SHUT DOWN CYBERCOMMAND — US CYBERCOMMANDER KEITH ALEXANDER DOESN'T THINK IT'S IMPORTANT

Back on March 12 — in the same hearing where he lied to Ron Wyden about whether the intelligence community collects data on millions of Americans — James Clapper also implied that "cyber" was the biggest threat to the United States.

> So when it comes to the distinct threat areas, our statement this year leads with cyber. And it's hard to overemphasize its significance. Increasingly, state and non-state actors are gaining and using cyber expertise. They apply cyber techniques and capabilities to achieve strategic objectives by gathering sensitive information from public- and private sector entities, controlling the content and flow of information, and challenging perceived adversaries in cyberspace.

That was the big takeaway from Clapper's Worldwide Threat Assessment. Not that he had lied to Wyden, but that that cyber had become a bigger threat than terrorism.

How strange, then, that the US CyberCommander (and Director of National Security) Keith Alexander mentioned cyber threats just once when he keynoted BlackHat the other day.

> But this information and the way our country has put it together is something that we should also put forward as an example for the rest of the world, because what comes out is we're

> collecting everything. That is not true. What we're doing is for foreign intelligence purposes to go after counterterrorism, counterproliferation, cyberattacks. And it's focused. [my emphasis]

That was it.

The sole mention of the threat his boss had suggested was the biggest threat to the US less than 5 months earlier. "Counterterrorism, counterproliferation, cyberattacks. and it's focused."

The sole mention of the threat that his audience of computer security professionals are uniquely qualified to help with.

Compare that to his 27 mentions of "terror" (one – the one with the question mark – may have been a mistranscription):

> terrorists … terrorism … terrorist attacks … counterterrorism … counterterrorism … terrorists … counterterrorism … terrorist organizations … terrorist activities … terrorist … terrorist activities … counterterrorism nexus … terrorist actor … terrorist? … terrorism … terrorist … terrorists … imminent terrorist attack … terrorist … terrorist-related actor … another terrorist … terrorist-related activities … terrorist activities … stopping terrorism … future terrorist attacks … terrorist plots … terrorist associations

That was the speech the US CyberCommander chose to deliver to one of the premiere group of cybersecurity professionals in the world.

Terror terror terror.

> Sitting among you are people who mean us harm

… US CyberCommander Alexander also said.

Apparently, Alexander and Clapper's previous intense focus on stopping hacktavists and cyberattacks and cybertheft and cyber espionage have all been preempted by the necessity of scaring people into accepting the various dragnets that NSA has deployed against Americans.

Which, I guess, shows us the true seriousness of the cyber threat.

To be fair to our CyberCommander, he told a slightly different story back on June 27, when he addressed the Armed Forces Communications and Electronics Association International Cyber Symposium.

Sure, he started by addressing Edwards Snowden's leaks.

But then he talked about a debate he was prepared to have.

> I do think it's important to put that on the table, because as we go into cyber and look at—for cyber in the future, we've got to have this debate with our country. How are we going to protect the nation in cyberspace? And I think this is a debate that is going to have all the key elements of the executive branch—that's DHS, FBI, DOD, Cyber Command, NSA and other partners—with our allies and with industry. We've got to figure how we're going to work together.

How are we going to protect the nation in cyberspace? he asked a bunch of Military Intelligence Industrial Complex types.

At his cyber speech, Alexander also described his plan to build, train, and field one-third of the force by September 30 — something you might think he would have mentioned at BlackHat.

Not a hint of that.

Our US CyberCommander said – to a bunch of industry types – that we need to have a debate about how to protect the nation in cyberspace.

But then, a month later, with the group who are probably most fit to debate him on precisely those issues, he was all but silent.

Just terror terror terror.