THE PERSISTENT CONCERNS ABOUT ALTERED FINANCIAL DATA

Remember that weird passage in the President's Review Group Report warning against changing the account numbers in financial accounts as part of offensive cyberattacks?

> (2) Governments should not use their offensive cyber capabilities to change the amounts held in financial accounts or otherwise manipulate the financial systems;
>
> Second, governments should abstain from penetrating the systems of financial institutions and changing the amounts held in accounts there. The policy of avoiding tampering with account balances in financial institutions is part of a broader US policy of abstaining from manipulation of the financial system. These policies support economic growth by allowing all actors to rely on the accuracy of financial statements without the need for costly re-verification of account balances. This sort of attack could cause damaging uncertainty in financial markets, as well as create a risk of escalating counter-attacks against a nation that began such an effort. The US Government should affirm this policy as an international norm, and incorporate the policy into free trade or other international agreements.

It was the kind of warning that left the strong impression that the US had already been engaged in such books-baking.

It's back again, in James Clapper's Global Threats Report (curiously, it was not in last

year's Global Threats Report).

> Integrity of Information
>
> Most of the public discussion regarding cyber threats has focused on the confidentiality and availability of information; cyber espionage undermines confidentiality, whereas denial-of-service operations and data-deletion attacks undermine availability. In the future, however, we might also see more cyber operations that will change or manipulate electronic information in order to compromise its integrity (i.e., accuracy and reliability) instead of deleting it or disrupting access to it. Decisionmaking by senior government officials (civilian and military), corporate executives, investors, or others will be impaired if they cannot trust the information they are receiving.
>
> - *Successful cyber operations targeting the integrity of information would need to overcome any institutionalized checks and balances designed to prevent the manipulation of data, for example, market monitoring and clearing functions in the financial sector.*

Altering data to misinform decision-makers is not new – part of the Stuxnet attack involved making the Iranians believe everything was going swimmingly even though centrifuges were spinning out of control (though it's not clear how much

of this involved data and how much visuals).

But the persistent concern that the US not engage in such behaviors and now the apparent rising concern that someone would do the same to us sure raises questions about which financial institutions have already had their books cyber-cooked.