IN WAKE OF REVELATIONS ABOUT CORRUPTION AND COERCION, OCC WAILS ABOUT BANK CYBERSECURITY

Over 3 months ago, the Guardian revealed that the President reserved the right to declare "inherent right of self defense" to access private networks deemed part of our critical infrastructure in the name of cybersecurity.

2 weeks ago, the Guardian, ProPublica, and NYT reported that, to make it easier to spy on others, the NSA had "deliberately weakened the international encryption standards adopted by developers."

Also 2 weeks ago, FP reported that "many corporate participants" in an NSA initiative to protect US critical infrastructure "say Alexander's primary motive" in that initiative "has not been to share what the NSA knows about hackers. It's to get intelligence from the companies."

And just this week, Spiegel provided details of how NSA conducts Man-in-the-Middle attacks — hacks — on financial giants like VISA and SWIFT.

Yet none of those revelations prevented Comptroller of the Currency Thomas Curry to give a fairly breathtaking speech yesterday about financial cybersecurity.

In it, a member of the Executive Branch that has made everyone less security by corrupting encryption said,

> The growing sophistication and frequency of cyberattacks is a cause for concern, not only because of the potential for disruption, but also because of the

> potential for destruction of the systems and information that support our banks. These risks, if unchecked, could threaten the reputation of our financial institutions as well as public confidence in the system.

A member of a regime that is routinely hacking financial entities said,

> The global nature of the Internet means they can conduct their activity from almost anywhere, including in countries with regimes that, at worst, sponsor attacks and, at a minimum, act as criminal havens by turning a blind eye toward criminal behavior.

And a member of the government that has hacked key third party providers like SWIFT and cooperated with third party telecoms to just steal data said,

> Banks not only operate their own networks, they also rely on third parties to support their systems and business activities. Some of these third parties have connections to other institutions and servicers. Each new relationship and connection provides potential access points to all of the connected networks and introduces different weaknesses into the system.

I recognize the cybersecurity threat to banks is real. I'd like to be protected against criminals trying to steal my money online and I endorse OCC including IT security among things bank inspectors review. I grant that Curry may well be operating in good faith when he says all these things. But when he talks about partnerships like this, he simply loses credibility.

> Clearly, much of the responsibility for assessing cyber threats is housed in

> other agencies, from the Department of Homeland Security to the FBI to the National Security Agency. They are on the front lines, and they are the ones that are doing the most within government to identify, evaluate, and respond to threats in this area. However, we – the OCC, the FFIEC, and the other regulatory agencies individually – are working closely with them to strengthen the coordination and overall effectiveness of government's approach to cybersecurity of critical infrastructure.
>
> [snip]
>
> But this is not a problem that can be addressed by one agency alone or by any one institution acting on its own. It is a threat that we can deal with only if we work together in a collegial and collaborative way for the good of our country.

The banks' regulators may believe he is in a position to lecture about collegiality in the face of threats. But since the government is one of the biggest of those threats, it doesn't strike me as all that convincing.