Office of the Secretary of Defense.