NATIONAL COUNTERINTELLIGENCE DIRECTOR EVANINA ABOUT OPM BREACH: “NOT MY JOB”

I’ve been tracking Ron Wyden’s efforts to learn whether the National Counterintelligence and Security Center had anticipated how much of a counterintelligence bonanza the Office of Personnel Management’s databases would be. Wyden sent National Counterintelligence Executive William Evanina a set of questions last month.

1. Did the NCSC identify OPM’s security clearance database as a counterintelligence vulnerability prior to these security incidents?
2. Did the NCSC provide OPM with any recommendations to secure this information?
3. At least one official has said that the background investigation information compromised in the second OPM hack included information on individuals as far back as 1985. Has the NCSC evaluated whether the retention requirements for background investigation information should be reduced to mitigate the vulnerability of maintaining personal

> information for a significant period of time? If not, please explain why existing retention periods are necessary?

Evanina just responded. His answer to the first two questions was basically, “Not my job.”

> In response to the first two questions, under the statutory structure established by the Federal Information Security Management Act of 2002 (FISMA), as amended, executive branch oversight of agency information security policies and practices rests with the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS). For agencies with Inspectors General (IG) appointed under the Inspector General Act of 1978 (OPM is one of those agencies), independent annual evaluations of each agency’s adherence to the instructions of OMB and DHS are carried out by the agency’s IG or an independent external auditor chosen by the agency’s IG. These responsibilities are discussed in detail in OMB’s most recent annual report to Congress on FISMA implementation. The statutory authorities of the National Counterintelligence Executive, which is part of the NCSC, do not include either identifying information technology (IT) vulnerabilities to agencies or providing recommendations on how to secure their IT systems.

Of course, this doesn’t really answer the question, which is whether Evanina — or the NCSC generally — had identified OPM’s database full of clearance information as a critical CI asset. Steven Aftergood has argued it should have been, according to the Office of Director of National Intelligence’s definition if not bureaucratic limits. Did the multiple IG reports showing OPM was vulnerable, going back to 2009 and continuing until this year, register on NCSC's radar?

I'm guessing, given Evanina's silence on that issue, the answer is no.

No, the folks in charge of CI didn't notice that this database of millions of clearance holders' records might be a juicy intelligence target. Not his job to notice.

Evanina's response to the third question — whether the government really had to keep records going back to Reagan's second term — was no more satisfying.

> [T]he timelines for retention of personnel security files were established by the National Archives General Records Schedule 18, Item 22 (September 2014). While it is possible that we may incur certain vulnerabilities with the retention of background investigation information over a significant period of time, its retention has value for personnel security purposes. The ability to assess the "whole person" over a long period of time enables security clearance adjudicators to identify and address any issues (personnel security or counterintelligence-related) that may exist or may arise.

In other words, just one paragraph after having said it's not his job to worry about the CI implications of keeping 21 million clearance holders' records in a poorly secured database, the Counterintelligence Executive said the government needed to keep those records (because the government passed a policy deciding they'd keep those just a year ago) for counterintelligence purposes.

In a statement on the response, Wyden, like me, reads it as Evanina insisting this key CI role is not his job. To which Wyden adds, putting more data in the hands of these insecure agencies under CISA would only exacerbate this problem.

> The OPM breach had a huge counterintelligence impact and the only response by the nation’s top counterintelligence officials is to say that it wasn’t their job. This is a bureaucratic response to a massive counter-intelligence failure and unworthy of individuals who are being trusted to defend America. While the National Counterintelligence and Security Center shouldn’t need to advise agencies on how to improve their IT security, it must identify vulnerabilities so that the relevant agencies can take the necessary steps to secure their data.
>
> The Senate is now trying to respond to the OPM hack by passing a bill that would lead to more personal information being shared with these agencies. The way to improve cybersecurity is to ensure that network owners take responsibility for plugging security holes, not encourage the sharing of personal information with agencies that can’t protect it adequately.

Somehow, the government kept a database full of some of its most important secrets on an insecure server, and the guy in charge of counterintelligence can only respond that we had to do that to serve counterintelligence purposes.

ANOTHER REASON GM MAY HAVE COME AROUND TO CISA

Last week, Wired had a story about a hack of GM vehicles that the car company took 5 years to fix. As the story explains, while GM tried to fix the vulnerability right away, their efforts didn’t completely fix the problem until GM quietly sent a fix to its vehicles over their Verizon network earlier this year.

> GM did, in fact, make real efforts between 2010 and late 2014 to shield its vehicles from that attack method, and patched the flaws it used in later versions of OnStar. But until the surreptitious over-the-air patch it finished rolling out this year, none of its security measures fully prevented the exploit in vehicles using the vulnerable eighth generation OnStar units.

The article uses this is a lesson in how ill-equipped car companies were in 2010 (notably, right after they had been put through bankruptcy) to fix such things, and how much more attentive they’ve gotten in the interim.

> GM tells WIRED that it has since developed the ability to push so-called “over-the-air” updates to its vehicles. The company eventually used that technique to patch the software in its OnStar computers via the same cellular Internet connection the UCSD and UW researchers exploited to hack the Impala. Starting in November of 2014, through the first months of 2015, the company says it silently pushed out a software update over its Verizon network to millions of vehicle with the vulnerable Generation 8 OnStar computer.

> Aside from the strangely delayed timing of that patch, even the existence of any cellular update feature comes as a surprise to the UCSD and UW researchers. They had believed that the OnStar computers could be patched only by driving them one-by-one to a dealership, a cumbersome and expensive fix that would have likely required a recall.
>
> GM chief product cybersecurity officer Jeff Massimilla hints to WIRED that performing the cellular update on five-year-old OnStar computers required some sort of clever hack, though he refused to share details. "We provided a software update over the air that allowed us to remediate the vulnerability," Massimilla writes in an email. "We were able to find a way to deliver over-the-air updates on a system that was not necessarily designed to do so."

What Wired doesn't note is that GM was in the thick of recall hell by November 2014 because of its delay, during the same period, in fixing ignition problems. It's not just the network problem GM wasn't fixing, it was more traditional problems as well. Whatever hack GM pulled off, starting in November 2014 as a kluge to fix a long-running problem, GM did so while under great pressure for having sat on other (more obviously dangerous) problems with their cars. GM also did so knowing their recognizable Impala would be shown on 60 Minutes exhibiting this problem.

> In late 2014, they demonstrated it yet again for a *60 Minutes* episode that would air in February of 2015. (For both shows they carefully masking-taped the car's logos to prevent it from being identified, though car blog Jalopnik nonetheless identified the Impala from the *60 Minutes* demo.)

So GM had a lot more urgency to find curious hacks in November 2014 than they did in 2010.

That obvious urgency doesn't stop GM from claiming they've changed their ways, pointing to a quick fix they made in July (though they said nothing about the apparent vulnerability of Escalades to the same hack researchers used on a Jeep Cherokee).

> Massimilla also admits that GM took so long to fully protect its vehicles because it simply wasn't ready in 2010 to deal with the threat of car hackers. He contrasts that response to GM's cybersecurity practices today, such as issuing a fix in just two days when it was alerted to a flaw in its iOS OnStar app in July. "The auto industry as a whole, like many other industries, is focused on applying the appropriate emphasis on cybersecurity," he writes. "Five years ago, the organization was not structured optimally to fully address the concern. Today, that's no longer the case."

While I think the article pays too little attention to the recall bonanza in the industry and how that may have changed GM's attentiveness to cybersecurity flaws, it claims that one thing that has motivated quicker responses is that, unlike the researchers who did the original hack on OnStar, researchers are now releasing their results generally. Significantly, the researchers that found this problem have now switched to full disclosure of their results.

> Savage says that if he were doing the same research today, he'd reconsider the decision to shield GM from public pressure. When he, Koscher, and other researchers revealed another car hacking technique in August, for instance—this time hijacking cars through a common Internet-connected gadget many drivers plug into their dashboards for insurance

> purposes—they publicly named every company whose bugs they'd exploited.

I raise all this not just for what it says about cars and hacking but also — of course — because of what it says about cybersecurity policy.

As I've noted, GM was actually a late supporter of CISA, writing a letter to announce their support just before recess in August, when business groups were making a big push to get it passed. I suggested at the time that GM might have been motivated by their Escalade vulnerability, hoping (possibly knowing) that if they revealed such vulnerabilities to authorities the government — the entire government, according to the plain letter of CISA — would be unable to launch any action against the company. On its face, it would appear that limitation would apply to NHTSA.

I'm not sure how this would work in practice — and neither are any of the lawyers I've been asking about this. But GM now knows that NHSTA is under far more pressure to order expansive recalls. And it also knows that researchers will default to publishing their research on vehicle insecurities, unlike what they did for this hack 5 years ago.

Those two things may well explain GM's sudden interest in sharing information with the government.

THE SPECIAL SANGER CYBER UNICORN: IRAN WARMONGER EDITION

I noted earlier that the reporting on the US not imposing cybersanctions on China appears to have credulously served its purpose in creating a narrative that may have helped create the environment for some kind of deal with China.

NYT’s David Sanger did his own version of that story which deserves special focus because it is so full of nonsense — and nonsense that targets Iran, not China.

Sanger starts his tale by quoting something President Obama said at Fort Meade over the weekend out of context. In response to a question about the direction of cybersecurity in the next 5-10 years, Obama spoke generally about both state and non-state actors.

> Q Good afternoon, Mr. President. You alluded to in your opening remarks the threat that cyber currently is. And there’s been a lot of talk within the DOD and cyber community of the possibility of a separate branch of the military dedicated to cyber. I was wondering where you see cyber in the next five to ten years.
>
> THE PRESIDENT: Well, it’s a great question. We initiated Cyber Command, anticipating that this is going to be a new theater for potential conflict. And what we’ve seen by both state *and non-state actors* is the increasing sophistication of hacking, the ability to penetrate systems that we previously thought would be secure. And it is moving fast. So, offense is moving a lot faster than defense.
>
> Part of this has to do with the way the Internet was originally designed. It was not designed with the expectation that there would end up being three or four or five billion people doing commercial transactions, et cetera. It was thought this was just going to be an academic network to share papers and formulas and whatnot. And so the architecture of the Internet makes it very difficult to defend consistently.

> We continue to be the best in the world at understanding and working within cyber. But other countries have caught up. The Russians are good. The Chinese are good. The Iranians are good. *And you've got non-state hackers who are excellent.* And unlike traditional conflicts and aggression, oftentimes we don't have a return address. If somebody hacks into a system and goes after critical infrastructure, for example, or penetrates our financial systems, we can't necessarily trace it directly to that state *or that actor*. That makes it more difficult as well. [my emphasis]

Sanger excised all reference to "excellent" non-state hackers, and instead made this a comment about hacking by state actors.

> "Offense is moving a lot faster than defense," Mr. Obama told troops on Friday at Fort Meade, Md., home of the National Security Agency and the United States Cyber Command. "The Russians are good. The Chinese are good. The Iranians are good." The problem, he said, was that despite improvements in tracking down the sources of attacks, "we can't necessarily trace it directly to that state," making it hard to strike back.

Sanger then took this comment very specifically directed at the upcoming Xi visit and China,

> And this is something that we're just at the infancy of. Ultimately, one of the solutions we're going to have to come up with is to craft agreements among at least state actors about what's acceptable and what's not. And so, for example, I'm going to be getting a visit from President Xi of China, a state visit here coming up in a couple of weeks. We've made very clear to the Chinese that there are certain practices

> that they’re engaging in that we know are emanating from China and are not acceptable. And we can choose to make this an area of competition — which I guarantee you we’ll win if we have to — or, alternatively, we can come to an agreement in which we say, this isn’t helping anybody; let’s instead try to have some basic rules of the road in terms of how we operate.

And suggested it was directed at other states more generally.

> Then he issued a warning: “There comes a point at which we consider this a core national security threat.” If China and other nations cannot figure out the boundaries of what is acceptable, “we can choose to make this an area of competition, which I guarantee you we’ll win if we have to.”

Sanger then spends six paragraphs talking about how hard a time Obama is having “deterring” cyberattacks even while reporting that China and the US have forged some kind of deal that would establish norms that are different than deterrence but might diminish attacks. He also, rather curiously, talks (again) about “unprecedented” theft of personal information in the OPM hack that we need to deter — even though James Clapper has repeatedly said publicly that we do the same thing (and by some measures, on a much bigger scale).

After dispensing lots of nonsense about China, Sanger then pivots, with no transition, to Iran, beginning by refuting (sort of) NSA Director Mike Rogers’ public report [see after 1:39:30, which I’ll return to] that Iran has stopped hacking the US during the negotiation of the nuclear deal by claiming that Clapper said the same in secret but also said that Iran may turn to the cyber attacks it has voluntary given up.

> In classified sessions, American intelligence agencies have told members of Congress that while computer attacks on the United States emanating from Iran decreased during the negotiations over the nuclear accord, they believe that an Iran stymied in developing a nuclear ability over the next 10 to 15 years is likely to pour more resources into cyberweapons. Such weapons have already been used against the Navy, American banks, a Las Vegas casino and Saudi Arabia's largest oil producer, without setting off significant retaliation.

Sanger describes all those attacks ascribed to Iran and says there has been no retaliation (as if these attacks themselves shouldn't be considered rather pathetic retaliation against Stuxnet — which is unmentioned in the article — and aside from the sanctions and all that) without considering what it means that Iran ended them without retaliation.

A puzzle!

So having shown that, having not retaliated against Chinese hacking, the US had made some kind of deal on norms in cyberspace, and having not "retaliated" against Iran after beating it silly with StuxNet, Iran has stopped its cyberattacks against the US, Sanger then claims that Obama is having a hard time deterring Iran and China (somehow Russia, the country accused of the most recent hacks against us, has fallen out of this discussion, which I find curious).

> With both Iran and China, Mr. Obama is struggling with variants of the same problem: How do you contain a rising power that has discovered the benefits of an anonymous, havoc-creating weapon that can also yield vast troves of secret data? And how do you convince them that actions for which "they have paid no price," as the director of the N.S.A. and the Cyber Command, Adm.

> Michael S. Rogers, put it the other day, will no longer be cost-free?

Sanger then goes on to lay out the stakes of this, pointing to Iran's response to attacks in Iraq, Syria, and Yemen (though spinning that as its growing influence rather than US and Saudi idiocy) and China's efforts in the South China sea.

> With Iran and China, of course, cyberwarfare is only part of those middle-game challenges. Containing Iran's growing influence in Iraq, Syria, Yemen and throughout the region is central to the administration's post-accord challenge. And containing China's effort to reclaim islands in the South China Sea, a bet by Beijing that neither Washington nor Asian nations will stop it from developing a new base of operations and exclusive claims to air and sea territory, is the subtext of much of the tension with Mr. Xi's government.

That is, given our traditional conflicts with both these countries, Sanger has decided to write a very long article claiming we can't cyberdeter them, even while presenting evidence we've found some way to cyber discuss with them.

Sanger's erroneous reporting continues. First, he claims our response to North Korea's alleged hack of Sony had no visible response.

> So far, the administration's response has seemed inconsistent, and to many incoherent.
>
> When North Korea was identified as the country that attacked Sony, Mr. Obama — in possession of evidence gleaned from the N.S.A.'s yearslong penetration of North Korean networks — went to the White House press room, declared that the leadership in Pyongyang was

> responsible, and said the United States would retaliate at the time and in the manner of its choosing.
>
> The public retaliation was a series of modest financial sanctions that did little additional damage to the most sanctioned country on earth. If there was a lasting response to the attack, only North Korea knows about it.

This ignores that last week NSA Director Mike Rogers made it very clear North Korea has not cyberattacked any companies in the US since we did whatever we did to retaliate for Sony. Another piece of evidence that we got a country to stop, at least temporarily, which Sanger presents as evidence Obama is adrift.

Then there's Sanger's repetition of the bizarre claim that DOJ indicted a bunch of Chinese officials for IP theft last year.

> And when Unit 61398 of the People's Liberation Army in China was exposed as the force behind the theft of intellectual property from American companies, the Justice Department announced the indictment of five of the army's officers. Justice officials hailed that as a breakthrough. Inside the intelligence community and the White House, however, it was regarded as purely symbolic, and the strike on the Office of Personnel Management continued after the indictments were announced.

As I pointed out at the time, a good deal of what got charged in that indictment *was not IP theft*, but instead spying on communications during trade negotiations and disputes, something the US does itself. I mean, kudos to whatever DOJ official has gotten a slew of journalists covering cyber issues to brainlessly repeat that this was about IP theft, but it was at least as much about DOJ charging foreign officials for stuff US officials do too. It might better serve as a lesson in the idiocy of trying to retaliate against China for stuff the US does, which brings us back to the absurd notion we’re going to retaliate for the OPM hack.

Jeebus.

Sanger ends this screed by focusing again on Iran.

> And now Iran is part of the worry. Admiral Rogers told a House panel that while cyberattacks directed at the United States abated during talks over the nuclear deal, the country was now “fully committed” to using them as part of a revamped military strategy. The Iranians, another senior intelligence official said, discussing private intelligence assessments on the condition of anonymity, “will be looking intensely at how we handle the Chinese.”

This is, perhaps unsurprisingly given Sanger’s misrepresentation of what Obama said, a misrepresentation of what Rogers said, which was [1:39;30]:

> In the 2012-2013 time frame we were seeing significant Iranian activity directed against U, they US financial sector, trying to take down financial websites. Flowing out of ’13 as the negotiations kicked in in many ways we saw less activity directed directly against us, but I would remind people I have not seen the Iranians step back from their commitment to cyber as a tool and we see it being used against a variety of actors in the Gulf and the region, they continue to be fully committed to, how can they use this capability to achieve a broader set of national objectives.

Remember: those attacks against banks were DNS attacks, not anything striking at the heart of US financial integrity. And Iran has backed down from even that level of focus on the US. What they haven't done, Rogers' response suggests, is back down from attacks on the Saudis and Israelis (though one of Iran's most effective attacks in the US was against Sheldon Adelson's casino after he said the US should drop a nuke on Iran; the attack, which obtained intelligence, curiously took place in 2014, after Rogers said attacks against the US have stopped — does Rogers justifiably not consider this an unprovoked attack on a US company?). Which is perhaps unsurprising because Iran is involved in several proxy wars against them (especially the Saudis).

But the implication from Sanger's misinvocation of Rogers is that the US should be expected to retaliate against Iran for its use of cyberattacks in proxy wars or against entities — Israel! — that have conducted cyber acts of war on their soil.

I get that there are parts of Obama's cyber approach that need significant improvement, particularly with hardening the US government and its ill-considered rush to give corporations immunity. There are huge concerns Sanger could focus on if he wanted — as I mentioned, his silence about Russia is baffling. Non-state criminals did far more damage to JPMorgan Chase than Iran did, and non-state actors can continue to rival Iran elsewhere (as Obama said, some of them are "excellent"). But instead he chose to spin.

What Sanger has presented in this piece is evidence that the US has made progress with China, Iran, and North Korea (though in none of those cases does he admit the progress). Those are baby steps, undoubtedly, but especially with Iran and North Korea, top IC officials are the ones reporting this progress, not Sanger's secret Congressional sources. And yet for some reason Sanger wants to misrepresent evidence and claim that this amounts to worse than nothing.

CYBER-UNICORN JOURNALISTS SHOCKED THE UNICORN DIDN'T APPEAR, AGAIN

When last we checked in on claims the US was going to cyber-deter China, I suggested people should understand the underlying dynamics at work.

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

That was 11 days ago. Since then, James Clapper has claimed (I'm not necessarily endorsing this claim as true, especially given the timing) the US isn't even 100% sure China is behind the OPM hack — in part because we've lost some monitoring capabilities in recent years — all while making it clear we don't consider it an attack because we do precisely the same thing to China. At the same time, top level US and Chinese officials met in anticipation of Xi Jinping's visit. Here's the White House readout of that meeting.

> From September 9-12, senior Administration officials held a series of meetings with Secretary of the Central Political and Legal Affairs Commission of the Communist Party of China Meng Jianzhu in Washington, D.C. Mr. Meng traveled to Washington as President Xi Jinping's Special Envoy to discuss cybersecurity and other issues in advance of President Xi's State

> Visit. Secretary of Homeland Security Jeh Johnson hosted Mr. Meng during his visit. In this capacity, Secretary Johnson convened a meeting between members of the Chinese delegation and representatives from the Departments of State, Treasury, Justice, Federal Bureau of Investigation, and the Intelligence Community. In addition, FBI Director Comey also met with Mr. Meng at FBI headquarters for discussions. National Security Advisor Susan E. Rice received Mr. Meng for a meeting at the White House, where she had a frank and open exchange about cyber issues.

Remember: China is believed to have all of Jim Comey and Jeh Johnson's security clearance files (probably Susan Rice's as well). Comey in particular keeps raising that point. That surely adds something to such negotiations, knowing that your interlocutor has read a ready-made intelligence portfolio that your own government compiled on you.

Now the journalists who keep reporting that the US is about to, honest to god, this time they mean it, sanction China for its hacking report that sanctions are off the table for now, in part because those negotiations resulted in some kind of cyber agreement.

> The United States will not impose economic sanctions on Chinese businesses and individuals before the visit of China President Xi Jinping next week, a senior administration official said Monday.
>
> The decision followed an all-night meeting on Friday in which senior U.S. and Chinese officials reached "substantial agreement" on several cybersecurity issues, said the administration official, who spoke on the condition of anonymity because of the topic's sensitivity.

> The potential for sanctions in response to Chinese economic cyberespionage is not off the table and China’s behavior in cyberspace is still an issue, the official said. “But there is an agreement, and there are not going to be any sanctions” before Xi arrives on Sept. 24, the official said.
>
> The breakthrough averted what would have raised a new point of tension with the Chinese that could have overshadowed the meeting — and Xi’s first state visit.
>
> “They came up with enough of a framework that the visit will proceed and this issue should not disrupt the visit,” the official said. “That was clearly [the Chinese] goal.”

The reporting on this appears to be problematic, in part, because sources for these stories themselves misunderstand the issue.

> Yet what that agreement is remains unclear. Two U.S. officials told The Daily Beast that substantial disagreement remains between the U.S. and China. China insists that it’s the victim of cyber spying, not a perpetrator. But the U.S. has filed criminal charges against Chinese officials for their role in stealing trade secrets and intellectual property from American companies.
>
> [snip]
>
> [CSIS Deputy Director Scott] Kennedy noted that given the length of time Meng was in Washington, his visit almost certainly covered other issues, including China’s efforts to hunt down Chinese nationals accused of crimes who are living abroad. U.S. law enforcement officials have complained that Chinese state security operatives are working in this country illegally and trying to

> intimidate Chinese people living here legally.

Remember, “US official” is journalistic code often used for members of Congress or contractors. And if these (possible) members of Congress don’t understand that the US sensors embedded in China’s networks are incredibly invasive cyber spying, if whoever claimed that our indictment for stealing information on trade disputes (something we spy on too) believes that we indicted for stealing IP, if those sources can’t imagine we might respond to the OPM hack by cracking down on extraordinary Chinese agents in the US, then those sources aren’t appreciating the real power dynamics at stake. And we’re going to continue to have journalism on this topic that serves more to provide a convenient narrative than to inform.

Thank you for playing, thank you for providing the appearance of a threat to placate Congress and drive a narrative of a tough negotiation, all while not laying out how the OPM hack changes things.

Several things seem to have been missed in this recent round of cyber-deterrence unicorn reporting. While China’s crashing stock market (renewed again today) provides a bit more leverage for the US against China — among other things, it raises the value Chinese elites would place on their US property and holdings, though China itself wants to pressure some of the same elites — it is still not in our best interest to antagonize this relationship. Moreover, whatever additional leverage we’ve got economically is more than offset by the OPM and related hacks, which China could use in any number of ways to really damage the US, especially given so many of our other critical systems — public and private, and I suspect that’s part of what some of the related hacks have been designed to demonstrate — remain insecure.

Most importantly, even before the Snowden leaks, the US had a real interest in finding some kind of norms that would make the cyber realm less volatile. That's probably even more true now, because (as Clapper said, and this part I believe) our adversaries have been hardening their own defenses while stealing information that turns out to be more valuable to the US, meaning we don't have such asymmetric advantage in the cyber realm anymore.

This comes at a time when Congress has become adamantly opposed to anything that resembles negotiations, because to them it looks like weakness. And most seem not to understand the stakes behind the reasons why the OPM hack cannot be considered an attack.

So if some credulous reporting created the space for such an agreement, great!

JOHN DOE UNGAGGED: NICHOLAS MERRILL WINS THE RIGHT TO REVEAL CONTENTS OF 11-YEAR OLD NATIONAL SECURITY LETTER

Nicholas Merrill, who first challenged a National Security Letter 11 years ago, has won the right to talk about what he was ordered to turn over to the FBI in 2004. A key holding from the decision is that private citizens — as distinct from government officials who have signed non-disclosure agreements — cannot be prevented from talking about stuff that the government, as a whole, has already released.

> A private citizen should be able to disclose information that has already been publicly disclosed by

> any government agency — at least once the underlying investigation has concluded and there is no reason for the identities of the recipient and target to remain secret. Otherwise, it would lead to the result that citizens who have not received such an NSL request can speak about information that is publicly known (and acknowledged by other agencies), but the very individuals who have received such NSL requests and are thus best suited to inform public discussion on the topic could not. Such a result would lead to "unending secrecy of actions taken by government officials" if private citizens actually affected by publicly known law enforcement techniques could not discuss them.

The judge in the case, Victor Marrero, gave the government 90 days to appeal. If they don't (?!?!), Merrill will finally be ungagged after 11 years of fighting.

As noted, the FBI served the NSL back in 2004, when Merrill ran a small Internet Service Provider. Merrill sued under the name John Doe. He twice won court rulings that the gag orders were unconstitutional. But it wasn't until 2010 that he was allowed to ID himself as Doe, and it wasn't until 2014 — a decade after receiving the NSL — that he was able to tell the person whose records the FBI wanted. Even then, even after Edward Snowden revealed the need for more transparency about these things, the government fought Merrill's demand to disclose what he had been asked to turn over, which was included in an attachment to the NSL itself.

See this post and this post for background on Merrill's renewed fight to disclose how much FBI has demanded under an NSL.

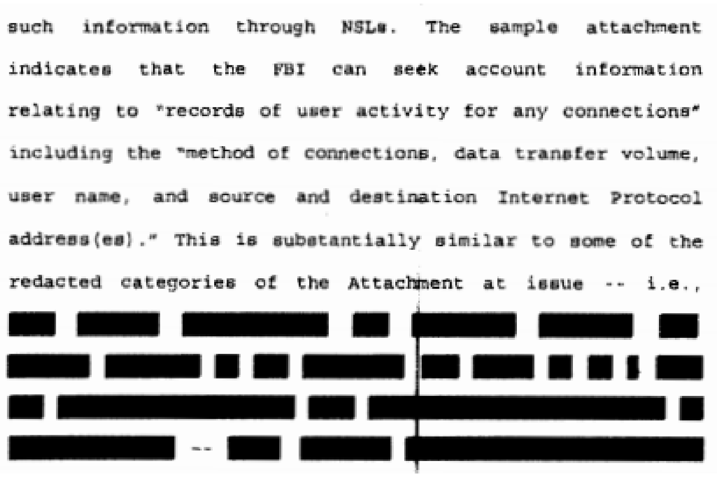
Marrero found that the government just didn't have really good reasons to gag this information, especially given that substantially similar information had been given out by other government agencies, and especially since the government admits it is only trying to hide the information from future targets, not anyone tied to the investigation that precipitated the NSL over a decade ago.

> For the reasons discussed below, the court finds that the Government has not satisfied its burden of demonstrating a “good reason” to expect that disclosure of the NSL Attachment in its entirety will risk an enumerated harm, pursuant to Sections 2709 and 3511.
>
> [snip]
>
> The Government argues that disclosure of the Attachment would reveal law enforcement techniques that the FBI has not acknowledged in the context of NSLs, would indicate the types of information the FBI deems important for investigative purposes, and could lead to potential targets of investigations changing their behavior to evade law enforcement detection. {See Gov’t Mem. at 6.) The Court agrees that such reasons could, in some circumstances, constitute “good” reasons for disclosure.
>
> [snip]
>
> The Government’s justifications might constitute “good” reasons if the information contained in the Attachment that is still redacted were not, at least in substance even if not in the precise form, already disclosed by government divisions and agencies, and thus known to the public. Here, publicly-available government documents provide substantially similar information as that set forth in the Attactunent. For that reason, the Court is not persuaded that it matters that these other documents were not disclosed

> by the FBI itself rather than by other government agencies, and that they would hold significant weight for a potential target of a national security investigation in ascertaining whether the FBI would gather such information through an NSL. The documents referred to were prepared and published by various government divisions discussing the FBI's authority to issue NSLs, the types of materials the FBI seeks, and how to draft NSL requests.
>
> [snip]
>
> Now, unlike earlier iterations of this litigation, the asserted Government interest in keeping the Attachment confidential is based solely on protecting law enforcement sensitive information that is relevant to future or potential national security investigations.
>
> [snip]
>
> [I]t strains credulity that future targets of other investigations would change their behavior in light of the currently-redacted information, when those targets (which, according to the Government, [redacted] see Perdue Deel. ¶ 56) have access to much of this same information from other government divisions and agencies.

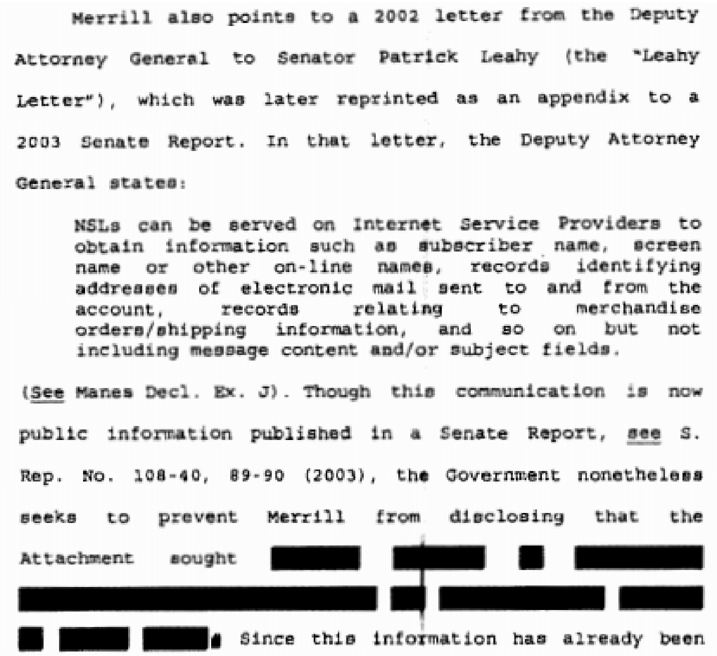
Effectively, Marrero is arguing that since the government has asserted potential national security targets are good at putting 2 plus 2 together, and 2 and 2 are already in the public domain, any targets can already access the information in the attachment.

Marrero's quotations from already released documents and the redactions from the attachment make it clear the government is trying to hide they were getting activity logs…



such information through NSLs. The sample attachment indicates that the FBI can seek account information relating to "records of user activity for any connections" including the "method of connections, data transfer volume, user name, and source and destination Internet Protocol address(es)." This is substantially similar to some of the redacted categories of the Attachment at issue -- i.e., [redacted] -- [redacted]

And the various identities tied to an account (which we know the government matches to better be able to map activity across multiple identities).



Merrill also points to a 2002 letter from the Deputy Attorney General to Senator Patrick Leahy (the "Leahy Letter"), which was later reprinted as an appendix to a 2003 Senate Report. In that letter, the Deputy Attorney General states:

> NSLs can be served on Internet Service Providers to obtain information such as subscriber name, screen name or other on-line names, records identifying addresses of electronic mail sent to and from the account, records relating to merchandise orders/shipping information, and so on but not including message content and/or subject fields.

(See Manes Decl. Ex. J). Though this communication is now public information published in a Senate Report, see S. Rep. No. 108-40, 89-90 (2003), the Government nonetheless seeks to prevent Merrill from disclosing that the Attachment sought [redacted] Since this information has already been

I'll lay more of this out shortly — effectively, Marrero has already done the mosaic work for targets, even without the attachment (though I suspect what the government is really trying to prevent is release of a document defendants can point to to support discovery requests).

Ultimately, Marrero points to the absurd — and dangerous, for a democracy — position that would result if the government were able to suppress this already public information.

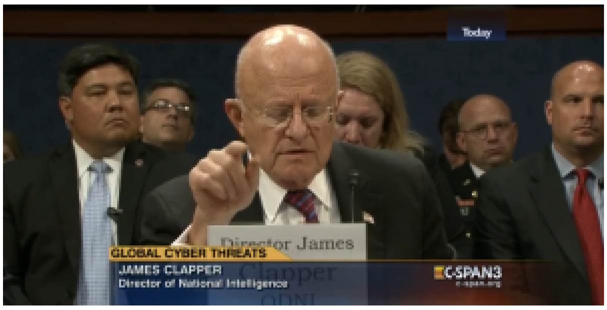
> If the Court were to find instead that the Government has met its burden of

> showing a good reason for nondisclosure here, could Merrillever overcome such a showing? Under the Government's reasoning, the Court sees only two such hypothetical circumstances in which Merrill could prevail: a world in which no threat of terrorism exists, or a world in which the FBI, acting on its own accord and its own time, decides to disclose the contents of the Attachment. Such a result implicates serious issues, both with respect to the First Amendment and accountability of the government to the people.

Especially at a time when the President claims to want to reverse the practice of forever gags on NSLs, Marrero finds such a stance untenable.

Let's see whether the government doubles down on secrecy.

WHAT IF THE INTELLIGENCE COMMUNITY IS LOOKING FOR THE WRONG MALICIOUS USE OF OPM DATA?


Today
Director James Clapper ODNI
GLOBAL CYBER THREATS
JAMES CLAPPER
Director of National Intelligence
C-SPAN3
c-span.org

The revelation in last week's cyber threats hearing the press has been most agog about is that James Clapper predicted hackers would get around to changing, rather than just stealing, data.

> [after 19:00] In the future I believe we'll see more cyber operations that will change or manipulate electronic information to compromise its integrity — in other words, compromise its accuracy and its reliability, instead of merely deleting it or disrupting access to it.
>
> [snip]
>
> [after 56:00] To this point, it's either been disruption — of a website, for example, but more commonly, just purloining information. As I indicated in my opening statement though, I believe the next push on the envelope here is going to be the manipulation or deletion of data, which will of course compromise its integrity.

Um. Really, journalists who cover this area?

The notion that a cyber operator will change data is not new. Proof of that concept happened years ago, with the StuxNet attack, when US and Israeli hackers made the Iranians think everything was going peachy with their centrifuges when in fact they were spinning out of control. No one may yet have manipulated *our* data, but we've manipulated others' data.

Which I guess means, according to Clapper's definition, StuxNet was an attack and not just a hack — in case you had any doubts.

One thing I found far more interesting was Clapper's repeated assertion that the IC has seen no use of the Office of Personnel Management data.

> [after 49:00; see also after 1:29] Clapper: What we've done is speculate how it could be used. And again the

> distinction I was just making with Congressman Westmoreland had to do with the terminology of saying that the OPM breach was an attack. Getting back to definitional issues, we wouldn't characterize it that way. What's of great concern with respect to the OPM breach, which I spoke to briefly in my opening statement had to do with potential uses of that data. And of course, we're looking. Thus far we haven't seen any evidence of their usage of that data.

I said as I was watching and others have said since that this likely just reflects China — almost universally believed to be the OPM perpetrator — playing the long game. It will use the knowledge when it's good and ready, all the while we'll know it has it.

All that said, the *other* thing Clapper said that I found very interesting was that the IC has varying degrees of confidence about who did this hack.

> [after 20:00] Clapper: And while speaking of the OPM breaches, let me say a couple of words about attribution, which is not a simple process and involves at least three related but distinct determinations: geographic point of origin, the identity of the actual perpetrator doing the keystrokes, and the responsibility for actually directing the attack. In the case of OPM, we've had differing degrees of confidence across the IC in our assessment of the responsibility for each of these elements. Of late, unauthorized disclosures and foreign defensive improvements have cost us some technical accesses.

Apparently, not everyone in the IC is completely convinced China did this. This is the kind of statement we never saw, as far as I remember, with regards to the Sony hack (though, admittedly, it’s a lot easier to make unsubstantiated accusations against North Korea than China). Are people really not convinced?

Note, too, the casual reference to the US losing some technical accesses, presumably in response to Snowden’s disclosures and the heightened awareness from our adversaries just how badly we’ve pawned them for years. Given the assumption China hacked OPM, this likely means we’ve lost some visibility into Chinese actions in the last two years.

The evidence China did this hack in part stems from its complexity; few — but not no — other actors could pull it off. That someone would hack United, in tandem with OPM, would support that, given that United flies so many flights from Dulles to China.

All that said is it possible — remotely — some other sophisticated state actor could have done this?

I’m going to assume Clapper is just downplaying the certainty here, possibly in advance of Xi Jinping’s visit to DC.

But if it is remotely true, would that have an effect on our ability to monitor for the use — or even manipulation — of OPM data? That is, if we were looking for Chinese use of the data — focusing on people of Chinese descent and/or people stationed there — would we miss attempts to compromise clearance holders another sophisticated state actor — say, Israel — might target? I’ll just remind that at a time when the US was trying to set up the IRGC for an assassination attempt, someone spamouflaged what likely included our target. I presume that as we got closer and then finalized the Iran deal, Israel’s targeting of our spooks has intensified.

In any case, Clapper seems confident that the data was not compromised here, which is something other commentators have raised as a worry (because doing so would allow you to create clearances for people who had not been vetted, for example).

> [after 1:29]My working definition of whether it's an attack or not and my characterization of it not being an attack in that there was no destruction of data or manipulation of data, it was simply stolen.

But if we're not 100% sure this is China (again, I'm skeptical we have much doubt), maybe we couldn't be so sure about whether the data has been manipulated or — at the very least — used to compromise our clearance holders.

WHY IS DEVIN NUNES RUSHING TO GIVE MORE DATA TO HACK-TASTIC DEPARTMENT OF ENERGY?

On several occasions, I've pointed out that the agencies that would automatically receive data shared with the federal government under cybersecurity bills being pushed through Congress aren't any more secure than Office of Personnel Management, which China hacked in spectacular fashion. Among the worst — and getting worse rather than better — is Department of Energy.

Earlier this week, USAT published more information on how bad things are at DoE.

> Cyber attackers successfully compromised the security of U.S. Department of Energy computer systems more than 150

> times between 2010 and 2014, according to a review of federal records obtained by USA TODAY.
>
> Incident reports submitted by federal officials and contractors since late 2010 to the Energy Department's Joint Cybersecurity Coordination Center shows a near-consistent barrage of attempts to breach the security of critical information systems that contain sensitive data about the nation's power grid, nuclear weapons stockpile and energy labs.
>
> The records, obtained by USA TODAY through the Freedom of Information Act, show DOE components reported a total of 1,131 cyberattacks over a 48-month period ending in October 2014. Of those attempted cyber intrusions, 159 were successful.

Yet at yesterday's Cyber Threats hearing (around 2 minutes), House Intelligence Chair Devin Nunes suggested he only learned of this detail from USAT's report. "[J]ust this morning we learned that Department of Energy was successfully hacked 159 times."

It's troubling enough that the guy overseeing much of the government's cybersecurity efforts didn't already know these details (and I presume that means Nunes is also unaware that DoE has actually been getting *worse* as the Administration tries to fix major holes). Especially given that DoE is part of the Intelligence Community.

But it's even more troubling given that HPSCI's Protecting Cyber Networks Act, like the Senate's Cyber Intelligence Sharing Act, automatically shares incoming cyber threat data with DoE (and permits private entities to share with DoE directly).

This is the height of irresponsibility. Devin Nunes is rushing to share this data – he pushed for quick passage of these bills in the same breath as noting how insecure DoE is –yet he hadn't even bothered to review whether the agencies that would get the data have a consistent history of getting pawned.

Nunes did say that we need to ensure these agencies are secure. But the data is clear: DoE *isn't* secure.

So why not plug those holes before putting more data in for hackers to get?

ADMIRAL MIKE ROGERS VIRTUALLY CONFIRMS OPM WAS NOT ON COUNTERINTELLIGENCE RADAR

For some time, those following the OPM hack have been asking where the intelligence community's counterintelligence folks were. Were they aware of what a CI bonanza the database would present for foreign governments?

Lawfare's Ben Wittes has been asking it for a while. Ron Wyden got more specific in a letter to the head of the National Counterintelligence and Security Center last month.

> 1. Did the NCSC identify OPM's security clearance database as a counterintelligence vulnerability prior to these security incidents?
> 2. Did the NCSC provide OPM with any recommendations to

secure this information?

3. At least one official has said that the background investigation information compromised in the second OPM hack included information on individuals as far back as 1985. Has the NCSC evaluated whether the retention requirements for background investigation information should be reduced to mitigate the vulnerability of maintaining personal information for a significant period of time? If not, please explain why existing retention periods are necessary?

And Steven Aftergood, analyzing a 2013 Intelligence Community Directive released recently, noted that the OPM database should have been considered a critical counterintelligence asset.

> A critical asset is “Any asset (person, group, relationship, instrument, installation, process, or supply at the disposition of an organization for use in an operational or support role) whose loss or compromise would have a negative impact on the capability of a department or agency to carry out its mission; or may have a negative impact on the ability of another U.S. Government department or agency to conduct its mission; or could result in substantial economic loss; or which may have a negative impact on the national security of the U.S.”

> By any reasonable definition, the Office of Personnel Management database of security clearance background investigations for federal employees and contractors that was recently compromised by a foreign adversary would appear to qualify as a "critical asset." But since OPM is not a member or an element of the Intelligence Community, it appears to fall outside the scope of this directive.

But in a private event at the Wilson Center last night, NSA Director Mike Rogers described NSA being brought in to help OPM — but only after OPM had identified the hack.

> After the intrusion, "as we started more broadly to realize the implications of OPM, to be quite honest, we were starting to work with OPM about how could we apply DOD capability, if that is what you require," Rogers said at an invitation-only Wilson Center event, referring to his role leading CYBERCOM.
>
> NSA, meanwhile, provided "a significant amount of people and expertise to OPM to try to help them identify what had happened, how it happened and how we should structure the network for the future," Rogers added.

That "as we started more broadly to realize the implications of OPM" is the real tell, though. It sure sounds like the Chinese were better able to understand the value of a database containing the security clearance portfolios on many government personnel then our own counterintelligence people.

Oops.

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

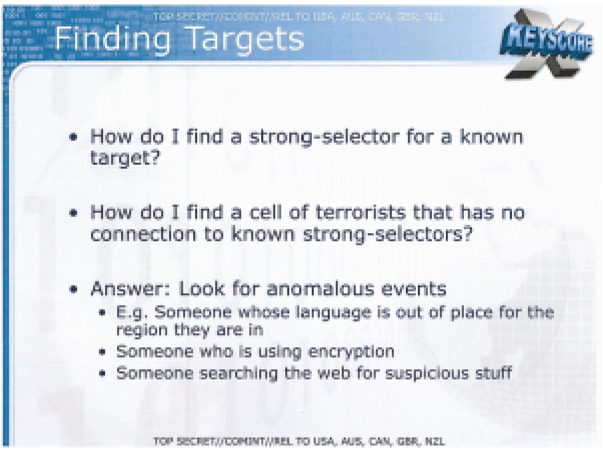
> > statements regarding those trade disputes and related legislative proposals, Wen stole e-mails from senior USW employees containing sensitive, non-public, and deliberative information about USW strategies, including strategies related to pending trade disputes. USW's computers continued to beacon 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.

THE LESSONS NSA TEACHES WHEN IT CONFLATES USE OF ENCRYPTION WITH TERRORISM



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Finding Targets

KEYSCORE

- How do I find a strong-selector for a known target?
- How do I find a cell of terrorists that has no connection to known strong-selectors?
- Answer: Look for anomalous events
  - E.g. Someone whose language is out of place for the region they are in
  - Someone who is using encryption
  - Someone searching the web for suspicious stuff

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Just a few days after our Egyptian allies sentenced 3 Al Jazeera journalists to 3 years in prison, Turkey joined the club, charging 2 UK Vice employees and their Turkish fixer with terrorism. Today, Al Jazeera explained why the Vice journalists got charged: because the fixer uses an encryption technique that members of ISIS also use.

> Three staff members from Vice News were charged with "engaging in terrorist activity" because one of the men was

> using an encryption system on his personal computer which is often used by the Islamic State of Iraq and the Levant (ISIL), a senior press official in the Turkish government has told Al Jazeera.
>
> Two UK journalists, Jake Hanrahan and Philip Pendlebury, along with their Turkey-based Iraqi fixer and a driver, were arrested on Thursday in Diyarbakir while filming clashes between security forces and youth members of the outlawed and armed Kurdistan Workers' Party (PKK).
>
> On Monday, the three men were charged by a Turkish judge in Diyarbakir with "engaging in terrorist activity" on behalf of ISIL, the driver was released without charge.
>
> The Turkish official, who spoke on condition of anonymity, told Al Jazeera: "The main issue seems to be that the fixer uses a complex encryption system on his personal computer that a lot of ISIL militants also utilise for strategic communications."

Note, the Vice journalists were reporting on PKK, not ISIS, but it wouldn't be the first time Turkey used ISIS as cover for their war against PKK.

A lot of people are treating this as a crazy expression of rising Turkish repression, that it conflates use of encryption — even a certain kind of encryption! — with membership in ISIS.

But they're not the only one who does so. As the slide above — and some other documents released by Snowden — makes clear, NSA makes the same conflation. How do you find terrorists without other information, this slide asks? Simple! You find someone using encryption.

While the US might not *arrest* people based on such evidence (though it did hold Al Jazeera journalist Sami al-Hajj for years without charge), they certainly make the same baseless connection.