US TRADE REP COMPLAINS OTHER COUNTRIES AREN'T LETTING NSA SPY

In the NYT, David Sanger describes US efforts to develop some common understanding over cyberattacks with China by briefing it on what our escalation process would be. Unsurprisingly, China (which hasn't had a massive data leak as an excuse to admit to information now in the public domain) has no reciprocated.

And while Sanger makes it clear the US is still not admitting to StuxNet, his US sources are coming to understand that the rationalizations we use to excuse our spying aren't really as meaningful as we like to tell ourselves.

> Mr. Obama told the Chinese president that the United States, unlike China, did not use its technological powers to steal corporate data and give it to its own companies; its spying, one of Mr. Obama's aides later told reporters, is solely for "national security priorities." But to the Chinese, for whom national and economic security are one, that argument carries little weight.
>
> "We clearly don't occupy the moral high ground that we once thought we did," said one senior administration official.

I especially love the spectacle of an SAO coming to grips with this, but doing so anonymously.

Yet this anonymous admission will not stop the US from imposing such double standards. On Friday, the US Trade Representative issued its yearly report on barriers to trade in telecom and related industries. (Reuters reported on the report here.) None of these complaints are

explicitly about the NSA. And some of USTR's demands — that Turkey stop shutting down services like Twitter — would make it harder for other countries to spy on their own citizens.

But many of the USTR's complaints single out measures that are either deliberately meant to undermine NSA's spying advantages, or would have the effect of doing so. So these complaints also amount to whining that other countries are making NSA's job harder.

Consider some of the complaints against China, whose top equipment manufacturer Huawei the US has excluded from not only the US, but also Korea and Australia.

It complains about China's limits on telecom providers — and pretends this is exclusively a trade issue, not a national security issue.

> Moreover, the Chinese Government still owns and controls the three major basic telecom operators in the telecommunications industry, and appears to see these entities as important tools in broader industrial policy goals, such as promoting indigenous standards for network equipment.

USTR criticizes China's categorization of business that can be used for spying — such as cloud computing firms — as a telecoms subject to licensing restrictions.

> China's equity restrictions on foreign participation constitute a major impediment to market access in China. These restrictions are compounded by China's broad interpretation of services requiring a telecommunications license (and thus subject to equity caps) and narrow interpretation of the specific services foreign firms can offer in these sub-sectors.
>
> [snip]
>
> Several VAS definitions in the draft

> Catalog also raise trade restriction concerns. First, the draft Catalog created a new category of “Internet Resource Collaboration Services” that appears to covers all aspects of cloud computing. (Cloud computing is a computer service or software delivery model, and should not be misclassified as a telecommunications service.) MIIT approach to cloud computing generally raises a host of broad concerns. Second, the draft Catalog significantly expanded the definition of “Information Services” to include software application stores, software delivery platforms, social networking websites, blogs, podcasts, computer security products, and a number of other Internet and computing services. These services simply use the Internet as a platform for providing business and information to customers, and thus should not be considered as telecommunications services.

USTR complains about Chinese requirements for encryption both for information systems tied to critical infrastructure.

> Starting in 2012, both bilaterally and during meetings of the WTO’s Committee on Technical Barriers to Trade, the United States raised its concerns with China about framework regulations for information security in critical infrastructure known as the Multi-Level Protection Scheme (MLPS), first issued in June 2007 by the Ministry of Public Security (MPS) and the Ministry of Industry and Information Technology (MIIT). The MLPS regulations put in place guidelines to categorize information systems according to the extent of damage a breach in the system could pose to social order, public interest, and national security. The MLPS regulations also appear to require

> buyers to comply with certain information security technical regulations and encryption regulations that are referenced within the MLPS regulations. If China issues implementing rules for the MLPS regulations and applies the rules broadly to commercial sector networks and IT infrastructure, they could adversely affect sales by U.S. information security technology providers in China.

And for providers on its 4G network.

> At the end of 2011 and into 2012, China released a Chinese government-developed 4G Long-Term Evolution (LTE) encryption algorithm known as the ZUC standard. The European Telecommunication Standards Institute (ETSI) 3rd Generation Partnership Project (3GPP) had approved ZUC as a voluntary LTE encryption standard in September 2011. According to U.S. industry reports, MIIT, in concert with the State Encryption Management Bureau (SEMB), informally announced in early 2012 that only domestically developed encryption algorithms, such as ZUC, would be allowed for the network equipment and mobile devices comprising 4G TD-LTE networks in China. It also appeared that burdensome and invasive testing procedures threatening companies' sensitive intellectual property could be required.
>
> In response to U.S. industry concerns, USTR urged China not to mandate any particular encryption standard for 4G LTE telecommunications equipment, in line with its bilateral commitments and the global practice of allowing commercial telecommunications services providers to work with equipment vendors to determine which security standards to incorporate into their networks.

Finally, USTR dubs China's limits on outsider VOIP services a trade restriction.

> Restrictions on VoIP services imposed by certain countries, such as prohibiting VoIP services, requiring a VoIP provider to partner with a domestic supplier, or imposing onerous licensing requirements have the effect of restricting legitimate trade or creating a preference for local suppliers, typically former monopoly suppliers.

All of these complaints, of course, can be viewed narrowly as a trade problem. But the underlying motivation on China's part is almost certainly about keeping the US out of its telecom networks, both to prevent spying and to sustain speech restraints behind the Great Firewall.

It's not just China about which USTR complains. It issues similar dual purpose (trade and spying) complaints against India and Colombia, among others.

And of course, it finds European plans to require intra-EU transit limits — a plan done largely to combat US spying — a 'draconian" trade restriction.

> In particular, Deutsche Telekom AG (DTAG), Germany's biggest phone company, is publicly advocating for EU-wide statutory requirements that electronic transmissions between EU residents stay within the territory of the EU, in the name of stronger privacy protection. Specifically, DTAG has called for statutory requirements that all data generated within the EU not be unnecessarily routed outside of the EU;
>
> [snip]
>
> The United States and the EU share common interests in protecting their citizens' privacy, but the draconian

> approach proposed by DTAG and others appears to be a means of providing protectionist advantage to EU-based ICT suppliers.

Meanwhile, even as I was writing this, one of the EU's top Data Privacy figures, Paul Nemitz, just floated making the reverse accusation against America, that its NSA spying is a trade impediment to European businesses trying to do business in the US.

Fun stuff.