US OFFICIAL POSITION SAYS HACKING IS PERMISSIBLE?

According to LAT's Ken Dilanian, it is the "official position" of the US government that some kinds of hacking are "permissible."

> The official U.S. position — that governments hacking governments for military and other official secrets is permissible, but governments hacking businesses for trade secrets is not — is a tougher sell these days.

He makes the claim in an article that originally claimed Edward Snowden's leaks have set back cybersecurity efforts, but then had to issue a correction acknowledging CISPA probably wasn't going to happen anyway.

> An article in the Feb. 2 Section A on the effects of Edward Snowden's leaks of National Security Agency secrets said the White House backed the Cyber Intelligence Sharing and Protection Act, a cybersecurity measure. The White House threatened to veto the proposed bill in April. —

I take from this correction that Dilanian was fairly uncritically repeating the claims of NSA boosters — as other reporters have credulously repeated claims about the way Snowden's leaks will affect cybersecurity initiatives.

Which is why I find his description of this "official position" so interesting.

I'm not aware of the US endorsing any official (public) policy on the kinds of hacks NSA (and CyberCommand) are permitted. Congress has tried to put some limits on it — or at least get briefing on it. And Keith Alexander successfully fought for a lot more autonomy over the hacks he

could do.

The Executive does, however, have an official policy **on SIGINT**: President Obama's recent Presidential Policy Directive. But a SIGINT official position and a hacking policy are not necessarily the same thing. While hacking is one way we collect SIGINT (though I don't think NSA has admitted to that), we also conduct hacking for offensive purposes.

Even assuming they were the same thing, Dilanian's characterization would be a misstatement of the policy in any case.

The actual policy permits the collection of SIGINT for broadly defined foreign intelligence purposes.

> Thus, " foreign intelligence " means " information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists,

Of course, corporations are, under US law, both "organizations" and "persons," so this definition permits spying on foreign corporations (other intelligence documents lay this out explicitly).

And the PPD does permit the collection of foreign private commercial information to protect US and allies' national security.

> The collection of foreign private commercial information or trade secrets is authorized only to protect the national security of the United States or its partners an d allies. It is not an authorized foreign intelligence or counterintelligence purpose to collect such information to afford a competitive advantage 4 to U.S. companies and U.S. business sectors commercially.

This is, frankly, where our hypocrisy on hacking

(and SIGINT) begins to fall apart, given that China would maintain that stealing our military (and energy and tech) secrets are a matter of national security, and the fact that our government maintains more nominal separation from the companies that develop such things than China does should not shield those companies from spying.

And then, finally, the limits on data collection don't apply when the NSA is working to develop SIGINT capabilities.

> it shall not apply to signals intelligence activities undertaken to test or develop signals intelligence capabilities.

Given that some of our alleged hacking seems to support efforts to develop new hacking capabilities, this exception could prove infinitely recursive, especially given the rules on information collection in the name of cyberdefense and attacks. And of course, when we exploited Siemens' SCADA industrial control systems to attack Iran, we used a corporate competitor's trade secrets in the name of national security.

That is, even ignoring how America's self-interested standard simply defines our national security in terms that legitimize our own hacking, when you get into the interaction of our intelligence to hack which serves to collect intelligence, the rules on SIGINT basically fall apart.

But hey. If the US says hacking of official government secrets is "permissible," then maybe DOJ will withdraw the charges against Edward Snowden?