THE IP POLICE ARMED WITH INTERNET VULNERABILITIES

The White House Cybersecurity Coordinator, Michael Daniel, has a post purporting to lay out "established principles" on when the Administration would and would not disclose software and hardware vulnerabilities.

I've got a more thorough read below the rule, but I want to focus on one particular line. Daniel describes the downside of disclosing vulnerabilities as losing intelligence.

> Disclosing a vulnerability can mean that we forego an opportunity to collect crucial intelligence that could thwart a terrorist attack [sic] stop the theft of our nation's intellectual property, or even discover more dangerous vulnerabilities that are being used by hackers or other adversaries to exploit our networks.

That is, Daniel lays out three threats — terrorism, "hackers or other adversaries," and IP thieves — that require we use vulnerabilities to combat.

The inclusion of terrorism is not a surprise. That's the excuse NSA has been using since last June to justify its work.

Cybersecurity ("hackers or other [presumably far more threatening] adversaries") is the threat that NSA was focused on until such time as it needed to chant terror terror terror to get people to buy into the dragnet. Not only is it not a surprise, but it's probably the most urgent reason to use vulnerabilities (even if the threat in question is really far more serious than hackers).

But IP thieves?

To be fair, by this Daniel may be meaning Lockheed-Martin's intellectual property, by which he really means that intellectual property that we fetishize as private property but is really national security. (I've got a question in with the White House on this point.) But stated as he does, it could as easily mean Monsanto and Pfizer and even Disney.

In fact, he may well mean that. As I noted, in its original statement, the Administration made quite clear they would use Zero Days for law enforcement as well as national security purposes. Moreover, as I have also noted, NSA rewrote the legally mandated minimization standards in its secret procedures to equate threats to property with threats to life and body, thereby permitting itself to keep data that reveals threats to property that are not otherwise evidence of crime indefinitely (with DIRNSA approval).

And all that's assuming only NSA will exploit Zero Days. There's no reason to assume that the FBI (and other law enforcement agencies, including DEA) aren't using them.

I'm not sure that's a bad thing either. Several great security experts recently endorsed using hacks for law enforcement, though insisted that overall security must not be compromised.

That's the point though: how low is the bar for exploiting vulnerabilities? And if they are going to be used for law enforcement purposes — to chase IP thieves rather than threats to our nation — why isn't it more public?

Here are some additional comments:

Note how Daniel refers to NSA's denial in Heartbleed:

> Earlier this month, the NSA sent out a Tweet making clear that it did not know about the recently discovered vulnerability in OpenSSL known as

> Heartbleed.

I find it notable that he was that specific given allegations of other NSA knowledge of SSL vulnerabilities.

Here's how Daniel describes the interagency process that was rolled out in secret in response to the Presidential Review Group.

> This spring, we re-invigorated our efforts to implement existing policy with respect to disclosing vulnerabilities — so that everyone can have confidence in the integrity of the process we use to make these decisions.
>
> [snip]
>
> We have also established a disciplined, rigorous and high-level decision-making process for vulnerability disclosure. This interagency process helps ensure that all of the pros and cons are properly considered and weighed.

He makes no mention, though, that it came in response to the PRG (which in turn came in response to Edward Snowden's disclosures, including disclosures about the Bullrun program aiming to create back doors). Nor does he describe us an even more basic detail: what entities get included in that interagency process (the PRG was quite specific about the entities that should be involved).

Note the description of the Internet's role in US power, including "projecting power."

> We rely on the Internet and connected systems for much of our daily lives. Our economy would not function without them. Our ability to project power abroad would be crippled if we could not depend on them. For these reasons, disclosing vulnerabilities usually makes sense. We need these systems to be secure as much as, if not more so, than everyone else.

That's a hint of an admission of the Internet's role in our own hegemonic position, though not an explanation of all that entails. Again, that's something that should be part of the public discussion.

Finally, here's the list of the questions Daniel says unnamed stakeholders in this process will ask.

- How much is the vulnerable system used in the core internet infrastructure, in other critical infrastructure systems, in the U.S. economy, and/or in national security systems?
- Does the vulnerability, if left unpatched, impose significant risk?
- How much harm could an adversary nation or criminal group do with knowledge of this vulnerability?
- How likely is it that we would know if someone else was exploiting it?
- How badly do we need the intelligence we think we can get from exploiting the vulnerability?
- Are there other ways we can get it?
- Could we utilize the vulnerability for a short period of time before we disclose it?
- How likely is it that someone else will discover

the vulnerability?
- Can the vulnerability be patched or otherwise mitigated?

Folks on Twitter yesterday suggested that some of these questions – especially the one purporting to know whether anyone else will find a vulnerability – betray a real arrogance about our ability to know these things.

I guess that makes it easier to use this stuff for law enforcement, as well as larger national security, problems.