COMPARE DOD'S AUTONOMY TO ENGAGE IN CYBER-WAR WITH OBAMA'S CLOSE CONTROL OVER DOD DRONE TARGETING

It will likely be some time, if ever, before one of our enemies succeeds at doing more than launching limited, opportunistic drone strikes at the US. By contrast, every day brings new revelations of how our enemies and rivals are finding new vulnerabilities in American cyber-defense.

Which is why it is so curious to compare this account of the multi-year process that has led to an expansion of DOD's authority to approve defensive cyber-attacks with this account of Obama's close hold on DOD's drone targeting.

In both cases, you had several agencies — at least DOD and CIA — in line to execute attacks, along with equities from other agencies like State.

> An interagency process had been started because cyber concerns confront a variety of agencies, the intelligence community and DoD as well as State, Homeland Security and other departments, with each expressing views on how the domain would be treated.

For much of Obama's term, it seems, both DOD drone attacks outside of the hot battlefield and cyberattacks had to be approved by the White House. With drones, Obama wanted to retain that control (over DOD, but not CIA) to prevent us from getting into new wars.

> But from the outset of his presidency, Obama personally insisted that he make

> the final decision on the military's kill or capture orders, so-called direct action operations. Obama wanted to assume the moral responsibility for what were in effect premeditated government executions. But sources familiar with Obama's thinking say he also wanted to personally exercise supervision over lethal strikes away from conventional battlefields to avoid getting embroiled in new wars. As responsibility for targeted strikes in places like Yemen, Somalia, and, over time, Pakistan shifts to the military's Joint Special Operations Command, Obama will be the final decider for the entire program.

With cyber, White House control was designed partly to limit blowback — almost the same purpose as his micromanagement of drone targeting — but also to mediate disputes between agencies.

> In every instance where cyber was involved, the NSC had to be involved. That helped settle some of the disputes between agencies by limiting any independent application of cyber capabilities, but was useful neither for expediting any cyber action nor for integrating cyber into larger military capabilities. Several sources said that this has slowed the integration of cyber into broader military tactics, possibly giving rivals without the same hesitation, like China, a chance to become more adept at military cyber.
>
> [snip]
>
> Because every decision had to be run through the West Wing, potential political blowback limited the use of cyber tools, the former senior intelligence official said. "If they can't be used without a discussion in the West Wing, the president's got no

> place to run if something goes wrong when he uses them," he said. Those decisions included what to do if the US confronted a cyberattack.

But over the course of the Obama Administration, DOD lobbied to increase its autonomy in both areas, in drones via the year-long process of crafting a drone rulebook, and with cyber, via the three year process of drafting new standing rules of engagement.

It had far more success in its efforts to expand autonomy with cyber.

With drone warfare, CIA pushed to let DOD have the same authorities to launch strikes without Presidential oversight that it had.

> Sources familiar with the process say no issue was more contentious than the question of what role the president should have in final killing decisions. The uniformed military, including the joint chiefs of staff, pushed to take the president out of the process. Once the president approved a particular battle plan in a country, individual targeting decisions should be left up to the regional commanders, they argued. Officials at the CIA, who had fought successfully to maintain control over its own targeting in the early days of the administration, backed the military.

But ultimately, Obama refused to expand DOD's autonomy to exercise the same autonomy that CIA already enjoys.

> A draft version of the new institutionalization policy, known informally as "the playbook," even contained the proposed change, the sources say. But after an intense counteroffensive by officials at the State Department and Justice Department, the status quo was restored. According

> to one official who participated in the discussions, it came down to a question of what level of accountability was required when the government was making grave killing decisions far from the traditional battlefield: “It didn’t make sense that while we were on the one hand raising the bar for these decisions, we would also remove the president from the decision-making chain.”

Contrast that with cyberwar, where in each of several reviews, DOD (specifically, General Keith Alexander, head of both NSA and CyberCommand) won greater autonomy, at least for defensive cyber responses.

> Not long afterward, that draft was rejected by a deputy of Gen. Keith Alexander, head of CYBERCOM and director of the National Security Agency, because it fell short of where “the SecDef wanted it to go,” said a former defense official.
>
> The problem was that the document didn’t allow for a sufficiently assertive response, the official added. In its efforts to achieve balance, the draft didn’t accommodate the strong stance the administration, and specifically CYBERCOM, wanted to take.
>
> So the rules were drafted again, designed to be “forward leaning,” permitting a stronger response. Once again they were rejected.
>
> [snip]
>
> According to the former defense official with knowledge of earlier drafts, the version on the verge of completion is “way far” from previous versions, authorizing far more assertive action than had been previously considered.

Perhaps this comparison is too strained. As described, at least, DOD will only have autonomy to engage in responses to cyber-attacks. With preemptive offensive attacks, the White House will remain in the loop.

To some level, the expected continuation of signature strikes in Pakistan, which inaccurately or not have been excused as a response to attacks on US troops stationed in Afghanistan, is similar to DOD's permission to engage in defensive counterattacks.

But the comparison is useful, I think. because it raises questions about where we should have in the past and should going forward be exercising closer oversight. I'm all in favor of sharply limiting the number of times we assassinate a human off the battlefield. But I also believe that cyber-war — even attacks billed as a counter response to an attack — have led to and will likely to lead to far more blowback even than drones.

With StuxNet we seem to have normalized a pretty aggressive bar for cyber-attacks. Each new example of doing so will, because of our extreme vulnerability, expose us to far more dangerous blowback.

TIME TO OUT THE CYBER-INSECURE DEFENSE CONTRACTORS

In its latest update on Chinese hacking of our defense programs, WaPo provides a list of defense programs that have been compromised, which includes many of our most important and error-prone programs.

> The designs included those for the advanced Patriot missile system, known

> as PAC-3; an Army system for shooting down ballistic missiles, known as the Terminal High Altitude Area Defense, or THAAD; and the Navy's Aegis ballistic-missile defense system.
>
> Also identified in the report are vital combat aircraft and ships, including the F/A-18 fighter jet, the V-22 Osprey, the Black Hawk helicopter and the Navy's new Littoral Combat Ship, which is designed to patrol waters close to shore.
>
> Also on the list is the most expensive weapons system ever built — the F-35 Joint Strike Fighter, which is on track to cost about $1.4 trillion. The 2007 hack of that project was reported previously.

WaPo also, having seen classified sections of a report that had previously been released in unclassified form, also places more emphasis on the potential impact not just of cybertheft, but cyber-sabotage, than it has in the past, basically pointing to this section of the report itself.

> The threats described in the previous section [which focus on sabotage at the microchip level] may impose severe consequences for U.S. forces engaged in combat:
>
> - *Degradation or severing of communication links critical to the operation of U.S. forces, thereby denying the receipt of command directions and sensor data*
> - *Data manipulation or*

> *corruption may cause misdirected U.S. operations and lead to lack of trust of all information Weapons and weapon systems may fail to operate as intended, to include operating in ways harmful to U.S. forces*
> - *Potential destruction of U.S. systems (e.g. crashing a plane, satellite, unmanned aerial vehicles, etc.).*
>
> At the national level, one could posit a large-scale attack on the U.S. critical infrastructure (e.g., power, water, or financial systems). An attack of sufficient size could impose gradual wide-scale loss of life and control of the country and produce existential consequences.

WaPo also provides a hint at our solutions and Chinese counter-responses. That is, as our prime contractors have become more adept at cyber-security, China has moved onto attack subcontractors.

> In an attempt to combat the problem, the Pentagon launched a pilot program two years ago to help the defense industry shore up its computer defenses, allowing the companies to use classified threat data from the National Security Agency to screen their networks for malware. The Chinese began to focus on subcontractors, and now the government is in the process of expanding the sharing of threat data to more defense contractors and other industries.

Yet the government won't take the obvious step of tying ongoing contracts to cyber-security, instead requiring only that contractors provide the government notice of cyber-attacks.

> An effort to change defense contracting rules to require companies to secure their networks or risk losing Pentagon business stalled last year. But the 2013 Defense Authorization Act has a provision that requires defense contractors holding classified clearances to report intrusions into their networks and allow access to government investigators to analyze the breach.

What's most interesting about all this, though, is that the report (at least the classified list the WaPo saw) didn't identify via which contractors in the supply chain China hacked these programs. But the US is not, apparently, keeping all of that information secret from China.

> U.S. officials said several examples were raised privately with senior Chinese government representatives in a four-hour meeting a year ago. The officials, who spoke on the condition of anonymity to describe a closed meeting, said senior U.S. defense and diplomatic officials presented the Chinese with case studies detailing the evidence of major intrusions into U.S. companies, including defense contractors.
>
> [snip]
>
> The list did not describe the extent or timing of the penetrations. Nor did it say whether the theft occurred through the computer networks of the U.S. government, defense contractors or subcontractors.

So if the government is sharing at least some

details of what it knows about China's hacks with China, then why is it keeping details about which contractors taxpayers are paying lots of money for cyber-attack induced rework to? Why can't it provide at least skeletal information about which contractors have let China compromise our security so much?

SOMEONE HACKED OUR MEMORY: "RETALIATION," "DETERRENCE," "ESCALATION"

The WSJ has a story developing on earlier WSJ and NYT reporting that someone — believed to be Iran — was using cyberattacks on energy companies in preparation to sabotage operations.

And while the WSJ responsibly includes a short paragraph noting that the US "has previously launched its own cyberattacks" on Iran to sabotage its nuke program, none of the people they interview seem to remember that we struck Iran first and that this should be regarded as retaliation to our own provocation, not vice versa.

> In response, U.S. officials warn that Iran is edging closer to **provoking U.S. retaliation**.
>
> "This is representative of stepped-up cyber activity by the Iranian regime. The more they do this, the more our concerns grow," a U.S. official said. "What they have done so far has certainly been noticed, and they should be cautious."

> [snip]
>
> Underscoring the Obama administration's growing concern, the White House held a high-level meeting late last month on how to handle the Iranian cybersecurity threat. No decisions were made at that meeting to take action, however, and officials will reconvene in coming weeks to reassess, a U.S. official said.
>
> "It's reached a really critical level," said James Lewis, a cybersecurity specialist at the Center for Strategic and International Studies, who frequently advises the White House and Capitol Hill. "We don't have much we can do **in response, short of kinetic warfare**."
>
> The Obama administration sees the energy-company infiltrations as a signal that **Iran hasn't responded to deterrence**, a former official said.
>
> In October, then-Defense Secretary Leon Panetta issued a veiled threat to Iran, which he did not name in his speech, by warning the Saudi Aramco hack represented a **dangerous escalation** in cyberwarfare. Since then, the Iranian attacks have only **ramped up**. [my emphasis]

One of the reasons we're likely left with little to do in response short of "kinetic warfare," of course, is we've already economically sabotaged Iran's economy with sanctions, gutting the already fewer targets we might hit to strike back. (Also, the countries that have exemptions to trade with Iran for oil likely would frown on any attempt on our part to further devastate Iran's energy sector.)

You'd think someone would have thought of this entirely predictable state of affairs before advising the most cyber-vulnerable nation on earth to pioneer the use of syberwar to sabotage

key infrastructure, huh?

THE SABOTAGE ATTACK ON THE SYRIAN COALITION

The NYT reports — adding to an earlier WaPo story — that hackers have attempted to sabotage a bunch of US energy companies.

> A new wave of cyberattacks is striking American corporations, prompting warnings from federal officials, including a vague one issued last week by the Department of Homeland Security. This time, officials say, the attackers' aim is not espionage but sabotage, and the source seems to be somewhere in the Middle East.

It ties these attacks to earlier attacks, claimed to have been launched by Iran, against ARAMCO and Qatar's RasGas.

> Two senior officials who have been briefed on the new intrusions say they were aimed largely at the administrative systems of about 10 major American energy firms, which they would not name. That is similar to what happened to Saudi Aramco, where a computer virus wiped data from office computers, but never succeeded in making the leap to the industrial control systems that run oil production.
>
> [snip]
>
> At Saudi Aramco, the virus replaced company data on thousands of computers with an image of a burning American flag. The attack prompted the defense

> secretary at the time, Leon E. Panetta, to warn of an impending "cyber 9/11" if the United States did not respond more efficiently to attacks. American officials have since concluded the attack and a subsequent one at RasGas, the Qatari energy company, were the work of Iranian hackers. Israeli officials, who follow Iran closely, said in interviews this month that they thought the attacks were the work of Iran's new "cybercorps," organized after the cyberattacks that affected their nuclear facilities.
>
> Saudi Aramco said that while the attackers had attempted to penetrate its oil production systems, they had failed because the company maintained a separation between employees' administrative computers and the computers used to control and monitor production. RasGas said the attack on its computers had failed for the same reason.

And while the adoption of earlier sabotage approach used with ARAMCO and RasGas infrastructure to US energy producers does not mean all members of the coalition to topple Bashar al-Assad have been attacked by an entity insinuated to be Iran (unless the European parters' energy companies have been attacked and we just don't know about it). But this attack does seem to be an assault on the coalition trying to undercut Iran by taking down its client regime in Syria.

Which has me wondering whether this is an Iranian attack — revenge, if you will, for StuxNet, serves the US right. Or if it's an attack launched by a coalition, possibly including Russia.

I also wonder whether the point of the sabotage isn't on the information side of the equation, rather than the operational one.

In other news, remember how former NSA head and all-around cyberwar profiteer Mike McConnell declared digital 9/11 warning based on the ARAMCO attack and some crude DNS attacks on banks here in the US? Guess who has become a player in Saudi (and Gulf generally) cybersecurity?

> During this event, Booz Allen Hamilton leadership shared their insights on global cyber security practices and the importance of a cross-border cooperative approach to protecting critical infrastructure in the Gulf.
>
> Commenting at the event, McConnell said, "The GCC states have become global hubs in finance. However, this growth introduces increased cyber security risks by threat actors who target this region for monetary or political gain. GCC states have already experienced significant cybercrime in the recent past, it is now more important than ever to ensure that these are not repeated."
>
> He also added, "Financial institutions are a prime target for cyber criminals, and as a result, they need to focus on staying ahead of cyber threats by developing the right human capital, developing appropriate training programmes and retaining the right skills and technology to properly access and protect corporate data."
>
> **Booz Allen Hamilton was recently registered by the Kingdom of Saudi Arabia Ministry of Commerce and Industry to pursue business opportunities in the Kingdom in support of domestic economic diversification**. The firm will provide services to government and commercial clients on critical issues related to the Kingdom's development, most notably in the areas of cyber security, information technology, financial

> services and other selected infrastructure. [my emphasis]

I'm guessing BAH's work in KSA has a lot to do with the expanded Technical Cooperation Agreement signed with the US in January, which added a cyber component onto the previous effort to create a 35,000 person security force Mohammed bin Nayef could use to protect the kingdom's oil infrastructure.

So if you're bummed that BAH gets to troll American networks with abandon, rest assured that it will now be doing so in Saudi Arabia, too.

SHELDON WHITEHOUSE: CYBERTHEFT IS [MAY BE] BIGGEST TRANSFER OF WEALTH IN HISTORY

In an attempt to scare Congress into passing the cybersecurity legislation they failed to pass last year, Sheldon Whitehouse scheduled a hearing on cybersecurity today. In the hearing — and in this op-ed he penned with Lindsey Graham — he repeated a claim he has made before: cybertheft may be the biggest "illicit" transfer of wealth in history.

> Almost every facet of American life is threatened when intruders exploit our cyber-vulnerabilities. And the risk is not from China alone. Foreign governments such as Iran and terrorist groups such as al-Qaida seek to worm into national infrastructure and threaten catastrophe here at home. Foreign agents raid companies, stealing plans, formulas and designs. Foreign

> criminal networks take money out of banks, defraud consumers with scams and sell illicit goods and products, cheating U.S. manufacturers. **It may be the greatest illicit transfer of wealth in history**. [my emphasis]

I think in the hearing itself, Whitehouse wasn't as careful to always use that word "might."

The greatest illicit transfer of wealth in history.

Don't get me wrong: cyberattacks of all sorts are a real threat. They cost consumers a great deal of inconvenience and, at times, lots of money. They cost defense contractors far more (though of course, some of that is built into our model of defense). They cost sloppy companies as well.

But the biggest illicit transfer of wealth in history?

Ignore recent unpunished giant transfers of wealth in the wake of the financial crisis, which the Senate Judiciary Committee has largely ignored.

I guess the reason I find this so stunning is all the obviously huge transfers of wealth it ignores that were part of slavery and colonization.

Were those licit?

Those were, like Chinese or Iranian or Russian cyberattacks on the US, examples of states (and private entities) taking advantage of vulnerabilities elsewhere. They were certainly considered legitimate at the time, because Europeans got to write the history of colonization, and because they made up claptrap about "civilization" to justify it. But from a distance they look more like the kind of exploitation states often engage in if they've got an obvious advantage over another state or organization.

All that's not to say Montezuma shouldn't have resisted the Spaniards. That's not to say we shouldn't defend against cyberattacks.

But what really makes the US so vulnerable to cyberattacks are 1) that we're so reliant on the Internet and 2) we're so reliant on intellectual property (indeed, the very claim that cybertheft is the biggest transfer of wealth relies on a certain understanding of IP as wealth that itself depends on a legal infrastructure that is contingent on our relative world power). And also that so much of our critical infrastructure and IP holders are in private hands and therefore much harder to demand diligence from. That is, our vulnerability to cyberattacks is in part a fragility of our own bases for power (a vulnerability that will probably end up being less lethal than the fact that the immune systems of indigenous peoples hadn't been exposed to European diseases).

Also, this entire discussion — which danced around the question of an international regime that might limit such attacks — completely ignored the StuxNet attack, the fact that a nation as vulnerable as we are pushed the limits of the offensive capability first. One of the witnesses (I think FBI Assistant Director Jonathan Demarast) even suggested that if our government were chartered to attack the private sector (cough, Echelon) of other countries we'd be damn good at it too — as if our attacks on the public infrastructure of Iran doesn't count.

I get the value of a good fear campaign (I wish Whitehouse would fearmonger more in his regular addresses on climate change). But there's fearmongering and there's absurdity. And I think suggesting that cybertheft is worse than the stealing of entire continents is the latter.

STEPHEN CAMBONE, HACKER PWN, USED TO HEAD DOD'S "INTELLIGENCE"

Stephen Cambone was the first ever Under Secretary of Defense for something called "Intelligence."

In that role, he oversaw a domestic spying program that targeted hippies and made GOP cronies rich. And then he went on to profit off that domestic spying program at a company called QinetiQ.

Which is why I'm having a hard time summoning much grief that Chinese hackers have pwned another US Defense Contractor — none other than QinetiQ (George Tenet, another noted "intelligence" figure, was there until 2008)!

Here are the kinds of things the hackers accessed, almost unimpeded.

> The lengthy spying operation on QinetiQ jeopardized the company's sensitive technology involving drones, satellites, the U.S. Army's combat helicopter fleet, and military robotics, both already-deployed systems and those still in development, according to internal investigations.

And here is the kind of access QinetiQ allowed both Chinese and Russian hackers.

> In 2008, a security team found that QinetiQ's internal corporate network could be accessed from a Waltham, Massachusetts, parking lot using an unsecured Wi-Fi connection. The same investigation discovered that Russian hackers had been stealing secrets from QinetiQ for more than 2 1/2 years through a secretary's computer, which

> they had rigged to send the data directly to a server in the Russian Federation, according to an internal investigation.

Read the whole thing — you won't know whether to laugh or cry.

Meanwhile, the government seems more intent on violating my privacy to fix this kind of wholesale hacking, rather than blackballing those contractors who are incapable of securing their networks.

> The State Department, which has the power to revoke QinetiQ's charter to handle restricted military technology if it finds negligence, has yet to take any action against the company.
>
> [snip]
>
> In May 2012, QinetiQ received a $4.7 million cyber-security contract from the U.S. Transportation Department, which includes protection of the country's critical transport infrastructure.

The same company that let China hack at will for years is being paid millions for cybersecurity.

That about says it all.

HACKERS PENETRATE FREEDOM; THE SHIP HAS ALREADY SAILED

Reuters has a report I found sort of punny, about how white hat hackers had managed to break into the computer systems of the lead ship of the Navy's Littoral Combat Ship program, the USS

Freedom.

> A Navy team of computer hacking experts found some deficiencies when assigned to try to penetrate the network of the USS Freedom, the lead vessel in the $37 billion Littoral Combat Ship program, said the official, who spoke on condition of anonymity.
>
> The Freedom arrived in Singapore last week for an eight-month stay, which its builder, Lockheed Martin Corp., hopes will stimulate Asian demand for the fast, agile and stealthy ships.

It may be ironic that Lockheed had a ship get hacked just before it sent the ship out on a sales trip to Asia. (Asia! Where our most fear hacking-rival is!)

But … um, Lockheed?

Lockheed, of course, couldn't keep the F-35 program safe from hackers either, and that time it wasn't white hats doing the hacking.

Before the government imposes fines for companies unwilling to sacrifice the security of their systems to program in a backdoor, as the WaPo reports is being debated …

> A government task force is preparing legislation that would pressure companies such as Facebook and Google to enable law enforcement officials to intercept online communications as they occur, according to current and former U.S. officials familiar with the effort.
>
> [snip]
>
> Susan Landau, a former Sun Microsystems distinguished engineer, has argued that wiring in an intercept capability will increase the likelihood that a company's servers will be hacked. "What you've done is created a way for someone to silently go in and activate a wiretap,"

> she said. Traditional phone communications were susceptible to illicit surveillance as a result of the 1994 law, she said, but the problem "becomes much worse when you move to an Internet or computer-based network."
>
> Marcus Thomas, former assistant director of the FBI's Operational Technology Division, said good software coders can create an intercept capability that is secure. "But to do so costs money," he said, noting the extra time and expertise needed to develop, test and operate such a service.

… Maybe we ought to instead focus on Lockheed's apparent inability to keep the hundreds of billion dollar weapons systems it produces safe from hackers?

A PARTIAL DEFENSE OF BILL KELLER'S COLUMN ON MANNING

Late Sunday, former New York Times Executive Editor Bill Keller put up an op-ed column at the NYT website on the state of Bradley Manning's case, his perception of Manning's motivations and what may have been different had Manning actually gotten his treasure trove of classified information to the Times instead of WikiLeaks. The column is well worth a read, irrespective of your ideological starting point on Mr. Manning.

Bradley Manning has ardent supporters and, predictably, they came out firing at Keller. Greg Mitchell immediately penned a blog post castigating Keller for not sufficiently understanding and/or analyzing the Manning/Lamo chat logs. Kevin Gosztola at Firedoglake also

had sharp words for Keller, although, to be fair, Kevin did acknowledge this much:

> It is an interesting exercise for Keller. Most of what he said is rational and, knowing Keller's history, he could have been more venerating in his description of how the Times would have handled Manning.

Frankly, many of the points Mitchell and Gosztola made, which were pretty much representative of a lot of the chatter about Keller's op-ed on Twitter, were fair criticism even if strident. And part of it seems to simply boil down to a difference in perspective and view with Keller, as evidenced in Keller's response to inquiry by Nathan Fuller, where he indicates he simply views some things differently.

This is all healthy give and take, difference in view and sober discussion by the referenced individuals. That cannot, however, be said to be the case with a journalist on Twitter by the name of Greg Palast. Palast blasted out this tweet early this morning:

> NY Times' Keller says Manning should get prison time for the stories published by the Times! As a reporter, this makes me puke.

Palast's comment is patently duplicitous. Keller said nothing of the sort in his op-ed and a read of his piece will prove that. In fact, the closest comment to sentencing recommendations Keller got was an indication that the NYT would, as they did with Daniel Ellsberg, be pleased if any prosecution of Manning failed. I wonder if Mr. Palast even bothered to read Keller's op-ed before firing off his scurrilous missive? I tried asking him on Twitter, but without any meaningful response. Either way, it does neither Mr. Manning, nor his greater cause, any favors for supporters like Palast to engage in such

patently false statements.

Which brings me to the real point of this post: Despite the quite arguable validity of many of the critiques of Bill Keller's column, as noted above, there was also actually much to like for Manning supporters. Keller stated:

> First of all, I can say with some confidence that The Times would have done exactly what it did with the archive when it was supplied to us via WikiLeaks: assigned journalists to search for material of genuine public interest, taken pains to omit information that might get troops in the field or innocent informants killed, and published our reports with a flourish. The documents would have made news — big news.

Establishing that much of the same result would have occurred with a traditional news outlet as did with WikiLeaks is key to mitigation in Manning's case, whether in the case in chief as to the espionage charge, or in sentence mitigation. But Keller went yet a step further and placed WikiLeaks within the same journalistic First Amendment sphere as the New York Times:

> But if Manning had been our direct source, the consequences might have been slightly mitigated. Although as a matter of law I believe WikiLeaks and The New York Times are equally protected by the First Amendment, it's possible the court's judgment of the leaker might be colored by the fact that he delivered the goods to a group of former hackers with an outlaw sensibility and an antipathy toward American interests. Will that cost Manning at sentencing time? I wonder.

Granted, Keller could have omitted the

gratuitous editorializing as to the nature of the WikiLeaks organization (it really was unnecessary), but the firm statement on the journalistic equivalence under First Amendment consideration is important for both Manning and any future consideration by the government as to prosecution of WikiLeaks and/or Julian Assange. It is an extremely important concept for both the DOJ and Judge Lind to see and understand, and for Keller and the NYT to print in the "paper of record".

Lastly, Keller blasted the espionage charge levied at Manning and his deplorable initial confinement conditions:

> Once he was arrested, we'd surely have editorialized against the brutality of his solitary confinement — as The Times has already done — and perhaps protested the disturbing overkill of the "aiding the enemy" charge. (If Manning's leak provided comfort to the enemy, then so does every news story about cuts in defense spending, or opposition to drone strikes, or setbacks in Afghanistan.)

Disturbing overkill of the "aiding the enemy charge" indeed. That is exactly right and, again, it is important that Keller and the NYT are on record taking this position. Mr. Manning will not be facing a jury, his fate is in the hands of the government and Judge Denise Lind. It seems unlikely at this point that the government will reconsider the imposition of said charge, but there is time between now and the conclusion of trial to change that. A voice like Keller's, and the Times, is large in making that argument.

So, while commenters like Kevin Gosztola, Greg Mitchell, and most others, were right to take issue with some of Keller's op-ed, not to mention that Keller did occasionally engage in gratuitous editorializing that weakened his overall effect, there were several powerful positives that came out as well. The criticism

is more than fair, but a measure of credit is also due.

WONDERING WEDNESDAY: SUICIDE IN SINGAPORE, DRONE OVER BROOKLYN, AND TELCO TATTLERS

Help me get over the hump and clue me in on a few things. I've been scratching my head wondering about these topics.

Suicide in Singapore – The recent "suicide" of a U.S. electronics engineer in Singapore looks fishy to me. It looked not-right to Financial Times as well; it appears no other domestic news outlet picked up this case for investigative reporting before FT. The deceased, who'd worked for a government research institute on a project related to Chinese telecom equipment company Huawei, is alleged to have hung himself, but two details about this case set off my hinky meter.

- Every photo I've seen of engineer Shane Todd depicts a happy chap. Sure, depressed folks can hide their emotions, but comparing a photo of his family after his death to photos of him and you'll see the difference. My gut tells me that if he was truly depressed, he should have looked more like his folks—flat, withdrawn, low affect. Perhaps meds could have messed with his head more than depression itself. But I'm not a psychologist or a pharmacologist, what do I know?

- Among all the details of the case, it's said the victim's face postmortem was white when his body was discovered. This doesn't strike me as consistent with hanging; there should have been

lividity above the ligature. Conveniently, Singapore's law enforcement cleaned everything up so quickly there was no chance to see the crime scene or the body as found. Law enforcement also snagged the victim's laptop and all other work-related stored content, save for a hard drive that looked like a speaker. Everything he was working on "disappeared" except for the contents of that drive.

The engineer had been very concerned about technology he was working on and its possible transfer, which included gallium nitride transistors with potential for both commercial and military applications. After poking around for some time on gallium compounds used in various computing, communications and other technology, nothing screams at me as highly sensitive technology that might get someone "suicided." But…as I went through abstracts, it seems odd there are a substantive number of Chinese researchers working in on GaN-based technologies.

Thought these two points in particular jar my senses, more than just these two points don't sit well. Read the story at the link above and see for yourself. (Original FT link here.)

What do you make of this case? Suicide or no? Strategic technology or no?

Drone over Brooklyn – On Tuesday an Alitalia pilot reported an unmanned craft flying within 200 feet of his plane over Brooklyn. Both the FBI and FAA are investigating and have asked for witnesses' help. As of this post, there's been no additional information published about this incident.

Was this the first case where drone usage preceded adequate regulation about their usage? Was this simply a consumer product like the AR Parrot drone gone astray? Or was there something more sinister at work?

If you've heard anything more on this situation, please share in comments.

Telco Tattlers — Voice carriers Verizon and AT&T complain that they are unfairly targeted by new cybersecurity requirements; the two businesses claim technology companies like Google, Apple, and Microsoft should be subjected to the same regulations.

With all three of Google, Apple, and Microsoft in some way involved with voice-related technologies using their operating systems, one has to wonder why they weren't included as well as other similar technology companies.

BUT…perhaps it's because none of these technology companies has nationwide network infrastructure with NSA-furnished secret rooms attached (that we know of)—rooms that terrorists could otherwise access OR be used to shut down telecommunications networks in case of a cyber attack.

Why do you think there's such an exclusion of consumer-facing technology companies?

Okay, your turn. Go ahead, wonder away.

DOD USES SEQUESTER TO EXCUSE 5 YEAR DELAY IN IMPLEMENTING BASIC NETWORK SECURITY

More than 22 months ago, I wrote a post analyzing Congressional testimony describing the gaping holes in DOD network security 3 years after a nasty malware infection and a year after the publication of Collateral Murder by WikiLeaks.

Almost two years later, Assistant Secretary of Defense Zachary Lemnios says sequestration might

hold up improving network security on classified and unclassified networks.

> Zachary J. Lemnios, the assistant secretary of defense for research and engineering, was asked by Sen. Rob Portman (R-Ohio) to describe the "most significant" impacts on cybersecurity that could follow from the anticipated cuts to the Pentagon's budget.
>
> Mr. Lemnios replied that "cuts under sequestration could hurt efforts to fight cyber threats, including […] improving the security of our classified Federal networks and addressing WikiLeaks."

This is news not just for the specific details offered about how bad DOD's network security remains (click through for more details). But also for the tacit admission that 3 years after a breach DOD considers tantamount to aiding the enemy, and 5 years after a malware infection that badly affected DOD's networks in Iraq, DOD still hasn't completed security enhancements to its networks.