THE CONTINUED BELIEF IN UNICORN CYBER DETERRENCE

For some reason, people continue to believe Administration leaks that they will retaliate against China (and Russia!) for cyberattacks — beyond what are probably retaliatory moves already enacted.

I think Jack Goldsmith's uncharacteristically snarky take is probably right. After cataloging the many past leaks about sanctions that have come to no public fruition, Goldsmith talks about the cost of this public hand-wringing.

> As I have explained before, figuring out how to sanction China for its cyber intrusions is hard because (among other reasons) (i) the USG cannot coherently sanction China for its intrusions into US public sector (DOD, OPM, etc.) networks since the USG is at least as aggressive in China's government networks, and (ii) the USG cannot respond effectively to China's cyber intrusions in the private sector because US firms and the US economy have more to lose than gain (or at least a whole lot to lose) from escalation—especially now, given China's suddenly precarious economic situation.
>
> But even if sanctions themselves are hard to figure out, the public hand-wringing about whether and how to sanction China is harmful. It is quite possible that more is happening in secret. "One of the conclusions we've reached is that we need to be a bit more public about our responses, and one reason is deterrence," a senior administration official in an "aha" moment told Sanger last month. One certainly hopes the USG is doing more in

> secret than in public to deter China's cybertheft. Moreover, one can never know what cross-cutting machinations by USG officials lie behind the mostly anonymous leaks that undergird the years of stories about indecisiveness.

This performance seems to be directed at domestic politics, because the Chinese aren't impressed.

A still crazier take, though, is this one, which claims DOJ thought indicting 5 PLA connected hackers last year would have any effect.

> But nearly a year and a half after that indictment was unveiled, the five PLA soldiers named in the indictment are no closer to seeing the inside of a federal courtroom, and China's campaign of economic espionage against U.S. firms continues. With Chinese President Xi Jinping set to arrive in Washington for a high-profile summit with President Barack Obama later this month, the question of how — and, indeed, if — the United States can deter China from pilfering American corporate secrets remains very much open. The indictment of the PLA hackers now stands out as a watershed moment in the escalating campaign by the U.S. government to deter China from its aggressive actions in cyberspace — both as an example of the creative ways in which the United States is trying to fight back and the limits of its ability to actually influence Chinese behavior.
>
> [snip]
>
> In hindsight, the indictment seems less like an exercise in law enforcement than a diplomatic signal to China. That's an argument the prosecutor behind the case, U.S. Attorney David Hickton, resents. "I believe that's absolute nonsense,"

> Hickton told Foreign Policy. “It was not the intention, when we brought this indictment, to at the same time say, ‘We do not intend to bring these people to justice.’”
>
> But it’s unclear exactly what has happened to the five men since Hickton brought charges against them. Their unit suspended some operations in the aftermath of the indictment, but experts like Weedon say the group is still active. “The group is not operating in the same way it was before,” she said. “It seems to have taken new shape.”
>
> Hickton, whose office has made the prosecution of cybersecurity cases a priority, says he considers the law enforcement effort against hackers to be a long-term one and likens it to indictments issued in Florida against South American drug kingpins during the height of the drug war. Then, as now, skeptics wondered what was the point of bringing cases against individuals who seemed all but certainly beyond the reach of U.S. law enforcement. Today, Hickton points out, U.S. prisons are filled with drug traffickers. Left unsaid, of course, is that drugs continue to flow across the border.

That’s because it fundamentally misunderstands what the five hackers got indicted for.

This indictment was not, as claimed, for stealing corporate secrets. It was mostly not for economic espionage, which we claim not to do.

Rather – as I noted at the time – it was for stealing information during ongoing trade disputes.

> But the other interesting aspect of this indictment coming out of Pittsburgh is that – at least judging from the charged

> crimes — there is far less of the straight out IP theft we always complain about with China.
>
> In fact, much of the charged activity involves stealing information about trade disputes — the same thing NSA engages in all the time. Here are the charged crimes committed against US Steel and the United Steelworkers, for example.
>
> > In 2010, U.S. Steel was participating in trade cases with Chinese steel companies, including one particular state-owned enterprise (SOE-2). Shortly before the scheduled release of a preliminary determination in one such litigation, Sun sent spearphishing e-mails to U.S. Steel employees, some of whom were in a division associated with the litigation. Some of these e-mails resulted in the installation of malware on U.S. Steel computers. Three days later, Wang stole hostnames and descriptions of U.S. Steel computers (including those that controlled physical access to company facilities and mobile device access to company networks). Wang thereafter took steps to identify and exploit vulnerable servers on that list.
> >
> > [snip]
> >
> > In 2012, USW was involved in public disputes over Chinese trade practices in at least two industries. At or about the time USW issued public statements regarding those trade disputes and related legislative proposals, Wen stole e-mails

> > from senior USW employees containing sensitive, non-public, and deliberative information about USW strategies, including strategies related to pending trade disputes. USW's computers continued to beacon to the conspiracy's infrastructure until at least early 2013.
>
> This is solidly within the ambit of what NSA does in other countries. (Recall, for example, how we partnered with the Australians to obtain information to help us in a clove cigarette trade dispute.)
>
> I in no way mean to minimize the impact of this spying on USS and USW. I also suspect they were targeted because the two organizations partner together on an increasingly successful manufacturing organization. Which would still constitute a fair spying target, but also one against which China has acute interests.
>
> But that still doesn't make it different from what the US does when it engages in spearphishing — or worse — to steal information to help us in trade negotiations or disputes.
>
> We've just criminalized something the NSA does all the time.

The reason this matters is because all the people spotting unicorn cyber-retaliation don't even understand what they're seeing, and why. I mean, Hickton (who as I suggested may well run for public office) may have reasons to want to insist he's championing the rights of Alcoa, US Steel, and the Steelworkers. But he's not implementing a sound deterrence strategy because — as Goldsmith argues — it's hard to imagine one

that we could implement, much less one that wouldn’t cause more blowback than good.

Before people start investing belief in unicorn cyber deterrence, they’d do well to understand why it presents us such a tough problem.