THE MIAMI COLLAPSE [UPDATED!]

The Miami collapse is beyond disturbing, but what else is there to come?

HAL MARTIN SENTENCING LEAVES ALL QUESTIONS UNANSWERED

Hal Martin’s sentencing yesterday offers no further explanation for the Shadow Brokers releases.

ON THE CURIOUS TIMING OF DANIEL EVERETTE HALE’S ARREST

It’s not surprising the government indicted Daniel Everette Hale as the Intercept’s suspected Drone Wars source. It’s surprising they waited five years.

CONFIRMED: LISTENING

TO WHISTLEBLOWER JOHN REIDY COULD HAVE SAVED THE LIVES OF NUMEROUS CIA ASSETS

Yahoo confirms something I've suspect for some time: the communications vulnerability that allowed China to roll up the CIA's network of spies is the same vulnerability John Reidy first started warning about in 2007.

SENATE INTELLIGENCE COMMITTEE DOESN'T THINK THE INTELLIGENCE COMMUNITY INSPECTOR GENERAL DOES ENOUGH ALL-IC OVERSIGHT

Along with the unclassified sensible policy in the Intel Authorization this year (and the stupid WikiLeaks one), it appears the Senate Intelligence Committee is trying to make the Intelligence Community Inspector General more functional, which is a good thing.

THREE THINGS: BAD, WORSE, AND JUST DEAL ALREADY

Not so artistic deal on air craft; sketchy deal handing radioactive materials on our dime; and just freaking cut a deal already. This is an open thread.

DID CHINA AND RUSSIA REALLY NEED OUR HELP TARGETING SPOOK TECHIES?

LAT has a story describing what a slew of others — including me — have already laid out. The OPM hack will enable China to cross-reference a bunch of databases to target our spooks. Aside from laying all that out again (which is worthwhile, because not a lot of people are still not publicly discussing that), LAT notes Russia is doing the same.

But other than that (and some false claims the US doesn't do the same, including working with contractors and "criminal" hackers) and a review of the dubiously legal Junaid Hussain drone killing, LAT includes one piece of actual news.

> At least one clandestine network of American engineers and scientists who provide technical assistance to U.S. undercover operatives and agents overseas has been compromised as a result, according to two U.S. officials.

I would be unsurprised that China was rolling up actual HUMINT spies in China as a result of the

OPM breach (which would explain why we'd be doing the same in response, if that's what we're doing). But the LAT says China (and/or Russia) is targeting "engineers and scientists who provide technical assistance" to spooks — one step removed from the people recruiting Chinese (or Russian) nationals to share its country's secrets.

I find that description rather curious because of the way it resembles the complaint by CIA contractor whistleblower John Reidy in an appeal of a denial of a whistleblower complaint by CIA's Inspector General. (Marisa Taylor first reported on Reidy's case.) As I extrapolated from redactions some weeks ago, it looks like Reidy reported CIA's reporting system getting hacked at least as early as 2007, but the contractors whose system got (apparently) hacked got him fired and CIA suppressed his complaints, only to have the problem get worse in the following years until CIA finally started doing something about it — with incomplete information — starting in 2010.

> Reidy describes playing three roles in 2005: facilitating the dissemination of intelligence reporting to the Intelligence Community, identifying Human Intelligence (HUMINT) targets of interest for exploitation, and (because of resource shortages) handling the daily administrative functions of running a human asset. In the second of those three roles, he was "assigned the telecommunications and information operations account" (which is not surprising, because that's the kind of service SAIC provides to the intelligence community). In other words, he seems to have worked at the intersection of human assets and electronic reporting on those assets.
>
> Whatever role he played, he described what by 2010 had become a "catastrophic intelligence failure[]" in which

> "upwards of 70% of our operations had been compromised." The problem appears to have arisen because "the US communications infrastructure was under siege," which sounds like CIA may have gotten hacked. At least by 2007, he had warned that several of the CIA's operations had been compromised, with some sources stopping all communications suddenly and others providing reports that were clearly false, or "atmospherics" submitted as solid reporting to fluff reporting numbers. By 2011 the government had appointed a Task Force to deal with the problem he had identified years earlier, though some on that Task Force didn't even know how long the problem had existed or that Reidy had tried to alert the CIA and Congress to the problem.
>
> All that seems to point to the possibility that tech contractors had set up a reporting system that had been compromised by adversaries, a guess that is reinforced by his stated desire to bring a "*qui tam* lawsuit brought against CIA contractors for providing products whose maintenance and design are inherently flawed and yet they are still charging the government for the products." In his complaint, he describes Raytheon employees being reassigned, suggesting that contracting giant may be one of the culprits, but all three named contractors (SAIC, Raytheon, and Mantech) have had their lapses; remember that SAIC was the lead contractor that Thomas Drake and friends exposed.

Reidy's appeal makes it clear that one of the things that exacerbated this problem was overlapping jurisdiction, with a functional unit apparently taking over control from a geographic unit. While that in no way rules out China, it

sounded as much like the conflict between CIA's Middle East and Counterterrorism groups that has surfaced in other areas as anything else.

The reason I raise Reidy is because — whether or not the engineers targeted as described in the LAT story are the same as the ones Reidy seems to describe — Reidy's appeal suggests the problem he described *arose from contractor incompetence and cover-ups*.

I guess you could say the same about the OPM hack (though it was also OPM's incompetence). Except in the earlier case, you're talking far more significant intelligence contractors — including SAIC and Raytheon, who both do a lot of cybersecurity contracting on top of their intelligence contracting — and a years-long cover up with the assistance of the agency in question.

All while assets were being exposed, apparently because of insecure computer systems.

China's hacking is a real threat to the identities of those who recruit human sources (and therefore of the human sources themselves).

But if Reidy's complaint is true, then it's not clear how much work China really needs to do to compromise these identities.

THE DANGER OF SOMEONE CRITICIZING POLITICAL PORK LANDING ON THE CAPITOL LAWN

The WaPo has a good review of how postal service worker Doug Hughes managed to fly his gyrocopter onto the Capitol lawn without being spotted by

the Secret Service or other security forces.

But the best part of the story cites corporate sucklings Chuck Schumer and Ron Johnson expressing dismay that the security theater draping DC didn't prevent Hughes from landing a harmless aircraft on their lawn.

> On Capitol Hill, there was less concern Thursday about Hughes's message than how he delivered it — flying into the heart of the nation's capital and alighting on the Capitol lawn about 1:30 p.m. in what amounts to an airborne go-cart, powered by something like a lawn mower engine, and kept aloft by an overhead rotor and a small propeller.
>
> "How did it happen?" Sen. Charles E. Schumer (D-N.Y.) wondered aloud. "How did the helicopter get through? Why weren't there alarm bells that went off? Why wasn't it intercepted? Did we know about it? How far from the Capitol grounds did we know?"
>
> Schumer, the Senate's third-ranking Democrat, added: "Just saying it's a little helicopter, or it's one person, or it was harmless, does not answer these questions. And we need to know what happened."
>
> Sen. Ron Johnson (R-Wis.), chairman of the Homeland Security and Governmental Affairs Committee, said in a statement: "I am deeply concerned that someone has the ability to fly for over an hour through the most restricted airspace in our country, past the White House, and land on the lawn of the Capitol."
>
> He added that he wants "a full accounting by all federal organizations entrusted with securing the United States from this and similar events." That Hughes was able to pull off the stunt, Johnson said, is "a reminder that the risk to America and Americans is

> ever present."

As Nancy Pelosi noted in comments yesterday (which were almost, but not quite, this shrill), there are reasons to want the Capitol to remain fairly open. And it is fairly open — easier to get into than an airport, for example. That makes it accessible to the thousands of local lobbying and school groups who want to see their Representatives' office.

But it also makes it permeable by lobbyists.

The big money lobbyists, of course, do far more damage to this country than a gyrocopter ever could, damage that Schumer and Johnson are enthusiastic participants in.

Which is sort of Hughes' point.

I expect more ironic symbolism from this event going forward, as a bunch of security-industry intoxicated Congressmen take as a lesson from this that they need to insulate themselves even more from the people warning about them insulating themselves form their constituents.

INTERNET CATS, WEAPONIZED: US DEFENSE CONTRACTOR CONSULTED ON TARGETED NETWORK INJECTION SURVEILLANCE FOR

COMMERCIAL SALES ABROAD

[photo: liebeslakritze via Flickr]

First, a caveat: I would not click on the links embedded in the story I'm recommending (I'm this || close to swearing off embedded links forever). I don't trust traffic to them not to be monitored or exploited.

But as Jeremy Scahill tweeted last evening, read this piece by WaPo's Barton Gellman on malicious code insertion. This news explains recent changes by Google to YouTube once it had been disclosed to the company that exploits could be embedded in video content as CitizenLab.org explains:

> "… the appliance exploits YouTube users by injecting malicious HTML-FLASH into the video stream. …"
> "… the user (watching a cute cat video) is represented by the laptop, and YouTube is represented by the server farm full of digital cats. You can observe our attacker using a network injection appliance and subverting the beloved pastime of watching cute animal

> videos on YouTube. …”

The questions this piece shake loose are Legion, but as just as numerous are the holes. Why holes? Because the answers are ugly and complex enough that one might struggle with them. Gellman’s done the best he can with nebulous material.

An interesting datapoint in the first graf of the story is timing — fall 2009.

You’ll recall that Google revealed the existence of a cyber attack code named Operation Aurora in January 2010, which Google said began in mid-December 2009.

You may also recall news of a large batch of cyber attacks in July of 2009 on South Korean targets.

The U.S. military had already experienced a massive uptick in cyber attacks in 1H2009, more than double the rate of the entire previous year.

And neatly sandwiched between these waves and events is a visit by a defense contractor CloudShield Technologies engineer from California, to Munich, Germany with British-owned Gamma Group.

Note the WaPo article contains no references whatsoever to zero day exploits, though Microsoft and Adobe are mentioned. Chinese-launched Operation Aurora made use of these in what appears to be an intelligence gathering effort. Yet reading the underlying report by CitizenLab.org upon which the WaPo article was based you’ll see “0-day” exploits have been involved. Probably just coincidence since zero day exploits have been problematic whether the originator is private hacker or state actor. But the likelihood Gamma Group was working on a non-state exploit for intelligence gathering intended for commercialization seems slim given the timeframe.

Plus the whole off-the-books bit — yeah, legal

commercialized products for global marketplace need only an NDA, not the covert slinking around. CloudShield engineer Eddy Deegan said,

> “Nothing came of the work I was involved in at the time,” he said. “I asked, and was assured that nothing illegal was undertaken. I have no further comment.”

Because Deegan could see the line item entry in Gamma Group’s books where it said PROJECT TERMINATED. At this point an emoji depicting the act of laughing one’s self to death would be appropriate.

This bit in WaPo really jogs a lot of questions:

> The computer exploitation industry markets itself to foreign government customers in muscular terms. One Gamma brochure made public by WikiLeaks described its malware injection system, called FinFly ISP, as a “strategic, countrywide” solution with nearly unlimited “scalability,” or capacity for expansion. Hacking Team, similarly, says it provides “effective, easy-to-use offensive technology to the worldwide law enforcement and intelligence communities.”
>
> In rare comments to the general public, the companies use the term “lawful intercept” to describe their products and say they do not sell to customers on U.S., European or U.N. black lists.
>
> “Our software is designed to be used and is used to target specific subjects of investigation,” said Eric Rabe, a U.S.-based spokesman for Hacking Team, in an extended e-mail interview. “It is not designed or used to collect data from a general population of a city or nation.”
>
> He declined to discuss details of the Citizen Lab report, which is based in part on internal company documents

> leaked to Marquis-Boire, but he appeared to acknowledge indirectly that the material was authentic.

You can drive a 40-foot dry van through the term "lawful intercept." This technology could be easily transferred to any another entity, especially since key parties are located overseas, ostensibly out of U.S. purview. How can we be expected to believe this is only being sold to the "good guys" when even the "good guys" are sketchy and worse these days? What's to say this technology isn't being used on U.S. citizens right now by multiple entities at any one time, and Deegan's allegedly terminated efforts were only a parallel alternative proof-of-concept for the injection tool deployed?

BENGH– BLACKWATER!

You should definitely read the James Risen story describing how the head of Blackwater's operations in Iraq threatened to kill an investigator into the company's practices in the period before the Nisour Square. It definitely confirms every concern that has been raised about mercenaries generally and Blackwater specifically.

But I want to look at the frame Risen gave the story, which I suspect few will read closely.

> His memo and other newly disclosed State Department documents make clear that the department was alerted to serious problems involving Blackwater and its government overseers before the Nisour Square shooting, which outraged Iraqis and deepened resentment over the United States' presence in the country.
>
> [snip]

> Condoleezza Rice, then the secretary of state, named a special panel to examine the Nisour Square episode and recommend reforms, but the panel never interviewed Mr. Richter or Mr. Thomas.
>
> Patrick Kennedy, the State Department official who led the special panel, told reporters on Oct. 23, 2007, that the panel had not found any communications from the embassy in Baghdad before the Nisour Square shooting that raised concerns about contractor conduct.
>
> "We interviewed a large number of individuals," Mr. Kennedy said. "We did not find any, I think, significant pattern of incidents that had not — that the embassy had suppressed in any way."

The reason this is coming out — aside from the fact the government is trying to try the Nisour Square killers again — is to show that contrary to what Patrick Kennedy said after having done a review of security practices in 2007, there had been a pattern of incidents, and they had been suppressed by the Embassy.

Now consider how that reflects on the GOP's second favorite scandal, Benghazi. Not only was Kennedy the key judge about the events leading up to that event (which is normal — he's been a key player in State for a very long time; I'm beginning to believe he's State's institutional defender in the same way David Margolis was at DOJ), but the question of security oversight is important there: Blue Mountain Group appears to have done its job inadequately (and there are some sketchy things about its contract and contractors).

Benghazi is actually not a bigger scandal than that State suppressed knowledge of Blackwater's problems. But there does seem to be continuity.