WHY THE IRAQ AUMF STILL MATTERS

The big headline that came out of yesterday's American Bar Association National Security panels is that DOD General Counsel Jeh Johnson and CIA General Counsel Stephen Preston warned that US citizens could be targeted as military targets if the Executive Branch deemed them to be enemies.

> U.S. citizens are legitimate military targets when they take up arms with al-Qaida, top national security lawyers in the Obama administration said Thursday.
>
> [snip]
>
> Johnson said only the executive branch, not the courts, is equipped to make military battlefield targeting decisions about who qualifies as an enemy.

We knew that. Still, it's useful to have the Constitutional Lawyer President's top aides reconfirm that's how they function.

But I want to point to a few other data points from yesterday's panels (thanks to Daphne Eviatar for her great live-tweeting).

First, Johnson also said (in the context of discussions on cyberspace, I think),

> Jeh Johnson: interrupting the enemy's ability to communicate is a traditionally military activity.

Sure, it is not news that the government (or its British allies) have hacked terrorist "communications," as when they replaced the AQAP propaganda website, "Insight," with a cupcake recipe (never mind whether it's effective to delay the publication of something like this for just one week).

But note what formula Johnson is using: they've justified blocking speech by calling it the communication of the enemy. And then apparently using Jack Goldsmith's formulation, they have said the AUMF gives them war powers that trump existing domestic law, interrupting enemy communications is a traditional war power, and therefore the government can block the communications of anyone under one of our active AUMFs.

Johnson also scoffed at the distinction between the battlefield and the non-battlefield.

> Jeh Johnson: the limits of "battlefield v. Non battlefield is a distinction that is growing stale." But then, it's not a global war. ?

Again, this kind of argument gets used in OLC opinions to authorize the government targeting "enemies" in our own country. On the question of "interrupting enemy communication," for example, it would seem to rationalize shutting down US based servers.

Then, later in the day Marty Lederman (who of course has written OLC opinions broadly interpreting AUMF authorities based on the earlier Jack Goldsmith ones) acknowledged that Americans aren't even allowed to know everyone the US considers an enemy.

> Lederman: b/c of classification, "we're in armed conflicts with some groups the American public doesn't know we're in armed conflict with."

Now, as I've noted, one of the innovations with the Defense Authorization passed yesterday is a requirement that the Executive Branch actually brief Congress on who we're at war with, which I take to suggest that Congress doesn't yet necessarily know everyone who we're in "armed conflict" with.

Which brings us to how Jack Goldsmith defined the "terrorists" whom the government could wiretap without a warrant.

> the authority to intercept the content of international communications "for which, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are reasonable grounds to believe … [that] a party to such communication is a group engaged in international terrorism, or activities in preparation therefor, or any agent of such a group," as long as that group is al Qaeda, an affiliate of al Qaeda **or another international terrorist group** that the President has determined both **(a) is in armed conflict with the United States and (b) poses a threat of hostile actions within the United States**;

It's possible the definition of our enemy has expanded still further since the time Goldsmith wrote this in 2004. Note Mark Udall's ominous invocation of "Any other statutory or constitutional authority for use of military force" that the Administration might use to authorize detaining someone. But we know that, at a minimum, the Executive Branch used the invocations of terrorists in the Iraq AUMF–which are much more generalized than the already vague definition of terrorist in the 9/11 AUMF–to say the President could use war powers against people he calls terrorists who have nothing to do with 9/11 or al Qaeda.

So consider what this legal house of cards is built on. Largely because the Bush Administration sent Ibn Sheikh al-Libi to our Egyptian allies to torture, it got to include terrorism language in an AUMF against a country that had no tie to terrorism. It then used that language on terrorism to justify ignoring domestic laws like FISA. Given Lederman's language, we can assume the Administration is still using the Iraq AUMF in the same way Goldsmith did. And yet, in spite of the fact that the war is ending, we refuse to repeal the

AUMF used to authorize this big power grab.

ROBERT MUELLER ONCE AGAIN CLAIMS ANNA CHAPMAN A BIGGER THREAT TO US THAN LLOYD BLANKFEIN

Robert Mueller addressed the Commonwealth Club in San Francisco today. He repeated a familiar theme: the biggest threats to the United States are terrorists (even aspirational ones), spies, and cyber attacks.

> Terrorism, espionage, and cyber attacks are the FBI's top priorities. Terrorists, spies, and hackers are always thinking of new ways to harm us.

As he tends to do when spreading this propaganda, Mueller once again focused on Anna Chapman and her band of suburban spies.

> Consider the arrest last year of 10 agents of the Russian Foreign Intelligence Service. Many of you may have seen TV news stories and videos covering the techniques we used in our investigation, code-named Ghost Stories. It featured the stuff of a John Le Carré novel—dead-drops in train tunnels, brush passes at night, and clandestine meetings in cafés.

Though he did add the example of Kexue Huang, who sent information on organic pesticides and food to Germany and China, to his list of scary spies who threaten our country.

> Last month, Kexue Huang, a former scientist for two of America's largest agricultural companies, pled guilty to charges that he sent trade secrets to his native China.
>
> While working at Dow AgriSciences and later at Cargill, Huang became a research leader in biotechnology and the development of organic pesticides. Although he had signed non-disclosure agreements, he transferred stolen trade secrets from both companies to persons in Germany and China. His criminal conduct cost Dow and Cargill millions of dollars.

Finally, Mueller added a neat new twist to his list of people who pose a big threat to this country. The hackers who hacked into the BART website **after** BART cops killed the unarmed Oscar Grant and later Charles Blair Hill, and **after** BART shut down cell service to interrupt free speech will bring anarchy!

> And "hacktivist" groups are pioneering their own forms of digital anarchy. Here in the Bay Area, you witnessed their work firsthand when individuals hacked the BART website and released personal data of BART customers.

Because it's not anarchy when cops shoot unarmed or drunk men. It's not anarchy when transit companies unilaterally shut down your phone. It's only anarchy when the hackers get involved.

You'll note what's missing, as it always is, from Mueller's list of scary threats to the country? Not a peep about the banksters whose systematic fraud has done—and continues to do—far more financial damage than 9/11.

It's anarchy, apparently, when bunch of kids break into a website. But it's not anarchy when banksters rewrite property law to steal the homes of millions of Americans.

CHINA! AND RUSSIA! AND [AN UNNAMED ALLY THAT IS LIKELY ISRAEL] ARE STEALING OUR STUFF!

Last week, ODNI released a report on cyberwarfare that is raising eyebrows for the way it named China and Russia as the sponsors of cyberespionage explicitly.

Jack Goldsmith wonders what naming them will accomplish.

> I am sure that naming the Chinese and Russians specifically and openly was a big deal inside the government. The *Wall Street Journal* reports that a "senior intelligence official said it was necessary to single out specific countries in order to confront the problem and attempt contain a threat that has gotten out of control." Perhaps so, but naming names alone will not accomplish much. For one thing, the U.S. government has presented no public evidence on Chinese and Russian

> cyberespionage, and those countries generally deny it. (Chinese Embassy spokesman Wang Baodang said yesterday, in response to the DNI Report, that China opposes "any form of unlawful cyberspace activities.") For another, Cyberespionage does not violate international law. For yet another, the United States itself, while it does not engage in broad-ranging industrial or economic espionage, does do so on a limited scale.
>
> [snip]
>
> In light of these factors, it is hard for me to understand what naming names is supposed to accomplish, especially since the Chinese and Russian hand in industrial espionage is widely known.

Whereas Shane Harris compares this moment to Churchill's Iron Curtain speech.

> The report marks the first time the United States government has unequivocally stated, in empathetic and highly publicized fashion, that China and Russia are responsible for a pervasive electronic campaign to steal American intellectual property, trade secrets, negotiating strategies, and sensitive military technology. This is not the first time sitting US officials have singled out Chinese and Russian cyber theft. But those complaints were largely off the record and carefully calibrated not to be read as a shot across the bow of America's strategic adversaries. This report, however, is that shot.
>
> [snip]
>
> And one is tempted to draw parallels to pivotal moments of the last cold war, which were underappreciated at the time, or even ridiculed. The release of this

> report may turn out to be the Internet's Iron Curtain moment. Though it landed with much less ceremony and eloquence than Sir Winston Churchill's fateful 1946 address, it nevertheless does the same job: It makes clear the stakes as the United States intelligence community sees them, and it throws down a challenge against Russia and China, which are judged to be the two greatest strategic threats to American prosperity and influence.

But there's something funny about this grand moment. Sure, the report names and shames China and Russia. But it also makes clear that our allies [cough, Israel] are also stealing our stuff. Here's how the executive summary presents the culprits.

> - *Chinese actors are the world's most active and persistent perpetrators of economic espionage. US private sector firms and cybersecurity specialists have reported an onslaught of computer network intrusions that have originated in China, but the IC cannot confirm who was responsible.*
> - *Russia's intelligence services are conducting a range of activities to collect economic information and technology from US*

> *targets.*
>
> - *Some US allies and partners use their broad access to US institutions to acquire sensitive US economic and technology information, primarily through aggressive elicitation and other human intelligence (HUMINT) tactics. Some of these states have advanced cyber capabilities.*

If this theft is such a big deal, then it’s a big deal whether China does it or Israel. Hell, since Israel often steals our defense information than sells others the war toys we sell to them, in some ways it presents a more immediate threat.

And whatever the significance of naming China and Russia might be if they were the only culprits, shaming them while at the very same time admitting that our buddies do the same thing sort of makes us look like chumps or hypocrites.

Which is all the more hysterical given that the report cover features a thumb drive–the means by which we continue to make it child’s play to give us viruses that make stealing our stuff easier–wielded like a bright red gun to represent the danger.

WHY DOES DUQU MATTER?

The short answer is that if your PC got infected by Stuxnet last year, you were just collateral damage, unless you were operating a very specific set of uranium enrichment centrifuges. If you get Duqu this year, your network is under attack from a CIA/Mossad operation. They might seem a little outrageous, but bear with me while we get into the weeds of what Duqu is all about. I will lay out a set of assertions that lead to the conclusion that Duqu really is the “precursor to the next Stuxnet” as Symantec say in their whitepaper.

1. Stuxnet was created by the CIA and the Mossad

Although no one has officially claimed responsiblity for Stuxnet, both the U.S. and Israeli governments have done everything but take offical responsibility. Neither government has ever denied responsibilty, even when directly asked. In fact, officials in both governments have been reported as breaking out in big smiles when the subject comes up.

2. Duqu is from the same team that created Stuxnet.

The first clue that Duqu is from the Stuxnet team is the similarities between the rootkit components in both pieces of malware. The folks who have studied the two most closely are sure that Duqu is based on the Stuxnet component’s source code. Despite what you may have read on the internet, the actual source code to Stuxnet is not publicly available. Some folks have reverse-engineered some of the Stuxnet source code from the binaries that are available, for various technical reasons, I’m sure that these don’t serve as the basis for Duqu.

Duqu even has a fix for a bug in Stuxnet. Also, the only two pieces of malware in history to install themselves with as Windows device drivers with legitimate, but stolen, digital certificates are Stuxnet and Duqu. Both Stuxnet and Duqu were active in the wild and managed to evade detection for many months. While that's not unheard of for malware, it is another point of similarity.

Stuxnet targeted a specific industrial control system (ICS) installation (the Siemens PLCs that were used to control the centrifuges at Natanz). Here's the lastest on what Duqu targets:

> Some of the companies affected or targeted by Duqu include the actual equipment that an ICS would control such as motors, pipes, valves and switches. To date, the vendors that make the PLC, controllers and systems/applications found in control centers are not yet affected, although this information could change as more variants are identified and these vendors look more closely at their systems.

There are no other instances of computer malware that target these sorts of installations.

3. Stuxnet was a worm, Duqu is not.

Stuxnet was a very aggressive computer worm. It had to be to jump the "air gap" that protects a secure ICS such as the system that ran the Natanz installation. When Stuxnet was discovered, the A-V vendors quickly discovered millions of computers had been (benignly) infected with Stuxnet. Duqu, on the other hand, has been found on only a handful of computers. Interestingly, no one has yet discovered the dropper, that is, the program used to place the Duqu rootkit on the infected machines. This is almost certainly because Duqu is being placed on these machines via a spear phishing attack. In spear phishing, specific targets are chosen and the attack is customized to the target.

4. Duqu is being used to download a RAT (Remote Access Trojan)

The rootkit component was used to download a standalone program designed to steal information from the computer that it has infected (including screenshots, keystrokes, lists of files on all drives, and names of open windows). Duqu is doing computer network reconnaissance. The information gathered by Duqu is very useful for planning future attacks. Before the command and control server was taken off-line, Symantec observed Duqu downloading three additional files to an infected machine. The first was a module that could be injected into other processes running on the machine to gather some process-specific information as well as the computer's local and system times (including time zone and daylight savings time bias). Another downloaded module was used to extend the normal 36-day limitation on Duqu installations. The last downloaded module was a stripped down version of the standalone RAT, lacking the key logging and file exploration functionality.

5. Put it all together and it adds up to a well-executed, highly targeted covert operation

For the last ten months, Duqu has been quietly stalking a small number of industrial manufacturers. No one even noticed before early September and it wasn't until last week that the nature of the threat was clear to anyone. Duqu is spying on a handful of companies, gathering data that will be used for the design and development of the true Stuxnet 2.0. One thing we don't know is who the target of Stuxnet 2.0 will be. But I have a suspicion. Nothing indicates that the ultimate target (i.e., Iran) of the Stuxnet team has changed. In August of this year, Iran announced that it had activated its first pre-production set of his newer IR-2m and IR-4 centrifuges. These are the successors to the centrifuges that Stuxnet attacked. If you wanted to do these centrifuges what Stuxnet did to the earlier IR-1 centrifuges, you would need a lot of specific data about the safe operating specs of the various components that go into making advanced centrifuges. If you knew or suspected who was supplying Iran with these components, you might want to gather some data from the internal networks of those suppliers. That’s what I think the point of Duqu really is.

YET ANOTHER “LADY GAGA” EXPOSURE FORCES DOD TO WIPE DRONE CONTROL COMPUTERS

On Friday, Wired broke the news that the DOD suffered yet another breach because they continue to leave computers exposed to outside storage systems. (h/t WO) In this case, the Ground Control Stations they use to control drones got infected with a keylogger virus.

> But time and time again, the so-called “air gaps” between classified and public networks have been bridged, largely through the use of discs and removable drives. In late 2008, for example, the drives helped introduce the agent.btz worm to hundreds of thousands of Defense Department computers. The Pentagon is still disinfecting machines, three years later.
>
> Use of the drives is now severely restricted throughout the military. But the base at Creech was one of the exceptions, until the virus hit. Predator and Reaper crews use removable hard drives to load map updates and transport mission videos from one computer to another. The virus is believed to have spread through these removable drives. Drone units at other

> Air Force bases worldwide have now been ordered to stop their use.

After a virus was introduced into computers in Iraq three years ago via thumb drive, DOD claimed it had prohibited the use of any removable media with their computers. But then Bradley Manning allegedly removed hundreds of thousands of classified cables from SIPRNet using a Lady Gaga CD. Rather than making all computers inaccessible to removable media at that point, DOD left 12% of their computers vulnerable, deploying a buddy-system to prevent people from taking files inappropriately; but human buddy systems don't necessarily prevent the transmission of viruses.

The good news is that the Host-Based Security System implemented in response to Wikileaks discovered the virus–two weeks ago.

But here's the other interesting wrinkle. To get rid of these viruses, techs have resorted to wiping the hard drives of the targeting computers.

> In the meantime, technicians at Creech are trying to get the virus off the GCS machines. It has not been easy. At first, they followed removal instructions posted on the website of the Kaspersky security firm. "But the virus kept coming back," a source familiar with the infection says. Eventually, the technicians had to use a software tool called BCWipe to completely erase the GCS' internal hard drives. "That meant rebuilding them from scratch" — a time-consuming effort.

Given what little we know about the Anwar al-Awlaki assassination (which, as Wired points out, happened after the virus had knowingly infected these computers), this should not affect the computers that ten days ago killed two US citizens with no due process. The

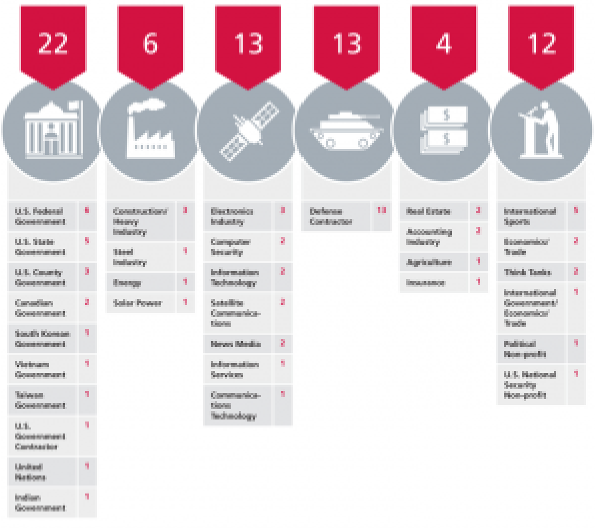
Newsweek story describing the CIA’s targeting process says **that** targeting is done in VA, not NV, where the virus hit.

But particularly given the questions about Samir Khan’s death, consider if that weren’t the case. That would mean a key piece of evidence about whether or not the US knowingly executed an American engaging in speech might be completely eliminated, wiped clean to fix a predictable virus.

That’s not the only risk, of course. We’ve talked before about how long it’ll take for Iran or Mexican drug cartels to hack our armed drones. If this virus were passed via deliberate hack, rather than sloppiness, then we might be one step closer to that eventuality.

All because DOD continues to refuse to take simple steps to secure their computers.

THE OMNIVORE BITES BACK



Source: McAfee

Okay, okay, I should have used a pun on “Echelon” for my title here, not “Carnivore.” After all, it was that earlier SigInt program that the US and its Anglophone partners used to steal industrial secrets in the 1990s.

The point being that, while I am concerned by McAfee's description of the extent of the data theft carried out in the last six years using a hack it calls Shady RAT, I am also cognizant that the US has used equivalent tactics to steal intellectual property in the past and present.

> What we have witnessed over the past five to six years has been nothing short of a historically unprecedented transfer of wealth — closely guarded national secrets (including from classified government networks), source code, bug databases, email archives, negotiation plans and exploration details for new oil and gas field auctions, document stores, legal contracts, SCADA configurations, design schematics and much more has "fallen off the truck" of numerous, mostly Western companies and disappeared in the ever-growing electronic archives of dogged adversaries.
>
> What is happening to all this data — by now reaching petabytes as a whole — is still largely an open question. However, if even a fraction of it is used to build better competing products or beat a competitor at a key negotiation (due to having stolen the other team's playbook), the loss represents a massive economic threat not just to individual companies and industries but to entire countries that face the prospect of decreased economic growth in a suddenly more competitive landscape and the loss of jobs in industries that lose out to unscrupulous competitors in another part of the world, not to mention the national security impact of the loss of sensitive intelligence or defense information.

McAfee provides all the clues to make it clear

China is behind these hacks–though it never says so explicitly.

> The interest in the information held at the Asian and Western national Olympic Committees, as well as the International Olympic Committee (IOC) and the World Anti-Doping Agency in the lead-up and immediate follow-up to the 2008 Olympics was particularly intriguing and potentially pointed a finger at a state actor behind the intrusions, because there is likely no commercial benefit to be earned from such hacks. The presence of political non-profits, such as the a private western organization focused on promotion of democracy around the globe or U.S. national security think tank is also quite illuminating. Hacking the United Nations or the ASEAN (Association of Southeast Asian Nations) Secretariat is also not likely a motivation of a group interested only in economic gains.

The report is perhaps most interesting because of some of the entities–along with the defense contractors and US and other government agencies–described as targets of this hack: a number of construction companies (which could include companies like KBR), real estate firms, various state and county governments, two think tanks, and the NY and Hong Kong offices of a US media company. These are where the secrets China wants to steal are kept.

The problem, of course, is that our intellectual property is one of the few advantages the US has left. Our exports are increasingly limited to things that rely on legally enforcing intellectual property to retain its value: drugs, movies and music, software, GMO ag. Which sort of makes China's ability to sit undetected in the servers of these kinds of organizations for up to 28 months a bit of a problem.

Good thing the FBI is busy going after hacktavists and whistleblowers instead.

THOMAS DRAKE PROVED TO BE BLOODY WELL RIGHT

Thanks to POGO's FOIA release here, we now know that not only was the persecution of Tom Drake by the DOJ completely bogus and vindictive, Tom Drake was bloody well right about TRAILBLAZER versus THIN THREAD to start with. Who couldda predicted?

ANOTHER NSA-PRIVATE SECTOR PARTNERSHIP

Ellen Nakashima reports on a partnership between the NSA, defense contractors, and their Internet service providers to find hackers before they hack.

> The National Security Agency is working with Internet service providers to deploy a new generation of tools to scan e-mail and other digital traffic with the goal of thwarting cyberattacks against defense firms by foreign adversaries, senior defense and industry officials say.
>
> [snip]
>
> Officials say the pilot program does not involve direct monitoring of the contractors' networks by the government. The program uses NSA-developed "signatures," or fingerprints of malicious code, and sequences of suspicious network behavior to filter

> the Internet traffic flowing to major defense contractors. That allows the Internet providers to disable the threats before an attack can penetrate a contractor's servers. The trial is testing two particular sets of signatures and behavior patterns that the NSA has detected as threats.
>
> The Internet carriers are AT&T, Verizon and CenturyLink. Together they are seeking to filter the traffic of 15 defense contractors, including Lockheed, Falls Church-based CSC, McLean-based SAIC and Northrop Grumman, which is moving its headquarters to Falls Church. The contractors have the option, but not the obligation, to report the success rate to the NSA's Threat Operations Center.

From a technical stand-point, this is probably a better way to find hackers than waiting until they steal your data. But of course, it raises all sorts of privacy issues.

But for all the generalized concerns I have about it, I kept thinking of HB Gary when I read this story. After all, the NSA is surely working with contractors on their own side of this. And threat detection like this is precisely the kind of thing HB Gary did, before they started pitching the Chamber of Commerce to spy on activists.

So who are the other contractors involved in this, and what else are they doing with the technology?

CHINA IS HIDING ITS

COUNTERFEIT ELECTRONICS PARTS

The Senate Armed Services Committee is trying to investigate how allegedly counterfeit parts get into the military supply chain. But China won't give visas—or promise freedom of movement without minders—to its investigators.

> Two key US senators on Tuesday accused China of hampering a congressional probe into how counterfeit electronics end up in the US military supply chain by denying entry visas to investigators.
>
> [snip]
>
> And the senators said China had required that government minders attend any interviews conducted in China as part of the investigation, which was announced in March, but agreed that request was a "non-starter."
>
> Levin and McCain said that they had worked for weeks to get entry visas for staff to visit the city of Shenzhen in Guangdong province, which they described as the epicenter of the fake parts trade based on US government reports.

The development is interesting for several reasons. First, while the article cites F-15 and USMDA parts as the problem, most cybersecurity initiatives these days suggest we've got parts that are helping people hack our network. Thus, while Levin suggests China isn't really our adversary, these "counterfeit" parts may well be designed for more than failure. It seems someone has gotten a backdoor into some of our networks because of hardware vulnerabilities.

Then there's the more obvious issue raised by this. If military contractors can't source parts to China without being "infiltrated" with counterfeit parts, and if China won't let us investigate how these counterfeit parts keep getting into our supply chain, then why are we still allowing contractors to use Chinese parts? It seems to me this shows precisely why our outsourcing—and the consequent loss of manufacturing capacity—is really a defense issue.

IMF BLAMES STATE ACTOR FOR HACK

Over the weekend, I expressed some curiosity over who hacked the IMF. They at least say it was a state actor.

> Security experts said the source seemed to be a "nation state" aiming to gain a "digital insider presence" on the network of the IMF, the inter-governmental group that oversees the global financial system and brings together 187 member countries.
>
> Tom Kellermann, a cybersecurity expert who has worked for the IMF and was in charge of cyberintelligence in the World Bank's treasury team, said the intrusion could have yielded a treasure trove of non-public economic data used by the IMF to promote exchange rate stability, support balanced international trade, and provide resources to remedy members' balance-of-payments crises. "It was a targeted attack," said Kellermann, who serves on the International Cyber Security Protection Alliance.
>
> [snip]
>
> An internal memo issued on 8 June from the IMF's chief information officer, Jonathan Palmer, told staff that suspicious file transfers had been

> detected and that an investigation had shown a desktop computer “had been compromised and used to access some Fund systems”. Significantly, he said that he had “no reason to believe that any personal information was sought for fraud purposes”.

The article mentions alleged Chinese hacks in three other places, suggesting they may be trying to cast blame.

But now this has gotten me thinking. If you were to talk about a country establishing a “digital insider presence” on computer networks looking to collect sensitive financial data, you could be describing this alleged hacker or … the United States’ wiretappers. And that’s even before we threaten to wiretap the SWIFT database so we can take what SWIFT won’t just give us.

I’m not suggesting, mind you, that we’re the ones who hacked IMF. Presumably we can just go and get what we want. But given that we are taking financial information on foreign powers that flows across the telecommunications backbones that transit our country, what’s to distinguish our spying from other countries’ hacking?