I TOLD YOU SO, IT'S ABOUT CYBERSECURITY EDITION

When James "Least Untruthful" Clapper released the first version of PRISM success stories and the most impressive one involved thwarting specific cyberattacks, I noted that the NSA spying was about hackers as much as terrorists.

When "Lying Keith" Alexander answered a question about hacking China from George Stephanopoulos by talking about terror, I warned that these programs were as much about cybersecurity as terror. "Packets in flight!"

When the Guardian noted that minimization procedures allowed the circulation of US person communications collected incidentally off foreign targets if they were "necessary to understand or assess a communications security vulnerability," I suggested those procedures fit cybersecurity targets better than terror ones.

When Ron Wyden and Mark Udall caught Lying Keith (again) in a lie about minimization, I speculated that the big thing he was hiding was that encrypted communications are kept until they are decrypted.

When I compared minimization procedures with the letter of the law and discovered the NSA had secretly created for itself the ability to keep US person communications that pose a serious threat to property (rather than life or body), I suggested this better targeted cyber criminals than terrorists.

When Joel Brenner suggested Ron Wyden was being dishonorable for asking James Clapper a yes or no question in March 2013, I noted that Wyden's question actually referred to lies Lying Alexander had told the previous year at DefCon that hid, in part, how hackers' communications are treated.

When the Guardian happened to publish evidence the NSA considers encryption evidence of terrorism the same day that Keith Alexander spokes to a bunch of encrypters exclusively about terrorism, I suggested he might not want to talk to those people about how these programs are really used.

And when I showed how Lying Keith neglected his boss' earlier emphasis on cyber in his speech to BlackHat in favor of terror times 27, I observed Lying Keith's June exhortation that "we've got to have this debate with our country," somehow didn't extend to debating with hackers.

I told you it would come to this:

> ***U.S. officials say NSA leaks may hamper cyber policy debate***

Over two months after Edward Snowden's first disclosures, the cyberwarriors are now admitting disclosures about how vast is NSA's existing power — however hidden behind the impetus of terror terror terror — might lead Congress to question further empowering NSA to fight cyberwar.

I told you so.

> Despite the emerging consensus that U.S. cyber defenses must be improved, the conversation has sputtered amid disagreements about liability and privacy protections, the creation of new industry standards and other critical elements.
>
> Now, cybersecurity leaders say the leaked details of the vast scope of NSA's online data gathering may hamper efforts to draft cyber policies, such as

> greater information-sharing between government and industry.
>
> "It's opened up a big can of worms about what the government's role is, which is already a big open question in cyberspace," said Bruce McConnell, the Department of Homeland Security's Acting Deputy Undersecretary for Cybersecurity. "I don't think this is going to be helpful in making Congress, who tends to be risk-averse, forge new policy agreements."

As Reuters notes, Congress wasn't even willing to give the government the authorities it wanted before the Snowden revelations. And yet, even though no one besides me is talking about how these tools are used against cyber targets, Congress is likely to be far more skeptical about giving Lying Keith more power or private corporations more immunity.

And yet for all their silence about how central cyber has been to these disclosures, the cyberwarriors claim remorse that we haven't been having this debate all along.