THE MISUNDERSTANDINGS OF THE ANTI-TRANSPARENCY HILLARY-EXONERATING LEFT

It wasn't enough for Matt Yglesias to write a widely mocked piece calling for less transparency, now Kevin Drum has too. It all makes you wonder whether there's some LISTERV somewhere — the successor to JOURNOLIST, from which leaked emails revealed embarrassing discussions of putting politics above principle, perhaps — where a bunch of center-left men are plotting about how to finally end the email scandal that Hillary herself instigated with a stupid decision to host her own email. Especially given this eye-popping paragraph in Drum's piece:

> Part of the reason is that Hillary Clinton is a real object lesson in how FOIA can go wrong when it's weaponized. Another part is that liberals are the biggest fans of transparency, and seeing one of their own pilloried by it might make them take a second look at whether it's gone off the rails. What we've seen with Hillary Clinton is not that she's done anything especially wrong, but that a story can last forever if there's a constant stream of new revelations. That's what's happened over the past four years. Between Benghazi committees and Judicial Watch's anti-Hillary jihad, Clinton's emails have been steadily dripped out practically monthly, even though there's never been any compelling reason for it. It's been done solely to keep her alleged corruption in the public eye.

Even setting aside that his piece generally ignores (perhaps, betrays no knowledge of) the widely-abused b5 exemption that already lets people withhold precisely the kinds of deliberations that Drum wants to kill FOIA over (and is used to withhold a lot more than that), this paragraph betrays stunning misunderstanding about the Clinton email scandal. Not least, the degree to which many of the delays have arisen from Clinton's own actions.

It led me to go back to read this post, which engages in some cute spin and selective editing, but really gives up the game in this passage.

> Oddly, the FBI never really addresses the issue of whether Hillary violated federal record retention rules. They obviously believe that she should have used a State email account for work-related business, but that's about it. I suppose they decided it was a non-issue because Hillary did, in fact, retain all her emails and did, in fact, turn them over quickly when State requested them.
>
> There's also virtually no discussion of FOIA. What little there is suggests that Hillary's only concern was that her *personal* emails not be subjected to FOIA simply because they were held on the same server as her work emails.

Of *course* the FBI never really addresses how Hillary violated the Federal Records Act. Of *course* the FBI never really addresses how Hillary tried to avoid FOIA. (Note too that Drum ignores that some of those "personal" emails have been found to be subject to FOIA and FRA and Congressional requests; they weren't actually personal.)

That's because this wasn't an investigation into violating the Federal Records Act. As I wrote in this post summarizing Jim Comey's testimony to Oversight and Government Reform:

> The FBI investigation that ended yesterday *only pertained to that referral about classified information*. Indeed, over the course of the hearing, Comey revealed that it was narrowly focused, examining the behavior of only Clinton and four or five of her close aides. And it only pertained to that question about mishandling classified information. That's what the declination was based on: Comey and others' determination that when Hillary set up her home-brew server, she did not intend to mishandle classified information.
>
> This caused some consternation, early on in the hearing, because Republicans familiar with Clinton aides' sworn testimony to the committee investigating the email server and Benghazi were confused how Comey could say that Hillary was not cleared to have her own server, but aides had testified to the contrary. But Comey explained it very clearly, and repeatedly. While FBI considered the statements of Clinton aides, they did not review their sworn statements to Congress for truth.
>
> That's important because the committee was largely asking a different question: whether Clinton used her server to avoid oversight, Federal Record Act requirements, the Benghazi investigation, and FOIA. That's a question the FBI did not review at all. This all became crystal clear in the last minutes of the Comey testimony.
>
> > Chaffetz: Was there any evidence of Hillary Clinton attempting to avoid compliance with the Freedom of Information Act?
> >
> > Comey: That was not the subject of our criminal investigation so I can't answer that sitting here.

> Chaffetz: It's a violation of law, is it not?
>
> Comey: Yes, my understanding is there are civil statutes that apply to that. I don't know of a crimin—
>
> Chaffetz: Let's put some boundaries on this a little bit — what you didn't look at. You didn't look at whether or not there was an intention or reality of non-compliance with the Freedom of Information Act.
>
> Comey: Correct.

Having started down this path, Chaffetz basically confirms what Comey had said a number of times throughout the hearing, that FBI didn't scrutinize the veracity of testimony to the committee *because the committee did not make a perjury referral*.

> Chaffetz: You did not look at testimony that Hillary Clinton gave in the United States Congress, both the House and the Senate?
>
> Comey: To see whether it was perjurious in some respect?
>
> Chaffetz: Yes.
>
> Comey: No we did not.
>
> [snip]
>
> Comey: Again, I can confirm this but I don't think we got a referral from Congressional committees, a perjury referral.
>
> Chaffetz: No. It was the Inspector General that initiated this.

> Now, let me jump to the punch and predict that OGR will refer at least Hillary's aides, and maybe Hillary herself, to FBI for lying to Congress. They might even have merit in doing so, as Comey has already said her public claims about being permitted to have her own email (which she repeated to the committee) were not true. Plus, there's further evidence that Hillary used her own server precisely to maintain control over them (that is, to avoid FOIA).

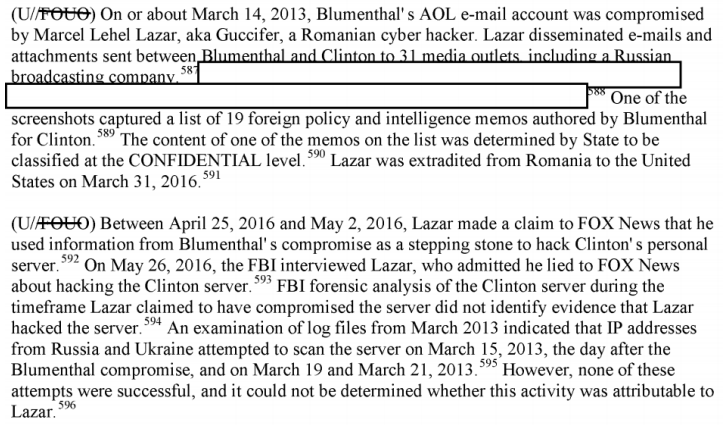
As I said in my earlier post, I'm loathe to admit this, because I'd really like to be done with this scandal (I'd like, even more, to come up with sensible policy proposals like fixing email and text archiving to prevent this from happening in every presidential administration). All the questions about whether Hillary chose to keep her own server to avoid oversight (or, as Chaffetz asked today, to obstruct OGR's investigation) has never been investigated by FBI. Those requests even have more merit than Democrats are making out — in part for precisely this reason, FBI has never considered at least some evidence to support the case Hillary deliberately avoided FRA, including a string of really suspicious timing. As I wrote in my other post, I also think they won't amount to anything, in part because these laws (including laws prohibiting lying to Congress) are so toothless. But they are a fair question.

All that said, it is incorrect to take a report showing the FBI not charging Hillary for intentionally mishandling classified information and conclude from that that hers is an example of FRA and FOIA gone amuck. On the contrary. Hillary has never been exonerated for trying to avoid FOIA and FRA. The evidence suggests it would be hard to do that.

GUCCIFER 1'S POTENTIALLY RUSSIAN IP ADDRESS

I'm a bit late to the FBI report on Hillary's emails. I'm reading it now for all the details that don't serve to reinforce one's assumptions about Hillary's email scandal (as the report honestly can do for all sides).

But I wanted to point to this detail. In the report's short discussion of Guccifer 1's hack of Sidney Blumenthal, the report suggests that Guccifer may have tried to hack Hillary in the days after hacking Blumenthal.



(U//~~FOUO~~) On or about March 14, 2013, Blumenthal's AOL e-mail account was compromised by Marcel Lehel Lazar, aka Guccifer, a Romanian cyber hacker. Lazar disseminated e-mails and attachments sent between Blumenthal and Clinton to 31 media outlets, including a Russian broadcasting company.[587] [redacted][588] One of the screenshots captured a list of 19 foreign policy and intelligence memos authored by Blumenthal for Clinton.[589] The content of one of the memos on the list was determined by State to be classified at the CONFIDENTIAL level.[590] Lazar was extradited from Romania to the United States on March 31, 2016.[591]

(U//~~FOUO~~) Between April 25, 2016 and May 2, 2016, Lazar made a claim to FOX News that he used information from Blumenthal's compromise as a stepping stone to hack Clinton's personal server.[592] On May 26, 2016, the FBI interviewed Lazar, who admitted he lied to FOX News about hacking the Clinton server.[593] FBI forensic analysis of the Clinton server during the timeframe Lazar claimed to have compromised the server did not identify evidence that Lazar hacked the server.[594] An examination of log files from March 2013 indicated that IP addresses from Russia and Ukraine attempted to scan the server on March 15, 2013, the day after the Blumenthal compromise, and on March 19 and March 21, 2013.[595] However, none of these attempts were successful, and it could not be determined whether this activity was attributable to Lazar.[596]

The passage is appropriately ambiguous. Guccifer (Lazar) successfully hacked Blumenthal on March 14, 2013. The next day — and again on March 19 and 21 — there were unsuccessful probes on Hillary's server. The FBI suggests those may have been Guccifer, though states it doesn't know whether it is or not (which is weird, because Guccifer has been in US custody for some time, though I suppose his lawyer advised him against admitting he tried to hack Hillary).

I find all this interesting because those probes were made from Russian and Ukrainian IPs. That's not surprising. Lots of hackers use Russian and Ukrainian IPs. What's surprising is there has been no peep about this from the Russian fear industry.

That may be because the FBI isn't leaking wildly about this. Or maybe FBI has less interest to pretend that all IPs in Russia are used exclusively by state agents of Vlad Putin (not least because then they should have been looking for Russians hacking the DNC?).

It's just an example of what an attempted hack might look like without that Russian fear industry.

JIM COMEY IMPUGNS POT SMOKERS AGAIN

Reason reports that the American Legion just passed a resolution calling on Congress to reclassify cannabis.

> One of the potential medical values of medical marijuana is as a treatment for Post-Traumatic Stress Disorder (PTSD). And in what must certainly at this point make it abundantly clear where the majority of Americans stand on marijuana use, the American Legion has just voted at its national convention to support a resolution calling on Congress to legislatively reclassify cannabis and place it in a category that recognizes its potential value.
>
> The resolution, readable here at marijuana.com, highlights a number of important statistics that have helped push the Legion to support it. Across two years, the Department of Veterans Affairs have diagnosed thousands of Afghanistan and Iraq War veterans as having PTSD or Traumatic Brain Injuries (TBI). More than 1,300 veterans in fiscal year 2009 were hospitalized for

> brain injuries. And the resolution notes that systems in the brain can respond to 60 different chemicals found in cannabis.
>
> Therefore, the American Legion wants the DEA to license privately-funded medical marijuana and research facilities and to reclassify marijuana away from being lumped in with drugs like cocaine and meth.

If veterans suffering from PTSD were able to use cannabis as treatment, we would have to add them to the list of people — like Malia Obama — whom Jim Comey thinks don't have integrity.

For the second time in as many months, Comey last week used the example of people who smoke pot (on their way to an interview, at least) to describe a lack of integrity.

> To have a cyber special agent, you need three buckets of attributes. You need integrity, which is non-negotiable. You need physicality. We're going to give you a gun on behalf of the United States of America, you need to be able to run, fight, and shoot. So there's a physicality required. And obviously there's an intelligence we need for any special agent, but to be a cyber special agent, we need a highly sophisticated, specialized technical expertise.
>
> Those three buckets are rare to find in the same human being in nature. We will find people of great integrity, who have technical talent, and can't squeeze out more than two or three push-ups. We may find people of great technical talent who want to smoke weed on the way to the interview. So we're staring at that, asking ourselves, "Are there other ways to find this talent, to equip this talent, to grow this talent?" One of the things we're looking at is, if we find

> people of integrity and physicality and high intelligence, can we grow our own cyber expertise inside the organization? Or can we change the mix in cyber squads? A cyber squad today is normally eight special agents—gun-carrying people with integrity, physicality, high intelligence, and technical expertise. Ought the mix to be something else? A smaller group of this, and a group of high-integrity people with technical expertise who are called cyber investigators?

I get that this cute labeling of pot smokers as lacking integrity is part of his script (he used almost the same lines in both speeches), perhaps to avoid thinking about what it means that our nation can't best fight the alleged biggest threat to it because of outdated laws. But either he has given no thought about the words that are falling out of his mouth (indeed, he also seems to have no understanding of the the words "adult" and "mature" mean, which are other words he tends to wield in profoundly troublesome fashion), or the nation's top cop really can't distinguish between law — and that, not even in all states anymore — and ethics.

FBI'S FANCY BEAR CYBER STRUCTURE

Back in July, I noted this passage in the latest DOJ IG report on FBI's cyber prioritization.

> According to the FBI, computer intrusion matters Involving national security are the highest priority matters investigated by the FBI Cyber Division. National security computer intrusion

> matters are intrusions or attempted intrusions into any computer or information system that may compromise the confidentiality, integrity, or availability of critical infrastructure data, components, or systems (e.g., cyber national security incidents or threats to the national Information infrastructure) by or on behalf of a foreign power, or an agent of a to include designated international terrorist groups. [half paragraph redacted]
>
> In FY 2015, to ensure t hat the highest ranked threats are efficiently investigated, the Cyber Division implemented its Cyber Threat Team (CIT) model. A CTT focuses on the investigation of and operations against a specific national security threat. Each CTT is comprised of lead field office, called a Strategic Threat Execution office, up to five field offices assisting in specific aspects of the threat called Tactical Threat Execution offices, and a Cyber Division headquarters threat manager. The CTT bears the responsibility for managing the strategy, operations, and intelligence for its assigned threat. [half paragraph redacted]
>
> The intention of the Cyber Division's err model is to facilitate the allocation of resources to cyber national security threats, increase efficiency in addressing those threats, and facilitate the development of subject matter expertise within various field offices. Additionally, the CTT model is intended to enable each field office to focus on specific, assigned threats, helping to prevent the previous diffusion of efforts wherein multiple field offices were working the same cyber threat and not coordinating

> efforts. Prior to the implementation of the err, such overlapping investigations were a great challenge for the FBI. While its field offices each have a territory for which they are responsible, cyber threats are not restricted by geographical boundaries, so a territorial model proved ineffective. Lastly, the err model is intended to assist the FBI in prioritizing and properly allocating resources to each field office based on the threats on which they are assigned to work.
>
> The Cyber Division organizes its headquarters national security intrusion threat operational units geographically, including sections responsible for identifying, pursuing, and defeating cyber adversaries emanating from Asia, Eurasia, and Middle East/Africa. Such geographic delineations of responsibility do not present the same problems at Cyber Division Headquarters, since responsibility for the threats is based on their point or area of origin, and not the multiple U.S. jurisdictions where they might have an impact. The threat operational units coordinate with the errs and with units of the Cyber Intelligence Section, which also are geographically organized and provide actionable intelligence information.

In other words, at both the field office level and at the national level, the FBI's cyber agents have reorganized around the geography of the threat rather than the geography of the target.

Jim Comey elaborated on this reorganization in a speech on cyber (and back dooring encryption) last week.

> The challenge we face today, with a threat that comes at us at the speed of

> light from anywhere in the world, is that physical place isn't such a meaningful way to assign work any longer. Where did "it" happen when you're talking about an intrusion that's coming out of the other side of the globe, aimed at multiple enterprises either simultaneously or in sequence? That "it" is different than it ever was before.
>
> So we've changed the way we're assigning work. We have now created a Cyber Threat Team model, where we assign the work in the FBI based on ability. Which field office has shown the chops to go after which slice of the threat we face—that stack? And then assign it there.
>
> This does two things for us. It allows us to put the work where the expertise is, and it creates a healthy competition inside the FBI. Everybody wants to be at the front of the list to own important threats that come at us. We assign, in the Cyber Threat Team model, a particular threat. *Let's imagine it's a particular threat that comes at us from a certain nation-state actor set. We assign that to the Little Rock Division because the Little Rock Division has demonstrated tremendous ability against that threat.*
>
> But we're not fools about important physical manifestations, because that threat is going to touch particular enterprises around the country. And the CEOs of those enterprises and their boards are going to want to know, "Has the FBI been here to talk to us? And what's the nature of the investigation? And how is it going?" To make sure we accommodate that need, we're going to allow up to four other offices to help the team that is assigned the threat in Little Rock. If a company is hit in

> Indianapolis, and one is hit in Seattle, and one is hit in Miami, those field offices will also be able to assist in the investigation, but the lead will be in Little Rock. Then, the air traffic control for all of that to make sure we are not duplicating effort, or sending confusing messages, will come from the Cyber Division at Headquarters.
>
> We're trying this. We've been doing it now for about a year in a half. Seems to be working pretty well. It has set very, very healthy competition inside the FBI, which is good for us. But we're confronting a challenge and a way of doing work that we've never seen before, so we're eager to get feedback and then iterate as make sense. We want to be humble enough to understand that just as our world has been transformed in our lifetimes, the way in which we do our work is being transformed. We have to be open to changing when it makes sense.
>
> So the Cyber Threat Team model is at the core of our response. Also at the core of our response is a "fly team" of experts that we've put together that we call the CAT team—the Cyber Action Team. Just as in terrorism, we have pre-assigned pools of expertise that can jump on an airplane and go anywhere in the world in response to a terrorism threat, we're building that, and have built, that same capability in respect to cyber, so that, if there is a particular intrusion—let's say Sony in Los Angeles—we have the talent, the agent talent, the analyst talent, the technical talent, that's already assigned to the Cyber Action Team that's ready to deploy at a moment's notice to literally fly to Los Angeles to support the investigation.

Comey had just defined "the stack" he refers to

here as the priority of threats the FBI faces; nation-states, with China, Russia, Iran, and North Korea named, followed by multinational criminal syndicate, followed by "purveyors of ransomware," followed by hactivists, with terrorists (who Comey says aren't yet developing a hacking capability) last. This would suggest that this means no ransomware is perpetrated by multinational crime organizations, which would surprise me.

Now, I get the logic of such organization. Not only can network intrusions be launched from anywhere, but they usually hide where they're launched from. So geographical location, in this scheme, appears to be about holding corporate CEO hands (I guess they get different victim service from the FBI than the rest of us), not investigative venue.

But it also raises a few concerns for me.

Will devolution of cyber lead to more abuse of venue?

First, questions of venue for prosecution. We've already seen, with Weev, DOJ prosecuting a hacker (I'm not sure where Weev would be defined in this stack, because he wasn't doing it for political reasons) in an improper venue because of the nifty precedents there. With Playpen, we've got DOJ — before Rule 41 gets rewritten — hacking thousands based off one Eastern District of Virginia magistrate's warrant.

This dispersed focus would seem to encourage such legally problematic moves.

To the Fancy Bear watchers everything looks like a Fancy Bear

In addition, there's a potential problem with assigning cases by perceived perpetrator, one that replicates a problem in the private

contracting world, where contractors routinely hype the threat of the day (which today is Russia, but which a few years ago was China) because it drove sales.

That is, at some level, FBI appears to be assigning cases based on preliminary evidence to specific CTTs. This seems potentially very problematic from an investigative standpoint, as it answers the question, "whodunnit," at the beginning of the process, not the end. And that particular CTT has an incentive to keep any big flashy case in its own hands, meaning they're going to be disinclined to see any other potential actors out there.

Moreover, if a case — say the DNC hack —that could involve multiple intrusions or actors with competing interests gets assigned to the group whose bureaucratic imperative requires it to be just one actor, it is far less likely they're even going to see the evidence that something more may be going on.

Again, this is just a potential problem, but it could be a very serious one, as it could reverse the investigative model that FBI has traditionally used.

FBI's 702 activities have been devolved as well and with that devolution undergo less oversight

Finally, this potentially exacerbates a concern I have with how FBI manages Section 702. The most recent batch of Semiannual reports that came out show that more 702-related functions are devolving to FBI Field offices, with one redaction (see italics) suggesting there might be some role involving tasking going on at Field offices. And as this passage from the October 2014 report suggests, ODNI is not monitoring things as closely.

> During this reporting period, NSD continued to conduct minimization

> reviews at FBI field offices in order to review the retention and dissemination decisions made by FBI field office personnel with respect to Section 702-acquired data. As detailed in the attachments to the Attorney General's Section 707 Report, NSD conducted minimization reviews at sixteen FBI field offices between June 1, 2013, through November 30, 2013 and reviewed *[redacted]* involving Section 702-tasked facilities.
>
> ODNI participated in one of these reviews,10 and received written summaries regarding any issues discovered in the other reviews. (U//FOUO) NSD's review of field offices coincided with FBI's broadening of the use of Section 702-acquired data at these field offices. Although there were isolated instances of noncompliance with the FBI minimization procedures and/or FBI policy, NSD and ODNI found that overall agents understood and were properly applying the requirements of FBI policy and the minimization procedures.11
>
> 10 (U) ODNI joins NSD on these reviews when the FBI field offices are located in or within reasonable driving distance of the Washington, D.C. area (e.g., the Washington Field Office and the Baltimore Field Office). During this reporting period, ODNI joined NSD for the Baltimore Field Office review. ODNI plans to continue to accompany NSD during the minimization reviews of the FBI Washington and Baltimore field offices and is continuing to explore the feasibility of joining NSD on reviews of other FBI field offices.
>
> 11 (S//NF) NSD's review found only one instance where U.S. person information was not properly handled as required by

> the minimization procedures. Specifically, the agent improperly disseminated U.S. person information that did not meet the standard minimization procedures requirement. Although the information reasonably appeared to be foreign intelligence information, it did not seem to have met the requirement that such information shall not be disseminated in a manner that identifies a United States person unless such person's identity is necessary to understand foreign intelligence information or to assess its importance. In this case, upon NSD's review, the agent agreed that the disseminated U.S. person identity did not meet the above standard. NSD confirmed that the agent recalled the dissemination and re-issued the dissemination without identifying the U.S. person.

Along with some interesting new redactions in the boilerplate about FBI's roles in 702, the October 2014 and June 2015 report both include this paragraph:

> While prior Joint Assessments provided figures regarding the number of reports FBI had identified as containing minimized Section 702-acquired United States person information, in 2013 FBI transitioned much of its dissemination from FBI Headquarters to FBI field offices. NSD is conducting oversight reviews of FBI field offices use of these disseminations, but because every field office is not reviewed every six months, NSD no longer has comprehensive numbers on the number of disseminations of United States person information made by FBI. FBI does, however, report comparable information on an annual basis to Congress and the FISC pursuant to 50 U.S.C. §1881a(l)(3)(i).

Ummm. We know that the FBI's numbers on NSLs are bullshit — and FBI doesn't much care. And when asked about those inaccuracies, FBI told DOJ's IG,

> [T]he FBI told the OIG that while 100 percent accuracy can be a helpful goal, attempting to obtain 100 percent accuracy in the NSL subsystem would create an undue burden without providing corresponding benefits. The FBI also stated that it has taken steps to minimize error to the greatest extent possible.

I've even asked ODNI about FBI's funny NSL numbers, twice, and gotten this response:

> ¯_(□)_/¯

So we already know that the FBI's legally mandated reports to Congress on NSL numbers are bogus. Now we learn that FBI has devolved its 702 work to field offices which has led to the discontinuation of one of the key oversight mechanisms on their counting process: an outside check.

That seems like a potentially big oversight loophole.

WEDNESDAY: IF I HAD A HEART

> *Crushed and filled with all I found*
> *Underneath and inside*
> *Just to come around*
> *More, give me more, give me more*
>
> — excerpt, If I Had a Heart by Fever Ray

Today's featured single is from Fever Ray's eponymous debut album 'Fever Ray', the stage name for Swedish singer, songwriter and record producer Karin Elisabeth Dreijer Andersson. If her work sounds familiar, it may be that she and her brother Olof Dreijer also performed as The Knife. Karin's work is reminiscent of Lykke Li's and Bjork's electronic/ambient works, redolent with dark rhythms and layers of deep and high-pitched vocals – very Nordic feminine.

Fever Ray has been very popular with television programmers; the cut featured here is the theme song for History Channel's Vikings series. It's also been used in AMC's Breaking Bad and WB's The Following. Other songs by Karin as Fever Ray including Keep the Streets Empty for Me have been used by CBS' Person of Interest and Canadian TV's Heartbeats as well as a number of films. I'm looking forward to her next work, wondering if it will be just as popular TV and film industry.

Fossil feud

- TransCanada approval hearing delayed due to protests (Reuters) – Not just U.S. and Native Americans protesting oil pipelines right now; Canada's National Energy Board deferred this week's hearings due to security concerns (they say). The board is scheduled to meet again in early October about the planned pipeline from Alberta to Canada's east coast. There may be more than security concerns holding up these hearings, though…
- Big projects losing favor

with Big Oil (WaPo-Bloomberg) – The ROI on big projects may be negative in some cases, which doesn't service massive debt Big Oil companies have incurred. They're looking at faster turnaround projects like shale oil projects – except that these quick-hit projects have poorly assessed externalities which will come back and bite Big Oil over the long run, not to mention the little problem of fracking's break-even point at $65/barrel.

- Big Insurance wants G20 to stop funding Big Fossil Fuel (Guardian) – Deadline the biggest insurers set is 2020; by then, Big Insurance wants the G20 nations to stop subsidizing and financing fossil fuels including Big Oil because subsidies and preferential financing skew the true cost of fossil fuels (hello, externalities).
- Standing Rock Sioux continue their protest against the North Dakota Access Pipeline (Guardian) – Video of the protest at that link. Calls to the White House supporting the Sioux against

the DAPL are solicited. Wonder if anybody's pointing out fracked shale oil is a losing proposition?

Zika-de-doo-dah

- Adult mosquitoes can transmit Zika to their offspring (American Journal of Tropical Medicine and Hygiene) – Study looked at infected *Aedes aegypti* and *albopictus* mosquitoes and found the virus in subsequent larva. My only beef with this study is that *Culex* species were not also studied; they aren't efficient carriers of Zika, but they do carry other flavivirus well and there are too many cases with unexplained transmission which could have been caused by infected *Culex*. Clearly need to do more about pre-hatch mosquito control regardless of species.
- Three drugs show promise in halting Zika damage in humans (Johns Hopkins Univerity Hub) – Important to note some of the same researchers who demonstrated Zika caused damage in mice brain models earlier this year have now rapidly

screened existing drugs to test against mice brain models. The drugs include an anti-liver damage medication (emricasan), an anti-parasitic (niclosamide), and an experimental antivirus drug. The limitation of this research is that it can't tell how the drugs act across placenta to fetus and whether they will work as well and safely once through the placenta on fetuses. More research (and funding!) is needed.

- Contraception no big deal, says stupid old white male GOP senator's staffer (Rewire) – Right. If only McConnell and his staff could experience the panic of being poor and at risk of Zika. Not everybody in Puerto Rico has ready access to the "limited number of public health departments, hospitals, and Medicaid Managed Care clinics," let alone other states like Texas which has such awful women's reproductive care in terms of access and funding the maternal mortality rate has doubled in two years, up 27%. Pro-life, my ass. By the way, this lack of access

> to contraception affects men, too, who may unknowingly be infected with Zika and tranmit it to their sexual partners.

Longread Must-read: Super court
If you haven't already done so, you need to read this investigative report by Chris Hamby at BuzzFeed. While it answers a lot of questions about the lack of perp walks, it spawns many more.

Hasta luego, compadres!

BREAKING: RUSSIANS CLAIM THEY'VE FOUND EXTRATERRESTRIAL LIFE TO TAMPER WITH OUR ELECTIONS

Russians secretly found what might be a sign of life coming from a star 95 light years away and people are in a tizzy.

> An international team of scientists from the Search for Extraterrestrial Intelligence (SETI) is investigating mysterious signal spikes emitting from a 6.3-billion-year-old star in the constellation Hercules—95 light years away from Earth. The implications are extraordinary and point to the possibility of a civilization far more advanced than our own.
>
> The unusual signal was originally detected on May 15, 2015, by the Russian Academy of Science-operated RATAN-600

> radio telescope in Zelenchukskaya, Russia, but was kept secret from the international community. Interstellar space reporter Paul Gilster broke the story after the researchers quietly circulated a paper announcing the detection of "a strong signal in the direction of HD164595."

It turns out, however, that the story got way overhyped.

> "No one is claiming that this is the work of an extraterrestrial civilization, but it is certainly worth further study," wrote Paul Glister, who covers deep space exploration on the website Centauri Dreams. He seems to have missed headlines like "Alien Hunters Spot Freaky Radio Signal Coming From Nearby Star," "Is Earth Being Contacted by ALIENS? Mystery Radio Signals Come From a Sun-like Star" and "SETI Investigating Mysterious, Extraterrestrial Signal From Deep Space Star System."
>
> [snip]
>
> "God knows who or what broadcasts at 11 GHz, and it would not be out of the question that some sort of bursting communication is done between ground stations and satellites," he told Ars Technica, explaining that the signal was observed in the radio spectrum used by the military. "I would follow it if I were the astronomers, but I would also not hype the fact that it may be at SETI signal given the significant chance it could be something military."
>
> In other words, there's a good chance the signal is the product of terrestrial activity rather than a missive crafted by extraterrestrial life on a distant exoplanet. For those who prefer a

> different outcome, there are plenty of movies that can offer more thrilling narratives.

So in the spirit of the silly season that our election has become, I'm going to go one better, taking the word "Russia" and some very thin evidence and declare this an election year plot. Everything *else* that has thin evidence and the word Russia is an election year plot, after all.

Consider the latest panic, caused by someone leaking Michael Isikoff an FBI alert on two attacks on voter files that took place this summer. Isikoff wasted no time in finding a cyber contractor willing to sow panic about Russians stealing the election.

> The FBI has uncovered evidence that foreign hackers penetrated two state election databases in recent weeks, prompting the bureau to warn election officials across the country to take new steps to enhance the security of their computer systems, according to federal and state law enforcement officials.
>
> The FBI warning, contained in a "flash" alert from the FBI's Cyber Division, a copy of which was obtained by Yahoo News, comes amid heightened concerns among U.S. intelligence officials about the possibility of cyberintrusions, potentially by Russian state-sponsored hackers, aimed at disrupting the November elections.
>
> [snip]
>
> "This is a big deal," said Rich Barger, chief intelligence officer for ThreatConnect, a cybersecurity firm, who reviewed the FBI alert at the request of Yahoo News. "Two state election boards have been popped, and data has been taken. This certainly should be concerning to the common American voter."

> Barger noted that one of the IP addresses listed in the FBI alert has surfaced before in Russian criminal underground hacker forums. He also said the method of attack on one of the state election systems — including the types of tools used by the hackers to scan for vulnerabilities and exploit them — appears to resemble methods used in other suspected Russian state-sponsored cyberattacks, including one just this month on the World Anti-Doping Agency.

Ellen Nakashima claimed the FBI had stated "Russians" were behind the attack and then talked about how Russia (rather than journalists overhyping the story) might raise questions about the integrity of our elections.

> Hackers targeted voter registration systems in Illinois and Arizona, and the FBI alerted Arizona officials in June that Russians were behind the assault on the election system in that state.
>
> The bureau described the threat as "credible" and significant, "an eight on a scale of one to 10," Matt Roberts, a spokesman for Arizona Secretary of State Michele Reagan (R), said Monday. As a result, Reagan shut down the state's voter registration system for nearly a week.
>
> It turned out that the hackers had not compromised the state system or even any county system. They had, however, stolen the username and password of a single election official in Gila County.
>
> Roberts said FBI investigators did not specify whether the hackers were criminals or employed by the Russian government.
>
> [snip]
>
> Until now, countries such as Russia and

> China have shown little interest in voting systems in the United States. But experts said that if a foreign government gained the ability to tamper with voter data — for instance by deleting registration records — such a hack could cast doubt on the legitimacy of U.S. elections.

She also cites the same Barger fellow that Isikoff did who might make a buck off sowing fear.

Then Politico quoted an FBI guy and someone who works with state election officials (who are not on the normal circulation lists for these alerts) stating that an alert of a kind that often goes to other recipients but which because we've recently decided election systems are critical infrastructure is now going to election officials is unprecedented.

> But some cyber experts said the FBI's alert, first revealed by Yahoo News on Monday, could be a sign that investigators are worried that foreign actors are attempting a wide-scale digital onslaught.
>
> A former lead agent in the FBI's Cyber Division said the hackers' use of a particular attack tool and the level of the FBI's alert "more than likely means nation-state attackers." The alert was coded "Amber," designating messages with sensitive information that "should not be widely distributed and should not be made public," the ex-official said.
>
> One person who works with state election officials called the FBI's memo "completely unprecedented."
>
> "There's never been an alert like that before that we know of," said the person, who requested anonymity to discuss sensitive intergovernmental conversations.

> Multiple former officials and security researchers said the cyberattacks on Arizona's and Illinois' voter databases could be part of a suspected Russian attempt to meddle in the U.S. election, a campaign that has already included successful intrusions at major Democratic Party organizations and the selective leaking of documents embarrassing to Democrats. Hillary Clinton's campaign has alleged that the digital attacks on her party are an effort by Russian President Vladimir Putin's regime to sway the election to GOP nominee Donald Trump. Moscow has denied any involvement.

Then David Sanger used a logically flawed Harry Reid letter calling for an investigation to sow more panic about the election (question: why is publishing accurate DNC documents considered "propaganda"?).

It turns out the evidence from the voting records hacks in the FBI alert suggests the hacks involved common tools that could have been deployed by anyone, and the Russian services were just one of several included in the hack.

> Those clued-in to the incidents already knew that SQL Injection was the likely cause of attack, as anyone familiar with the process could read between the lines when it came to the public statements.
>
> The notion that attackers would use public VPS / VPN providers is also a common trick, so the actual identity of the attacker remains a mystery. Likewise, the use of common SQL Injection scanners isn't a big shock either.
>
> The interesting takeaway in all of this is that a somewhat sensitive memo was leaked to the press. The source of the leak remains unknown, but flash memos

> coded to any severity other than Green rarely wind-up in the public eye. Doing so almost certainly sees access to such information revoked in the future.
>
> And yet, there is nothing overly sensitive about the IOCs contained in this memo. The public was already aware of the attacks, and those in the industry were certain that something like SQL Injection was a possible factor. All this does is prove their hunches correct.
>
> As for the attribution, that's mostly fluff and hype, often used to push an agenda. Those working in the trenches rarely care about the ***Who***, they're more interested in***What*** and ***How***, so they can fix things and get the business back to operational status.

And Motherboard notes that stealing voter data is sort of common.

> On Monday, Yahoo reported the FBI had uncovered evidence that foreign hackers had breached two US state election databases earlier this month. The article, based on a document the FBI distributed to concerned parties, was heavily framed around other recent hacks which have generally been attributed to Russia, including the Democratic National Committee email dump.
>
> The thing is, voter records are not some extra-special commodity that only elite, nation-sponsored hackers can get hold of. Instead, ordinary cybercriminals trade this sort of data, and some states make it pretty easy to obtain voter data through legal means anyway.
>
> In December of last year, CSO Online reported that a database of some 191 million US voter records had been exposed online. They weren't grabbed

> through hacking, per se: the dump was available to anyone who knew where to look, or was happy to just cycle through open databases sitting on the internet (which, incidentally, common cybercriminals are).

In other words, by all appearances there is no evidence to specifically tie these hacks even to Russian criminals, much less the Russian state. But the prior panic about the DNC hack led to a lower trigger for alerts on a specific kind of target, voter rolls, which in turn has fed the panic such that most news outlets have some kind of story suggesting this is a Russian plot to steal our election (by stealing 200K voter files?). It's like finding Russian life on Mars based on the shadows you see in the sand.

It's not the Russians who are raising questions about the voting integrity — beyond questions that have persistently been raised for 15 years which have already *justifiably* lowered confidence in our voting system. It is shitty reporting.

So I'm going to join in. These ETs 95 light years away? I'm positive they want to steal our election.

MONDAY: A DIFFERENT ARK

[*Caution: some content in this video is NSFW*]
Today's Monday Movie is a short film by Patrick Cederberg published three years ago. This short reflects the love life of a youth whose age is close to that of my two kids. A few things have changed in terms of technology used — I don't think either Facebook or Chatroulette is as popular now with high school and college students as it was, but the speed of internet-

mediated relationships is the same. It's dizzying to keep up with kids who are drowning in information about everything including their loved ones.

Their use of social media to monitor each other's commitment is particularly frightening; it's too easy to misinterpret content and make a snap decision as this movie shows so well. Just as scary is the ease with which one may violate the privacy of another and simply move on.

Imagine if this youngster Noah had to make a snap decision about someone with whom they weren't emotionally engaged. Imagine them using their lifetime of video gaming and that same shallow, too-rapid decision-making process while piloting a drone.

Boom.

Goodness knows real adults with much more life experience demonstrate bizarre and repeated lapses in judgment using technology. Why should we task youths fresh out of high school and little education in ethics and philosophy with using technology like remote surveillance and weaponized drones?

Speaking of drones, here's an interview with GWU's Hugh Gusterson on drone warfare including his recommendations on five of books about drones.

A, B, C, D, USB…

- USBKiller no longer just a concept (Mashable) –$56 will buy you a USB device which can kill nearly any laptop with a burst of electricity. The only devices known to be immune: those without USB ports. The manufacturer calls this device a "testing device." Apparently the

score is Pass/Fail and mostly Fail.

- Malware USBee jumps air-gapped computers (Ars Technica) – Same researchers at Israel's Ben Gurion University who've been working on the potential to hack air-gapped computers have now written software using a USB device to obtain information from them.
- Hydropower charger for USB devices available in 2017 (Digital Trends) – Huh. If I'm going to do a lot of off-grid camping, I guess I should consider chipping into the Kickstarter for this device which charges a built-in 6,400mAh battery. Takes 4.5 hours to charge, though – either need a steady stream of water, or that's a lot of canoe paddling.

Hackety-hack, don't walk back

- Arizona and Illinois state elections systems breached (Reuters) – An anonymous official indicated the FBI was looking for evidence other states may also have been breached. The two states experienced different levels of breaches – 200K

voters' personal data had been downloaded from Illinois, while a single state employee's computer had been compromised with malware in Arizona, according to Reuters' report. A report by CSO Online explains the breaches as outlined in an leaked FBI memo in greater detail; the attacks may have employed a commonly-used website vulnerability testing application to identify weak spots in the states' systems. Arizona will hold its primary election tomorrow, August 30.

- Now-defunct Australian satellite communications provider NewSat lousy with cyber holes (Australian Broadcasting Corp) – ABC's report said Australia's trade commission and Defence Science Technology Group have been attacked frequently, but the worst target was NewSat. The breaches required a complete replacement of NewSat's network at a time when it was struggling with profitability during the ramp-up to launch the Lockheed Martin Jabiru-1 Ka-

band satellite. China was named as a likely suspect due to the level of skill and organization required for the numerous breaches as well as economic interest. ABC's Four Corners investigative reporting program also covered this topic – worth watching for the entertaining quotes by former CIA Director Michael Hayden and computer security consultant/hacker Kevin Mitnick in the same video.

- Opera software users should reset passwords due to possible breach (Threatpost) – Thought users' passwords were encrypted or hashed, the browser manufacturer still asks users to reset passwords used to sync their Opera accounts as the sync system "showed signs of an attack." Norwegian company Opera Software has been sold recently to a Chinese group though the sale may not yet have closed.

That's a wrap for now, catch you tomorrow! Don't forget your bug spray!

THURSDAY: ONLY YOU

Sometimes when I go exploring for music I find something I like but it's a complete mystery how it came to be. I can't tell you much of anything about this artist – only that he's German, he's repped by a company in the Netherlands, and his genre is house/electronica. And that's it, apart from the fact he's got more tracks you can listen to on SoundCloud. My favorites so far are this faintly retro piece embedded here (on SoundCloud at Only You) and Fade – both make fairly mellow listening. His more popular works are a little more aggressive, like Gunshots and HWAH.

Caught a late summer bug, not firing on all cylinders. Here's some assorted odds and ends that caught my eye between much-needed naps.

- Infosec firm approached investment firm to play short on buggy medical devices (Bloomberg) – Jeebus. Bloomberg calls this "highly unorthodox," but it's just grossly unethical. Why didn't this bunch of hackers at MedSec go to the FDA and the SEC? This is a shakedown where they get the market to pay them first instead of ensuring patients are protected and shareholders of St. Jude medical device manufacturer's stock are appropriately informed. I call bullshit here – they're trying to game the system for profit and don't give a

shit about the patients at risk. You know when the maximum payout would be? When patient deaths occurred and were reported to the media.

- Apple iPhone users, update your devices to iOS 9.3.5 stat: serious malware designed to spy and gain control of iPhone found (Motherboard) – Hey look, a backdoor applied after the fact by a "ghost" government spyware company. The malware has been around since iPhone 5/iOS 7; it could take control of an iPhone and allow a remote jailbreak of the device. Interesting this Israeli spyware firm received a big chunk of cash from U.S. investor(s).
- Apple filed for patent on unauthorized user biometric data collection system (AppleInsider) – If an "unauthorized user" (read: thief) uses an iPhone equipped with this technology, the device could capture a photo and fingerprint of the user for use by law enforcement. Not exactly rocket science to understand how this might be used by law enforcement

remotely to assure a particular contact (read: target) is in possession of an iPhone, either. Keep an eye on this stuff.

- India-France submarine construction program hacked (NDTV) – The Indian Navy contracted construction of (6) Scorpene-class submarines from French shipbuilder DCNS. Tens of thousands of pages of information from this classified project were leaked; the source of the documents appears to be DCNS, not India. The French government as well as India is investigating the hack, which is believed to be a casualty in "economic war."
- Hacking of Ghostbusters' star Leslie Jones under investigation (Guardian) – Jones' website and iCloud accounts were breached; initial reports indicated the FBI was investigating the matter, but this report says Homeland Security is handlng the case. Does this mean an overseas attacker has already been identified?
- Taiwanese White hat hacker and open government activist named to digital policy role

(HKFP) – Audrey Tang, programmer and consultant for Apple, will shift gears from private to public sector now that she's been appointed an executive councillor for digital policy by Taiwan. Tang has been part of the Sunflower Student Movement which has demanded greater transparency and accountability on Cross-Strait Service Trade Agreement with China while resisting Chinese reunification.

- Oops! Recent Google Apps outage caused by…Google? (Google Cloud) – Change management boo-boo borked an update; apparently engineers working on an App Engine update didn't know software updates on routers was in progress while they performed some maintenance. Not good.
- Gyroscope made of tiny atomic chamber could replace GPS navigation (NIST.gov) – A miniature cloud of atoms held in suspension between two states of energy could be used as a highly accurate mini-gyroscope. National Institute of Standards and

Technology has been working a mini-gyro for years to provide alternate navigation in case GPS is hacked or jammed.

- Tim Berners-Lee wants to decentralize the internet (Digital Trends) – The internet has centralized into corporate-owned silos of storage and activities like Facebook, Google and eBay. Berners-Lee, who is responsible for the development of browsing hyperlinked documents over a network, wants the internet to be spread out again and your data in your own control.

That's enough to chew on for now. Hope to check in Friday if I shake off this bug.

TAKEDOWNS OF SHADOW BROKERS FILES AFFIRM FILES AS STOLEN

I've been wondering something.

Almost immediately after the Shadow Brokers posted their Equation Group files, GitHub, Reddit, and Tumblr took down the postings of the actual files. In retrospect, it reminded me of

the way Wikileaks was booted off PayPal in 2010 for, effectively, publishing files.

So I sent email to the three outlets asking on what basis they were taken down. GitHub offered the clearest reason. In refreshingly clear language, its official statement said,

> Per our Terms of Service (section A8), we do not allow the auction or sale of stolen property on GitHub. As such, we have removed the repository in question.

Mind you, A8 prohibits illegal purpose, not the auction of stolen property:

> You may not use the Service for any illegal or unauthorized purpose. You must not, in the use of the Service, violate any laws in your jurisdiction (including but not limited to copyright or trademark laws).

Moreover, at least in its Pastebin explanation, Shadow Brokers were ambiguous about how they obtained the files.

> How much you pay for enemies cyber weapons? Not malware you find in networks. Both sides, RAT + LP, full state sponsor tool set? *We find* cyber weapons made by creators of stuxnet, duqu, flame. Kaspersky calls Equation Group. We follow Equation Group traffic. *We find Equation Group source range*. *We hack Equation Group. We find many many Equation Group cyber weapons*. You see pictures. We give you some Equation Group files free, you see. This is good proof no? You enjoy!!! You break many things. You find many intrusions. You write many words. But not all, we are auction the best files.

They state they “found” the files, or at least traces of the files, and only say they “hacked”

to obtain them to get to the latest stage. If they (in the Russian theory of the files) were "found" on someone's own system, does that count as "stealing" property?

Tumblr wasn't quite as clear as GitHub. They said,

> Tumblr is a global platform for creativity and self-expression, but we have drawn lines around a few narrowly defined but deeply important categories of content and behavior, as outlined in our Community Guidelines. The account in question was found to be in violation of these policies and was removed.

But it's not actually clear what part of their user guidelines Shadow Brokers violated. They've got a rule against illegal behavior.

> - ***Unlawful Uses or Content.*** *Don't use Tumblr to conduct illegal behavior, like fraud or phishing. That should be pretty obvious to you, a decent human being.*

I guess the sale of stolen property is itself illegal, but that goes back to the whole issue of Shadow Brokers' lack of clarity of how they got what they got. Their property specific guidelines require someone to file a notice.

> Intellectual property is a tricky issue, so now is as good a time as any to explain some aspects of the process we use for handling copyright and trademark complaints. We respond to notices of alleged copyright infringement as per our Terms of Service and the Digital Millennium Copyright Act; please see our

> DMCA notification form to file a copyright claim online. Please note that we require a valid DMCA notice before removing content. Parties asserting a trademark infringement claim should identify the allegedly infringing work and the legal basis for their claim, and include the registration and/or application number(s) pertaining to their trademark. Each claim is reviewed by a trained member of our Trust and Safety team.
>
> If we remove material in response to a copyright or trademark claim, the user who posted the allegedly infringing material will be provided with information from the complainant's notice (like identification of the rightsholder and the allegedly infringed work) so they can determine the basis of the claim.

The tech companies might claim copyright violations here (or perhaps CFAA violations?), but the files came down long before anyone had publicly IDed them as the victims. So the only "owner" here would be the NSA. Did they call Tumblr AKA Verizon AKA a close intelligence partner of the NSA?

Finally, Shadow Brokers might be in violation of Tumblr's unauthorized contests.

> - ***Unauthorized Contests, Sweepstakes, or Giveaways.*** *Please follow our guidelines for contests, sweepstakes, and giveaways.*

The guidelines say you can link to whackjob contest (which this is) elsewhere, but

you do have to make certain disclosures on Tumblr itself.

One more thing about Tumblr, though. It claims it will give notice to a user before suspending their content.

Finally, there's Reddit, which blew off my request altogether. Why would they take down Shadow Brokers, given the range of toxic shit they permit to be posted?

They do prohibit illegal content, which they describe as,

> Content may violate the law if it includes, but is not limited to:
>
> - *copyright or trademark infringement*
> - *illegal sexual content*

Again, GitHub's explanation of this as selling stolen property might fit this description more closely than copyright infringement, at least of anyone who would have complained early enough to have gotten the files taken down.

The more interesting thing about Reddit is they claim they'll go through an escalating series of warning before taking down content, which pretty clearly did not happen here.

> We have a variety of ways of enforcing our rules, including, but not limited to
>
> - *Asking you nicely to knock it off*
> - *Asking you less nicely*
> - *Temporary or permanent suspension of accounts*
> - *Removal of privileges from, or adding restrictions to, accounts*

> - *Adding restrictions to Reddit communities, such as adding NSFW tags or Quarantining*
> - *Removal of content*
> - *Banning of Reddit communities*

Now, don't get me wrong. These are dangerous files, and I can understand why social media companies would want to close the barn door on the raging wild horses that once were in their stable.

But underlying it all appears to be a notion of property that I'm a bit troubled by. Even if Shadow Brokers stole these files from NSA servers — something not at all in evidence — they effectively stole NSA's own tools to break the law. But if these sites are treating the exploits themselves as stolen property, than so would be all the journalism writing about it.

Finally, there's the question of how these all came down so quickly. Almost as if someone called and reported their property stolen.

THE TWO TALES OF RUSSIA HACKING NYT

Yesterday, CNN posted this "first on CNN" story:

> Hackers thought to be working for Russian intelligence have carried out a series of cyber breaches targeting reporters at The New York Times and other US news organizations, according to US officials briefed on the matter.
>
> *The intrusions, detected in*

> *recent months, are under investigation by the FBI and other US security agencies. Investigators so far believe that Russian intelligence is likely behind the attacks and that Russian hackers are targeting news organizations as part of a broader series of hacks that also have focused on Democratic Party organizations, the officials said.*

Here's what the NYT's own account of the hacking (attempt) is:

> The New York Times's Moscow bureau was the target of an attempted cyberattack this month. But so far, there is no evidence that the hackers, believed to be Russian, were successful.
>
> "We are constantly monitoring our systems with the latest available intelligence and tools," said Eileen Murphy, a spokeswoman for The Times. "We have seen no evidence that any of our internal systems, including our systems in the Moscow bureau, have been breached or compromised."
>
> [snip]
>
> The New York Times's Moscow bureau was the target of an attempted cyberattack this month. But so far, there is no evidence that the hackers, believed to be Russian, were successful.
>
> "We are constantly monitoring our systems with the latest available intelligence and tools," said Eileen Murphy, a spokeswoman for The Times. "We have seen no evidence that any of our

> internal systems, including our systems in the Moscow bureau, have been breached or compromised."

So CNN tells an alarming story about specific reporters being targeted that fits into a larger narrative, citing both the FBI (in which Evan Perez has very good sources) and "other US security agencies," which presumably means the NSA. NYT tells an entirely different story, stating that an attack on its bureau in Russia was targeted unsuccessfully, relying solely on official sources as the FBI. One wonders why the NYT story required Nicole Perloth *and* David Sanger, and also why David Sanger didn't cite any of his extensive sources at NSA, where these allegations appear to derive.

It's quite possible both of these stories are misleading. But they do raise questions about why the spooks want to sensationalize these Russian hacks while NYT chooses to downplay them.