WHAT OBAMA'S PRESIDENTIAL POLICY DIRECTIVE ON CYBERWAR SAYS ABOUT NSA'S RELATIONSHIP WITH CORPORATIONS

The Guardian has had three big scoops this week: revealing that Section 215 has, indeed, been used for dragnet collection of US person data, describing PRISM, a means of accessing provider data in real-time that was authorized by the FISA Amendments Act, and publishing Obama's Presidential Directive on offensive cyberwar.

The latter revelation has received a lot less coverage than the first two, perhaps because it doesn't affect most people directly (until our rivals retaliate). "Of course Obama would have a list of cybertargets to hit," I heard from a number of people, with disinterest.

But I thought several passages from Obama's PPD-20 are of particular interest for the discussion on the other two scoops — particularly what degree of access PRISM has to corporate networks real-time data. First, consider the way definitions of several key terms pivot on whether or not network owners know about a particular cyber action.

> Network Defense: Programs, activities, and the use of tools necessary to facilitate them (including those governed by NSPD-54/HSPD-23 and NSD-42) **conducted on a computer network, or information or communications system by the owner or with the consent of the owner and, as appropriate, the users** for the primary purpose of protecting (1) that computer, network, or system; (2) data stored on, processed on, or transiting that computer, network, or

> system; or (3) physical and virtual infrastructure controlled by that computer, network, or system. **Network defense does not involve or require accessing or conducting activities on computers, networks, or information or communications systems without authorization from the owners or exceeding access authorized by the owners**. (u)
>
> [snip]
>
> Cyber Collection: Operations and related programs or activities conducted by or on behalf of the United States Government, in or through cyberspace, for the primary purpose of collecting intelligence – including from information that can be used for future operations – from computers, information or communications systems, or networks with the intent to remain undetected. **Cyber collection entails accessing a computer, information system, or network without authorization from the owner** or operator of the computer, information system, or network or from a party to a communication **or by exceeding authorized access**. Cyber collection includes those activities essential and inherent to enabling cyber collection, such as inhibiting detection or attribution, even if they create cyber effects. (C/NF)
>
> Defensive Cyber Effects Operations (DCEO): Operations and related programs or activities – other than network defense or cyber collection – conducted by or on behalf of the United States Government, in or through cyberspace, that are intended to enable or produce cyber effects outside United States Government networks for the purpose of defending or protecting against imminent threats or ongoing attacks or malicious

> cyber activity against U.S. national interests from inside or outside cyberspace. (C/NF)
>
> Nonintrusive Defensive Countermeasures (NDCM): The subset of DCEO that **does not require accessing computers, information or communications systems, or networks without authorization from the owners or operators** of the targeted computers, information or communications systems, or networks exceeding authorized access and only creates the minimum cyber effects needed to mitigate the threat activity. (C/NF)

So you've got:

- 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 other words, this schema (there are a few more categories, including strictly offensive attacks) seems to be about ensuring there is additional review for defensive attacks (but not strictly data collection) intended to use non-consensual network access.

As I suggested, these attacks based on nonconsensual access is all supposed to be primarily focused externally, unless the President approves.

> The United States Government shall conduct neither DCEO nor OCEO that are intended or likely to produce cyber effects within the United States unless approved by the President. A department or agency, however, with appropriate authority may conduct a particular case

> of DCEO that is intended or likely to produce cyber effects within the United States if it qualifies as an Emergency Cyber Action as set forth in this directive and otherwise complies with applicable laws and policies, including Presidential orders and directives. (C/NF)

Of course, a lot of the networks or software outside of the US are still owned by US corporations (and the implication seems to be that these categories remain even if they're not). Consider, for example, how central Microsoft exploits have been to US offensive attacks on Iran. How much notice has MS gotten that we planned to use the insecurity of their software?

Nevertheless, a big chunk of this PPD — the part that has received endless discussion publicly — pertains to that network defense, getting corporations to either defend their own networks properly or agree to let the government do it for them. (Does the USG bill for that, I wonder?)

Which partly explains the language in the PPD on partnerships with industry, treated as akin to partnerships with states or cities.

> 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)

One thing I'm most curious about this PPD is the treatment of the Department of Commerce. Why is DOC treated differently than sector-specific agencies? Do they have some kind of unseen leverage — a carrot or a stick — to entice cooperation that we don't know about?

Aside from that, though, there are two possibilities (which probably amounts to just one) when the government will go in and defend a company's networks without their consent.

Imminent threat, inherent right to self-defense.

Ultimately, this seems to suggest that the government will negotiate access, but if it deems your networks sufficiently important (Too Big To Hack) and you're not doing the job, it'll come in and do it without telling you.

And of course, nothing in this PPD explicitly limits cyber collection – that is, the non-consensual access of networks to collect information. I will wait to assume that suggests what it seems to, but it does at least seem a giant hole permitting the government to access networks so long as it only takes intelligence about the network.

Which brings us to these two categories included among the policy criteria.

> Transparency: The need for consent or notification of network or computer owners or host countries, the potential for impact on U.S. persons and U.S. private sector networks, and the need for any public or private communications strategies after an operation; and
>
> Authorities and Civil Liberties: The available authorities and procedures and the potential for cyber effects inside the United States or against U.S. persons. (S/NF)

Neither is terrifically well-developed. Indeed, it doesn't seem to consider civil liberties, as such, at all. Which may be why the Most Transparent Administration Evah™ considers transparency to consist of:

- Informing corporations that own networks
- Accounting for the impact on US persons (but not informing them, apparently, though Network Defense allows users to be informed "as appropriate")

- Prepping propaganda for use after an operation

The entire PPD lays out potential relationships with corporations as negotiated, potentially leveraged, but coerced if need be. But at least corporations are assumed be entitled to some “transparency.”