KEITH ALEXANDER'S "PACKETS IN FLIGHT" TURN HACKERS INTO TERRORISTS

Keith Alexander showed up to chat with a typically solicitous George Stephanopoulos yesterday. The interview demonstrates something I'll be increasingly obsessed with in upcoming weeks.

The government is using the limited success of NSA's counterterrorism spying to justify programs that increasingly serve a cybersecurity function — a function Congress has not enthusiastically endorsed.

The interview starts with Alexander ignoring Steph's first question (why we didn't find Snowden) and instead teeing up 9/11 and terror terror terror.

> And when you think about what our mission is, I want to jump into that, because I think it reflect on the question you're asking.
>
> You know, my first responsibility to the American people is to defend this nation. And when you think about it, defending the nation, let's look back at 9/11 and what happened.
>
> The intel community failed to connect the dots in 9/11. And much of what we've done since then were to give us the capabilities — and this is the business record FISA, what's sometimes called Section 215 and the FAA 702 — two capabilities that help us connect the dots.
>
> The reason I bring that up is that these are two of the most important things from my perspective that helps us understand what terrorists are trying to

> do. And if you think about that, what Snowden has revealed has caused irreversible and significant damage to our country and to our allies.
>
> When – on Friday, we pushed a Congress over 50 cases where these contributed to the understanding and, in many cases, disruptions of terrorist plots.

Steph persists with his original question and gets Alexander to repeat that they've "changed the passwords" at NSA to prevent others from leaking.

Steph then asks Alexander about Snowden's leaks of details on our hacking of China (note, no one seems to be interested in this article, which is just as revealing about our hacking of China as Snowden's revelations).

Note how, even here, Alexander says our intelligence collection in China is about terrorism.

> STEPHANOPOULOS: In the statement that Hong Kong put out this morning, explaining why they allowed Snowden to leave, they also say they've written to the United States government requesting clarification on the reports, based on Snowden's information, that the United States government attacked (ph) computer systems in Hong Kong.
>
> He said that the NSA does all kinds of things like hack Chinese cell phone companies to steal all of your SMS data.
>
> Is that true?
>
> ALEXANDER: Well, we have interest in those who collect on us as an intelligence agency. But to say that we're willfully just collecting all sorts of data would give you the impression that we're just trying to canvas the whole world.

> The fact is what we're trying to do is get the information our nation needs, the foreign intelligence, that primary mission, **in this case and the case that Snowden has brought up is in defending this nation from a terrorist attack**.

Alexander then shifts the issue and suggests we're collecting on China because it is collecting on us.

> Now we have other intelligence interests just like other nations do. That's what you'd expect us to do. We do that right. Our main interest: who's collecting on us?

Alexander next goes on to answer Steph's question about whether we broke Hong Kong law by saying this hacking doesn't break our law. He also says he doesn't "track" WikiLeaks, but knows who Julian Assange is, which I take to be confirmation NSA targets Assange and collects on everyone else he talks to.

Then Steph tees up the 50 plots prevented, without noting that, of the four publicly released, there are major holes in the claims made about the three most serious plots. He asks for proof in these cases and Alexander provides nothing new (indeed, he actually comes close to admitting that the FISA programs played just a role in connecting the dots).

After letting Alexander continue on about these 50 plots for over 400 words, he moves onto challenging, sort of, the claims that the US can't listen into an American side of a conversation. Interestingly, Steph asks about Cuba, but Alexander responds by focusing on terrorism. Again.

> But is that statement correct? I would assume – and tell me if I'm wrong here, that if the NSA (inaudible) tracking someone, say, in Cuba or someone overseas, who then calls the United

> States, you're going to listen to that phone call, correct?
>
> ALEXANDER: Right. You're asking a different set of questions.
>
> So let me put, first of all, the prime directive on the table. The FISA law makes it clear: in order for the NSA to target the content of a U.S. persons communications, anywhere in the world — anywhere — NSA requires probable cause and a court order, a specific court order.
>
> So if we're targeting outside the U.S. a terrorist, and they happen to talk to a U.S. person inside the United States, yes, we would follow that law.

Alexander doesn't address Steph's question (he says the NSA abides by minimization rules, which do permit accessing the US person side of the call), but he does use the word "target" a lot.

And then, having not mentioned FAA's role in cybersecurity during this entire extended debate about it, Steph switches to Alexander's role in cyberwar, asking about NSA's pre-emptive strike ability. This is where Alexander raises his authority to "stop packets in flight" as parallel to a nuclear assault.

> ALEXANDER: So to be clear, what I can do on my own right now is within our networks to launch offensive measures to stop somebody from getting into the networks.
>
> Anything that I want to do outside the networks that is offensive in nature, we would have to call the secretary and the president to get their approval.
>
> So there are things that we can do to **stop packets in flight**. But from our perspective, any actions that's offensive in nature would require the policymakers. This is no different than

> if you think about the **nuclear situation**. [my emphasis]

Steph ends the interview by teeing up one of Alexander's (and Sheldon Whitehouse's) favorite claims about cybersecurity, that it represents a transfer of wealth greater than slavery or colonization did.

> STEPHANOPOULOS: Finally, the chairman of the House Intelligence Committee, Mike Rogers, was on this program a short while ago. And he said we're losing the cyber war to China.
>
> Is he right?
>
> ALEXANDER: Well, I think our nation has been significantly impacted with intellectual property, the theft of intellectual property by China and others. That is the most significant transfer of wealth in history.
>
> And it goes right back to your initial question: who's taking our information? Is one of the things I believe the American people would expect me to know. That's one of my missions. Who's doing this to us? And why?
>
> So when you asked your initial question, why, there's part of the answer. Who's coming after us? We need to know that so we can defend this nation.

It's the greatest transfer of wealth in history, Alexander lies, but he still doesn't admit in this entire interview that FAA also serves a key role in cybersecurity.

As I said, I will be increasingly obsessed with this in upcoming weeks. The government is hiding its use of these newly exposed authorities behind a lot of fearmongering about terrorism.

And Keith Alexander was so intent on maintaining that approach he even accused China of

terrorism.