

TIMELINE: IS VOLKSWAGEN'S 'BUG' AN EU FEATURE? [UPDATED]



[photo: macwagen via Flickr]

Reports this last week that Volkswagen deployed “defeat devices” – software designed to cheat diesel passenger vehicle emissions controls tests – revealed more than an automobile manufacturing group run amok. One might suspect European Union’s emissions governance after looking at a timeline of events.

NOTE: This timeline is in progress and is subject to updating as new items are identified.
[Update 7:00 pm EDT – note added about translation, and note added to citation [4]]

– 1970 –

February 1970 – The Council of the European Communities issued the *Council Directive 70/156/EEC*, which established a mutual baseline for technical specifications of vehicles sold across the member states. This included 3.2.20. *Measures taken against air pollution.*

– 1992 –

July 1992 – The first standard for passenger vehicle emissions, Euro 1 through 6, is implemented. Level Euro 1 for new diesel-fueled vehicles limited emissions of carbon monoxide

(CO) to 2.72 grams per kilometer, with no initial limit on nitrous oxides (NOx) alone, but a combined limit of hydrocarbon+nitrous oxides (HC+NOx) at 0.97 g/km.

– 2004 – 2009 –

Dates Vary – Vehicle manufacturers phased in the remaining Euro 4 through 6 emissions standards.

19 October 2004 – European Environment Agency published a press release, Poor European test standards understate air pollution from cars, which summarized the problem:

Inadequate test standards are underestimating emissions of harmful air pollutants from new cars and evidence indicates that many diesel car owners are making things worse by modifying their engines to increase power, the European Environment Agency warned today.

No specific orders or directions were offered to resolve the problem with emissions test standards.

– 2007 –

(*Month TBD*) – Volkswagen subsidiary Audi launched its “Truth in Engineering” ad campaign. This tagline remains in use to present.

– 2008 –

(*Month TBD*) – VW announced its “Clean Diesel” (TDI model) technology, and began selling it in 4-cylinder diesel Jetta, Beetle, Audi A3, and Golf cars to the US market.

(*Month TBD*) – *Green Car Journal* named VW’s 2009 Jetta TDI “Green Car of the Year.”

– 2009 –

September 2009 – European emission standard Euro 5a for diesel passenger vehicles enacted, limiting CO to 0.50 grams per kilometer, NOx to 0.180 g/km , and HC+NOx to 0.230 g/km.

These levels are a reduction from Euro 4 standard implemented in January 2005 (CO=0.05,

NO_x=0.25, HC+NO_x=0.30).

– 2011 –

September 2011 – EU emission standard Euro 5b phased in, using same levels as 5a, but applying a specific particulate measure of 6×10¹¹th).

December 2011 – Report in *Atmospheric Environment* [1] says,

...The lack of a decrease in the concentration of NO_x and in particular NO₂ is of concern given European air quality standards are set in law. The lack of decrease in the concentration of NO_x and NO₂ is also in clear disagreement with emission inventory estimates and projections. ... **We find that there are significant discrepancies between current UK/European estimates of NO_x emissions and those derived from the remote sensing data for several important classes of vehicle.** In the case of light duty diesel vehicles it is found that NO_x emissions have changed little over 20 years or so over a period when the proportion of directly emitted NO₂ has increased substantially. For diesel cars it is found that absolute emissions of NO_x are higher across all legislative classes than suggested by UK and other European emission inventories. Moreover, the analysis shows that more recent technology diesel cars (Euro 3–5) have clear increasing NO_x emissions as a function of Vehicle Specific Power, which is absent for older technology vehicles. ... [*emphasis mine*]

– 2012 –

April 2012 – The International Council on Clean Transportation (ICCT), an independent nonprofit, published a report, Discrepancies between type-approval and real-world fuel consumption and CO₂ values in 2001-2011 European passenger cars. Its summary is rather benign, though it does suggest there are discrepancies in emissions reporting:

This paper compares fuel consumption / CO2 values of passenger cars from different sources and aims at quantifying the discrepancy between laboratory type-approval values and real-world values, including a retrospective analysis for the years 2001-2011 to determine if the gap between the two datasets has increased over time. Potential explanations for the discrepancies found are discussed and possible practical solutions for the future outlined.

The report expressed concerns about consumers' perceptions that fuel efficiency does not match figures reported at time of sale, and that consumers might resist emissions controls because efficiency does not yield an offset in fuel savings.

– 2013 –

November 2013 – An op-ed by Christian Wüst in Der Spiegel, Artists of the Dynamometer (Artisten des Prüfstands), criticized automakers for failing to install particulate filters costing an estimated 100 euros per each gasoline-powered vehicle. Though Wüst had training as a mechanic as well as education in journalism, he may have been fooled by reports on diesel-powered vehicle emissions tests, with regard to soot-particulate filters.

... Die schon beim Diesel bewährten Filter hingegen könnten all diese Trickserei überflüssig machen. Sie fangen mehr als 99 Prozent der Partikel ein. Selbst auf Messfahrt bei Vollgas bliebe ein Benzinauto mit diesem Gerät weit unter dem zulässigen Grenzwert. ...

[Translation: The already proven diesel filter on the other hand could make all this tricks superfluous. They capture more than 99 percent of the particles. Even on test runs at full throttle, a gasoline car with this device is far below the allowable limit. ...]*

(*Month TBD*) – West Virginia University’s Center for Alternative Fuels, Engines & Emissions (CAFEE) researchers are commissioned by the ICCT to test Volkswagen diesel passenger car emissions.

– 2014 –

May 2014 – WVU’s CAFEE researchers issue a Final Report [2] to ICCT.

(*Month TBD*) – VW began selling “Clean Diesel” Passats in the US market.

September 2014 – Emissions standard Euro 6 implemented, with CO limit unchanged at 0.50 g/km; NOX 0.080, HC+NOX 0.170, and particulate unchanged at 6×10(11th).

28 September 2014 – ICCT published a report [3] updating previous work and extending “an analysis of the gap between official and real-world fuel consumption and CO₂ emissions for passenger cars in Europe, which reached 38% in 2013 and continues to grow at an accelerated pace.” The report calls for implementation of “new Worldwide Harmonized Light Vehicles Test Procedure (WLTP), a more appropriate test that will produce more realistic type-approval values.”

11 October 2014 – ICCT published another report [4] – in summary:

Documents the discrepancy between type-approval and real-world NOx emissions from new diesel passenger cars. On average, on-road NOx emissions from the vehicles tested for this analysis were about **seven times higher than the limits set** by the Euro 6 standard. [*emphasis mine*]

– 2015 –

(*Month TBD*) – VW’s 2015 Passat TDI named by Cars.com the “Eco-friendly Car of the Year.”

18 September 2015 – U.S. Environmental Protection Agency issued to Volkswagen AG, Audi

AG, and Volkswagen Group of America, Inc., a Notice of Violation (NOV) of the Clean Air Act, alleging:

...four-cylinder Volkswagen and Audi diesel cars from model years 2009-2015 include software that circumvents EPA emissions standards for certain air pollutants. California is separately issuing an In-Use Compliance letter to Volkswagen, and EPA and the California Air Resources Board (CARB) have both initiated investigations based on Volkswagen's alleged actions. ...

20 September 2015 – VW halted sales of some 4-cylinder diesel-powered vehicles in the U.S.

22 September 2015 – VW admitted that 11 million vehicles had been fitted with the “defeat device” software to thwart accurate testing of emissions.

23 September 2015 – VW's CEO Martin Winterkorn resigned; law firm Kirkland & Ellis, which represented BP after the Deepwater Horizon disaster in 2010, was retained by VW.

(If you have a point you believe is critical to this timeline, feel free to share it in comments for consideration.)

Initial Conclusion:

On first pass, it appears that the EU did not have adequate mechanisms in place to investigate the disparities between actual emissions and test emission levels reported over the course of the last handful of years. Until the U.S. regulatory body took action, the EU did not appear to respond at all beyond press release(s).

It's not clear what happened between the time ICCT received their commissioned report from WVU-CAFEE and the U.S. EPA gave VW its NOV. This gap in time may have been the normal bureaucratic lag from reporting a problem through the federal government's validation of

the problem – but this gap meant 16 months of additional air pollution and more new vehicles sold with the cheating software on board.

The lack of prompt, effective action despite years of evidence mirrors the EU's response to the refugee crisis. Both issues are at complete odds with the EU's response to Greece's economic crisis. This begs the question whether the EU has outsourced pollution monitoring to the U.S., and whether the EU itself has real function beyond policing economic policy and banking legislation.

We might ask if the disparity in EU reaction to different crises a bug or a feature, or is the EU merely asleep at the wheel? Whatever the case, thousands of U.S. and EU citizens have sickened or died prematurely because of exposure to air pollution, and climate change has only grown worse, setting up conditions for more crises ahead.

Note:

* Translation here in question. By *all diese Trickseriei überflüssig machen*, did Wüst mean:

- all these tricks are made superfluous, or
- all this trickery is superfluous

In either case, you get the gist, I'm sure.

Citations:

[1] Carslaw, D., Beevers, S., Tate, J., Westmoreland, E., & Williams, M. (2011). Recent evidence concerning higher NO_x emissions from passenger cars and light duty vehicles. *Atmospheric Environment*, 45(39), 7053-7063.

[2] Thompson, Dr. Gregory J., Daniel K. Carder, Marc C. Besch, Arvind Thiruvengadam, and Hemanth K. Kappanna. In-Use Emissions Testing of Light-Duty Diesel Vehicles in the United States. Report (PDF), May 15, 2014.

[3] Mock, Peter, and Uwe Tietge, Vicente Franco, John German, Anup Bandivadekar (ICCT), Norbert Ligterink (TNO), Udo Lambrecht (IFEU), Jörg

Kühlwein (KISU), and Iddo Riemersma (Sidekick Project Support). From Laboratory to Road: A 2014 Update. *The International Council on Clean Transportation*. 28 Sept. 2014.

[4] Franco, Vicente, and Francisco Posada Sánchez, John German, Peter Mock. Real-world exhaust emissions from modern diesel cars. *The International Council on Clean Transportation*. 11 Oct. 2014. [EDITED: Note this is PART 1: AGGREGATED RESULTS of the entire study; PART 2: DETAILED RESULTS has been requested as it is not available online.]

AIR TRAVEL, DISRUPTED: WELCOME TO THE NEW NORMAL

Air travelers along the U.S. east coast experienced flight cancellations and delays this past Saturday, due to initially unspecified “technical issues” attributed to the air traffic control system.

Beginning some time late morning, hundreds of flights were affected by the problem. The FAA’s service was restored around 4:00 p.m. EDT, though it would take hours longer for the airlines to reschedule flights and flyers.

Although 492 flights were delayed and 476 flights were canceled, the FAA’s Twitter account did not mention the outage or mass flight disruptions until 4:06 p.m., when it said service had been restored.

In a tweet issued long after the outage began, the Federal Aviation Administration said, “The FAA is continuing its root cause analysis to determine what caused the problem and is working closely with the airlines to minimize impacts to travelers.”

The FAA's Safety Briefing Twitter account made no mention at all of the outage, though it has advised of GPS system testing at various locations across the country.

Various news outlets were conflicted: airports were blamed, then the FAA blamed, and the public knew nothing at all except they were stuck for an indeterminate period.

Get used to this. There's no sign FAA will change its communications methodology after several air travel disruptions this year alone "due to technical issues" or whatever catchy nondescript phrase airlines/airports/government chooses to use.

Is this acceptable? Hell no. Just read the last version of WaPo's article about the outage; the lack of communication causes as much difficulty as the loss of service. How can travelers make alternative plans when they hear nothing at all about the underlying problem? They're stuck wherever they are, held hostage by crappy practices if not policies.

It doesn't help that the media is challenged covering what appears to be a technology problem. The Washington Post went back and forth as to the underlying cause. The final version of an article about this disruption is clean of any mentions of the FAA's En Route Automation Modernization (ERAM) system, though earlier versions mention an upgrade to or component of that system as suspect.

The most recent statement issued by the FAA on Monday evening blames an upgrade to ERAM for the outage. It's troubling that an upgrade applied to a key regional air traffic control facility wasn't identified more promptly as the problem. Software testing and change management processes are also in question; why was this problem identified in a production environment and not a test environment? Was this the slowest traffic period for implementation of an upgrade? And why so long to cut over to local, lower level air traffic control since they knew there had been a

recent upgrade? Didn't they anticipate a possible fail-over?

Equally troubling is government communication long after air travel disruption, as well as the media's follow-up coverage, in spite of what appears to be an uptick in air travel disruption.

What happened after United Airline's July 8th outage? Was there an investigation? If so, what were the findings?

Was the outage, characterized in some reports as automation-related, like this past weekend's outage? It, too, was characterized by at least one news outlet as an automation issue.

Whatever the cause, how will outages like that on July 8th be prevented in the future?

And what happened after United Airline's June 2nd outage? After the hour-long grounding of unspecified origin, was there an investigation and corrective action?

Were these two outages manifestations of the same problem – upgrades to existing software – or were they hardware problems?

Without follow-through by the FAA and follow-up by the media, the public can't be certain that network equipment failures caused by hackers aren't a wider problem. Or that airlines, airports, and the government have or haven't done an adequate job of shielding air travel systems from solar storm radiation.

Oh, yeah, that...there was a G2-3 level solar storm, combined with the effects of an earlier coronal mass ejection on Saturday, too, which impacted electronics including ham radio. This is at least the second time in a year when an air travel-related outage occurred about the same time as a solar event. The most obvious was New Zealand's June 23 loss of aviation radar during one of the largest solar storms this solar cycle. Was it a coincidence that the radar went down during the storm? We don't know

because we haven't heard anything specific about the outage's cause.

It's little comfort to know that New Zealand's aviation system isn't any better at communicating than the FAA.

You'd think the American public would learn more and faster about the loss of air traffic control of flights in and out of Washington, D.C.

Or didn't any of the piles of tax dollars we spent post-9/11 actually do anything about *communicating* U.S. air traffic conditions?

WAS CHRYSLER'S VEHICLE HACKING RISK AN SEC DISCLOSURE REPORTABLE EVENT?

Remember the data breach at JPMorgan Chase, exposing 76 million accounts to "hack-mapping"? Last October, JPMorgan Chase publicly disclosed the intrusion and exposure to investors in an 8-K filing with the Securities and Exchange Commission. The statement complied with the SEC's CF Disclosure Guidance: Topic No. 2 – Cybersecurity.

Other companies whose customers' data have been exposed also disclosed breaches in 8-Ks, including Target, TJX Companies, Heartland Payment, EMC and Google. (Firms NASDAQ, Citigroup and Amazon have not.)

Disclosure of known cybersecurity threats or attacks with potential material risks allows investors to make informed decisions. Stock share pricing will fluctuate and reflect the true market value once risk has been factored by investors – and not remain artificially high.

Fiat Chrysler America (FCA; NYSE:FCAU) has known for nearly a year about the risk that Chrysler vehicles could be hacked remotely, according to Fortune magazine Thursday.

Yet to date no filing with the SEC has been made, disclosing this specific cyber risk to investors, customers, and the public.

The SEC's Disclosure Guidance, though, is just that – guidance. There aren't any firm rules yet in place, and the guidance itself was published in October 2011. A lot has happened and changed about technology and cybersecurity risks since then; the guidance has not reflected the increasing threats and attacks to business' data.

Nor does the SEC's guidance distinguish between cybersecurity threats to service products (like banking services), versus hardlines or manufactured goods (like automobiles which offer software as an additional, non-essential feature). The software industry's chronic security patching confuses any distinction; should software companies likewise include all security patches in their SEC filings, or continue as they have without doing so? It's easy to see how revelations about Adobe Flash after Hacking Team was hacked have materially hurt Adobe and all companies relying on Flash – yet Adobe hasn't released a statement at its website. (Only a statement addressing the 2013 threat to customer accounts is posted.)

Are financial services firms any more obligated than software firms? Are automobile companies, which claim ownership of on-board software, any more obligated than software companies?

It's likely FCA chose not to reveal the vehicle hacking threat until efforts to mitigate potential damage had been completed. The now-released security patch for Chrysler vehicles is an obvious indication of this attempt.

Less visible to the public and to investors is any financial effort to reduce future financial exposures. Has FCA established a protocol for

investigating any suspect vehicle accidents?
Were reserves set up for future claims should there be (or have been) an accident caused by hacking of their vehicle software?

Can investors adequately account for their own financial risk if they do not know what actions FCA has taken? At this point, investors only know what Chrysler owners and the public know: FCA issued a recall Friday on 1.4 million vehicles at risk, in order to patch their UConnect systems.

Senators Richard Blumenthal (D-CT) announced Friday that he and Ed Markey (D-MA) are working on new legislation, to ensure the National Highway Traffic Safety Administration (NHTSA) and the Federal Trade Commission (FTC) establish new safety standards for software features in vehicles, in response to the kind threat revealed this week. This is problematic – members of Congress have proven repeatedly they are not able to grasp technological subtleties and details. We'll have to hope for the best.

But business reporting must likewise keep up with technology; the SEC should revisit cybersecurity disclosure guidance immediately, given the size and scope cybersecurity threats pose to the public. Disclosure to investors and the public should not be a hit-or-miss proposition.

**“TECHNICAL
DIFFICULTIES”: UNITED
AIRLINES GROUNDED,
NYSE HALTED, WHAT’S**

NEXT?

This is a working post for discussion of today's outages. United Airlines grounded its flights for roughly two hours this morning; the FAA's advisory indicated an automation-related issue, and subsequent communications from United said it was a "network connectivity" problem.

UAL also briefly grounded flights on June 2nd, due to "automation issues."

Now the New York Stock Exchange has halted all trading shortly before noon, cancelling all open orders, due to "technical difficulties."

There are reports that CNBC and WSJ websites are down, but they could simply be swamped by traffic.

Who's or what's next?

UPDATE – 12:55 pm EDT –

Looks like CNBC may only have had a brief burp due to high traffic as there are no further complaints about service interruption. WSJ's website has been slowly working its way back to normal service; the media outlet posted an abbreviated version for 15-20 minutes once its technical problems had been resolved. No indication yet that anything apart from high traffic volume may have spiked the site.

UPDATE – 1:35 pm EDT –

You know what cracks me up, in a *ha-ha-ouch* kind of way? FBI Director Jim Comey puling about the need for back doors into technology in front of Congress today, while a major airline and the most important stock market in the world demonstrate exactly how ugly it could get if hackers with malicious intent used the back doors he demands for evil rather than good. The "technical difficulties" both UAL and NYSE experienced today could be duplicated by hackers using back doors.

The U.S. Government is an aircraft carrier, very

slow to turn even when under fire. Hackers are speedboats. Asking for back doors across all technology while facing myriad fleet-footed nemesis is like chasing 38-foot Cigarette Top Gun speedboats with a carrier. Unless the carrier can see Cigarettes coming from a distance and train gun on them, Cigarettes will fly up its backside. The U.S. Government has already proven it can't see very far ahead, stuck in a defensive posture while using its offense in ways that only ensure more attacks.

UPDATE – 2:20 pm EDT –

Fortune reports the NYSE halt was due to a “failed systems upgrade.”

Right. Upgrade. Let's roll out an upgrade in the middle of the week, in the middle of the month, when both China's stock market and Europe's bankers are freaking out. Let's not manage traders expectations in advance of the day's trading, either.

Somebody needs to retake a course in Change Management 101 – or there's some additional explaining required.

Reuters assures us, too:

The U.S. Department of Homeland Security said there were no signs” that the problems at NYSE and United Airlines stemmed from “malicious activity,” CNN reported.

Good to know, huh? Can't believe they went to CNN for that.

UPDATE – 3:30 pm EDT –

The buzz since 2:00-ish pm is that Anonymous *might* be to blame for the NYSE “glitch.” The Hill, Salon, and a few other outlets reported about a cryptic tweet from @YourAnonNews late last evening:



Wonder if tomorrow is going to be bad for Wall Street.... we can only hope.

11:45 PM - 7 Jul 2015

But another Anonymous affiliate laughed it off, saying:



@BiellaColeman @NerdProf It was in reference to Greece and China, but this is too hilarious to issue an official statement we didn't do it

2:37 PM - 8 Jul 2015

Timing is incredible, though; the NYSE, WSJ, and UAL outages all happened concurrent with a Congressional hearing at which FBI Director Jim Comey discussed the need for back doors into everything. What an incredible series of coincidences today.

UPDATE – 3:55 pm EDT –

Best take by far on today's NYSE "technical difficulties", gonzo reporting with a feminine touch from Molly Crabapple:

I was met by fires in the streets, the screams of the dying tourists and the shouts of former traders offering sacrifices to their new gods

UPDATE – 5:00 pm EDT –

NYSE re-opened again around 3:00 pm EDT, with trading a bit jittery. Financial news outlets speculated the market closed at 17,515.42, down -261.49 (-1.47%) due to concerns over China's tanked stock market and Greece's EU debt woes. The Shanghai market had closed the previous day at 3,507.19 down -219.93 (-5.90%).

Feeling iffy over the Shanghai index, Hong Kong's Hang Seng Index closed at 23,516.56 down -1,458.75 (-5.84%); Japan's Nikkei 225 closed at 19,737.64 down -638.95 (-3.14%).

But these Asian markets weren't affected by the NYSE's technical difficulties today. Wonder how they will open on July 9th their local time – flat or down? I wouldn't put my money on an uptick, but I'm not a financial adviser, either.

I imagine the bars and pubs around Wall Street saw greater-than-average action. I might put money on that.

TO TALK OF MANY THINGS: OF VANDALS, AND CUTS, AND CABLES, AND PINGS

*The time has come,' the Walrus said,
To talk of many things:
Of shoes – and ships – and sealing-wax –
Of cabbages – and kings –
And why the sea is boiling hot –
And whether pigs have wings.'*

(Excerpt, Lewis Carroll's The Walrus and the Carpenter)

Here's an open information security topic worth examining more closely: the recent *vandalization* of yet another fiber optic cable on the west coast.

A total of eleven cuts have been made since last July on fiber optic cables in the greater San Francisco/Oakland area. The most recent cut occurred on June 30th. The FBI had already asked the public for help with information about the first ten cuts, made in these general locations at the time and date indicated here:

- 1) July 6, 2014, 9:44 p.m. near 7th St. and Grayson St. in Berkeley
- 2) July 6, 2014, 11:39 p.m. near Niles Canyon Blvd. and Mission Blvd. in Fremont

- 3) July 7, 2014, 12:24 a.m. near Jones Road and Iron Horse Trail in Walnut Creek
- 4) July 7, 2014, 12:51 a.m. near Niles Canyon Blvd. and Alameda Creek in Fremont
- 5) July 7, 2014, 2:13 a.m. near Stockton Ave. and University Ave. in San Jose

-
- 6) February 24, 2015, 11:30 p.m. near Niles Canyon Blvd. and Mission Blvd. in Fremont
 - 7) February 24, 2015 11:30 p.m. near Niles Canyon Blvd. and Alameda Creek in Fremont

-
- 8) June 8, 2015, 11:00 p.m. near Danville Blvd. and Rudgear Road in Alamo
 - 9) June 8, 2015, 11:40 p.m. near Overacker Ave and Mowry Ave in Fremont

-
- 10) June 9, 2015, 1:38 p.m. near Jones Road and Parkside Dr. in Walnut Creek

The FBI presented these first ten cuts as a single, undivided list. After looking at the dates and times, one can see these cuts may have occurred not as discrete events, but as three separate clusters of cuts. The first cluster occurred within a five-hour span; the second occurred nearly simultaneously at two points; and the third cluster occurred within three hours. The three clusters took place after dark, during the same evening. The tenth cut may be a one-off, or it may be connected to the third cluster as it took place within 14 hours of the eighth and ninth cuts.

The most recent cable cut, occurring this week, did not fit a pattern like the previous ten cuts. Reports indicate the cut was near Livemore – a new location much farther to the south and east in comparison, and only one cut reported rather than two or more.

Is this latest cut an outlier, or were perpetrators interrupted before they could cut again?

Taking a closer look at the previous cut events, we can see there must have been more than one individual involved in the cuts, and they may

have been coordinated.

Cluster 1: The first cluster from one year ago, the evening of July 6-7, took place over a distance of roughly 34 miles. Cuts 1 and 2 are nearly 30 miles apart; by private car they are more than 40 minutes drive or more than an hour and a half apart by public transportation. At two hours between events it's possible the same single perpetrator made these cuts, but only if they traveled by private car and if they knew exactly where to go and what to cut.

Cuts 2 and 3 are also about 30 miles apart, in the opposite direction. It would be nearly impossible for the same single perpetrator to make these two cuts back-to-back since the time window between the cuts is only 55 minutes. Could a single person make it up out of a manhole from one cut, into a vehicle, drive nearly 40 minutes, park, open and climb into another manhole, then cut a fiber optic cable?

Cuts 3 and 4 were not made by the same single perpetrator. They are roughly 34 miles apart, and the time window between the cuts is less than 30 minutes. To cut-exit-manhole-drive-park-enter-manhole-cut would require traveling at speed that would surely draw attention, even at 12:30-ish in the morning.

Cuts 4 and 5 were made one hour and 24 minutes apart, and the sites are about 20 miles apart. This last cut was the farthest south of the first cluster.

Cluster 2: The second cluster from February this year, consisting of only two cuts happening at what appears to be the same time, suggests there was more than one perpetrator involved. The two cuts occurred at the same time, but within 0.2 miles apart – as if two persons within line of sight cut at the same time. The cuts also occurred near or at two of the previous locations from the first cluster.

Cluster 3: Cuts 8 and 9 occurred 40 minutes apart, yet the sites are roughly 30 miles apart – too far once again for a single perpetrator.

Both happened within the hour before midnight local time.

The tenth cut may have been related to third cluster, as noted previously – but it broke from the established pattern. The first nine cuts all occurred after 9:00 p.m. but before 3:00 a.m. local time. The tenth occurred at 1:38 p.m., in broad daylight.

Cut 11, the most recent on June 30th shared this same attribute. It happened some time between 4:20 a.m. and 7:45 a.m. local time (14:45 UTC), near Livermore, CA, to the east of the previous ten cuts.

Were the same so-called vandals at work for all eleven cuts? If so, were they getting cocky, having not been caught on nine earlier occasions?

Or were they getting desperate?

The implication, assuming desperation, is that these were not the acts of vandals, but a focused effort dedicated to network disruption?

Or perhaps not disruption with intent to halt or disturb, but disruption to map network response and content movement?

What might these vandals have been looking for, as they cut at one end of an area across the bay from Palo Alto and Mountainview across to an area east of Silicon Valley?

Did they finally learn something when Microsoft issued a formal status notice regarding disruption of its Azure cloud services – perhaps which fiber served the Azure data farm?

6/30

Network Infrastructure – West US, South Central US – Advisory

From approximately 14:45 UTC to 21:45 on 30 Jun, 2015 UTC customers may have experienced intermittent connectivity issues to Azure services deployed in West US and South Central US. Root cause

for this issue is attributed to a fiber cuts in the Western US Region. This incident has now been mitigated.

Or were they looking for fiber optics serving the Lawrence Livermore National Laboratory, home to other data farms and a number of sensitive research projects?

Or were they looking for the fiber running out of San Francisco, serving headquarters of businesses headquartered in the city like Wells Fargo?

UPDATE – 5:10 PM EDT – Here's the graphic as promised, mapping the approximate location of cuts per the FBI's list. The 11th cut is arbitrarily parked near Livermore as more specific site information was not provided. Cuts are labeled in chronological order.

SONY PICTURES POSTMORTEM REVEALS DEATH BY STUPID

We
already
knew
Sony
Pictures
Entertainment
's
(SPE)
hack
was

In a statement, Lawson argues that "any suggestion Sony Pictures Entertainment should have been able to defend itself against this attack is deeply flawed and ignores essential findings and comments made by the FBI and [Sony's cybersecurity consultant] Kevin Mandia—the two parties most knowledgeable of the nation state threat and the evidence in this investigation. Joseph Demarest, then assistant director of the FBI's cyber division, could not have been clearer when he told a U.S. Senate hearing that **the malware that was used would have slipped, probably would have gotten past 90% of the net defenses that are out there today in private industry, and I would challenge to even say government.**" Mandia, the statement continues, "has also explained how the sophistication of the exfiltration methods used in this attack made them virtually undetectable. And both Mandia and the FBI have stated that the malware used was undetectable by industry standard antivirus software."

[Source: Sony Pictures: Inside the Hack of the Century, Peter Elkind, FORTUNE 25JUN2015 Online at: <https://fortune.com/sony-hack-part-1/>]

bad. We knew that the parent, Sony Group, had been exposed to cyber attacks of all kinds for years across its subsidiaries, and slow to effect real changes to prevent future attacks.

And we knew both Sony Group and SPE shot themselves in the feet, literally asking for trouble by way of bad decisions. Sony Electronics' 2005 copy protection rootkit scandal and SPE's utter lack of disregard for geopolitics opened the businesses to risk.

But FORTUNE magazine's expose about the hacking of SPE – of which only two of three parts have yet been published – reveals a floundering conglomerate unable to do anything but flail ineffectively.

It's impossible to imagine any Fortune 500 corporation willing to tolerate working with 1990s technology for any length of time, let alone one which had no fail-over redundancies or backup strategies, no emergency business continuity plan to which they could revert in the event of a catastrophe. But FORTUNE reports SPE had been reduced to using fax machines to distribute information, in large part because many of its computers had been completely wiped by malware used in the attack.

Pause here and imagine what you would do (or perhaps, have done) if your computer was completely wiped, taking even the BIOS. What would you do to get back in business? You've given more thought about this continuity challenge than it appears most of SPE's management invested prior to last November's hack, based on reporting to date.

A mind-boggling part of FORTUNE's expose is the U.S. government's reaction to SPE's hack. The graphic above offers the biggest guffaw, a quote by the FBI's then-assistant director of its cyber division. Knowing what we know now about the Office of Personnel Management hack, the U.S. government is a less-than-credible expert on hacking prevention. While the U.S. government maintains North Korea was responsible, it's hard to take them seriously when they've failed so egregiously to protect their own turf.

A fast read of Part 1 of the expose validates previous concerns about SPE's and Sony Group's

approach to security. At a minimum, each of the following issues would have been addressed by a savvy business, substantially reducing risk:

- Adequate physical site security
- Secured hardware, cordoned off by its function, by way of physical location, firewalls, other services
- Adequate security software from mobile devices to servers
- Monitoring of all content transmissions for size, frequency, pattern, authorization
- 2-step authentication across organization, with frequent mandatory resets
- Catastrophic business continuity planning (especially important in an earthquake-prone area)
- Security screening of all new hire personnel and contractors
- Personnel trained on IP security practices, appropriate to job level, refreshed regularly
- Appropriate response time to security threats and breaches
- Geopolitical risk assessment on all content production
- Ethics reporting mechanism allowing employees to notify management of suspect behavior
- Process improvement mechanism through which employees can suggest improvements and receive rewards for same
- Accountability throughout management chain
- Management aware of risks inherent to digitized intellectual property

The FORTUNE expose, nor any previous reporting by any other outlet, indicates that these issues were addressed before the November hack as part of corporate policy and practices.

It's clear there is a serious problem at SPE from FORTUNE's opening grafs. It's hard to imagine any Fortune 100 business allowing unvetted visitors to sit unattended with ready access to unsecured computers and network. The rest of the article is equally disturbing,

casting the U.S. State Department and the FBI in equally unflattering light.

Why didn't the State Department and the FBI come right out and tell SPE it was at serious risk of cyber attack, given what they already knew about North Korea's alleged attacks on other U.S. systems and businesses?

Why didn't the State Department spell out just how big a risk Seth Rogen's ego-inflating boy flick *The Interview* was, even if it meant giving SPE executives and Rogen a basic history lesson in Japanese-North Korean/U.S.-Korean history?

We know there's a relationship between the Department of Defense and Hollywood – why wasn't the DOD likewise involved to provide assistance with shaping message and providing cyber defense?

Given the tepid efforts offered by the U.S. government, one can only wonder if SPE and Sony Group weren't a sacrificial offering in cyber warfare.

Bait, as it were. Or a propaganda opportunity.

INFO SECURITY FIRMS AND THEIR ANTIVIRUS SOFTWARE MONITORED (HACKED?) BY NSA, GCHQ

Let's call this post a work in progress. I'm still reading through a pile of reporting from different outlets to see if it's all the same information but rebranded, or if there's a particular insight one outlet picked up, missed by the rest. Here are a few I've been working on today:

7:03 am – Popular Security Software Came Under Relentless NSA and GCHQ Attacks (The Intercept)

7:12 am – US and British Spies Targeted Antivirus Companies (WIRED)

9:48 am – Spies are cracking into antivirus software, Snowden files reveal (The Hill)

12:18 pm – GCHQ has legal immunity to reverse-engineer Kaspersky antivirus, crypto (Ars Technica-UK)

12:57 pm* – US, UK Intel agencies worked to subvert antivirus tools to aid hacking [Updated] (Ars Technica)(*unclear if this is original post time or time update posted))

~3:00 pm – NSA Has Reverse-Engineered Popular Consumer Anti-Virus Software In Order To Track Users (TechCrunch)
(post time is approximate as site only indicates rounded time since posting)

The question I don't think anyone can answer yet is whether the hack of Kaspersky Lab using Duqu 2.0 was part of the effort by NSA or GCHQ, versus another nation-state. I would not be surprised if the cover over this operation was as thin as letting the blame fall on another entity. We've seen this tissue paper-thin cover before with Stuxnet.

For the general public, it's important to note two things:

- Which firms were not targeted (that we know of);
- Understand the use of viruses and other malware that already threaten and damage civilian computing systems only creates a bigger future threat to civilian systems.

Once a repurposed and re-engineered exploit has been discovered, the changes to it are quickly shared, whether to those with good intentions or criminal intent. Simply put, criminals are benefiting from our tax dollars used to help

develop their future attacks against us.

There's a gross insufficiency of words to describe the level of shallow thinking and foresight employed in protecting our interests.

And unfortunately, the private sector cannot move fast enough to get out in front of this massive snowball of shite rolling towards it and us.

EDIT – 5:55 pm EDT –

And yes, I heard about the Polish airline LOT getting hit with a DDoS, grounding their flights. If as the airline's spokesman is correct and LOT has recent, state-of-the-art systems, this is only the first such attack.

But if I were to hear about electrical problems on airlines over the next 24-48 hours, I wouldn't automatically attribute it to hacking. We're experiencing effects of a large solar storm which may have caused/will cause problems over the last few hours for GPS, communications, electricals systems, especially in North America.

EDIT – 1:15 am EDT 23JUN2015 –

At 2:48 pm local time Christchurch, New Zealand's radar system experienced a "fault" – whatever that means. The entire radar system for the country was down, grounding all commercial flights. The system was back up at 4:10 pm local time, but no explanation has yet been offered as to the cause of the outage. There were remarks in both social media and in news reports indicating this is not the first such outage; however, it's not clear when the last fault was, or what the cause may have been at that time.

It's worth pointing out the solar storm strengthened over the course of the last seven hours since the last edit to this post. Aurora had been seen before dawn in the southern hemisphere, and from northern Europe to the U.S. Tuesday evening into Wednesday morning. It's possible the storm affected the radar system –

but other causes like malware, hacking, equipment and human failure are also possibilities.

ILLIBERAL HOLLYWOOD: IT'S 1984 — OR IS IT 1964? CAN'T TELL FROM EEOC'S INACTION

If you haven't watched this Bloomberg-produced video yet, you should. The women directors interviewed are highly skilled and have been fighting Hollywood's not-at-all-liberal misogyny for decades.

And yes, decades — nothing substantive has happened since 1983 when Reagan-appointee Judge Pamela Rymer ruled for two major studio defendants in the Directors Guild of America's lawsuits against them for their discriminatory hiring practices. There was an uptick for about one decade after the suit; by 1995, roughly 16% of movies were directed by women.

But since then the numbers have fallen, and neither the DGA nor the federal Equal Employment Opportunity Commission (EEOC) have done anything about it.

We could cut some slack on the first decade, between 1995 and 2005, right? Congress was full of right-wing zealots chasing the president over a blowjob, and the president who followed him was hyper-focused on going to war, pushed by Dick Cheney's hand up his backside. Their administrations drifted along with them, shaped by their leaders' attentions.

But a second decade now — over thirty years in all since 1983 — and the EEOC gave the matter no

attention at all? It's not as if the film and television industries aren't right under the noses of people charged with paying attention. Who can work in government and say they haven't watched any television or film in thirty years? Hello, West Wing?

Or is that an answer in itself, that the film and television industries are merely acting with government sanction, that it is U.S. government policy to discriminate in entertainment media because it serves national interests?

We know that the Pentagon actively works with the film industry to ensure that the military is portrayed in a positive light. Just how far does this reach go, though?

How can we not ask this, given President Obama's own response to the Sony Pictures' hack, when he implied by seeking additional cybersecurity measures that Sony – a Japanese-owned corporation – is part of critical U.S. infrastructure?

The DGA's negligence for thirty years on gender equity only assures the dust surrounding the government's relationship with Hollywood effectively obscures whatever the truth may be.

It's hard to tell, too, whether the DGA saw Judge Rymer's rulings as marching orders. Why didn't DGA ever appeal? Or address Rymer's problems with the suit and re-tackle the problem? Or did the DGA simply not want to buck the implied policy established at a remove by the only president with Hollywood background?, even though Judge Rymer felt DGA was "partially responsible for the small amount of women and minority film and television directors hired"? (pdf)

It's 2015 – the entertainment industry is nothing at all like it was in 1983. Yet the EEOC and DGA are frozen in time. The EEOC has continued to ignore a fundamental problem with leaving enforcement of federal employment law in the hands of a labor organization led by men, and the DGA's leadership refuses to represent

ALL of its members effectively, as other unions do.*

If the government and the DGA were ever worried another Leni Riefenstahl might rise from the ranks of women directors, they need not have worried. They've done a fine job manipulating public opinion to promote the government, while suppressing women's rights all on their own. Message read, loud and clear.

* Examples (source: EEOC.gov):

- UAW International v. Johnson Controls (1991) – *“...The Court rules that the employer's restriction against fertile women performing “dangerous jobs” constitutes sex discrimination under Title VII. ...”* DGA could still represent women in class action suits, as it did in 1983, and as other unions like the UAW have.
 - United Steel Workers of America v. Weber (1979) – *“...the Supreme Court holds that private sector employers and unions may lawfully implement voluntary affirmative action plans to remedy past discrimination. The Court holds that an employer and union do not violate a collectively bargained plan by reserving 50 percent of the slots in a training program in a traditionally segregated industry for black employees. The program is lawful because it does not “unnecessarily trammel the interests of white employees,” does not “create an absolute bar to the advancement of white employees,” and is “a temporary measure . . . not intended to maintain racial balance, but simply to eliminate a manifest racial imbalance.”* Further, the DGA could sue for remedies as well as compliance with employment law on behalf of women.
-

SUMMER SPORTS: WHAT'S GOOD THIS WEEKEND?

I admit it freely – I'm the least *sportif* member of the Emptywheel team. As years have gone by, sports have lost their shine for me. The full-body contact of politics has been far more interesting.

But I need to get that shine back. My oldest is in a relationship with a sportsy guy, and I need to be able to talk with him without trying too hard and sounding like a total moron.

So, help a girl out. Auto racing. Baseball. Golf. That's all that's in my cable channel lineup right now, and I can't muster enough excitement. Tell me what you think I should look for to get heated up about one of these, and is there something really juicy going on tomorrow?

– NHRA in Bristol, TN on ESPN right now looks much as it did over the past couple decades. Is there some big technological breakthrough that makes these races different now than they were pre-2000? Fill me in.

– Folks in my other social media about were using lots of shouty caps about baseball and some guy named Scherzer. What happened? Which is/was the better game to watch: Detroit Tigers v New York Yankees, or LA Dodgers v SF Giants?

– And Tiger Woods has no game left they say, missing the cut at the U.S. Open. I did see this much in my timeline. I imagine poor Papa Earl is rolling in his grave, saying he was right that Tiger could only be stopped by a woman. I think it was the comprehensive use of word, "woman," as in all women. Tiger hasn't really had it together for any length of time since his marriage fell apart. Besides the current golden boy McIlroy, who else should I watch at the U.S. Open?

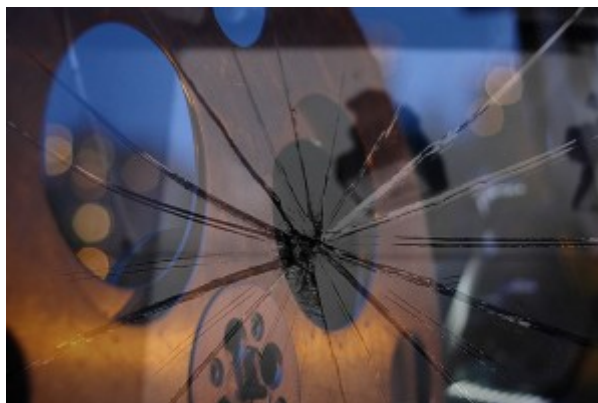
Golf has a little more appeal for me this summer. I used to play until a handful of years ago, when it just wasn't fun any more. I lost my game, too, couldn't spend enough time on the course. But now my youngest has landed his first job as bag boy at the nearby club. When he comes home after his shift it's a hoot to listen to him describe navigating his inaugural work experience, let alone hear all the goofy things that happened to him on the job.

Like today, his first Saturday morning opening the course – he sent me a text mid-shift that read, HOLY TIPS. Came home with a wad of bills in his pocket, yelling how much he loved old dudes who played golf.

Now for this I can worked up.

ILLIBERAL HOLLYWOOD: WHAT'S THE POINT OF A UNION IF IT DOESN'T REPRESENT MEMBERS?

This
year
contin
ues to
be a
big
one
for
women
in



film. Films featuring women as leads and/or directed by women made beaucoup at the box office. Mad Max: Fury Road, Pitch Perfect 2, Insurgent, and Fifty Shades of Grey are among the top ten films out of more than 284 released so far this year. Two of these films were

directed by women; all four featured female leads. And two of these films put to lie once again the bullshit claim that 'women can't lead action films.'

The immense popularity of these movies – especially with women – demonstrates how much Hollywood underserves the female audience, in spite of repeated studies revealing how much women contribute to box office results. Women want women's stories, told by women, and they've gotten them too rarely.

You'd think that Hollywood would actively court the single largest demographic by catering to its desires – but no. The film production pipeline remains solidly weighted toward men, still chasing the increasingly distracted 18-25 year-old male demographic.

It's not as if women aren't available as actors or directors. The Directors Guild of America (DGA) – the labor organization representing directors – counts among its ranks roughly 1200 female directors, reflecting the parity of female students who've been through film school or learned on the job in other production roles.

Which makes one wonder why actor/director/producer George Clooney said in a recent interview, *"...there's something like 15 female directors in a town of directors ..."*

If a household name like Clooney doesn't know more female directors, what exactly is it the DGA is doing for its female membership? It's clearly not representing them within their own organization, let alone to studios and the public.

The ACLU's May 12th letter to the federal Equal Employment Opportunity Commission (EEOC) spelled out DGA's complicity with Hollywood's exclusion of female directors, when it asked the EEOC to investigate discriminatory practices. DGA has denied the use of short lists, but apart from preparing regular reports on diversity in hiring, it's not clear at all what the DGA does to further the hiring of women directors.

During the course of its history, DGA hasn't been entirely useless to its female members:

1939 – Screen Directors Guild (SDG) recognized as bargaining agent by major studios
(SDG evolves into Directors Guild of America (DGA) over time and mergers with other entertainment industry labor groups).

MAR 1969 – U.S. Equal Employment Opportunity Commission (EEOC) sponsors a one-day hearing in Hollywood to discuss “patterns or practice of discrimination in violating Title VII of the Civil Rights Act of 1964.”

1978 – California Advisory Committee to the U.S. Commission on Civil Rights publishes a report of its study on employment opportunities for women and minorities in film industry in southern California.

1979 – DGA's Women's Steering Committee (WSC) formed to examine gender discrimination in employment by major studios.

1980 – DGA-WSC entered discussions with executives from film studios, TV networks, and production companies, introducing affirmative action quota recommendations.

JAN 1983 – President Ronald Reagan appoints conservative judge Pamela Rymer to U.S. District Court for the Central District of California.

1983 – Employers ‘unilaterally withdrew’ from the voluntary quota program; Columbia claimed DGA's contract limited ability to hire women and minorities.

JUL 1983 – DGA files lawsuit in U.S. District Court for the Central District of California against major studio Warner Bros under 1964 Civil Rights Act, Title VII.

DEC 1983 – DGA files lawsuit in U.S. District Court for the Central District of California against major studio Columbia

Pictures under 1964 Civil Rights Act, Title VII.

1985 – Judge Rymer sides with major studios against DGA, indicating DGA is in part responsible for inequity as directors' control over subordinate production employees limits ability of studios to effect quotas.

1985-? – After Rymer's decisions, DGA establishes The Freelance Live and Tape Television Agreement (FLTTA), Article 19, to affirm with TV producers compliance with anti-discrimination laws; a provision includes appointment of DGA officers to monitor diversity in hiring.

1985-2015 – Profit! Just kidding – not for female directors. Major studios' employment of female directors crawls up from 0.5% to 16% at its highest level over three decades.

AUG 2011 – Former DGA lawyer Jill Killion sues DGA for discrimination due to inequitable pay. Status TBD.

MAR 2015 – DGA presented a proposal to count women directors employed by studios in addition to the existing measure of minority directors employed, tracking increase/decrease in employment numbers.

APR 2015 – DGA-WSC rejects proposal to count women directors employed by studios in addition to the existing measure of minority directors employed.

MAY 2015 – ACLU submits letter to the EEOC asking for federal investigation of gender inequality among directors hired by major studios

Though the DGA exerted itself in the late 1960s and 1970s on behalf of its female constituents, its work was ineffectual. Flaws in film production hiring process outlined by the failed 1983 lawsuits were never remedied. Efforts on behalf of women in television were somewhat more

muscular with FLTTA's establishment, but recent gains do not appear to have anything to do with DGA role in representation.

All the women of DGA have to show for their membership dues is lip service – a handful of diversity reports affirming what they already know, and the knowledge that DGA's male leaders have pulled down millions in compensation for some nebulous representation.

Nebulous, meaning any meetings with studios in which gender equity is discussed are not shared with the membership. Do they actually have any such meetings, or is this just happy talk?

Nebulous, meaning any effort to enforce agreements with Alliance of Motion Picture and Television Producers (AMPTP) or compliance with Title VII remain undisclosed, challenging the concept of "acting in good faith." Are female members supposed to pay their rent with "good faith"?

The DGA does not appear to have used the opportunity presented by leaked information from the Sony Pictures' hack. Female actors like Jennifer Lawrence and Charlize Theron have benefited from evidence that they have been discriminated against in compensation compared to their male cohort. But there's no evidence of similar improvements to gender equity in director hiring.

For the amount that women directors pay in dues for DGA's lack of progress, one has to wonder if they wouldn't be better served by a different labor organization – perhaps one that actually does effective work on behalf of its female members, like Service Employees International Union (SEIU). The EEOC, having erred in the 1970s by leaving hiring diversity enforcement to the DGA, could rectify this by demanding other, more effective alternatives in representation.

(For that matter, what does the DGA do for ANY of its members? Have you seen any major disputes between an aggregate of male directors and studios on compensation or employment? Is it

just a boys' club with a secret handshake and a knowing wink between DGA leaders and the studios?)

.

So what does this mean to you, the general public, when women are excluded from filmmaking? It's not just a loss of women's stories told by women, potentially making money for shareholders.

The public develops a highly skewed perception of the world. Ask yourself how much our acceptance of violence has been shaped by films normalizing it as it targets a demographic consisting of boys and young men. Or hypersexualization of girls along with society's marginalization of women – how much can be attributed to films produced by and for the male gaze?

Women as leaders in all industries and academia are not the norm, in part because the images the public, industry, and academia have seen do not depict women in these roles in percentages weighted to their portion of the population. This persists, though women have made up more than 50% of graduates in many fields for at least two decades.

Our children acquire unhealthy perceptions of women based on tropes too often used in male-centric films – women are wallpaper, arm candy, victims stuffed in refrigerators, and not active agents with autonomy.

The challenges we face require different solutions, not more of the same. If the last 40-50 years of film excluding women behind the camera have resulted in the world we live in today, do we dare continue with the status quo?

Can we really afford that risk?

[Graphic: mash-up, Matt Olson and Ryan Gilchrist via Flickr]