# NSA APOLOGISTS NOW BLAMING SNOWDEN FOR NSA'S OWN CYBERDEFENSE FAILURES

Read this claim about NSA spying, but don't laugh.

> "None of what the U.S. is doing is benefiting American business."

Did you manage not laughing at the notion that the US is spending $70 billion a year on spying and none of it — not one little bit of it! — benefits American businesses?

Didn't think so.

That quote, from Mandiant Chief Security Officer Richard Bejtlich, is just one of the utter absurdities built into this Kurt Eichenwald piece attempting to blame Edward Snowden for our failure to stop Chinese hacking of us.

Here's the logic.

> In May, [Tom] Donilon flew to Beijing to meet senior government officials there and set the framework for a summit between Obama and Chinese President Xi Jinping; Donilon and other American officials made it clear they would demand that hacking be a prime topic of conversation. By finally taking the step of putting public — and, most likely, international — pressure on the Chinese to rein in their cyber tactics, the administration believed it was about to take a critical step in taming one of the biggest threats to America's economic security.

> But it didn't happen. The administration's attempt to curb China's assault on American business and government was crippled — perhaps forever, experts say — by a then-unknown National Security Agency contractor named Edward Snowden.
>
> Snowden's clandestine efforts to disclose thousands of classified documents about NSA surveillance emerged as the push against Chinese hacking intensified. He reached out to reporters after the public revelations about China's surveillance of the *Times*'s computers and the years of hacking by Unit 61398 into networks used by American businesses and government agencies. On May 24, in an email from Hong Kong, Snowden informed a *Washington Post* reporter to whom he had given documents that the paper had 72 hours to publish them or he would take them elsewhere; had the *Post* complied, its story about American computer spying would have run on the day Donilon landed in Beijing to push for Chinese hacking to be on the agenda for the presidential summit.
>
> The first report based on Snowden's documents finally appeared in *The Guardian* on June 5, two days before the Obama-Xi meeting, revealing the existence of a top-secret NSA program that swept up untold amounts of data on phone calls and Internet activity. When Obama raised the topic of hacking, administration officials say, Xi again denied that China engaged in such actions, then cited *The Guardian* report as proof that America should not be lecturing Beijing about abusive surveillance. [my emphasis]

Let's review what Eichenwald has done here.

First, he has taken the Administration at its word that publicly shaming China, and then negotiating with them, would have slowed their cybertheft.

Next, he has insinuated — though not provided evidence — that both Snowden's initial leaks and the timing of their release (which, after all, took place at different times) were all intentionally rather than coincidentally linked to the US effort to rein in Chinese hacking, and done at the direction of Snowden (that may be the case, but he hasn't presented it, and if that were Snowden's real intent, you would think he would have leaked specifics about our attacks on China weeks before he did).

He has highlighted an email (did he somehow get the content of an Edward Snowden email to Barton Gellman? Because I can't imagine Gellman sharing this.) threatening to take his documents somewhere else, without thinking through what it means that he already had gone somewhere else or considering other reasons (he was holed in a hotel room, for example) why Snowden might have had some urgency for publishing. [Update: Here's where that claim came from.]

And then he has Xi's comments on America's own hacking, which Eichenwald suggests was a response to the Section 215 and PRISM disclosures—"top-secret NSA program that swept up untold amounts of data on phone calls and Internet activity"

With me so far?

Curiously, Eichenwald makes no mention of the document that might actually bolster his case and which almost certainly was the reference Xi intended: the Presidential Policy Directive on cyberwar, which was released just hours before Obama's meetings with Xi started in CA.

But that would require painting a very different picture of what the US does in cyberspace than this one.

> The activities of the two sides,

> however, are vastly different in scope and intent. The United States engages in widespread electronic espionage, but that classified information cannot legally be handed over to private industry. China is using its surveillance to steal trade secrets, harm international competitors and undermine American businesses.

The US has, after all, conducted the most sophisticated cyberattack publicly known, StuxNet. Suggesting its activities consist solely of collection of intelligence (and suggesting that the US doesn't use the intelligence it collects to advance the interests of US companies, even while abundant evidence proves that incorrect, even sharing it with its defense contractors) minimizes both what it really does and — just as importantly — minimizes what China knew at that meeting. Moreover, in an article that describes China turning to hacking in response to seeing our military might in the first Gulf War, it doesn't consider what it would take for China to give up a weapon which offers it a more effective defense against the US than traditional military toys.

Nevertheless, some Obama types apparently believe — or at least are telling a very credulous Eichenwald they believe — that public shaming would have gotten a country that knew we had weaponized cyberspace to stop its own use of cyberattacks.

To get a sense of whether the claim that public shaming would have ended Chinese hacking, read this post from Jack Goldsmith, written as the Administration was pursuing this approach and 4 months before the first Snowden leak.

> [B]ecause talks with the Chinese haven't worked, "the Obama administration is *now considering* a range of actions," including "threats to cancel certain visas or put major purchases of Chinese

> goods through national security reviews." The story cites two former officials for the proposition that the USG is preparing a new National Security Estimate (NIE) that will "underscore the administration's concerns about the threat, and will put greater weight on plans for more pointed diplomatic and trade measures against the Chinese government." (The AP story sometimes talks of the threat from "cyber attack" but it is pretty clear from the context that the topic of the story is cyber exploitation.)
>
> What is puzzling is the tentativeness and slowness of the USG reaction given what the USG has been telling us – openly, and through leaks – about the enormous scale of the problem. One reason for tentativeness is that, as I once wrote, "the United States itself engages in [cyberexploitations] extensively abroad and [] cyber exploitations do not violate international law, and thus would not justify a large-scale military response, kinetic or cyber." This is a large hurdle, I think, that leaves the United States with only relatively weak diplomatic tools to address the problem – and tools, by the way, that open it up to reciprocal retaliation.
>
> [snip]
>
> I can imagine a norm developing where certain large-scale cyber exploitations are such a threat or violation of sovereignty and national security that they warrant an attack – kinetic or not – in response. I also believe, as I have long said, that the United States will not be able to clamp down on China's cyber exploitations by others unless it is willing to consider clamping down on its own

> cyberexploitations — both directly by the USG, and through its support of hacktivism in China. [my emphasis]

Goldsmith, months before any Snowden leaks, was saying that our own hacking would prevent this approach from working.

And, of course, Eichenwald's entire story doesn't consider whether the US has used the correct approach to defending our own networks. That is, he doesn't consider whether the US should have, instead of trying to shame someone for hacking that we were ourselves are hacking, instead invested in a better defense.

Again, we can go to commentary, from Thomas Rid, from that period in February when the US was just rolling out the shaming strategy.

> Indeed, the Obama administration has been so intent on responding to the cyber threat with martial aggression that it hasn't paused to consider the true nature of the threat. And that has lead to two crucial mistakes: first, failing to realize (or choosing to ignore) that offensive capabilities in cyber security don't translate easily into defensive capabilities. And second, failing to realize (or choosing to ignore) that it is far more urgent for the United States to concentrate on developing the latter, rather than the former.
>
> At present, the United States government is one of the most aggressive actors when it comes to offensive cyber operations, excluding commercial espionage. The administration has anonymously admitted that it designed Stuxnet (codenamed Olympic Games) a large-scale and protracted sabotage campaign against Iran's nuclear enrichment facility in Natanz that was unprecedented in scale and

> sophistication.
>
> [snip]
>
> Developing sophisticated, code-borne sabotage tools requires skills and expertise; they also require detailed intelligence about the input and output parameters of the targeted control system. The Obama administration seems to have decided to prioritize such high-end offensive operations. Indeed, the Pentagon's bolstered Cyber Command seems designed primarily for such purposes. But these kinds of narrowly-targeted offensive investments have no defensive value.
>
> So amid all the activity, little has been done to address the country's major vulnerabilities. The software that controls America's most critical infrastructure—from pipeline valves to elevators to sluices, trains, and the electricity grid—is often highly insecure by design, as the work of groups like Digital Bond illustrates. Worse, these systems are often connected to the internet for maintenance reasons, which means they are always vulnerable to attack.
>
> [snip]
>
> Defending these areas ought to be the government's top priority, not the creation of a larger Cyber Command capable of going on the offense.

Here's the thing: the US was failing in its efforts to combat Chinese hacking all by itself, long before Snowden even got hired at Booz. It has almost certainly been pursuing ineffective approaches to dealing with it, and that's even before you consider the way its enthusiasm for offensive cyberweapons has led it to tolerate holes and weak encryption in public software. Clearly, Snowden's leaks have made the shaming

strategy the Administration intended to pursue next harder, but to believe it would have worked in the first place would require underestimating Chinese interests in defending itself.

Snowden's disclosures may well have created a slew of difficulties, both diplomatic and tactical, for the US. But to blame our failure to stop Chinese hacking on Snowden is nothing more than scapegoating NSA's own failures.