TERRORIST HOBGOBLINS BITE THE INTELLIGENCE COMMUNITY IN ITS EFFICACY ASS

I just finished watching the House Intelligence Committee hearing on the NSA programs revealed by Edward Snowden. I'll have a lot more to say about the content of the revelations in the next few days. But first, a general observation.

Since the initial Snowden revelations, the Intelligence Community and other Administration surrogates have been trying to minimize our understanding of the scope of their surveillance and use traditional fearmongering to justify the programs by focusing on the importance of the Section 702 collection to stopping terrorism. While James Clapper's office has made it clear that Section 702 goes beyond counterterrorism by revealing that its successes include counterproliferation and cybersecurity successes, as well as counterterrorism ones, the focus has nevertheless been on TERROR TERROR TERROR.

Today's hearing was really the culmination of that process, when Keith Alexander boasted up upwards of 50 terrorist plots — about 40 of which were overseas — that Section 702 has prevented.

Of the four plots the government has revealed — David Headley, Najibullah Zazi, as well as these two today…

> Mr. Joyce described a plot to blow up the New York Stock Exchange by a Kansas City man, whom the agency was able to identify because he was in contact with "an extremist" in Yemen who was under surveillance. Mr. Joyce also talked about a San Diego man who planned to send financial support to a terrorist group in Somalia, and who was identified

> because the N.S.A. flagged his phone number as suspicious through its database of all domestic phone call logs, which was brought to light by Mr. Snowden’s disclosures.

… the government has either overblown the importance of these programs and their success or are fairly minor plots.

None of the four may be as uniquely worthwhile as the cyberattack described by Clapper’s office a week ago, which it has not, however, fleshed out.

> Communications collected under Section 702 have provided significant and unique intelligence regarding potential cyber threats to the United States, including specific potential network computer attacks. This insight has led to successful efforts to mitigate these threats.

That is, the government might—might!—be able to make a far better case for the value of these programs in discussing their role in preventing cyberattacks rather than preventing terrorist plots.

And yet it hasn’t done so, even as it pushes one after another attempt to legislate internet access in the name of protecting Intellectual Property and critical infrastructure.

Given the increasing focus on cybersecurity — and the already dishonest claims people like Mike Rogers have made about the means to accomplish that focus — this is the discussion we need to be having, rather than digging up terror plots first developed in 2004 that never happened. But in the same way the government shied away from conducting an honest discussion with us in 2001 and again in 2006 about these programs, it is refusing to conduct an honest discussion about cybersecurity today.

And, ironically, that refusal is preventing them from describing the value of a program that surely contributes more to countering cyberattacks than terror attacks at this point.