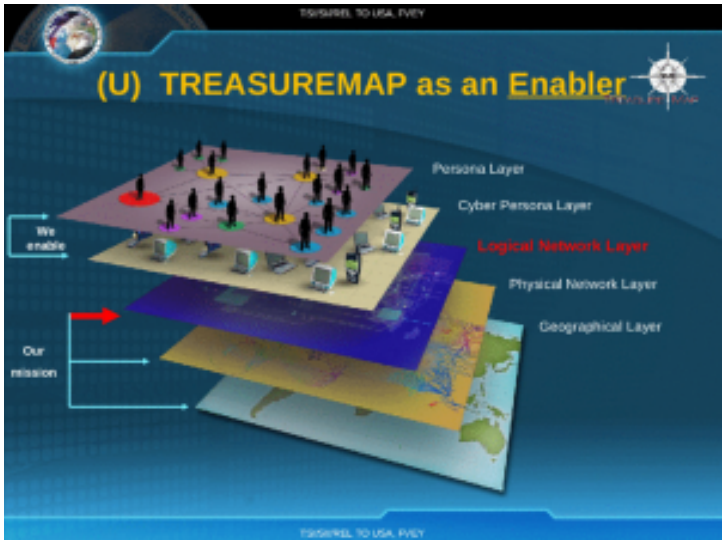
SOMEONE TREASURE MAPPED JP MORGAN



> Map the entire Internet — any device, anywhere, all the time. — NSA TREASUREMAP PPT

Last week, The Intercept and Spiegel broke the story of NSA's TREASUREMAP, an effort to map cyberspace, relying on both NSA's defensive (IAD) and offensive (TAO) faces.

As Rayne laid out, it aspires to map out cyberspace down to the device level. As all great military mapping does, this will permit the US to identify strategic weaknesses and visualize a battlefield — even before many of adversaries realize they're on a battlefield.

Against that background, NYT provided more details on the penetration of JP Morgan's networks that has been blamed on Russia. The new details make it clear this was about reconnaissance, not — at least not yet — theft.

> Over two months, hackers gained entry to dozens of the bank's servers, said three people with knowledge of the bank's investigation into the episode who spoke on the condition of anonymity. This, they said, potentially gave the hackers a window into how the bank's individual

> computers work.
>
> They said it might be difficult for the bank to find every last vulnerability and be sure that its systems were thoroughly secured against future attack.
>
> The hackers were able to review information about a million customer accounts and gain access to a list of the software applications installed on the bank's computers. One person briefed said more than 90 of the bank's servers were affected, effectively giving the hackers high-level administrative privileges in the systems.
>
> Hackers can potentially crosscheck JPMorgan programs and applications with known security weaknesses, looking for one that has not yet been patched so they can regain access.

Though the infiltrators did observe metadata — which, the NSA assures us, is not really all that compromising.

> A fourth person with knowledge of the matter, also speaking on condition of anonymity, said hackers had not gained access to account holders' financial information or Social Security numbers, and may have reviewed only names, addresses and phone numbers.

I'm not trying to make light of the mapping of one of America's most important banks. Surely, such surveillance may enable the same kind of sophisticated attack we launched against Iran, having done similar kind of preparation.

But we should keep in mind what the US has been doing as we consider these reports. If and when Russia or Germany catch us conducting similar reconnaissance on the networks of their private companies, they will surely make a big stink, as

we have been with JP Morgan (though the response to the Spiegel story has been muted enough I suspect Germany's intelligence services knew about that one, particularly given NSA's reliance on Germany for targets in Africa).

But if the US is going to treat digital reconnaissance as routine spying (and the President's cyberwar Presidential Policy Directive makes it pretty clear we consider our own similar reconnaissance to be mere clandestine spying), then we should expect the same treatment of our most lucrative targets.

That doesn't make it legal or acceptable. But that does make it equivalent to what we're doing to the rest of the world.

One final point. If you're going to map the entire Internet, any device, anywhere, by definition you need to map America's Internet as well. Are we so sure our own Intelligence Community hasn't been snooping in JP Morgan's networks?