CISA'S TERRORISTS ARE NOT JUST FOREIGN TERRORISTS

In addition to hunting hackers, the Cybersecurity Information Security Act — the bill that just passed the Senate Intelligence Committee — collects information domestically to target terrorists if those so-called terrorists can be said to be hacking or otherwise doing damage to property.

Significantly, as written, the bill doesn't limit itself to targeting terrorists with an international tie. That's important, because it essentially authorizes intelligence collection domestically with no court review. Thus, the bill seems to be — at least in part — a way around *Keith*, the 1971 ruling that prohibited domestic security spying without a warrant.

It takes reading the bill closely to understand that, though.

The surveillance or counterhacking of a "terrorist" is permitted in three places in the bill. In the first of those, one might interpret the bill to associate the word "foreign" used earlier in the clause with the word terrorist. That clause authorizes the disclosure of cyber threat indicators for "(iii) the purpose of identifying a cybersecurity threat involving the use of an information system by a foreign adversary or terrorist."

But the very next clause authorizes information sharing to mitigate "a terrorist act," with no modifier "foreign" in sight. It authorizes information sharing for "(iv) the purpose of responding to, or otherwise preventing or mitigating, an imminent threat of death, serious bodily harm, or serious economic harm, including a terrorist act or a use of a weapon of mass destruction;"

And the last mention of terrorists — reserving

the authority of the Secretary of Defense to conduct cyberattacks in response to malicious cyber activity — includes the article "a" that makes it clear the earlier use of "foreign" doesn't apply to "terrorist organization" in this usage.

> (m) AUTHORITY OF SECRETARY OF DEFENSE TO RESPOND TO CYBER ATTACKS.—Nothing in this Act shall be construed to limit the authority of the Secretary of Defense to develop, prepare, coordinate, or, when authorized by the President to do so, conduct a military cyber operation in response to a malicious cyber activity carried out against the United States or a United States person by a foreign government or an organization sponsored by a foreign government or a terrorist organization.

Frankly, I'm of the belief that the distinction that has by and large applied for the last 14 years of spying betrays the problem with our dragnet targeted on Muslims. America in general seems perfectly willing to treat some deaths — even 168 deaths — perpetrated by terrorists as criminal attacks so long as they are white Christian terrorists. If white Christian terrorists can be managed as the significant law enforcement problem they are without a dragnet, then so, probably, can FBI handle the losers it entraps in dragnets and then stings.

But here, that distinction has either apparently been scrapped or Richard Burr's staffers are just bad at drafting surveillance bills. It appears that whatever anyone wants to call a terrorist — whether it be Animal Rights activists, Occupy Wall Street members, Sovereign Citizen members, or losers who started following ISIL on Twitter — appears to be fair game. Which is particularly troubling given that CISA makes explicit what NSA used to accomplish only in secret — the expansion of "imminent threat of death or serious bodily harm" to incorporate harm to property. How much harm to a movie

studio or some other IP owner does it take before someone is branded a “terrorist” engaged in the “act” of doing “serious economic harm,” I wonder?

Note, too, that according to OTI’s redlined version of this bill, most of the application of this surveillance to foreign and domestic terrorists is new, added even as SSCI dawdles in the face of imminent Section 215 sunset.

As I’ll show in a later post, one function of this bill may be to move production that currently undergoes or might undergo FISC or other court scrutiny out from under a second branch of government, making a mockery out of what used to be called minimization procedures. If that’s right, it would also have the effect of avoiding court scrutiny on just whether this surveillance — renamed “information sharing” — complies with Supreme Court prohibition on warrantless spying on those considered domestic security threats.