NSA DENIES THEIR EXISTING DOMESTIC CYBERDEFENSIVE EFFORTS, AGAIN

James Risen and Laura Poitras have teamed up to analyze a 4-year plan the NSA wrote in 2012, in the wake of being told its collection of some US person content in the US was illegal. I'll discuss the document itself in more depth later. But for the moment I want to look at the denials anonymous senior intelligence officials (SIOs) gave Risen and Poitras about their domestic cyberdefensive efforts.

As a reminder, since before 2008, the government has been collecting bulk Internet data from switches located in the US by searching on selectors in the content. Some of that collection searches on identifiers of people (for example, searching for people sharing Anwar al-Awlaki's email in the body of a message). But the collection also searches on other identifiers not tied to people. This collection almost certainly includes code, in an effort to find malware and other signs of cyberattacks.

We know that's true, in part, because the Leahy-Sensenbrenner bill not only restricts that bulk domestic collection to actually targeted people, but also because it limits such collection only to terrorism and counterproliferation, thereby silently prohibiting its use for cybersecurity. The bill gives NSA 6 months to stop doing these two things — collecting non-person selectors and doing so for cybersecurity — so it's clear such collection is currently going on.

So in 2012, just months after John Bates told NSA that when it collected domestic communications using such searches, it was violating the Constitution (the NSA contemplated appealing that decision), the NSA said (among other things),

> The interpretation and guidelines for applying our authorities, and in some cases the authorities themselves, have not kept pace with the complexity of the technology and target environments, or the operational expectations levied on NSA's mission.

The document then laid out a plan to expand its involvement in cybersecurity, citing such goals as,

> Integrate the SIGINT system into a national network of sensors which interactively sense, respond, and alert one another at machine speed

Cyberdefense and offense are not the only goals mapped out in this document. Much of it is geared towards cryptanalysis, which is crucial for many targets. But it only mentions "non-state actors" once (and does not mention terrorists specifically at all) amid a much heavier focus on cyberattacks and after a description of power moving from West to East (that is, to China).

Which is why the SIO denials to Risen and Poitras ring so hollow.

When asked what authorities haven't kept up with their programs, the SIOs cite the roamer problem (and flat out lie about the current state of the law).

> Senior intelligence officials, responding to questions about the document, said that the N.S.A. believed that legal impediments limited its ability to conduct surveillance of terrorism suspects inside the United States. Despite an overhaul of national security law in 2008, the officials said, if a terrorism suspect who is under surveillance overseas enters the United States, the agency has to stop monitoring him until it obtains a

> warrant from the Foreign Intelligence Surveillance Court.

Remember, first of all, that NSA's own internal documents (from 2012, in fact) claim this problem stems from the number of Chinese targets traveling to the US, not terrorists. Moreover, NSA can already continue surveilling targets when they come in the US, but has to get emergency authorization to do so. This new bid for authority must stem from NSA not tracking these targets closely enough to realize they're in the US for 72 hours, and not wanting to involve the FISC for a time. But the NSA does not currently have to stop monitoring them until they get a warrant — that claim is simply false.

But clearly, the roamer problem is not the most pressing issue at hand (which Keith Alexander admits, on the record, with more captive NYT journalists). It's cybersecurity. And yet, the SIOs issuing obviously false denials to Risen and Poitras deny even that, as in this response to a question about the "sensors" comment above.

> Senior intelligence officials said that the system of sensors is designed to protect the computer networks of the Defense Department, and that the N.S.A. does not use data collected from Americans for the system.

The government currently has sensors at DOD and is negotiating to deploy them on critical infrastructure, but it wants sensors more broadly. And, as noted, it already partners with the telecoms to filter data searching for malicious code. Their programs already exceed their claims here, but they're still going to claim to the contrary nevertheless.

Most of the rest of the claims these SIOs made — most denying that it collects or intends to collect data from within the US — ring equally hollow; many can be disproven with public documents. But that all makes sense. Because,

whatever the targets, the document itself reveals a determination to increase the bulk collection and sorting approach. especially in the US.

Chalk this up to another example of NSA lying most unconvincingly when it tries to deny its illegal domestic wiretapping.