LINDSEY GRAHAM CALLS RAYMOND DAVIS AN "AGENT"

AFP has a report (notably picked up by Pakistan's Dawn) on the Senate's hand-wringing over whether we should tie aid to Pakistan to the release of Raymond Davis, the "consulate employee" who shot two alleged Pakistani spies. Here's what Lindsey Graham had to say:

> But Senator Lindsey Graham, the top Republican on Leahy's subcommittee, strongly warned against any rollback of assistance to Pakistan, citing the need for help in the war in Afghanistan and the hunt for suspected terrorists.
>
> "Our relationship's got to be bigger than this," Graham said.
>
> "This is a friction point, this is a troubling matter, it doesn't play well in Afghanistan. **We can't throw this agent over**, I don't know all the details, but we cannot define the relationship based on one incident because it is too important at a time when we're making progress in Afghanistan," he said. [my emphasis]

Lindsey, Lindsey, Lindsey! Under Ben Cardin's proposed law criminalizing leaks (and, frankly, under existing law), you could go to jail for such honesty. Good thing you have immunity as a member of Congress.

Though in the spirit of Bob Novak—who claimed to be thinking of a political professional running congressional campaigns in Dick Cheney's state when he called Valerie Plame an "operative"—I suppose Graham could claim he just thought Davis serves some kind of service employee at the consulate, one of the "agents" that help with visas or some such nonsense.

Not that that'll help the tensions over this incident in Pakistan at all.

POLITICAL GIVING AND WILLINGNESS TO CAVE TO LAW ENFORCEMENT

When Jason Leopold linked to a WSJ report titled, "Obama breaks bread with Silicon Valley execs," I quipped, "otherwise known as, Obama breaks bread w/our partners in domestic surveillance." After all, some of the companies represented—Google, Facebook, Yahoo—are among those that have been willingly sharing customer data with federal law enforcement officials.

Which is why I found this Sunlight report listing lobbying and political donations of the companies so interesting.

	Lobbying (2010)	Contributions to Obama (2008)
Apple	$1,610,000.00	$92,141.00
Google	$5,160,000.00	$803,436.00
Facebook	$351,390.00	$34,850.00
Yahoo	$2,230,000.00	$164,051.00
Cisco Systems	$2,010,000.00	$187,472.00
Twitter	$0.00	$750.00
Oracle	$4,850,000.00	$243,194.00
NetFlix	$130,000.00	$19,485.00
Stanford University	$370,000.00	$448,720.00
Genentech	$4,922,368.00	$97,761.00
Westly Group	$0.00	$0.00

Just one of the companies represented at the meeting, after all, has recently challenged the

government's order in its pursuit of WikiLeaks to turn over years of data on its users: Twitter. And the difference between Twitter's giving and the others' is stark.

Does Twitter have the independence to challenge the government WikiLeaks order because it hasn't asked or owed anyone anything, politically?

Mind you, there's probably an interim relationship in play here, as well. Those companies that invest a lot in politics also have issues—often regulatory, but sometimes even their own legal exposure—that they believe warrant big political investments. Which in turn gives the government some issue with which to bargain on.

Maybe this is all a coinkydink. And maybe having broken bread with Obama, Twitter will cave on further government orders.

But I do wonder whether there's a correlation between those telecommunication companies that try to buy political favors and those that offer federal law enforcement favors in return.

HUNTON & WILLIAMS LEFT FINGERPRINTS AT SEIU

Hunton & Williams, the law firm that solicited HBGary and two other security firms to spy on Chamber of Commerce opponents, has remained silent so far about its efforts.

But it hasn't covered its tracks. The SEIU reports that people from Hunton & Williams spent 20 hours last November—at the time when Themis was pitching H&W to use a JSOC approach to go after Chamber opponents—on the SEIU sites.

> Server logs and leaked emails reveal that employees at Hunton & Williams, the principal law firm of the U.S. Chamber of Commerce, spent 20 hours on SEIU websites last November while partners from the firm were working with private security firms on an illegal “dirty tricks” campaign aimed at undermining the credibility of the Chamber’s political opponents, including the Service Employees International Union (SEIU).

And of course SEIU is able to see precisely what H&W was looking at in that period: top H&W page views in 2010 include SEIU’s page on the Chamber and on big banks. People from H&W searched on individuals at SEIU as well as on SEIU’s organizing of protests outside of BoA’s General Counsel. They even searched on “hourly pay for SEIU organizers.” (Whatever that is, it’s less than Themis was going to charge for its paid trolls.)

No wonder H&W has been so quiet about their role in this campaign.

Update: This post has been edited for accuracy.

STUXNET: THE CURIOUS INCIDENT OF THE SECOND CERTIFICATE

“Is there any point to which you would wish to draw my attention?”

“To the curious incident of the dog in the night-time.”

“The dog did nothing in the night-time.”

“That was the curious incident,” remarked

Sherlock Holmes.

Arthur Conan Doyle (Silver Blaze)

[From ew: William Ockham, who knows a whole lot more about coding than I, shared some interesting thoughts with me about the Stuxnet virus. I asked him to share those thoughts it into a post. Thanks to him for doing so!]

The key to unraveling the mystery of Stuxnet is understanding the meaning of a seemingly purposeless act by the attackers behind the malware. Stuxnet was first reported on June 17, 2010 by VirusBlokAda, an anti-virus company in Belarus. On June 24, VirusBlokAda noticed that two of the Stuxnet components, Windows drivers named MrxCls.sys and MrxNet.sys, were signed using the digital signature from a certificate issued to Realtek Semiconductor. VirusBlokAda immediately notified Realtek and on July 16, VeriSign revoked the Realtek certificate. The very next day, a new Stuxnet driver named jmidebs.sys appeared, but this one was signed with a certificate from JMicron Technology. This new Stuxnet driver had been compiled on July 14. On July 22, five days after the new driver was first reported, VeriSign revoked the JMicron certificate.

The question I want to explore is **why** the attackers rolled out a new version of their driver signed with the second certificate. This is a key question because this is the one action that we know the attackers took deliberately after the malware became public. It's an action that they took at a time when there was a lot of information asymmetry in their favor. They knew exactly what they were up to and the rest of us had no clue. They knew that Stuxnet had been in the wild for more than a year, that it had already achieved its primary goal, and that it wasn't a direct threat to any of the computers it was infecting in July 2010. Rolling out the new driver incurred a substantial cost, and not just in monetary terms. Taking this action gave away a lot of information. Understanding why

they released a driver signed with a second certificate will help explain a lot of other curious things in the Stuxnet saga.

It’s easy to see why they signed their drivers the first time. Code signing is designed to prove that a piece of software comes from a known entity (using public key infrastructure) and that the software hasn’t been altered. A software developer obtains a digital certificate from a “trusted authority”. When the software is compiled, the certificate containing the developer’s unique private key is used to “sign” the code which attaches a hash to the software. When the code is executed, this hash can be used to verify with great certainty that the code was signed with that particular certificate and hasn’t changed since it was signed. Because drivers have very privileged access to the host operating system, the most recent releases of Microsoft Windows (Vista, Win7, Win2008, and Win2008 R2) won’t allow the silent installation of unsigned drivers. The Stuxnet attackers put a lot of effort into developing a completely silent infection process. Stuxnet checked which Windows version it was running on and which anti-virus software (if any) was running and tailored its infection process accordingly. The entire purpose of the Windows components of Stuxnet was to seek out installations of a specific industrial control system and infect that. To achieve that purpose, the Windows components were carefully designed to give infected users no sign that they were under attack.

The revocation of the first certificate by VeriSign didn’t change any of that. Windows will happily and silently install drivers with revoked signatures. Believe it or not, there are actually good reasons for Windows to install drivers with revoked signatures. For example, Realtek is an important manufacturer of various components for PCs. If Windows refused to install their drivers after the certificate was withdrawn, there would be a whole lot of unhappy customers.

The release of a Stuxnet driver signed with a new certificate was very curious for several reasons. As Symantec recently reported [link to large pdf], no one has recovered the delivery mechanism (the Trojan dropper, in antivirus lingo) for this driver. We don't actually know how the driver showed up on the two machines (one in Kazakhstan and one in Russia) where it was found on July 17, 2010. This is significant because the driver is compiled into the Trojan dropper as resource. Without a new dropper, there's no way for that version of the virus to have infected additional computers. And there is no evidence that I'm aware of that Stuxnet with the new driver ever spread to any other machines.

The release of the newly signed driver did exactly one thing: Increase publicity about Stuxnet. The inescapable conclusion is that the Stuxnet attackers wanted to make headlines in July 2010. As Holmes says in *Silver Blaze*, "one true inference invariably suggests others". From this one inference, we can begin to understand the most puzzling parts of the Stuxnet project. Who would publicize their secret cyber attack on an enemy? Why were there clues to the identity of the attackers left in the code? Why did the last version of Stuxnet use multiple 0-day exploits? Why did the attackers only take minimal steps to hide the true nature of the code? The answer to these questions is relatively simple. The Stuxnet project was never intended to stay secret forever. If it had been, there would never have been a new Stuxnet driver in July 2010. That driver helps put all the other pieces in context: the clues left inside the code ("myrtus", "guava", and using May 9, 1979 as a magic value); the aspects of the code that have led various experts to label Stuxnet as amateurish, lame, and low quality; even the leak campaign by the U.S. and Israeli governments to unofficially take credit for Stuxnet. Rather than being mistakes, these were elements of the larger Stuxnet project.

Stuxnet was more than a cyber attack. It was a

multi-pronged project. The design of the code supports the overall mission. The mission included a publicity campaign, or as the military and intelligence folks style it, a PSYchological OPeration (PSYOP). Unlike a typical malware attack, Stuxnet had (at least) two distinct phases. Phase 1 required a stealthy cyber attack against the Iranian nuclear program. Phase 2 required that the effects of that cyber attack become widely known while giving the perpetrators plausible deniability. That may seem a little strange at first, but if you put yourself in the shoes of the attackers, the strategy is more than plausible.

In fact, the attackers have explained it all. Take a look back at the story told in the New York Times article on January 15, 2011. According to the NYT, the Stuxnet project started as an alternative to an Israeli airstrike:

> Two years ago, when Israel still thought its only solution was a military one and approached Mr. Bush for the bunker-busting bombs and other equipment it believed it would need for an air attack, its officials told the White House that such a strike would set back Iran's programs by roughly three years. Its request was turned down.

Couple that statement with the reason the article appeared when it did:

> In recent days, American officials who spoke on the condition of anonymity have said in interviews that they believe Iran's setbacks have been underreported.

Imagine that you're an American policymaker who has to choose between launching a cyber attack and allowing a close ally to launch an actual military attack. If you choose the cyber attack option, how will anyone know that you've succeeded? If no one knows that you've

successfully delayed the Iranian nuclear program, you'll be vulnerable to right-wing attacks for not doing enough to stop Iran and the pressure to bomb-bomb-bomb of Iran will grow. There's another reason to publicize the attack. If you're a superpower who starts a cyber war, you have to realize that your country contains a lot of very soft targets. You would want to make a big splash with this malware so that your industrial base starts to take the cyber war seriously. So, from the very beginning, the project included planning for the inevitable discovery and understanding of the Stuxnet malware. Just like the spread of the malware itself, the psyop will be impossible to directly control, but easy enough to steer in the appropriate direction. The attackers likely didn't know it would be Symantec and Ralph Langner who would start to unravel the exact nature of the Stuxnet malware, but they knew someone would. And they knew they would be able to get the New York Times to print the story they wanted to get out (I'm not demeaning the work of the reporters on this story, but I would hope they realize that there is a reason they aren't being investigated for publishing a story about our efforts to undermine Iran's nuclear program and James Risen was).

CONFIRMED: OUR GOVERNMENT HAS CRIMINALIZED BEAUTY PRODUCTS

A year and a half ago, I warned that if you bought certain beauty supplies—hydrogen peroxide and acetone—you might be a terrorism suspect.

> I'm going to make a wildarsed guess and suggest that the Federal Government is

> doing a nationwide search to find out everyone who is buying large amounts of certain kinds of beauty products. And those people are likely now under investigation as potential terrorism suspects.

Shortly thereafter, John Kyl basically confirmed that the government had been tracking certain people buying hydrogen peroxide.

Yesterday, FBI Director Robert Mueller did so in even more explicit terms.

> Federal Bureau of Investigation Director Robert Mueller appeared to indicate for the first time Wednesday that his agency uses a provision of the PATRIOT Act to obtain information about purchases of hydrogren peroxide—a common household chemical hair bleach and antiseptic that can also be turned into an explosive.
>
> The comment in passing by Mueller during a Senate Intelligence Committee hearing was noteworthy because critics have suggested that the FBI is using a provision in the PATRIOT Act to conduct broad surveillance of sales of lawful products such as hydrogen peroxide and acetone.
>
> "It's been used over 380 times since 2001," Mueller said of the so-called business records provision, also known as Section 215. "It provides us the ability to get records other than telephone toll records, which we can get through another provision of the statutes. It allows us to get records such as Fedex or UPS records….**or records relating to the purchase of hydrogen peroxide**, or license records—records that we would get automatically with a grand jury subpoena on the criminal side, the [Section] 215 process allows us to get on the national security

> side.” (Emphasis original)

Emptywheel: where you read today about the civil liberties infringements your government will confirm years from now.

What Mueller didn’t confirm, but what we can pretty much conclude at this point, is that they’ve used the 215 provision to investigate as terrorists perfectly innocent (and possibly Muslim) purchasers of beauty supplies.

Recall how I first figured out the government was using Section 215 to track beauty supplies. After DiFi blabbed that they had used Section 215 in the Najibullah Zazi case, I examined the detention motion on Zazi to see what kind of evidence they used to justify refusing him bail. It included this:

> Evidence that “individuals associated with Zazi purchased unusual quantities of hydrogen and acetone products in July, August, and September 2009 from three different beauty supply stores in and around Aurora;” these purchases include:
>
> - *Person one: a one-gallon container of a product containing 20% hydrogen peroxide and an 8-oz bottle of acetone*
> - *Person two: an acetone product*
> - *Person three: 32-oz bottles of Ion Sensitive Scalp Developer three different times*

The federal government argued, in part, that

Zazi had to be denied bail because three people "associated with him" bought beauty supplies "in and around Aurora."

Last February, Zazi accepted a plea agreement and has been cooperating with investigators; the government has twice delayed his sentencing, suggesting he's still fully cooperating. Since that time, the only people arrested for participating in the actual plot—as opposed to obstructing justice by trying to hide the evidence of Zazi's bomb-making, with which both Zazi's father and uncle were charged—are in NY or Pakistan.

That is, it appears that Zazi had no accomplices "in and around Aurora."

That's particularly interesting given that Zazi is reported to have had few close ties in the Denver area. He only moved there in January 2009, 8 months before his arrest. And both his employer and the other worshipers at his mosque describe him as keeping to himself.

> Unlike most drivers at ABC, who drove eight- or nine-hour shifts, Zazi routinely worked 16-to-18-hour days, often putting in as many as 80 hours a week ferrying passengers to and from DIA. "He was a regular kind of guy, but he worked hard and he wanted money," says Hicham Semmaml, a Moroccan-born ABC driver. "I would have never suspected any of this."
>
> [snip]
>
> "He kept to himself pretty much, and he never gave any outward signs of being connected with anybody," Gross said.
>
> [snip]
>
> Zazi would turn up for afternoon prayers each Friday — Islam's holy day — parking the ABC van in the parking lot outside the sprawling brick complex with its black dome and narrow minaret. Other

> regular worshippers agreed that he never spoke to anyone and usually rushed off immediately once the service ended.

All the currently available evidence suggests that these three Zazi "associates" buying beauty supplies turned out to be completely innocent. That would mean that one of the reasons the government said Zazi should be held without bail (there were plenty of others) basically amounts to innocent people with some attenuated tie to Zazi buying beauty supplies.

But consider what their beauty supply purchase has exposed them to—particularly if the association involved amounts to membership in the same mosque as him. Their purchase of beauty supplies undoubtedly made them a target for further investigation, presumably FBI agents asking questions of their neighbors and employers, probably the use of other PATRIOT provisions to track their calls and emails, and possibly even a wiretap.

So these three people, because they worshiped at the same mosque as Zazi or drove an airport van but presumably in the absence of any evidence of actual friendship with him had their lives unpacked by our government because they bought a couple bottles of beauty supplies.

THEMIS APPLIES JSOC TECHNIQUES TO CITIZENS "EXTORTING" FROM CORPORATE CLIENTS

It was Berico Technologies' Deputy Director who sent out these documents adopting a military

targeting approach for responding to citizens engaging in free speech.

CALIFORNIA SUPREME COURT TO HEAR PERRY PROP 8 QUESTION

The breaking news out of the California Supreme Court is that they WILL entertain a full merits consideration of the question certified to them by the 9th Circuit in the Perry v. Schwarzenegger.

CURVEBALL: I LIED TO GET RID OF SADDAM

Almost eight years after he helped start a war, the Iraqi behind the US claim that Iraq had mobile weapons labs admitted in an interview with the Guardian that he lied. (h/t Hissypit)

> Rafid Ahmed Alwan al-Janabi, codenamed Curveball by German and American intelligence officials who dealt with his claims, has told the Guardian that he fabricated tales of mobile bioweapons trucks and clandestine factories in an attempt to bring down the Saddam Hussein regime, from which he had fled in 1995.

The article as a whole provides fascinating details of how the German intelligence, BND, service basically fed Curveball the details he'd need to fabricate his lies.

But I'm particularly interested in two new

details he reveals. First, BND and British intelligence met with Curveball's boss in mid-2000; the boss debunked Curveball's claims.

> Janabi claimed he was first exposed as a liar as early as mid-2000, when the BND travelled to a Gulf city, believed to be Dubai, to speak with his former boss at the Military Industries Commission in Iraq, Dr Bassil Latif.
>
> The Guardian has learned separately that British intelligence officials were at that meeting, investigating a claim made by Janabi that Latif's son, who was studying in Britain, was procuring weapons for Saddam.
>
> That claim was proven false, and Latif strongly denied Janabi's claim of mobile bioweapons trucks and another allegation that 12 people had died during an accident at a secret bioweapons facility in south-east Baghdad.
>
> The German officials returned to confront him with Latif's version. "He says, 'There are no trucks,' and I say, 'OK, when [Latif says] there no trucks then [there are none],'" Janabi recalled.

So this is yet another well-placed Iraqi who warned western intelligence that the WMD evidence that would eventually lead to war was baseless (one George Tenet and others haven't admitted in the past).

And Curveball describes how BND returned to his claims in 2002, then dropped it, then returned to it just before Colin Powell's Feruary 5, 2003 speech at the UN.

We've known the outlines of these details before. But it sure adds to the picture of the US dialing up the intelligence it needed — however flimsy — to start a war.

CHET UBER CONTACTED HBGARY BEFORE HE PUBLICIZED HIS ROLE IN TURNING IN BRADLEY MANNING

A reader found a very interesting email among the HBGary emails: Chet Uber emailed—after having tried to call—HBGary CEO Greg Hoglund on June 23, 2010.

> Sir,
>
>
>
> I would like to speak to Mr. Hoglund. My name is Chet Uber
> and I was given his name by common associates as someone I should speak with.
> The nature of our work is highly sensitive so no offense but I cannot explain
> the details of my call. I was given a URL and a phone number. I was not given
> his direct line and every time I try to get an attendant you phone system
> disconnects me. Would you please forward him this email to him. The links below
> are new and as much information as we have ever made public.
>

> >
>
> Sorry for the mystery but in my world we are careful about
>
> our actions and this is something interpreted as rudeness. I am being polite,
>
> so any cooperation you can provide is greatly appreciated.

Uber copies himself, Mark Rasch, George Johnson, and Mike Tomasiewicz, and sends links to two stories about Project Vigilant, which had been posted on the two proceeding days.

In response to the email, Hoglund asks Bob Slapnick to check Uber out with someone at DOD's CyberCrime Center.

Chet Uber, as you'll recall, is the guy who held a press conference at DefCon on August 1 to boast about his role in helping Adrian Lamo turn Bradley Manning in to authorities. Mark Rasch is the former DOJ cybercrimes prosecutor who claims to be Project Vigilant's General Counsel and who says he made key connections with the government on Manning.

Mind you, the multiple versions of Uber's story of his involvement in turning in Manning are inconsistent. At least a couple versions have Lamo calling Uber in June, after Manning had already been arrested.

So there are plenty of reasons to doubt the Lamo and Uber story. And security insiders have suggested the whole Project Vigilant story may be nothing more than a publicity stunt.

Furthermore, this email may be more of the same. Uber may have been doing no more than cold-calling Hoglund just as he was making a big publicity push capitalizing on the Manning arrest.

But consider this.

Lamo's conversations with Manning have always looked more like the coached questions of someone trying to elicit already-suspected details than the mutual boasting of two hackers. Because of that and because of the inconsistencies and flimsiness of the Project Vigilant story, PV all looked more like a cover story for why Lamo would narc out Bradley Manning than an accurate story. And Uber's email here and his DefCon press conference may well be publicity stunts. But then, that's what Aaron Barr's research on Anonymous was supposed to be: a widely publicized talk designed to bring new business. But a key part of the PV story was the claim that Adrian Lamo had volunteered with the group working on "adversary characterization."

> Uber says Lamo worked as a volunteer research associate for Project Vigilant for about a year on something called adversary characterization, which involved gathering information for a project on devising ways to attribute computer intrusions to individuals or groups. He helped define the roles, tools and methods intruders would use to conduct such attacks.

While it is described as more technical, that's not all that different from what Aaron Barr was doing with social media on Anonymous.

One more thing. Consider what DOJ has been doing since the time Lamo turned in Manning and now: asking social media providers for detailed information about a network of people associated with Wikileaks. That is, DOJ appears to have been doing with additional legal tools precisely what Barr was doing with public sources.

That's likely all a big coinkydink. But these security hackers all seem to love turning their freelance investigations into big publicity stunts.

OUR DOJ REFUSES TO SEND OFFICIALS TO JAIL – SCOTT BLOCH EDITION

The Obama Administration and Holder Justice Department were not willing to make misrepresentations and disingenuous arguments to cravenly insure that Executive Branch officials, including Scott Bloch, lying to Congress do not serve so much as a day in jail.