NSA'S CORRUPTION OF CRYPTOGRAPHY AND ITS METHODS OF COERCION

Just one more day to give as part of Emptywheel's fundraising week.

I want to return to last week's Edward Snowden related scoop (Guardian, ProPublica/NYT) that the NSA has corrupted cryptography. Remember, there are several reasons the story was important:

- NSA lost the battle for the Clipper Chip and turned instead to achieve the same goals via means with less legal sanction
- NSA broke some companies' encryption by "surreptitiously stealing their encryption keys or altering their software or hardware"
- NSA also worked to "deliberately weaken[] the international encryption standards adopted by developers"

One key result of this — as Rayne and Julian Sanchez have emphasized — is to make everyone more exposed to hackers.

> This is a bit like publishing faulty medical research just to prevent a particular foreign dictator from being cured. It makes everyone on the Internet more vulnerable, increasing the chances that dissidents will be uncovered by despotic regimes and that corporations

> will fall victim to cybercriminals.
>
> [snip]
>
> Bear this in mind the next time you see people on Capitol Hill wringing their hands about the threat of a possible "Digital Pearl Harbor"—especially if they think the solution is to give more data and authority to the NSA. Because the agency is apparently perfectly happy to hand weapons to criminals and hostile governments, as long as it gets to keep spying too.

And since then, the NSA has responded to rampant cyberattacks and threats of them against targets it cares about by demanding yet more access to those targets' data, as explained by Shane Harris in a Keith Alexander profile.

> Under the Defense Industrial Base initiative, also known as the DIB, the NSA provides the companies with intelligence about the cyberthreats it's tracking. In return, the companies report back about what they see on their networks and share intelligence with each other.
>
> Pentagon officials say the program has helped stop some cyber-espionage. But many corporate participants say Alexander's primary motive has not been to share what the NSA knows about hackers. It's to get intelligence from the companies — to make them the NSA's digital scouts. What is billed as an information-sharing arrangement has sometimes seemed more like a one-way street, leading straight to the NSA's headquarters at Fort Meade.
>
> "We wanted companies to be able to share information with each other," says the former administration official, "to create a picture about the threats against them. The NSA wanted the

> picture."
>
> After the DIB was up and running, Alexander proposed going further. "He wanted to create a wall around other sensitive institutions in America, to include financial institutions, and to install equipment to monitor their networks," says the former administration official. "He wanted this to be running in every Wall Street bank."
>
> That aspect of the plan has never been fully implemented, largely due to legal concerns. If a company allowed the government to install monitoring equipment on its systems, a court could decide that the company was acting as an agent of the government. And if surveillance were conducted without a warrant or legitimate connection to an investigation, the company could be accused of violating the Fourth Amendment. Warrantless surveillance can be unconstitutional regardless of whether the NSA or Google or Goldman Sachs is doing it.
>
> "That's a subtle point, and that subtlety was often lost on NSA," says the former administration official. "Alexander has ignored that Fourth Amendment concern."

With all that as background, I want to return to a post I did months ago, laying out the methods the Presidential Policy Directive on Cyberwar envisioned for getting cooperation from private companies. It defines four kinds of access to private computer networks:

- Network defense, which is what network owners do or USG (or contractors) do at their behest to protect key

networks. I assume this like anti-virus software on steroids.

- Cyber collection that, regardless of where it occurs, is done in secret. This is basically intelligence gathering about networks.
- Nonintrusive Defensive Countermeausres, which is more active defensive attacks, but ones that can or are done with the permission of the network owners. This appears to be the subset of Defensive Cybereffects Operations that, because they don't require non-consensual network access, present fewer concerns about blowback and legality.
- Defensive Cybereffects Operations, which are the entire category of more active defensive attacks, though the use of the acronym DCEO appears to be limited to those defensive attacks that require non-consensual access to networks and therefore might cause problems. The implication is they're generally targeted outside of the US, but if there is

> an imminent threat (that phrase again!) they can be targeted in the US.

In the area of cyberdefense or offense (remember, this is an overlapping part of NSA's mission with cryptography) the government envisions collecting information (because cryptography overlaps with this mission, this might be included in that secret data collection) without a network owner's consent, conducting defensive measures with a network owner's consent, or conducting defensive measures without a network owner's consent (the latter is only supposed to happen in the US with the President's authorization).

Thus far, the way the government envisions cooperating with private entities seems to parallel how, according to the Snowden leak, it deals with cryptography: it gets it through open cooperation, persuasive "cooperation," stealing, and more intrusive access onto private networks (though it's unclear whether the latter, in the cyrptography context, requires Presidential approval).

Then there's the PPD section on partnerships to conduct cybersecurity, which also appear to involve carrots and sticks (including of the regulatory kind).

> The United States Government shall seek partnerships with industry, other levels of government as appropriate, and other nations and organizations to promote cooperative defensive capabilities, including, as appropriate, through the use of DCEO as governed by the provisions in this directive; and
>
> Partnerships with industry and other levels of government for the protection of critical infrastructure shall be coordinated with the Department of Homeland Security (DHS), working with the relevant sector-specific agencies

> and, as appropriate, the Department of Commerce (DOC). (S/NF)
>
> [snip]
>
> The United States Government shall work with private industry — through DHS, DOC, and relevant sector-specific agencies — to protect critical infrastructure in a manner that minimizes the need for DCEO against malicious cyber activity; however, the United States Government shall retain DCEO, including anticipatory action taken against imminent threats, as governed by the provisions in this directive, as an option to protect such infrastructure. (S/NF)
>
> The United States Government shall — in coordination, as appropriate, with DHS, law enforcement, and other relevant departments and agencies, to include sector-specific agencies — obtain the consent of network or computer owners for United States Government use of DCEO to protect against malicious cyber activity on their behalf, unless the activity implicates the United States' inherent right of self-defense as recognized in international law or the policy review processes established in this directive and appropriate legal reviews determine that such consent is not required. (S/NF) [my emphasis]

Again, this is an overlapping mandate, not coextensive with cryptography. But this does show what kind of relationships NSA envisions to combat security problems that NSA exacerbated. And it provides some idea of what carrots and sticks it might use to get companies to cooperate on cryptography (the biggest difference is that DHS would almost certainly not be involved in cryptography discussions).

If the relationships are similar, it suggests

the government would,

- Ask for voluntary cooperation in the name of national defense (most companies would have even less incentive to cooperate to compromise their cryptography, which may explain the financial companies unwillingness to let NSA on their networks, though this is the kind of cooperation AT&T seems happy to offer for a fee)
- Ask for cooperation with the involvement of sector-specific agencies that also happen to be regulators
- Involve Department of Commerce
- Invoke the inherent right to self defense (which is Article II authority) and take what is necessary without telling

There's a lot that is troubling in application of cybersecurity but would be at least as troubling if applied in the name of cryptography (remember, as with the Clipper Chip, Congress has refused to authorize this kind of broad access legislatively). But you can see how inherent self defense, applied to crytography in the same way it might be for cybersecurity, might be invoked to just take or steal.

But I keep coming back to the role of the Commerce Department. What role would the Commerce Department have that regulatory agencies specific to an industry would not?

While I don't think it begins to scratch the surface of any role that Commerce might have, remember that the standards body that NSA used to weaken an international encryption standard, National Institute of Standards and Technology, is part of Commerce. They've released a statement reopening public comment on the standard NSA weakened, but also explaining that they consult with NSA because they are required to by statute. (See more on NIST's efforts to restore confidence here.)

> NIST has a long history of extensive collaboration with the world's cryptography experts to support robust encryption. The National Security Agency (NSA) participates in the NIST cryptography development process because of its recognized expertise. NIST is also required by statute to consult with the NSA.
>
> Recognizing community concern regarding some specific standards, we reopened the public comment period for Special Publication 800-90A and draft Special Publications 800-90B and 800-90C to give the public a second opportunity to view and comment on the standards.

Again, I don't think mandated consultation with NSA would provide leverage to force a company to accept NSA's cybersecurity "help," but I find the possibility that the government is using these standards as pressure interesting.

In any case, it's sort of moot. So long as the President can invoke the inherent right to self defense to go thwart a cyberattack or (if that's the authority used) take some keys, it gives private companies little protection.