OBAMA AND XI SET UP A RED CYBERPHONE

Here are the terms of the cyber agreement announced today.

- The United States and China agree that timely responses should be provided to requests for information and assistance concerning malicious cyber activities. Further, both sides agree to cooperate, in a manner consistent with their respective national laws and relevant international obligations, with requests to investigate cybercrimes, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory. Both sides also agree to provide updates on the status and results of those investigation to the other side, as appropriate.
- The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent

of providing competitive advantages to companies or commercial sectors.

- Both sides are committed to making common effort to further identify and promote appropriate norms of state behavior in cyberspace within the international community. The United States and China welcome the July 2015 report of the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International security, which addresses norms of behavior and other crucial issues for international security in cyberspace. The two sides also agree to create a senior experts group for further discussions on this topic.
- The United States and China agree to establish a high-level joint dialogue mechanism on fighting cybercrime and related issues. China will designate an official at the ministerial level to be the lead and the Ministry of Public Security, Ministry of State Security, Ministry of Justice, and the State

> Internet and Information Office will participate in the dialogue. The U.S. Secretary of Homeland Security and the U.S. Attorney General will co-chair the dialogue, with participation from representatives from the Federal Bureau of Investigation, the U.S. Intelligence Community and other agencies, for the United States. This mechanism will be used to review the timeliness and quality of responses to requests for information and assistance with respect to malicious cyber activity of concern identified by either side. As part of this mechanism, both sides agree to establish a hotline for the escalation of issues that may arise in the course of responding to such requests. Finally, both sides agree that the first meeting of this dialogue will be held by the end of 2015, and will occur twice per year thereafter.

The structure of these bullets, which comes from the White House, is rather interesting. The first and last simply announce an effort to agree to cooperate on cyber issues, with the

first bullet announcing the principle and the last describing the nitty gritty of it. Basically, this is a call to implement a red phone — like the one Russia and the US had for nukes — for cybersecurity.

The third bullet, "welcoming" the UN Group of Government Experts report, is also about confidence building.

Which leaves the second bullet, which (unless I'm mistaken) goes far beyond what Obama noted in his press conference with Xi Jinping, but *Xi did note in his speech*: an agreement "that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors," that is, that China stop using hacks to steal from US companies. While the US does steal confidential business information, they don't do so for competitive advantage of commercial sectors, though I can imagine some scenarios that China might claim did so. I imagine they'll complain some about our spying on trade negotiations, for example, which probably would fall under this agreement.

I don't think anyone thinks China will do this (though note the wiggle room in the "conduct or knowingly support" language). Instead, I suspect all the other language about confidence building intends to provide the US a means to more directly complain about this (and perhaps trade off corruption targets for hacker targets?).

Finally, note what was not included: Any promise to end spying for intelligence, like the OPM hack and/or US use of XKeyscore to accomplish the same kind of bulk collection. As I've said, I think that hacking might, for the short term, actually help confidence building measures, as it might provide some kind of transparency, though not verification.

We shall see whether a Red Phone for cyber will

do any good.

Update: Herb Lin notes that the Red Phone idea is good in theory but hasn't always worked as it should with China.

> Clearly a good thing in principle. But implementation is an issue, and experience with other hotlines between the United States and China has not always been positive. A case in point is the military hotline between the United States and China, intended to enable direct communications between senior military leaders on both sides during crisis, has not always been operational even during routine tests of the system. On several occasions in which the line was tested for operational capability and also in the wake of the 2001 EP-3 incident over Hainan, the Chinese military failed to respond at all. In addition, the purview seems to be limited to cybercrime (whatever that might mean) and not to cyber issues related to national security.