

# WHAT IF CHINA NOT JUST HACKED — BUT SABOTAGED — THE F-35?

**Chinese cyberspies have hacked most Washington institutions, experts say**

Over the last week, two perennial stories have again dominated the news. China continues to be able to hack us — including top DC power players — at will. And the F-35 has suffered another setback, this time a crack in an engine turbine blade (something which reportedly happened once before, in 2007).

The coincidence of these two events has got me thinking (and mind you, I'm just wondering out loud here): what if China did more than just steal data on the F-35 when it hacked various contractors, and instead sabotaged the program, inserting engineering flaws into the plane in the same way we inserted flaws in Iran's centrifuge development via StuxNet?

We know China has hacked the F-35 program persistently. In 2008, an IG report revealed that BAE and some of the other then 1,200 (now 1,300) contractors involved weren't meeting security requirements; last year an anonymous BAE guy admitted that the Chinese had been camped on their networks stealing data for 18 months. In April 2009, WSJ provided a more detailed report on breaches going back to 2007.

The Joint Strike Fighter, also known as the F-35 Lightning II, is the costliest and most technically challenging weapons program the Pentagon has ever attempted. The plane, led by Lockheed Martin Corp., relies on 7.5 million lines of computer code, which the Government Accountability Office said is more than triple the amount used in the

current top Air Force fighter.

Six current and former officials familiar with the matter confirmed that the fighter program had been repeatedly broken into.

[snip]

Foreign allies are helping develop the aircraft, which opens up other avenues of attack for spies online. At least one breach appears to have occurred in Turkey and another country that is a U.S. ally, according to people familiar with the matter.

[snip]

Computer systems involved with the program appear to have been infiltrated at least as far back as 2007, according to people familiar with the matter. Evidence of penetrations continued to be discovered at least into 2008. The intruders appear to have been interested in data about the design of the plane, its performance statistics and its electronic systems, former officials said.

The intruders compromised the system responsible for diagnosing a plane's maintenance problems during flight, according to officials familiar with the matter.

[snip]

The spies inserted technology that encrypts the data as it's being stolen; as a result, investigators can't tell exactly what data has been taken.

And we know the data theft has been ongoing. The RSA secure ID hack two years ago, for example, was used to access Lockheed's computers (though at least in that case Lockheed discovered the breach within two weeks).

Incidentally, Pratt & Whitney – which makes the engines that are experiencing this latest problem – got a \$75 million wrist slap last year for violating export controls and dealing engine control module software to China that it then used to build a military attack helicopter, though that conduct dates back to the 2002 to 2006 period.

In any case, we know the Chinese have had a great deal of access to networks involved in the development of the program. The assumption has always been – publicly at least – that China was just stealing data, both to understand how to counter the plane's defenses but also to reverse engineer its own planes.

Yet we also know that China has dealt us hardware – “counterfeit” chips and the like – with backdoors to allow it access. That is, we know China has engaged in sabotage at a more granular level.

So why wouldn't China try to sabotage the F-35 more systematically, especially as the example of StuxNet unfolded?

Admittedly, it may be foolish to attribute to Chinese guile what can easily be explained by American incompetence. Indeed, it's clear mismanagement deserves a great deal of the blame for the plane's budgetary and performance woes.

But this Bloomberg article describes part of the reason why the F-35 would make such a juicy target for China. First, the F-35 is a central part of our industrial policy, providing jobs here and (if it ever gets off the ground) exports overseas.

It counts 1,300 suppliers in 45 states supporting 133,000 jobs – and more in nine other countries, according to Lockheed.

[snip]

The F-35 will probably become the dominant export fighter for the U.S.

aerospace industry, Gordon Adams, who served as the senior White House official for national security and foreign policy budgets under President Bill Clinton, said in a phone interview.

"This is the last U.S. export fighter standing, and that has saved this program," said Adams, now a foreign-policy professor at American University in Washington. "There is a huge economic element to the F-35."

Members of Congress are hesitant to make deep cuts to the project in part because it generates work in their states, Wheeler said. The F-35 supports 41,000 jobs in Texas alone, the most of any state, according to Lockheed's website. The company assembles the fighter in Fort Worth.

And the multinational development of the plane was supposed to cement a new kind of alliance. As members of that partnership begin to get cold feet, it may affect our larger relationship with those countries.

Overseas, the Pentagon's partners are balancing concerns about the F-35's cost with the amount of work sent to their companies.

Allies have agreed to purchase 721 fighters, yet the soaring price is painful for nations with shrinking defense budgets. The estimated cost of each plane has about doubled to \$137 million since 2001, according to a GAO report last year.

[snip]

Canada had dropped to 65 planes from 80. In December, it said it was reconsidering its commitment to purchase any of the jets after a consultant said

the price to buy and maintain them might reach about \$45 billion.

The F-35 program isn't so easy to exit, though. A Lockheed spokesman raised the possibility that Canada would lose its F-35-related business – and jobs – if it didn't buy planes.

[snip]

The partners' commitments should make the U.S. wary of making deep cuts to the F-35 program, said Dov Zakheim, a former defense comptroller who served under President George W. Bush.

"This program was advertised as a major collaborative program with a lot of allies," Zakheim said in a phone interview. "It was sold to our allies as such. What do we do now – pull the rug out from under them at the same time we're complaining they aren't spending enough on defense?"

This latest problem comes just as the those managing the F-35 program prepare to go to Australia to try to convince them to buy these planes rather than more existing Boeings.

Then there's just the sheer magnitude of this program. The program is expected to account for 38% of the Pentagon's procurement needs for 2011 programs. Its cost – \$395.7 billion – already rivals a significant war, and actually running the program may cost a trillion and a half. This is where an unbelievable amount of our time and financial resources are being directed, and anything China could do to raise those costs, or perhaps even convince us to give up on the sunk costs, I'm sure, would bring it huge strategic benefits. It's like half an Iraq War without the potentially dangerous disruptions in the Middle East, all wrapped up in a bow.

At this point, it's not clear that the plane

itself will ever represent a critical threat to China (though Japan has been one of the partners that has sustained its enthusiasm for the plane). The program is more interesting at this point for the way it causes us to blindly continue to pursue the catastrophic imperative that is our Military Industrial Complex. Which would make it the perfect opportunity for China, by sabotaging the program, to magnify and exacerbate our own stupidity.

I'd like to think such sabotage would be impossible to get past the quality control folks at Lockheed, but everything about this program suggests it might not be. The multinational development and the concurrent development schedule (a kind of testing as you go) would make it more likely such sabotage might be missed as well.

I don't know that we would ever know if this clusterfuck was caused with the assistance of China. It's not like Lockheed would publicize such information, just as it asked for another \$100 billion. And I don't want to underestimate the defense industry's ability to screw up all by themselves.

All that said, Chinese sabotage would help to explain part of why this program has been such a colossal clusterfuck.

---

## **JANE HARMAN NOW TARGETING INDIVIDUAL CYBERTARGETS WITH DRONE COURT**

Jane Harman's advocacy for a drone court suffers from the same problem I touched on here (and will lay out at more length in the next day or so): before you can have a Drone and/or Targeted

Killing Court, you need some law the court will apply. Harman seems to envision just applying the standards the Executive – not Congress – came up with, which isn't how Schoolhouse Rock taught me the government is supposed to work.

Congress, in her model, would just be fully apprised of what goes on in the Drone and/or Targeted Killing Court, not write law to limit what can be approved.

But I'm more interested – alarmed, really – by the way Harman seamlessly adds cybertargeting to her advocacy.

The FISA court, renamed the CT Court, could also oversee drones **and cyber**. A FISA court application must show that specific individuals are connected to a foreign power – which is defined, in part, as a group engaged in international terrorism. Drone **and cyber** applications could (1) list the individual/**cyber target** against whom the lethal operation is directed and (2) submit a finding of probable cause that the individual/**cyber target** is connected to a foreign power, is in a senior operational capacity and poses an imminent threat of violent attack against the United States.

Approved applications for drone strikes and **cyberattacks** would need to be renewed after a certain period, and discontinued if evidence is presented that the targets no longer meet the criteria. [my emphasis]

Granted, it would have been nice if the government had had to go to a court to explain why a publisher like WikiLeaks should be targeted with a persistent DNS attack, assuming that's what happened. But given that both our FISA targeting and our targeting killing targeting probably allow for far too much abuse of the First Amendment, I'm not convinced the

FISA Court would have noted the problem with that incident of prior restraint.

More generally, though, isn't Harman's neat inclusion of cyber targeting here a hint that our cyberattacks have gone beyond just Iran and WikiLeaks?

---

## **WHY SO SURPRISED? CIA, U.S. MILITARY KNEW CHINESE HACKERS EXPECTED SINCE 1999**

The breathless reporting about the alleged Chinese hacking at The New York Times is truly annoying because of the shock it displays. The surprise any major government or private corporate entity shows at this point about any network-based security breach that appears to originate from China should be treated as propaganda, or a display of gross ignorance.

In 1999, the CIA's Foreign Broadcast Information Service published a white paper entitled *Unrestricted Warfare*, written by the PRC's Col. Qiao Liang and Col. Wang Xiansui. The publication outlined the methodologies a nation-state could deploy as part of an asymmetric war. Further, the same work outlined the U.S.'s weaknesses at that time were it to confront such asymmetric warfare. It did not focus any other nation-state, just the U.S.\*

The colonels acknowledged that the U.S.—at the time of the paper—had considered using a range of tools in response to conflicts:

“...There's no getting around the opinions of the Americans when it comes to



discussing what means and methods will be used to fight future wars. This is not simply because the U.S. is the latest lord of the mountain in the world. It is more because the opinions of the Americans on this question really are superior compared to the prevailing opinions among the military people of other nations. The Americans have summed up the four main forms that warfighting will take in the future as: 1) Information warfare; 2) Precision warfare [see Endnote 8]; 3) Joint operations [see Endnote 9]; and 4) Military operations other than war (MOOTW) [see Endnote 10]. This last sentence is a mouthful. From this sentence alone we can see the highly imaginative, and yet highly practical, approach of the Americans, and we can also gain a sound understanding of the warfare of the future as seen through the eyes of the Americans. Aside from joint operations, which evolved from traditional cooperative operations and coordinated operations, and even Air-Land operations, the other three of the four forms of warfighting can all be considered products of new military thinking. General Gordon R. Sullivan, the former Chief of Staff of the U.S. Army, maintained that information warfare will be the basic form of warfighting in future warfare. For this reason, he set up the best digitized force in the U.S. military, and in the world. Moreover, he proposed the concept of precision warfare, based on the perception that "there will be an overall swing towards information processing and stealthy long-range attacks as the main foundations of future warfare." For the Americans, the advent of new, high-tech weaponry, such as precision-guided weapons, the Global Positioning System (GPS), C4I systems

and stealth airplanes, will possibly allow soldiers to dispense with the nightmare of attrition warfare. ...”

The rise of military tools like drones for precision-guided stealth attacks was predicted; quite honestly, the PRC’s current cyber warfare could be a pointed response to Gen. Sullivan’s statement about information warfare.

But in acknowledging the U.S.’s future use of MOOTW, the colonels also offered up the most likely approaches in an asymmetric assault or response: trade war, financial war, new terror war in contrast to traditional terror war, ecological war. Of these, they cited a specific example of new terror war entity and attacks:

“...In contradistinction to masked killers that rely on the indiscriminate slaughter of innocent people to produce terror, the “Falange Armed Forces”[...] group in Italy is a completely different class of high-tech terrorist organization. Its goals are explicit and the means that it employs are extraordinary. It specializes in breaking into the computer networks of banks and news organizations, stealing stored data, deleting programs, and disseminating disinformation. These are classic terrorist operations directed against networks and the media. This type of terrorist operation uses the latest technology in the most current fields of study, and sets itself against humanity as a whole. We might well call this type of operation “new terror war.”...

Note in particular that these Chinese military experts refer to attacks not on military targets, but on banks and the media.

Furthermore, the U.S. military could have predicted the Chinese investment in information

warfare, as a paper Operation Allied Force: The View from Beijing, by Dr. James D. Perry (2000) noted. Perry had already absorbed the paper, Unrestricted Warfare:

“...Two senior PLA officers observed that NATO’s “asymmetrical” strikes employed “a number of new combat modes.” Allied Force consisted of “a series of informationalized, digitized, and networked combat operations that surpassed those in the Gulf War.” In their view, networked fighting centers will replace individual fighting platforms in future warfare, and networked military organizations will replace “tree-shaped” military organizations. The United States uses air raids, EW, and information-control operations to maximize the asymmetric advantages of its high technology. Therefore, the PLA should “learn and master” anti-air-raid, anti-electronic-warfare, and anti-information-control operations. ...”

Perry also noted contributor Ye Lu of the state-owned Keji Ribao science and technology publication reported:


“...the US goal is to gain mastery of battlefield information and that the information enhancement of US weapons systems is already “an order of magnitude” greater than in the Gulf War. Before initiating combat,

*‘reconnaissance satellites, relay satellites, high-altitude reconnaissance aircraft, and low- and medium-altitude pilotless aircraft of all kinds are to be deployed in continuous, uninterrupted, all around, dynamic intelligence reconnaissance against military and civilian targets in Yugoslavian territory . . . while at the same time numerous intelligence*

*organizations and every means of intelligence collection are to be marshaled to conduct repeated position fixing and simulated attack exercises against all military and non-military targets that might be encountered in the battlefield to come.'*<sup>20</sup>

Ye considered that despite all its advantages, the United States did not gain "information supremacy" in Yugoslavia. This he attributed to the expansion of the information domain through radio and computer networks that enable "both aggressors and defenders to attack and counterattack to the best of their abilities." Ye drew the following conclusions from Allied Force:

- *China should research and develop high-tech precision weapons and should upgrade the information systems associated with existing weapons.*
- *China should develop IW equipment and techniques, especially those that can "reliably put constraints on the power of hostile forces."*
- *China needs a "corps of knowledgeable and experienced military information security personnel."*
- *China should create her own software for*



*national defense and  
should find military  
applications for  
civilian high  
technologies.21 ...”*

Again, the Chinese not only predicted the emergence of drone usage by the U.S., but spelled out a countervailing response including development of information technology for its national security.

The same report by Ye Lu, cited by Dr. Perry and published in a U.S. Air Force-Air University journal, was itself published by the CIA's FBIS. Clearly both our military and our intelligence agency have been on notice for over a decade about China's intentions with regard to cyber warfare.

We were warned; it could not be spelled out any more clearly. Not to mention other sources of intelligence, our government was handed a manual that not only laid out the likely routes of attack, including network-based assaults, but generously a description of the opportunities for improvement the U.S. should address to protect itself against non-traditional attacks, let alone improve the prospects to conduct assaults of their own in a similar fashion.

Granted, the document also suggests a unified structure for the U.S. or other nation-state to respond to all asymmetric attacks. This offering should be avoided for this reason—the unexpected is the element that offers the best chance to defend against non-traditional warfare.

But to have no organized response at all is absurd. In its absence we're left with a choice of which mask we should adopt in reaction to attacks: the “We've got this” fakery, or an open admission of ignorance and failure—or perhaps both.

One more point we should note is the Chinese

response by foreign minister's office spokesman Hong Lei in state-owned Xinhua News to the NYT's report:

"Groundless criticism is irresponsible and unprofessional, and it will not help to solve the problem," he said.

The infosecurity company Mandiant employed by NYT and the U.S., which had traced the source of the alleged hacking to a People's Liberation Army site, took this as an insult to their conduct and went public with their findings.

But was the response really aimed at Mandiant? Or was it aimed at other government and private corporate targets warned clearly more than a decade ago?

*\* Word analysis of the document published at Cryptome:*

*"U.S." appears 220 times; "Europe" appears 22 times; "Russia" appears 31 times, "China" appears 34 times. Occurrences counted in both text's body and in footnotes.*

---

## ENJOY A VALENTINE'S DAY SAMPLER

It's difficult lately for me to sit down and spend time on a blogpost. I manage a handful of minutes here and there to do reading or research. An email may take hours to draft.

But there's too much juicy stuff floating around deserving more attention. I'm going to gather content as I see it and aggregate it into a post when I have time, rather than let them slip by. Perhaps you can make more of them than I can.

- MIT Technology Review acknowledges the dawn of a new age in Welcome to the Malware-Industrial Complex. I'm rather surprised at the

tone of this piece; it's not au courant, rather a bit behind the times since the MIC launched more than a handful of years ago. Two important points emerge: 1) Zero-day exploits are being traded like weaponry—think very hard about the source of these exploits and ask yourself why they are tolerated in government computing environments, let alone any other production environment; 2) This new age is the military face of the paradigm shift from the industrial to the information age. Weapons are information; they are no longer separate from the weapons themselves. With this in mind, the last two graphs of this article display the already-anachronistic thinking of the author and his sources.

- Syracuse University MA/PhD student Seth Long performs a rather fascinating analysis on alleged cop killer Christopher Dorner's manifesto. But equally fascinating is his earlier analysis on Ted Kaczynski's Unabomber manifesto. Compare the two assessments, and then ask yourself what any blogger's online writings might say about them if Long's analytical process is eventually automated with algorithms. Scary, hmm?

- Really great long read at Bloomberg Businessweek on the unmasking of a Chinese hacker by a Dell Computers malware expert. This is a snapshot of asymmetric warfare in progress; it's not as if China has not told us rather candidly (and more than a decade ago) they would engage us in this manner as well as in other non-internet battlefields. Any surprise on the part of U.S. government officials at this point is utterly ridiculous—it's either feigned or it's should-get-another-day-job stupidity.

- I'm so annoyed by this long read in Aeon Magazine—a really great mag, by the way—that I may yet muster the time to write something longer. Author Damien Walter is rather specious in his identification of a new "creator culture" and its necessity to society's continued success. The problem isn't that we need to adopt

and nurture a new creator culture; it's that we killed the one we had quite willingly over the last 25-35 years by offshoring production and the subsequent commodification of goods. We allowed corporations and their one-percenter shareholders to tell us that getting our hands dirty through craftsmanship and in manufacturing was bad (mostly bad for their profit margins). We've become a culture that doesn't fix anything; we buy replacements made overseas in third world countries. We've lost our can-do spirit along with this shift, and only recently have both the economic crisis and a new hipster-hobbyist ethos encouraged a resurgence of the do-it-yourself handyperson. Unless we're conscious of our role in killing creativity, nurturing it again through supporting Etsy and Maker Faires is merely temporary relief from the crush of profit-driven consumerism.

- But perhaps all of this will be moot tomorrow if the cosmos decides to make a bank shot with asteroid 2012 DA14. This "small" asteroid will fly within 17,200 miles of earth tomorrow afternoon. This is awfully bloody close—close enough that scientists say disruption of cellphone and other satellite service is not impossible, but unlikely. That's a whisker's breadth, in cosmic scale. Best to check in tomorrow afternoon after 3:00 pm CST to see if we're still here. See you then.

---

**OBAMA WILL PROPOSE  
NEW EFFORTS TO MAKE  
OUR CREAKY  
PHYSICALLY**



# DANGEROUS CRITICAL INFRASTRUCTURE CYBERSAFE

One of Obama's key proposals in tonight's State of the Union will be yet another effort to shore up the cybersecurity of our critical infrastructure.

As a threshold matter, I find it a remarkable coinkydink that the WaPo just reported the leaked findings of an NIE saying that the Chinese (and Israelis and Russians and the French, but the Chinese are bigger and badder, apparently) continue to rob us blind via cybertheft. I look forward to learning whether this – unlike the convenient drone rule book leaks supporting John Brennan's confirmation – get reported as sanctioned leaks, as required under the Intelligence Authorization.

And speaking of John Brennan, he's the Homeland Security Czar. A big part of his job is keeping us safe from precisely these kinds of attacks. So why didn't he get a single question about why he should be CIA Director considering he has been such an abject failure keeping us safe from cyberattacks? (He was asked a question about CIA's role in cybersecurity, but not asked to explain why he has been such a failure in his current role.)

Now, frankly, I don't know that that is much John Brennan's fault. Folks will say that the problem is – as it has been since Richard Clarke first started fearmongering on this front – that corporations won't participate willingly and no one is going to make them.

But the proposal – which you'll see if you tune in – doesn't change that. It's still voluntary.

And here's the thing that all the cyberexperts in the world seem to be missing. Not only are the private owners of our critical infrastructure unwilling to fix their

cyberdefenses. They're not willing to keep their brick and mortar infrastructure up to date either. See, for example, PG&E or ConEd's recent records, for example.

Look, if these companies refuse to keep up their physical infrastructure **and** their cyber infrastructure, there's probably an underlying reason motivating their negligence that no amount of immunity or winks or risk-free information sharing on the cyber side is going to fix. Moreover, if they are physically fundamentally unsafe, no amount of tinkering with their cybersecurity is going to make them safe. They'll be vulnerable to a terrorist attack **and** be vulnerable to not entirely random failures and explosions.

You need to solve the underlying problem if you want to keep our critical infrastructure safe. And yet another EO, ~~particularly one limited to cybersecurity and not affect brick and mortar integrity~~, will not do that.

Updated: Reading Obama's longer proposal, it does aim to increase the "resiliency" of our physical infrastructure too. So it is not limited to cyber. That said, the underlying problem remains. Private companies aren't spending the money to invest in this, whether it is physical resilience (or bare minimum functionality) or cyberdefense.

---

## CABLES, CONFIRMED

I've long traced the severance and disconnection of various parts of the world from telecommunication cables on this blog, most recently in the wake of Syria losing Toobz access after it purportedly mixed some chemical weapons.

**I** Danger Room's sources aren't even asserting that both events—the mixing of

the CW on Wednesday and the Intertoobz blackout on Thursday—are both signs of Bashar al-Assad’s panic.

Which would sort of be the default unless intelligence sources had reason to know that the Intertoobz blackout had nothing to do with the CW mixing.

We’ve long traced interesting Intertoobz blackouts caused by cut cables on this blog: the recent blackout in Djibouti. to a cable in the Bay Area, to a number of cut cables in the Middle East back in 2008.

It appears to be an increasingly common tactic, one difficult to attribute to a specific actor.

But if one of those actors comes out a few days after an outage and says they have no reason to find that outage as suspicious as the mixing of CW, maybe it’s not so hard to attribute after all.

One of the interesting revelations in this profile on the guy who shot Osama bin Laden is that sending Seal Team Six to do **something** with underwater cables is apparently routine enough that’s what they were told the mission would be before they were read into the real target.

There was so much going on – the Libya thing, the Arab Spring. We knew something good was going to go down. We didn’t know how good.

The first day’s briefing, they actually kind of lied to us, being very vague. They mentioned underwater cables because of the earthquake in Japan or some craziness.

Consider me thoroughly unsurprised.

---

# MR. MORAL RECTITUDE'S SLEAZY PAYMENT

According to Defense News, John Brennan was paid roughly \$2,090 a day while working for The Analysis Corporation in 2008. He was paid roughly \$8,496 for each of the 20 days he worked in 2009 before he became Obama's counterterrorism czar.

A review of Brennan's financial disclosure reports indicates that in 2009, TAC paid him a total of \$169,923 in salary and bonus, which has not been previously reported. The financial disclosure reports, submitted as required of all White House employees, don't say why he'd receive a bonus if he was leaving the company to join the government, or why he'd received such a large salary if he worked for the company for only 20 days that year.

In November 2008, two months before Brennan joined the Obama administration, TAC announced that the CEO was taking a "leave of absence" from the firm. That is, it is not clear that he was actually on the clock for the transition period before he received that \$169,000.

Mind you, this isn't anything that such illustrious people as Dick Cheney haven't already done (and in larger figures, too).

Tim Shorrock provided some background on the company in his book.

There were questions about Brennan's ties to his former company when it was part of the investigation into the failure to connect-the-

dots before the UndieBomber attempted to strike the US, though as part of an ethics waver he agreed to recuse himself from anything specifically pertaining to TAC.

The White House has granted a special ethics waiver to allow President Obama's top counterterrorism adviser to conduct a review of the intelligence and screening breakdown that preceded the failed Christmas Day bombing attempt on an American passenger plane over Detroit.

[snip]

Mr. Brennan, who was a longtime C.I.A. officer, needed the waiver because for more than three years before his current post he was chief executive of the Analysis Corporation, an intelligence firm that provides services to the government. Norm Eisen, the White House ethics counsel, wrote on the White House Web site on Wednesday that Mr. Brennan's past ties to the company, were outweighed by his knowledge of the nation's intelligence system.

And, of course, Brennan's the guy who has sacrificed US privacy to get more data in databases.

The umbrella company that has absorbed TAC continues to get lots of contracts doing intelligence analysis.

---

## WHEN ALL YOU HAVE IS A CYBERHAMMER, YOU

# HAVE TO EXPECT TO GO TO WAR AGAINST NAILS

There are two things about this NYT article describing Obama's new cyberwar policy that deserve note.

A secret legal review on the use of America's growing arsenal of cyberweapons has concluded that President Obama has the broad power to order a pre-emptive strike if the United States detects credible evidence of a major digital attack looming from abroad, according to officials involved in the review.

[snip]

The rules will be highly classified, just as those governing drone strikes have been closely held.

First, according to the WaPo, the government has conducted a search of any and all government officials who have had contact with the lead author of the story, David Sanger.

Investigators, they said, have conducted extensive analysis of the e-mail accounts and phone records of current and former government officials in a search for links to journalists.

Frankly, I think the WaPo is naively ignoring the real possibility, given the updates to DOJ's Domestic Investigations and Operations Guide, that DOJ has accessed Sanger's email records directly.

Nevertheless, however they've gotten that information, the government now has a pretty good idea who speaks to David Sanger. Presumably, folks who talk to Sanger – particularly those privy to secret workings of the White House – are cognizant of this fact.

From that I assume it's likely – though by no means certain – that the Administration is not that unhappy about having an article boasting about its aggressive cyberwar stance, even while noting that the details of it will be remain legally classified.

Meanwhile, I'm struck by this claim.

Mr. Obama is known to have approved the use of cyberweapons only once, early in his presidency, when he ordered an escalating series of cyberattacks against Iran's nuclear enrichment facilities.

Sure, there's only been the one attack (or rather the serial set of attacks) on Iran.

But I'm struck – particularly in the wake of DOJ's filing making it clear they're investigating WikiLeaks as a spy, while refusing to tell us what laws it is using to conduct that investigation – that there has been a rather notable cyberattack whose author we don't know: the DDOS attacks on WikiLeaks as it first started to release the WikiLeaks cables, and then again last summer (a group called AntiLeaks claimed credit for the second one).

As Jack Goldsmith and Thomas Rid both point out, the Administration appears to be badly fumbling cyber defense (largely because the private sector doesn't want to play along and the Administration isn't prepared to make them), but they are very aggressively pursuing cyberoffense. Perhaps, as Goldsmith suggests, this leak to the journalist whose contacts are being monitored is intended to deter attacks on the US (though I'm not sure how a story in a newspaper that the Chinese have hacked is going to scare the Chinese from doing what they have been doing for years).

But if the US is so intent on bragging about its offensive capability, isn't it time we learned the scope of that offensive capability? Shouldn't we finally know whether the government

took down a publisher's website?

---

## THE 2011 DIOG PERMITS USING NSLS TO GET JOURNALIST CONTACTS

In what may be one of those stories telegraphing investigative details between people being investigated, the WaPo updates the StuxNet investigation.

Prosecutors are pursuing “everybody – at pretty high levels, too,” said one person familiar with the investigation. “There are many people who’ve been contacted from different agencies.”

The FBI and prosecutors have interviewed several current and former senior government officials in connection with the disclosures, sometimes confronting them with evidence of contact with journalists, according to people familiar with the probe.

Here’s the detail everyone is focusing on (and I’ve seen similar claims on reporting of other leak investigations).

Investigators, they said, have conducted extensive analysis of the e-mail accounts and phone records of current and former government officials in a search for links to journalists.

[snip]

Former prosecutors said these investigations typically begin by compiling a list of people with access to the classified information. When government officials attend classified



briefings or examine classified documents in secure facilities, they must sign a log, and these records can provide an initial road map for investigators.

**Former prosecutors** said investigators run sophisticated software to identify names, key words and phrases embedded in e-mails and other communications, including text messages, which could lead them to suspects.

The FBI also looks at officials' phone records – who called whom, when, for how long. Once they have evidence of contact between officials and a particular journalist, investigators can seek a warrant to examine private e-mail accounts and phone records, including text messages, former prosecutors said.

Prosecutors and the FBI can examine government e-mail accounts and government-issued devices, including cellphones, without a warrant. They can also look at private e-mail accounts without a warrant if those accounts were accessed on government computers. [my emphasis]

This description may well be how the government is conducting the StuxNet (and the UndieBomb 2.0 investigation, which the article also describes).

But if WaPo is relying solely on **former** prosecutors, this description may be totally outdated.

After all—as I've reported repeatedly in the past—the 2011 update of FBI's Domestic Investigations and Operations Guide permits using National Security Letters to get journalists' contacts in National Security investigations (as all of these would be).

A heavily-redacted section (PDF 166)

suggests that in investigations with a national security nexus (so international terrorism or espionage, as many leak cases have been treated) DOJ need not comply with **existing restrictions** requiring Attorney General approval before getting the phone records of a journalist. The reason? Because NSLs aren't subpoenas, and that restriction only applies to subpoenas.

Department of Justice policy with regard to the issuances of subpoenas for telephone toll records of members of the news media is found at 28 C.F.R. § 50.10. **The regulation concerns only grand jury subpoenas, not National Security Letters (NSLs) or administrative subpoenas.**

(The regulation requires Attorney General approval prior to the issuance of a grand jury subpoena for telephone toll records of a member of the news media, and when such a subpoena is issued, notice must be given to the news media either before or soon after such records are obtained.) The following approval requirements and specific procedures apply for the issuance of an NSL for telephone toll records of members of the news media or news organizations. [my emphasis]

So DOJ can use NSLs—with no court oversight—to get journalists' call (and email) records rather than actually getting a subpoena.

The section includes four different approval requirement scenarios for issuing such NSLs, almost all of which are redacted. Though one only partly

redacted passage makes it clear there are some circumstances where the approval process is the same as for anyone else DOJ wants to get an NSL on:

If the NSL is seeking telephone toll records of an individual who is a member of the news media or news organization [2 lines redacted] there are no additional approval requirements other than those set out in DI0G Section 18.6.6.1.3 [half line redacted]

And the section on NSL use (see PDF 100) makes it clear that a long list of people can approve such NSLs:

- *Deputy Director*
- *Executive Assistant Director*
- *Associate EAD for the National Security Branch*
- *Assistant Directors and all DADs for CT/CD/Cyber*
- *General Counsel*
- *Deputy General Counsel for the National Security Law Branch*
- *Assistant Directors in Charge in NY, Washington Field Office, and LA*
- *All Special Agents in Charge*

In other words, while DOJ does seem to offer members of the news media—which is itself a somewhat limited group—some

protection from subpoena, it also seems to include loopholes for precisely the kinds of cases, like leaks, where source protection is so important.

In other words, this story about starting with the sign-in logs of people who've been briefed on a particular topic, then gather call records of those officials?

That may be what happened.

Or it may work the other way, with the government identifying a story it doesn't like and then using call records to trace back from there to the potential sources of the story.

This curious phrasing would support the latter scenario.

[DC US Attorney Ronald] Machen is examining a leak to the Associated Press that a double agent inside al-Qaeda's affiliate in Yemen allowed the United States and Saudi Arabia to disrupt the plot to bomb an airliner using explosives and a detonation system that could evade airport security checks.

The AP, after all, didn't report that UndieBomb 2.0 was actually a sting set up by a Saudi-run infiltrator (and their reporting, at least, suggested they didn't know UndieBomber 2.0 was an informant). John Brennan and Richard Clarke told that story. And yet WaPo describes the investigation as focusing on the AP part of the story, not the more damning part about an infiltrator.

If and when John Brennan goes unpunished for revealing the most damning part of this story, it'll become increasingly clear: not only is the government starting with the journalists' phone and email contacts, but it is doing so with journalists it might otherwise want to silence.

---

# YET ANOTHER EDITION OF “YOU WERE WARNED”

**Dear unnamed power company/ies:** Thank you for providing me an opportunity to post one of my favorite videos.

AGAIN.

You were warned about the possibility of security threats to your systems. Repeatedly—the video above is just one such warning. What’s it take to get through to you—a clue-by-four alongside the head? A massive, lengthy power outage you can’t resolve for days or weeks, with consumers calling for managements’ heads on pikes? A complete tank of your company’s stock value? The Department of Energy on your doorstep, taking possession of your site as it investigates you?

I love this part at 32:28 into the video where Ralf Langer says,

“...many things we thought about cyberwarfare earlier just were proven wrong. ...”

Everything you thought you knew about infosec/cybersecurity needs to be revisited. The assumptions you’ve been using are clearly wrong.

Now get a frigging clue and revisit your security policies. STAT. You can start with checking these:

- No USB or other external media which have not been deeply screened for infection.
- External network connections to production equipment are to be avoided at all costs. Connections between corporate business and the

power grid should be closed, dedicated network. Revisiting appropriateness of traditional isolation of production networks might be worthwhile.

– No third-party contractors permitted on site that do not comply completely with power company security policies, including spot inspections. (You do spot inspections, right? Contractors are screened coming in and out of facilities, right?)

What are you doing here, reading this? Get to work. RUN.

**Dear U.S. Department of Energy:** Um, hello? Did your brains' functions suffer irreparable damage from exposure to BP's dispersants?

It's the only excuse I can think of as to why security measures and subsequent audits of the nation's power grid for infections and intrusions from network and external devices haven't removed these threats.

By the way, this 2009 document making suggestions to power companies about security measures is now out of date and needs to be revisited, in light of the Senate Intelligence Committee's authorization of cyber weapon deployment and subsequent blowback risk, let alone the case of USB devices laden with crimeware.

**Dear Fellow Americans:** I really hate feeling like Cassandra. I'd love to see the power industry and our government prove me wrong by preventing outages related to security breaches about which they've been warned. At the rate they're going, you're going to end up on the short end of the stick, without electricity to read my anticipated future post which I expect to entitle, "I told you so."

You might want to contact your government representatives and ask them what they know about power grid security and if they've actually done anything to investigate the safety of power in their district. If their

understanding is shaped by the Department of Energy's latency, they need to be brought up to speed and pronto. Don't wait until you don't have the juice to read my next post on this topic.