ONE YEAR AFTER COLLATERAL MURDER RELEASE, DOD'S NETWORKS ARE STILL GLARING SECURITY PROBLEM

As I have posted several times, the response to WikiLeaks has ignored one entity that bears some responsibility for the leaks: DOD's IT.

Back in 2008, someone introduced malware to DOD's computer systems. In response, DOD announced it would no longer allow the use of removable media in DOD networks. Yet that is precisely how Bradley Manning is reported to have gotten the databases allegedly leaked. In other words, had DOD had very basic security measures in place they had already been warned they needed, it would have been a lot harder for anyone to access and leak these documents.

Often, when I have raised this issue, people are simply incredulous that DOD's classified network would be accessible to removable media (and would have remained so two years after malware was introduced via such means). But it's even worse than that.

A little-noticed Senate Homeland Security hearing last month (Steven Aftergood is one of the few people who noticed) provided more details about the status of DOD's networks when the leaks took place and what DOD and the rest of government have done since. The short version is this: for over two months after DOD arrested Bradley Manning for allegedly leaking a bunch of material by downloading information onto a Lady Gaga CD, DOD and the State Department **did nothing**. In August, only after WikiLeaks published the Afghan War Logs, they started to assess what had gone wrong. And their description of what went wrong reveals not only

how exposed DOD was, but how exposed it remains.

Two months to respond

Bradley Manning was arrested on or before May 29. Yet in spite of claims he is alleged to have made in chat logs about downloading three major databases, neither DOD or State started responding to the leak until after the Afghan War Logs were published on July 25, 2010.

The joint testimony of DOD's Chief Information Officer Teresa Takai and Principal Deputy Under Secretary for Intelligence Thomas Ferguson explains,

> On August 12, 2010, immediately following the first release of documents, the Secretary of Defense commissioned two internal DoD studies. The first study, led by the Under Secretary of Defense for Intelligence (USD(I)), directed a review of DoD information security policy. The second study, led by the Joint Staff, focused on procedures for handling classified information in forward deployed areas.

In other words, "immediately" (as in, more than two weeks) after the publication of material that chat logs (published two months earlier) had clearly explained that Manning had allegedly downloaded via Lady Gaga CD months earlier, DOD commissioned two studies.

As State Department Under Secretary of Management Patrick Kennedy explained, their response was no quicker.

> When DoD material was leaked in July 2010, we worked with DoD to identify any alleged State Department material that was in WikiLeaks' possession.

It wasn't until November—at around the time when NYT was telling State precisely what they were going to publish—that State started responding in earnest. At that time—over four months after

chat logs showed Manning claiming to have downloaded 250,000 State cables—State moved its Net Centric Diplomacy database from SIPRNet (that is, the classified network) to JWICS (the Top Secret network).

DOD's exposed IT networks

Now, frankly, State deserves almost none of the blame here. Kennedy's testimony made it clear that, while the WikiLeaks leak has led State to enhance their limits on the use of removable media access, they have systems in place to track precisely who is accessing data where.

DOD won't have that across their system for another year, at least.

There are three big problems with DOD's information security. First, as the Takai/Ferguson testimony summarized,

> Forward deployed units maintained an over-reliance on removable electronic storage media.

It explains further that to make sure people in the field can share information with coalition partners, they have to keep a certain number of computers accessible to removable media.

> The most expedient remedy for the vulnerability that led to the WikiLeaks disclosure was to prevent the ability to remove large amounts of data from the classified network. This recommendation, forwarded in both the USD(I) and Joint Staff assessments, considered the operational impact of severely limiting users' ability to move data from SIPRNet to other networks (such as coalition networks) or to weapons platforms. The impact was determined to be acceptable if a small number of computers retained the ability to write to removable media for operational reasons and under strict controls.

As they did in 2008 after malware was introduced via thumb drive, DOD has promised to shut off access to removable media (note, Ferguson testified thumb drives, but not CDs, have been shut down for "some time"). But 12% of the computers on SIPRNet will still be accessed by removable media, though they are in the process of implementing real-time Host Based Security System tracking of authorized and unauthorized attempts to save information on removable media for those computers.

In response to a very frustrated question from Senator Collins, Ferguson explained that DOD started implementing a Host Based Security System in 2008 (the year DOD got infected with malware). But at the time of the leak, just 40% of the systems **in the continental US** had that system in place; it was not implemented outside of the US, though. They weren't implemented overseas, he explained, because a lot of the systems in the field "are cobbled together."

In any case, HBSS software will be in place by June. (Tech folks: Does this means those computers are still vulnerable to malware introduced by removable media? What about unauthorized software uploads?)

Then there's data access control. DOD says it can't (won't) password protect access to information because managing passwords to control the access of 500,000 people is too onerous for an agency with a budget larger than Australia's gross national product. Frankly, that may well be a fair approach given the importance of sharing information.

But what is astounding is that DOD is only now implementing public key infrastructure that will, first of all, make it possible to track what people access and—some time after DOD collects that data—to start fine tuning what they can access.

> DoD has begun to issue a Public Key Infrastructure (PKI)-based identity credential on a hardened smart card.

> This is very similar to the Common Access Card (CAC) we use on our unclassified network. We will complete issuing 500,000 cards to our SIPRNet users, along with card readers and software, by the end of 2012. This will provide very strong identification of the person accessing the network and requesting data. It will both deter bad behavior and require absolute identification of who is accessing data and managing that access.
>
> In conjunction with this, all DoD organizations will configure their SIPRNet-based systems to use the PKI credentials to strongly authenticate end-users who are accessing information in the system. This provides the link between end users and the specific data they can access – not just network access. This should, based on our experience on the unclassified networks, be straightforward.
>
> DoD's goal is that by 2013, following completion of credential issuance, all SIPRNet users will log into their local computers with their SIPRNet PKI/smart card credential. This will mirror what we already do on the unclassified networks with CACs.

[Takai defines what they're doing somewhat just before 88:00]

Note what this says: DOD is only now beginning to issue the kind of user-based access keys to protect its classified network that medium-sized private companies use. And unless I'm misunderstanding this, it means DOD is only now upgrading the security on its **classified** system to match what already exists on its **unclassified** system.

Let's hope nothing happens between now and that day in 2013 when all this is done.

And this particular problem appears to exist beyond DOD. While the two DIA witnesses mostly blew smoke rather than provide a real sense of where security is at (both blamed WikiLeaks on a "bad apple" rather than shockingly bad information security), the testimony of DNI's Intelligence Community Intelligence Sharing Executive Corin Stone seems to suggest other parts of the IC area also still implementing the kind of authentication most medium sized corporations employ.

> To enable strong network authentication and ensure that networks and systems can authoritatively identify who is accessing classified information, the IC CIO is implementing user authentication technologies and is working with the IC elements to achieve certificate issuance to eligible IC personnel in the first quarter of fiscal year 2012.

So that's the issue of removable media and individualized access tracking.

Which leaves one more big security hole. According to Takai/Ferguson, DOD didn't—**still didn't**, as of mid-March—have the resources in place to detect anomalous behavior on its networks.

> Limited capability currently exists to detect and monitor anomalous behavior on classified computer networks.

This confirms something Manning said in chat logs: no one is following the activity occurring on our networks in Iraq (or anywhere else on SIPRNet, from the sounds of things), and flagging activities that might be an intrusion.

The part of the Takai/Ferguson testimony that details very hazy plans to think about maybe implementing such a system (pages 6-7) is worth a gander just for the number of acronyms of titles of people who are considering maybe what to implement some time in the future. It's all a

bunch of bureaucratic camouflage, IMO, to avoid saying clearly, “we haven’t got it and we haven’t yet figured out how we’re going to get it.” But here are the two most concrete descriptions of what the Department of **Defense** plans to do to make sure no one is fiddling in their classified networks. First, once they get HBSS completely installed, then they will install an NSA audit program on top of that.

> One very promising capability is the Audit Extraction Module (AEM) developed by the National Security Agency (NSA). This software leverages already existing audit capabilities and reports to the network operators on selected audit events that indicate questionable behavior. A great advantage is that it can be integrated into the HBSS we have already installed on the network, and so deployment should be relatively inexpensive and timely. AEM is being integrated into HBSS now and will be operationally piloted this summer.

But in the very next paragraph, Takai/Ferguson admit there are better solutions out there. But DOD (again, with its budget larger than the GNP of most medium sized countries) can’t implement those options.

> Commercial counterintelligence and law enforcement tools – mostly used by the intelligence community – are also being examined and will be a part of the overall DoD insider threat program. These tools provide much more capability than the AEM. However, while currently in use in some agencies, they are expensive to deploy and sustain even when used in small, homogeneous networks. Widespread deployment in DoD will be a challenge.

In other words, DOD wants to be the biggest part of the intelligence community. But it and its

budget bigger than Brazil's GNP won't implement the kind of solutions the rest of the intelligence community use.

Department. Of. Defense.

Now, let me be clear: DOD's embarrassingly bad information security does not, in any way, excuse Bradley Manning or the other "bad apples" we don't know about from their oath to protect this information. (Note, there was also testimony that showed DOD's policies on information sharing were not uniformly accessible, but that's minor compared to these big vulnerabilities.)

But in a world with even minimal accountability, we'd be talking about fixing this yesterday, not in 2013 (five years, after all, after the malware intrusion). We'd have fired the people who let this vulnerability remain after the malware intrusion. We'd aspire to the best kind of security, rather than declaring helplessness because our very expensive DOD systems were kluged together. And we'd be grateful, to a degree, that this was exposed with as little reported damage as it has caused.

If this information is really classified for good reason, as all the hand-wringers claim, then we ought to be using at least the kind of information security implemented by the private sector a decade ago. But we're not. And we don't plan on doing so anytime in the near future.

DOD CONSIDERS ILLEGAL DATA MINING PART OF CAPITAL CRIME

I've written two posts on the software that Bradley Manning is alleged to have loaded onto SIPRNet (here, here). Wired has now gotten a

little more detail about what the software was: DOD says it was some kind of data mining software, though they won't say of what kind. Wired goes on to suggest that presence of the software may make it easier for DOD to prove intent with Manning (though I rather suspect the idea is to prove collaboration with WikiLeaks personnel; furthermore, Wired's tie of the data mining software to Manning's alleged illegal access of the State cables has one problem—that he probably couldn't access such things after he got demoted).

But the entire time I read the following passages, I couldn't help but think of the illegal data mining DOD's component, NSA, conducted on American citizens in 2004 even after Congress had specifically defunded such activities.

> Accused WikiLeaks source Pfc. Bradley Manning installed and used unauthorized "data-mining software" on his SIPRnet workstation during the time he allegedly siphoned hundreds of thousands of documents off that classified network, the Army said Friday in response to inquiries from Threat Level.
>
> Manning's use of unauthorized software was the basis of two allegations filed against him this year in his pending court martial, but the charge sheet listing those allegations was silent on the nature of that software.
>
> On Friday, an Army spokeswoman clarified the charges. "The allegations … refer to data-mining software," spokeswoman Shaunteh Kelly wrote in an e-mail. "Identifying at this point the specific software program used may potentially compromise the ongoing criminal investigation."
>
> [snip]
>
> If Manning installed data-mining software on his SIPRnet workstation,

> that could potentially strengthen the government's case against the alleged leaker.

After all, Wired at least suggests data mining is proof of guilt. Yet the agency that may be crafting such arguments not only violated privacy laws for years, but continued to data mine Americans for months after Congress had specifically prohibited funding from being used for such things. And DOD now wants to prosecute the person it alleges engaged in such illegal data mining with a capital crime.

Maybe the whole thing would be more credible if our government hadn't become such a criminal itself?

PJ CROWLEY EXPLAINS WHY MANNING'S TREATMENT IS RIDICULOUS, COUNTERPRODUCTIVE, AND STUPID

PJ Crowley has a very important Guardian piece on why he said the treatment of Bradley Manning was ridiculous, counterproductive, and stupid. After explaining that Manning, if convicted, "should spend a long, long time in prison," and then claiming that the overall narrative of the State Department cables shows a story of "rightdoing," he describes how Manning's treatment undermines our own strategic narrative.

> But I understood why the question was asked. Private Manning's family, joined

> by a number of human rights organisations, has questioned the extremely restrictive conditions he has experienced at the brig at Marine Corps base Quantico, Virginia. I focused on the fact that he was forced to sleep naked, which led to a circumstance where he stood naked for morning call.
>
> Based on 30 years of government experience, if you have to explain why a guy is standing naked in the middle of a jail cell, you have a policy in need of urgent review. The Pentagon was quick to point out that no women were present when he did so, which is completely beside the point.
>
> Our strategic narrative connects our policies to our interests, values and aspirations. While what we do, day in and day out, is broadly consistent with the universal principles we espouse, individual actions can become disconnected. Every once in a while, even a top-notch symphony strikes a discordant note. So it is in this instance.
>
> The Pentagon has said that it is playing the Manning case by the book. The book tells us what actions we can take, but not always what we *should* do. Actions can be legal and still not smart. With the Manning case unfolding in a fishbowl-like environment, going strictly by the book is not good enough. Private Manning's overly restrictive and even petty treatment undermines what is otherwise a strong legal and ethical position.
>
> When the United States leads by example, we are not trying to win a popularity contest. Rather, we are pursuing our long-term strategic interest. The United States cannot expect others to meet international standards if we are seen

> as falling short. Differences become strategic when magnified through the lens of today's relentless 24/7 global media environment.
>
> So, when I was asked about the "elephant in the room," I said the treatment of Private Manning, while well-intentioned, was "ridiculous" and "counterproductive" and, yes, "stupid".
>
> I stand by what I said. The United States should set the global standard for treatment of its citizens – and then exceed it. It is what the world expects of us. It is what we should expect of ourselves.

While I suspect DOD is on narrower procedural grounds than Crowley gives them credit for (but by doing so, his own argument is stronger), Crowley is right that the treatment of Manning belies America's claims to support the rule of law.

That said, I think Crowley is likely still too close to the government bubble to see how much else the entire WikiLeaks episode demonstrates the hollowness of "our interests, values and aspirations." Starting from when the government probably hacked and then shut down a media entity, even while scolding Tunisia for doing the same, down to the many cables where we've placed our interests above any claim to rule of law or human rights.

And those are just the secret cables.

But I think that's true of our policy-makers in general. Our country has totally lost its ability to invoke the myth of the noble America that made our hegemony more palatable globally. Manning's treatment is just one of the most salient examples of that.

FRONTLINE IGNORES MOST EMBARRASSING "CAUSE" OF WIKILEAKS LEAK

Greg Mitchell has a preview of the Frontline piece on Bradley Manning today. He points out that the big "scoop" of the story—that Manning's stepmother called the cops in 2006 after Bradley pulled out a knife during a family fight (but then immediately asked if his dad was okay).

The entire story seems to look to Manning's psychology to explain his alleged leak of classified information.

> *Frontline* says it will continue its report in May in a one-hour program which will, again, focus on Manning's personal life and how this "led" to his alleged leak; and his new outbursts, this time in the Army (all reported elsewhere)—and how the Army still gave him access to top-secret documents.
>
> [snip]
>
> The overall tone of tonight's report is sure to spark debate. Consider that *MilitaryTimes* opens its report today with this: "Could the global turmoil sparked by Wikileaks have started started with a son's anger for his father?" NPR's report is headlined: "Home Life Included a 911 Call."

Such spin, in the absence of a larger examination of what "led to" the alleged leak, is irresponsible.

If Manning is found to have leaked the cables, he deserves the bulk of responsibility for the

leak (though, as Mitchell points out, to explain it, it'd be well to look at his political views and, I'd add, the disclosure requirements for crimes like support for torture exposed in WikiLeaks as well).

But one entity that has thus far avoided all responsibility for the leak are the folks in charge of DOD's IT. As I have pointed out, DOD's network security was embarrassingly bad—worse than your average mid-sized corporation. But to make their negligent security even worse, they had already suffered a damaging compromise of their systems when, in 2008, malware was introduced into their system via removable media, the same means by which Manning is alleged to have downloaded the WikiLeaks cables.

> The Defense Department's geeks are spooked by a rapidly spreading worm crawling across their networks. So they've suspended the use of so-called thumb drives, CDs, flash media cards, and all other removable data storage devices from their nets, to try to keep the worm from multiplying any further.
>
> The ban comes from the commander of U.S. Strategic Command, according to an internal Army e-mail. It applies to both the secret SIPR and unclassified NIPR nets. The suspension, which includes everything from external hard drives to "floppy disks," is supposed to take effect "immediately."
>
> [snip]
>
> Servicemembers are supposed to "cease usage of all USB storage media until the USB devices are properly scanned and determined to be free of malware," one e-mail notes.
>
> Eventually, some government-approved drives will be allowed back under certain "mission-critical," but unclassified, circumstances. "Personally owned or non-authorized devices" are

> “prohibited” from here on out.

Not only did DOD’s failure to do what it claimed it would in response to this malware attack expose DOD’s networks to the kind of leak Manning is alleged to have committed, but it also exposed DOD’s networks to more secret, but potentially more damaging, leaks of targeted information that our enemies would like. The failure to implement the very minimal response to the malware attack is inexcusable.

But, as far as I know, no one is asking anyone be held responsible for that negligence.

None of this excuses what Manning is alleged to have done in the least. But shouldn’t the press be asking why DOD persisted with completely inadequate security after having been attacked already?

Update: “Stepmother” fixed.

RICHARD CLARKE: THE CHAMBER BROKE THE LAW

I’m really deep in the weeds on the Jack Goldsmith memo right now (I should have a weedy post up later).

But in case you’re bored w/bmaz’s rant about the assault on Miranda rights, I thought I’d point to this TP post describing Richard Clarke suggesting that the Chamber of Commerce (funded by foreign sources, he notes) may have broken the law in targeting Chamber opponents.

> Clarke denounced the scandal in no uncertain terms. Noting accurately that the Chamber “took foreign money in the last election,” a story also uncovered

> by ThinkProgress, Clarke said the Chamber had conspired to commit a "felony":
>
> > FANG: Hi. You talked a lot about classifying and recognizing cyber security threats, but you mostly focused on foreign threats. I'm curious about a story that broke last month, that the US Chamber of Commerce, the world's largest trade association, based here in DC, had contracted or attempted to contract military defense firms like HB Gary Federal, Palantir, and Berico, to develop proposals to use the same type of cyber warfare tactics normally reserved for Jihadi websites against left-wing activists, trade – labor unions, and left of center think tanks here in America. What do you think about that type of threat from a lobbyist or a corporation targeting political enemies, or perceived enemies here in the US?
> >
> > CLARKE: **I think it's a violation of 10USC. I think it's a felony, and I think they should go to jail.** You call them a large trade association, I call them a large political action group that took foreign money in the last election. But be that as it may, if you in the United States, if any American citizen anywhere in the world, because this is an extraterritorial law, so don't think you can go to Bermuda and do it, if any American citizen anywhere in the world engages in unauthorized penetration, or identity theft,

> accessing a number through identity theft purposes, that's a felony and if the Chamber of Commerce wants to try that, **that's fine with me because the FBI will be on their doorstep in a matter of hours.**

Now if only we had Feds anymore that would consider busting big business…

WHY WON'T JEH JOHNSON ANSWER HANK JOHNSON'S QUESTION ABOUT FORCED NUDITY?

The House Armed Services Committee is having a hearing on Law of War Detention. Much of it has focused on Jeh Johnson affirming that military commissions line up with American values. (In other words, it is fairly depressing.)

But an interesting exchange happened when Hank Johnson had his turn. He set up his question by talking about a recent trip to Gitmo. He described the good treatment he saw the detainees being subject to. Jeh Johnson said that we're following the Geneva Conventions.

Then he said (working from memory), so why is Bradley Manning being subject to worse treatment.

Frankly, Hank Johnson got a few details incorrect (for example, he said that Manning had to wear shackles in his cell). But he went through Manning's treatment reasonably well.

In response, Jeh Johnson reverted immediately to the importance of pretrial detention. He used

the same old lie about Manning being able to talk to others in his cell block. Here's a rough liveblog:

> not in solitary confinement. Public misinformation. It is public that he is currently in classification status called Maximum security. Someone in Max occupies same type of cell that a medium security pretrial detainee. Same time of cell. You could have Max security and medium confinee in the same row of cells and they could converse with one another.

(That would be true if anyone was in a cell close enough to him to be able to talk to, but there isn't.)

But perhaps most tellingly, Jeh Johnson didn't address Hank Johnson's question about the forced nudity Manning is being subject to.

Ultimately, Buck McKeon cut off Hank Johnson, saying that Jeh Johnson could answer him "off the record." (?) I hope he meant for the record; we shall see.)

But for now, at least, it appears that Jeh Johnson really doesn't want to talk about why Manning is being subject to a policy implemented—and then rejected—at Gitmo.

DYLAN RATIGAN, LAW PROFESSORS AND I ALL AGREE: OBAMA NEEDS TO EXPLAIN OR END

MANNING'S TREATMENT

On Friday, Dylan Ratigan and I had a podcast chat about the treatment of Bradley Manning. Among other things, we talked about the "Constitutional Law Professor" President's rather bizarre response when DOD told him it was standard procedure to strip an Army man of his clothes because of a trumped up claim that his underwear was a terrible threat to him.

> DYLAN: And what does that say to you about our President that he endorses such a ridiculous point of view?
>
> MARCY: I mean for starters it says he's giving the military way too much leeway. They said, "Well, this is standard operating procedure." And as I pointed out today in my blog, what they're doing to Manning, the forced nudity, goes right back to Gitmo and goes right back to the treatment they used with Abu Zubaydah. So him giving — he came in to office and on day 2 said, "We're going to close Gitmo. We're going to end these abusive techniques," and yet when DOD came to him and said, well, you know, it's all standard procedure to take away a man's underwear. The President just said, "Oh, okay."

That's one of the things a bunch of (real, active) law professors had to say in their letter calling on Obama to explain or end the treatment of Bradley Manning.

> The Administration has provided no evidence that Manning's treatment reflects a concern for his own safety or that of other inmates. Unless and until it does so, there is only one reasonable inference: this pattern of degrading treatment aims either to deter future whistleblowers, or to force Manning to implicate Wikileaks founder Julian

> Assange in a conspiracy, or both.
>
> If Manning is guilty of a crime, let him be tried, convicted, and punished according to law. But his treatment must be consistent with the Constitution and the Bill of Rights. There is no excuse for his degrading and inhumane pre-trial punishment. As the State Department's PJ Crowly put it recently, they are "counterproductive and stupid." And yet Crowley has now been forced to resign for speaking the plain truth.
>
> The Wikileaks disclosures have touched every corner of the world. Now the whole world watches America and observes what it does; not what it says.
>
> President Obama was once a professor of constitutional law, and entered the national stage as an eloquent moral leader. The question now, however, is whether his conduct as Commander in Chief meets fundamental standards of decency. He should not merely assert that Manning's confinement is "appropriate and meet[s] our basic standards," as he did recently. He should require the Pentagon publicly to document the grounds for its extraordinary actions –and immediately end those which cannot withstand the light of day.

Obama cannot be a leader on human rights by refusing to challenge a military that, for years, used forced nudity like they're using with Manning as part of systemic abuse of alleged terrorists.

But that's what he has been doing.

DOD GIVES MANNING CAVEMAN GOWN, SAYS THEY'RE NOT HUMILIATING HIM

With all the attention focused on Bradley Manning's treatment yesterday because of PJ Crowley's ouster, DOD has done a lot of pushback on the notion that taking away Manning's underwear is "ridiculous, counterproductive, and stupid."

The pushback has been so effective that a number of journalists have reported that Quantico no longer takes Manning's underwear away.

So let's be clear: Quantico is still taking Manning's underwear away. But they have now given him a gown to wear.

Josh Gerstein did some actual reporting on these gowns. The more elaborate version is made of two layers of backpack grade cordura nylon.

> [Ferguson Safety Products founder Lana] Speer said her company's smocks are made out of a "backpack-type material that was the strongest stuff we could find that could be washed." She was also blunt about the items being far from fashionable.
>
> "It's stupid looking," Speer said.

No offense to Speer (whose concerns deal with genuinely suicidal people), but the picture Ferguson uses to advertise the smocks—with the caveman looking models—doesn't help make them look any less stupid.

While it's unclear whether Quantico is using this particular gown or not, one thing is clear: what Manning is forced to wear is not comfortable. Here's how he described it.

> After apparent outside pressure on the Brig due to my mistreatment, I was given a suicide prevention article of clothing called a “smock” by the guards. Although I am still required to strip naked in my cell at night, I am now given the “smock” to wear. At first, I did not want to wear this item of clothing due to how coarse it was and how uncomfortable it felt. However, the Brig now orders me to wear the “smock” at night.

So for those who have gotten confused by DOD’s pushback: they are still taking away Manning’s very dangerous boxers at night (though they allow him to wear such dangerous items during the day). And then, in a bid to pretend they’re not trying to drive Manning crazy, they basically make him sleep in an uncomfortable duffel bag-like garment.

WIKILEAKS REVEALS HOW THE BRITISH LIED TO OECD ABOUT BAE BRIBERY

A WikiLeaks cable dated March 5, 2007 has raised new interest in the BAE bribery scandal (AP, WSJ, Telegraph). While no one seems to have noted this, the cable shows that the British lied to their counterparts at the OECD about details of the bribery investigation into BAE.

As the Guardian (which led the reporting on this story) reported three years ago, the UK’s Serious Fraud Office started investigating evidence of an elaborate kickback system by which the Brits would give money to the Saudis

for BAE contracts in 2004 (it turns out those kickbacks were allegedly used to fund covert operations). In 2006, Prince Bandar bin Sultan flew to London and threatened Tony Blair the Saudis would stop sharing information on terrorists if the SFO continued its investigation. As a result, in early 2007, the SFO stopped its investigation, citing public interest. The US settled its investigation of the same bribery scheme for $400 million last year.

The cable appears to be preparation for the March 2007 OECD meeting of the Working Group on Bribery; it serves as a review of what had happened in the previous, January 2007, meeting regarding the British decision to stop its investigation of the BAE bribery scheme. Much of the cable reviews the stance of each country regarding the UK decision, with France vocally complaining that the British decision violated the Convention on bribery's prohibition on invoking relations with foreign countries as reason to spike a bribery investigation, and Australia fully supporting the UK decision. According to the cable, the American delegation was in between those two positions (they were basically arguing for putting off a conclusion about the appropriateness of the decision until the March meeting for which this cable served as preparation):

> The U.S. delegation took note of the experience and professionalism of U.K. delegation members. The US del inquired into what appeared to be inconsistent accounts relating to differences in views of the SFO Director and Attorney General regarding the merits of the case, reports alleging British intelligence agencies had not joined the government's assessment that the case raised national and international security interests, and whether the SFO could provide WGB members with assurances that BAE would not continue to make corrupt payments to senior Saudi

> officials.
>
> [snip]
>
> The U.S. delegation commented that it was not appropriate at this juncture to conclude that Article 5 does not contemplate the proper invocation of national security interests.

Ultimately, the cable reveals, the group developed a consensus to revisit the issue in the March meeting after further review of the British investigation.

The cable is perhaps most interesting because it gives us a glimpse of what the British publicly told the international community about its investigation, the targets, and the reasons for dropping the investigation.

The SFO Deputy Director falsely portrayed the decision to end the investigation as voluntary

Most interestingly, the cable shows that SFO Deputy Director Helen Garlick portrayed SFO Director Robert Wardle's decision to terminate the investigate as entirely voluntary.

> Garlick started by underscoring the U.K. delegation's willingness to answer as much as possible the questions of the WGB, bearing in mind pending litigation in the U.K. Garlick reported that SFO and MOD Police investigators had expended more than 2 million pounds sterling on the BAE investigations. She said on December 14, SFO Director Robert Wardle had decided to discontinue the joint SFO/MOD Police investigation based on his personal, independent judgment.

The French doubted this (I'm guessing they were suspicious partly because Wardle did not brief the group himself). Shortly after the January meeting, the Guardian reported that Wardle disagreed with Lord Goldsmith's ultimate decision to spike the investigation and in 2008

Wardle testified that he strongly disagreed with the decision.

> Wardle told the court in a witness statement: “The idea of discontinuing the investigation went against my every instinct as a prosecutor. I wanted to see where the evidence led.”

All of which suggests the French were right to doubt that Wardle made this decision himself.

The Brits may have kept Bandar bin Sultan’s role in the bribery scheme secret

In addition, tt appears that the Brits **may have** kept Bandar bin Sultan’s rule in the bribery scheme secret—though it may be, instead, that the cable didn’t record the details of the briefing pertaining to Bandar. The cable describes the Brits exhorting their partners to keep the contents of the briefing on the investigation classified.

> U.K. delegation head Jo Kuenssberg said the U.K. recognized the level of interest of WGB members in the case and stressed the need to respect the confidentiality of the information contained in the U.K.’s briefing,

And then, among the details revealed in the investigation, the Brits described an “unnamed senior Saudi official” and “another very senior Saudi official” as recipients of some of the bribes in the scheme.

> Third, payments made under the al-Yamamah contract to an unnamed senior Saudi official: Garlick advised that in October 2005, the SFO had demanded BAE produce documents including payments related to the al-Yamamah contract. The company made representations to the AG on public interest grounds (political and economic considerations) as to why the investigation should be halted. The

> AG undertook a Shawcross Exercise and sought representations from various British officials regarding the case. The SFO Director wanted to continue the investigation. On January 25, 2006, the AG agreed that there was no impediment to continuing the investigation. The SFO sought Swiss banking records regarding agents of BAE. The SFO found reasonable grounds that another very senior Saudi official was the recipient of BAE payments. The SFO was poised to travel to Switzerland in connection with its Mutual Legal Assistance (MLA) request when the decision to discontinue the investigation was made;

The cable explicitly named Turki Bin Nasir, then the head of Saudi Arabia's Air Force and already by that point publicly tied to the bribery scheme. So these two must be others. I'm guessing that Bandar—whose receipt of $1 billion via the scheme would be broken by the Guardian in June 2007—is the "very senior Saudi official" mentioned, not least because his involvement seems to have been exposed at the Swiss bank account stage of the investigation. So the only question, then, is whether the Brits kept his name—as they did the "unnamed senior Saudi official"—secret from their counterparts at the OECD. It appears, however, they did.

In addition, the British review of the investigation far underplayed the amount involved here.

CROWLEY: "THE IMPACT … FOR WHICH I TAKE

FULL RESPONSIBILITY”?

While a number of media outlets have reported one line—“The exercise of power in today’s challenging times and relentless media environment must be prudent and consistent with our laws and values”—from PJ Crowley’s resignation statement, I wanted to remark on a few things in the larger statement.

> The unauthorized disclosure of classified information is a serious crime under U.S. law. My recent comments regarding the conditions of the pre-trial detention of Private First Class Bradley Manning **were intended to highlight the broader, even strategic impact of discreet actions undertaken by national security agencies every day and their impact on our global standing and leadership**. The exercise of power in today’s challenging times and relentless media environment must be prudent and consistent with our laws and values.
>
> **Given the impact of my remarks, for which I take full responsibility**, I have submitted my resignation as Assistant Secretary for Public Affairs and Spokesman for the Department of State.
>
> I am enormously grateful to President Obama and Secretary Clinton for the high honor of once again serving the American people. I leave with great admiration and affection for my State colleagues, who promote our national interest both on the front lines and in the quiet corners of the world. It was a privilege to help communicate their many and vital contributions to our national security. And I leave with deep respect for the journalists who report on foreign policy and global developments every day, in many cases under dangerous conditions and subject to serious threats. **Their efforts help make governments more**

> **responsible, accountable and transparent**. [my emphasis]

Note, first of all, the sentence, "Given the impact of my remarks, for which I take full responsibility." That has been interpreted as a reaffirmation of Crowley's statement that DOD's treatment of Manning is "ridiculous, counterproductive, and stupid." But there's actually some ambiguity to the statement: the antecedent of "for which" could be "remarks," as has been interpreted, but it also could be "impact." Given that Crowley has spent years crafting public statements in which any ambiguity would lead to international incident, I suspect the ambiguity, in a written statement issued during a time of heightened attention, is intentional.

If so, this is Crowley making it clear he intended all this to blow up (remember, too, the participants in the MIT session at which Crowley first made his remarks double checked that his statements were on the record before they posted them).

And he tells us that his intent was to raise attention to the impact that certain actions of our national security agencies have on our international standing.

While I hope Crowley has an opportunity to explain precisely which actions he had in mind—aside from Manning's treatment, of course—I wanted to point to a CAP paper Crowley wrote in 2008, linked by Rortybomb. The paper as a whole is a sound strategy for counter-terrorism (I'm particularly fond of Crowley's focus on building resilience at home). As Rortybomb points out, Crowley argues that part of the fight against terrorism must be about remaining on the right side of history.

> Most of the world now believes, fairly or not, that America is on the wrong side of history. While the Bush administration acknowledged the vital

> importance of winning hearts and minds in its revised 2006 counterterrorism strategy, **too often since 2001, U.S. policies have neither matched our values, nor what we preach to the rest of the world. We are perceived, accurately or not, as operating secret and illegal prisons, condoning torture, denying legal rights, propping up autocratic regimes, and subverting fair elections**.
>
> [snip]
>
> More importantly, the United States and its allies need to drive a wedge between affiliated groups and broader communities More importantly, the United States and its allies need to drive a wedge between affiliated groups and broader communities. On this front, Al Qaeda is actually vulnerable. The vision of Islamic society that bin Laden propagates—his bridge to the seventh century—is not shared by the masses. In Iraq and elsewhere, Muslims have turned against bin Laden once they recognized that Al Qaeda's violent attacks largely victimize fellow Muslims.
>
> But turning the tide is simply not possible as long as the United States pursues its current strategy—**occupying Iraq, defending autocratic leaders such as Musharraf and violating international norms regarding torture and the treatment of detainees**. Such actions create the perception of grievance that opens the door to radical recruitment. The key is making this struggle more about Al Qaeda's actions than those of the United States. [my emphasis]

Three years ago, Crowley argued that our detainee policies hurt us in the fight against terrorism. Is it any surprise, then, that he just got himself fired for speaking out against

the treatment of Manning. (I suspect Obama's recent embrace of indefinite detention didn't help, either.)

But there's another section of Crowley's paper I find just as relevant—where he talks about the importance of transparency and rule of law.

> Restore Government Transparency and Recommit to the Rule of Law
>
> Terrorism, while a serious threat, does not require altering the fundamental relationship between the government and the American people. Even during the Cold War we did not succumb to our worst fears. We should continue to rely on constitutional standards that as Supreme Court Justice Anthony Kennedy put it in Hamdan v. Rumsfeld, "have been tested over time and insulated from the pressures of the moment."174
>
> U.S. courts have consistently demonstrated their ability to deal with complex terrorism cases, even those involving secret and sensitive information. **Rather than being a constraint, treating terrorism as primarily a criminal matter in fair and transparent legal proceedings adds to our political legitimacy at the terrorists' expense**.175
>
> A key objective should be preserving continuity of and public confidence in government at all levels. Unless the United States is under an overwhelming threat of additional attack, or the impact of an incident completely overwhelms local and state government, the federal response should be to support rather than supplant civilian authority, particularly at the local level.
>
> **Public access to information and open debate is not dangerous, but rather is the essence of democracy that we present**

> **to the world as the antidote to violent extremism**. The removal of large quantities of public information since 9/11 is counter-productive. Rather than provide information to attackers, excessive secrecy more likely inhibits the development of effective countermeasures.176
>
> An effective homeland security program may require wider governmental access to personal information, such as telephone calls and emails. But privacy protections must keep pace. Otherwise, perceived intelligence dots may actually be stray bullets that wrongly implicate ordinary citizens. [my emphasis]

With Crowley's reference to the importance of "public access to information" (from his paper) and his celebration of how journalists "help make governments more responsible, accountable and transparent," go back and read the longer transcript of his comment at MIT.

> PJC: "I spent 26 years in the air force. What is happening to Manning is ridiculous, counterproductive and stupid, and I don't know why the DoD is doing it. Nevertheless, **Manning is in the right place**." **There are leaks everywhere in Washington – it's a town that can't keep a secret. But the scale is different. It was a colossal failure by the DoD to allow this mass of documents to be transported outside the network**. Historically, someone has picked up a file of papers and passed it around – the information exposed is on one country or one subject. But this is a scale we've never seen before. If Julian Assange is right and we're in an era where there are no secrets, do we expect that people will release Google's search engine algorithms? The formula for Coca Cola? Some things are best kept secret. If we're negotiating between the

> Israelis and the Palestinians, there will be compromises that are hard for each side to sell to their people — there's a need for secrets.

Admittedly, only the Manning comments appear to be a direct quote. But directly after Crowley asserted that Manning is in the right place—effectively endorsing rule of law (as he did in his paper)—Crowley lays into DOD for allowing "this mass of documents" to be leaked. As I have noted, DOD had warning that SIPRNet had a amateurish vulnerability, its ready access to removable media, three years ago. In spite of promises the vulnerability would be permanently fixed for classified networks (that is, for SIPRNet), it failed to do so.

Crowley seems to forge a middle ground, implicitly acknowledging the importance of transparency and pointing to our lack of resiliency as one of the biggest problems with Manning's alleged leaks.

One of the things revealed by WikiLeaks is Department of State pressure on Egypt, under Clinton, to end its indefinite detention under military law. Of all the cables revealing US hypocrisy in its diplomatic affairs, those are the cables that really demonstrate to me how we have lost our moral standing.