DIFI ADMITS SHE OKAYED UNLEASHING 21ST CENTURY WMD WITH INADEQUATE DETAILS

The reason Dianne Feinstein is so torqued about the StuxNet story, according to this SFChron piece, is because she learned things from it that she didn't know as a Gang of Four member.

> Feinstein declared, "This has to stop. When people say they don't want to work with the United States because they can't trust us to keep a secret, that's serious."
>
> A week later, Feinstein is more than halfway through New York Times reporter David E. Sanger's book, "Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power." She told me Wednesday, "You learn more from the book than I did as chairman of the intelligence committee, and that's very disturbing to me."

Now, as a threshold matter, I think DiFi and others are underestimating how much our foreign partners are leaking on these stories; not only did foreign sources serve as early confirmation on UndieBomb 2.0, but the Saudis and Yemenis exposed the last infiltrator the Saudis put into AQAP. And as for StuxNet, the Israelis are now complaining that Sanger didn't give them enough credit.

> The Israeli officials actually told me a different version. They said that it was Israeli intelligence that began, a few years earlier, a cyberspace campaign to damage and slow down Iran's nuclear intentions. And only later they managed

> to convince the USA to consider a joint operation — which, at the time, was unheard of. Even friendly nations are hesitant to share their technological and intelligence resources against a common enemy.

Plus, if and when Israel bombs Iran and has to deal with the retaliation, I can assure you the Israelis will be happy to work with us.

And there's a far bigger problem here. DiFi was not a Gang of Four member when this program started under Bush (Jay Rockefeller would have been the Democrat from the Senate Intelligence Committee). But she seems to say she got what passed for briefing on StuxNet.

Yet she's learning new details from Sanger.

StuxNet is, both because it can be reused by non-state actors and because of the ubiquity of the PLCs they affected, the 21st Century version of a WMD. And all that's before we learned Flame was using Microsoft's update function.

Now from the sounds of things, DiFi never had the opportunity to authorize letting StuxNet free; the Israelis don't have to brief the Gang of Four. But the possibility StuxNet would break free on its own always existed. One reason we have Congressional overseers is to counterbalance spooks whose enthusiasm for an op might cloud any judgment about the wisdom of pursuing that op.

The US, in partnership with Israel, released a WMD to anyone who could make use of it. And the people in charge of overseeing such activities got fewer details about the WMD than you could put in a long-form newspaper article.

And DiFi thinks there's too little secrecy?

SHELDON ADELSON COULD BUY BIBI A VERY EFFECTIVE OCTOBER SURPRISE

The Internet is abuzz today with Sheldon Adelson's announcement that he has already donated $10 million to Mitt Romney's SuperPAC and plans to provide limitless donations to defeat Obama.

> Forbes has confirmed that billionaire Sheldon Adelson, along with his wife Miriam, has donated $10 million to the leading Super PAC supporting presumptive Republican presidential nominee Mitt Romney—and that's just the tip of the iceberg. A well-placed source in the Adelson camp with direct knowledge of the casino billionaire's thinking says that further donations will be "limitless."

But the attention is mostly focused on the sheer numbers he's talking about, not what it suggests that Adelson—who already spent buckets of money to try to defeat Mitt in the primary—has now promised limitless donations to defeat Obama.

This is about Likud trying to decide the American elections.

Adelson doesn't hide the fact that this donation is about Israel as much as it is Obama's "socialism."

> Adelson, this source continues, believes that "no price is too high" to protect the U.S. from what he sees as Obama's "socialization" of America, as well as securing the safety of Israel. He added that Adelson, 78, considers this to be the most important election of his lifetime.

Nor is it surprising he's doing this. More than he is for any of these American politicians, Adelson is Bibi Netanyahu's Sugar Daddy. And Obama has been remarkably successful thus far in stymying Bibi's goal of forcing the US to attack Iran. In addition to the sanctions regime that has brought about negotiations, in recent months, the Administration has leaked both a white paper showing that an Iran attack would do nothing but set off a regional war and news of the bases in Azerbaijan Israel would use if it unilaterally attacked Iran. David Sanger quoted Presidential briefers and Joe Biden—Bibi's old nemesis—blaming Israel for freeing StuxNet, possibly intentionally. Leon Panetta has, on the record, told the entire world, including Iran, when Israel planned to attack. (I actually thought Panetta's latest 60 Minutes appearance might have been an attempt to placate Israel.)

It may appear to us that the Administration continues typical American policy of capitulating to Israel. But the Obama Administration has taken surprisingly strong measures to push back against Israel.

And now Sheldon Adelson has promised to use unlimited funds to get rid of President Obama.

As much as the money concerns me, that's not what I worry about the most. The Israelis have never been shy about running off-the-books operations to influence our policies. Indeed, they played a role in Iran-Contra, the start of which goes back to the last October Surprise plot to make sure a Democrat didn't get reelected in 1980. And the state of affairs in Israel's neighborhood (both Syria and Egypt would be excellent candidates, though if I were Turkey I'd be cautious, too) is such that it would be very very very easy to create an October Surprise that would make it a lot harder for Obama to get reelected.

Bibi's Sugar Daddy just announced the world he will do anything in his power to defeat Obama. You can be sure Bibi feels the same way.

Update: Iran/Israel confusion fixed, h/t vl.

"THE YEMENI SITUATION AND … THE IRANIAN CYBER SITUATION"

As MadDog noted yesterday, Dianne Feinstein seemed to answer a question I've written about here and here regarding the scope of the leak investigations.

> She said the U.S. attorneys would not face political pressures from the Obama administration and would "call the shots as they see them."
>
> "We can move ahead much more rapidly," Feinstein said. "Instead of one special prosecutor, you essentially have two here, one is the Yemeni situation and the other is the Iranian cyber situation. I think you're going to get there much quicker."

I'm not sure I agree with MD, though, that "the UndieBomb 2.0 and the Stuxnet leaks are the ones being investigated," meaning implicitly that just those two "leaks" are being investigated.

DiFi's quote seems to confirm that there is a distinct investigation into the source of the detail (one of the only new parts of David Sanger's StuxNet reporting) that Israel let StuxNet free, possibly deliberately. Since Eric Holder suggested there was a jurisdictional component to his choice of US Attorneys on these investigations, we can assume that Rod Rosenstein, US Attorney for the National Security Agency, will investigate that alleged leak.

But what does DiFi include when she says, "the

Yemeni situation”? Does it include only the leaks about UndieBomb 2.0? And if so, why isn’t it being investigated out of Eastern District of VA, the CIA’s US Attorney district, which purportedly had a lead on that operation in the US?

Further, MD suggested (though did not say explicitly) this means they’re not investigating the drone targeting leaks.

Now, as I’ve noted, one possible reason they wouldn’t investigate the drone targeting “leaks” would be if the stories reported falsehoods or—more charitably—a drone targeting process that was no longer in place, as the AP has reported to be the case and the White House, in their response to the AP story, seemed to confirm. That is, one possible reason why they wouldn’t investigate the “leaks” about drone targeting would be because those stories did not report accurate classified information (and I’ll remind here that the Klaidman story differs in some notable ways from the Joby Warrick story, which we now know came in part from Rahm Emanuel’s effort to publicize Baitullah Mehsud’s killing).

But there’s another possibility. I’m struck by DiFi’s description of “the Yemeni situation” rather than—as most people refer to it—the “thwarted” bomb “plot.” It’s possible that in DiFi’s mind—the mind of a Gang of Four member who has presumably been briefed on our ongoing operations in Yemen—that the leak of the bomb sting, the leak of the Saudi role in it, and the stories that made it clear that John Brennan is running a secret war against Yemeni insurgents using signature strikes out of the NSC largely at the behest of the Saudis all constitute for her “the Yemeni situation.” UndieBomb 2.0 is a part of that secret war—perhaps the legal justification for US involvement in it (and also a useful way to remove an asset and a key handler before the drones start wreaking havoc). But if this speculation is right, it may well be the other details—the report that this war is

being run out of NSC, the details that make it clear we're targeting insurgents, not just AQAP, the fact that we're clearly in an undeclared war—that DiFi worries about most.

Mind you, this is all supposition. It may be that DiFi was just using shorthand for the UndieBomb 2.0 plot. But to a great degree, all the stories about drone targeting were efforts to expose—and then cover up—the war we're engaging in Yemen. And that does seem like a secret the Administration is trying to prevent the American public from learning about.

STUXNET: COVERT OP-EXPOSING CODE IN, COVERT OP-EXPOSING CODE OUT

In this interview between David Sanger and Jake Tapper, Sanger makes a striking claim: that he doesn't know who leaked StuxNet.

> I'll tell you a deep secret. Who leaked the fact? Whoever it was who programmed this thing and made a mistake in it in 2010 so that the bug made it out of the Natanz nuclear plant, got replicated around the world so the entire world could go see this code and figure out that there was some kind of cyberattack underway. I have no idea who that person was. It wasn't a person, it wasn't a person, it was a technological error.

At one level, Sanger is just making the point I made here: the age of cyberwar may erode even very disciplined Administration attempts to cloak their covert operations in secrecy. Once StuxNet got out, it didn't take Administration

(or Israeli) sources leaking to expose the program.

But I'm amused that Sanger claims he doesn't know who leaked the information because he doesn't know who committed the "technological error" that allowed the code to escape Natanz. I find it particularly amusing given that Dianne Feinstein recently suggested Sanger misled her about what he would publish (while not denying she might call for jailing journalists who report such secrets).

> What you have are very sophisticated journalists. David Sanger is one of the best. I spoke—he came into my office, he saw me, we've worked together at the Aspen Strategy Institute. He assured me that what he was publishing he had worked out with various agencies and he didn't believe that anything was revealed that wasn't known already. Well, I read the NY Times article and my heart dropped because he wove a tapestry which has an impact that's beyond any single one thing. And he's very good at what he does and he spent a year figuring it all out.

Sanger claims, now that DiFi attacked him, he doesn't know who made this "technological error."

But that's not what he said in his article, as I noted here. His article clearly reported two sources—one of them a quote from Joe Biden—blaming the Israelis.

> An error in the code, they said, had led it to spread to an engineer's computer when it was hooked up to the centrifuges. When the engineer left Natanz and connected the computer to the Internet, the American- and Israeli-made bug failed to recognize that its environment had changed. It began replicating itself all around the world.

> Suddenly, the code was exposed, though its intent would not be clear, at least to ordinary computer users.
>
> "We think there was a modification done by the Israelis," one of the briefers told the president, "and we don't know if we were part of that activity."
>
> Mr. Obama, according to officials in the room, asked a series of questions, fearful that the code could do damage outside the plant. The answers came back in hedged terms. Mr. Biden fumed. "It's got to be the Israelis," he said. "They went too far."

And even though Sanger calls this code an "error," the quotations he includes show that the President's briefer and Joe Biden believe it was not an error at all.

In this post, I suggested that the Israelis coded StuxNet to escape, without telling the Americans, so as to undermine American attempts to occupy them with cyberwar to prevent hot war. That is, the implication of Sanger's article (which he now seems to be trying to retract) is that the Israelis deliberately exposed our cyberwar attack so as to make it more likely they could start a war with Iran.

But there is a far more ominous possibility. The Russians, based on analysis they did at Iran's Bushehr nuclear plant, have claimed StuxNet might have—and still might—cause Bushehr to explode, effectively setting off a nuclear bomb using code.

Is DiFi so angry at Sanger because he ham-handedly revealed that the Israelis deliberately turned StuxNet into a potential WMD?

GANG WARFARE TO PROTECT ISRAEL'S SECRETS

Easily the most overlooked line in David Sanger's story on StuxNet is this one:

> Mr. Obama concluded that when it came to stopping Iran, the United States had no other choice.
>
> If Olympic Games failed, he told aides, there would be no time for sanctions and diplomacy with Iran to work. Israel could carry out a conventional military attack, prompting a conflict that could spread throughout the region.

It's a sentiment he repeats in this worthwhile interview:

> FP: There haven't been thoughtful discussions about the consequences or the ethics or the international legal ramifications of this approach. Let's imagine for a moment that you're [Iranian President] Mahmoud Ahmadinejad and you are confronted with this. Isn't your first reaction, "How is them blowing up Natanz with a code any different from them blowing up Natanz with a bomb? And doesn't that justify military retaliation?"
>
> DS: Blowing it up with computer code, rather than bombs, is different in one big respect: It very hard for the Iranians in real time to know who the attacker was, and thus to make a public case for retaliating. It takes a long time to figure out where a cyber attack comes from.
>
> That was a big reason for the U.S. and Israel to attack Natanz in this way. But it wasn't the only reason, at least from

> the American perspective. One of the main driving forces for Olympic Games was to so wrap the Israelis into a project that could cripple Natanz in a subtle way that Israel would see less of a motivation to go about a traditional bombing, one that could plunge the Middle East into a another war. [my emphasis]

A key purpose of StuxNet, according to Sanger, was not just to set back the Iranian nuke program. Rather, it was to set back the nuke program in such a way as to set back Israel's push for war against Iran.

With that in mind, consider the way the article blamed the Israelis for letting StuxNet escape.

> An error in the code, they said, had led it to spread to an engineer's computer when it was hooked up to the centrifuges. When the engineer left Natanz and connected the computer to the Internet, the American- and Israeli-made bug failed to recognize that its environment had changed. It began replicating itself all around the world. Suddenly, the code was exposed, though its intent would not be clear, at least to ordinary computer users.
>
> "We think there was a modification done by the Israelis," one of the briefers told the president, "and we don't know if we were part of that activity."
>
> Mr. Obama, according to officials in the room, asked a series of questions, fearful that the code could do damage outside the plant. The answers came back in hedged terms. Mr. Biden fumed. "It's got to be the Israelis," he said. "They went too far."

After having explained that the whole point of StuxNet was to stop the Israelis from bombing

Iran, the article then goes on to say that what alerted the Iranians to StuxNet's presence in their systems—and effectively gave a very dangerous weapon to hackers around the world—was an Israeli modification to the code.

The Israelis went too far.

Those details are, IMO, some of the most interesting new details, not included the last time David Sanger confirmed the US and Israel were behind StuxNet on the front page of the NYT.

How very telling, then, that of all the highly revealing articles that have come out during this Administration—of all of the highly revealing articles that have come out in general, including Sanger's earlier one revealing some of the very same details—Congress is going apeshit over this one.

First, there's John McCain, pitching this as an election stunt.

> McCain first called attention to the issue with a fiery speech on the Senate floor Tuesday evening, pointing to a new book by New York Times journalist David Sanger that reveals U.S.-Israeli cybercampaigns used against Iran.
>
> McCain charged members of the administration with leaking classified information and called for an investigation by a special counsel. He also called for people to be prosecuted if guilt is found. His Democratic counterpart on the Senate Armed Services Committee, Sen. Carl Levin, D-Mich., agreed to hold a hearing to investigate.
>
> "It is difficult to escape the conclusion that these recent leaks of highly classified information, all of which have the effect of making the President look strong and decisive on national security in the middle of his re-election campaign, have a deeper

> political motivation," Mcain said.

Then there's John Kerry attacking the NYT.

> "I personally think there is a serious question whether or not that served our interest and whether the public had to know," Kerry, the Foreign Relations Committee chairman, told reporters. "To me it was such a nitty-gritty fundamental national security issue. And I don't see how the public interest is well served by it. I do see how other interests outside the United States are well served by it."

The worst is the Gang of Four—Dianne Feinstein, Saxby Chamblis, Dutch Ruppersberger, and Mike Rogers—rolling out new legislation to crack down on leaks.

> The four members of the intelligence committees also called the leaks "damaging and intolerable." They plan to modify and strengthen legislation regarding leaks. "We believe that significant changes are needed, in legislation, in the culture of the agencies that deal with classified information, in punishing leaks, and in the level of leadership across the government to make clear that these types of disclosures will not stand," the lawmakers said in the statement.

Oh, and DiFi sent Obama a classified letter. Ut oh.

And all this comes just a few weeks after the House passed an Amendment mandating an investigation into three stories which were pretty obviously designed to make it harder for Israel to attack Iran.

Our do-nothing Congress has found one issue on which there is broad bipartisan agreement: that

leaks are one thing, but leaks that thwart Israel's efforts to foment war against Iran must be criminalized.

REMEMBER WHEN WE ACCUSED IRAN OF HACKING?

I meant to mention this in my earlier post about David Sanger's StuxNet story, and this passage by Matthew Waxman reminded me.

> As I've argued elsewhere, it's likely that in many cyber-attack scenarios, *both* sides – the attacker and the attacked – will have great incentive to maintain very tight secrecy about it; among other reasons and aside from political considerations, the attacked will not want to disclose information about its vulnerabilities and responses. In light of the "secrecy and low visibility of some states' responsive actions [to cyber-attacks]… it will be difficult to develop consensus understandings even of the fact patterns on which states' legal claims and counterclaims are based, assuming those claims are leveled publicly at all." In writing this, I may have underestimated how much information might leak from the attacking side.

While he sources this information to the public comments of an Iranian general, Sanger suggests Iran has started its own cyberwar unit.

> Iran initially denied that its enrichment facilities had been hit by Stuxnet, then said it had found the worm

> and contained it. Last year, the nation announced that it had begun its own military cyberunit, and Brig. Gen. Gholamreza Jalali, the head of Iran's Passive Defense Organization, said that the Iranian military was prepared "to fight our enemies" in "cyberspace and Internet warfare." But there has been scant evidence that it has begun to strike back.

The thing is, while the US provided no detail to explain this claim, in February Treasury claimed that Iran's Ministry of Intelligence and Security participated with Hezbollah on some hacking projects.

> MOIS provides financial, material, or technological support for, or financial or other services to Hizballah, a terrorist organization designated under E.O. 13224. MOIS has participated in multiple joint projects with Hizballah in computer hacking.

I assume this is either an admission that Hezbollah has hit us or—perhaps more likely—Israel with attacks. (When I wrote this post, I wondered if the allegations that Hezbollah had hijacked Israeli drones—which quickly appeared to be Mossad sabotage instead—were the claimed hack.)

Whatever the basis for the claim, the US government, with a straight face, based part of its Iran sanctions on accusations that the mean old Persians have hacked … somebody.

OBAMA'S "ZOO ANIMAL" BROKE FREE AND "CROSSED THE RUBICON"

> At the bottom of it all has been the Bomb. For the first time in our history, the President was given sole and unconstrained authority over all possible uses of the Bomb.
>
> [snip]
>
> Every executive encroachment or abuse was liable to justification from this one supreme power.
>
> If the President has the sole authority to launch nation-destroying weapons, he has license to use every other power at his disposal that might safeguard that supreme necessity. If he says he needs other and lesser powers, how can Congress or the courts discern whether he needs them when they have no supervisory role over the basis of the claim he is making? To challenge his authority anywhere is to threaten the one great authority.
>
> —Garry Wills, Bomb Power

I suppose I'll eventually get around to discussing how the series of condoned leaks portraying President Obama as the Deciderer all rest on the pathetic but true fact that he is only borrowing George Bush's claim to that title.

But for now, I want to focus on the one part of David Sanger's mixed-metahpor saturated installment in the Deciderer 2.0 series that rings most true:

> Mr. Obama, according to participants in

> the many Situation Room meetings on Olympic Games, was acutely aware that with every attack he was pushing the United States into new territory, much as his predecessors had with the first use of atomic weapons in the 1940s, of intercontinental missiles in the 1950s and of drones in the past decade. He repeatedly expressed concerns that any American acknowledgment that it was using cyberweapons — even under the most careful and limited circumstances — could enable other countries, terrorists or hackers to justify their own attacks.
>
> "We discussed the irony, more than once," one of his aides said. Another said that the administration was resistant to developing a "grand theory for a weapon whose possibilities they were still discovering." Yet Mr. Obama concluded that when it came to stopping Iran, the United States had no other choice.

With cyberwar, with drones, and (to a lesser extent) with the embrace of the terrorists' transnational methods to fight terrorists, Obama has crossed into uncharted territory of the sort Wills explored in his book, *Bomb Power*. These changes are likely a step beyond the Bomb Power paradigm, whatever that entails.

Yet Obama has only barely begun to think through the ramifications of these tools. He has, instead, focused on the near and overblown threats of Iran and AQAP, not seeing both the strategic implications of even those choices, much less the implications of the sort Wills describes arose in the wake of our use of a nuclear bomb.

The President has embraced waging extralegal war using drones from the Oval Office. The President has embraced using easily manipulable code to wage physical war. What are the implications of these decisions?

Oh sure, Obama started paying attention after the fact. A year ago, he rolled out a "National Strategy for Cyberspace," calling for international cooperation to enforce responsible behavior of the sort we have already violated. Even more recently, DOD has been tinkering with our rules of engagement.

But there are signs it is already too late, the battle lines have been drawn. We've already seen the Executive Branch's refusal to share details with Congress, followed by flaccid attempts to force it to do so.

Sanger's article describes how in 2010 we began to see the unintended consequences of sloppy—or covert—coding.

> In the summer of 2010, shortly after a new variant of the worm had been sent into Natanz, it became clear that the worm, which was never supposed to leave the Natanz machines, had broken free, like a zoo animal that found the keys to the cage. It fell to Mr. Panetta and two other crucial players in Olympic Games — General Cartwright, the vice chairman of the Joint Chiefs of Staff, and Michael J. Morell, the deputy director of the C.I.A. — to break the news to Mr. Obama and Mr. Biden.
>
> An error in the code, they said, had led it to spread to an engineer's computer when it was hooked up to the centrifuges. When the engineer left Natanz and connected the computer to the Internet, the American- and Israeli-made bug failed to recognize that its environment had changed. It began replicating itself all around the world. Suddenly, the code was exposed, though its intent would not be clear, at least to ordinary computer users.
>
> "We think there was a modification done by the Israelis," one of the briefers told the president, "and we don't know

> if we were part of that activity."

Yet Sanger, like any obedient sanctioned journalist, doesn't mention the most ominous unintended potential consequence of StuxNet, one contemplated by the Russians: setting off an explosion at Bushehr. The possibility of setting off—perhaps unintentionally—nuclear explosions without attribution. And we know the Administration is preparing to act even more carelessly in the future. Meanwhile, all our military toys contains hundreds of backdoors, ripe for the picking.

More interesting is how Obama is willingly chipping away at the Bomb Power President, perhaps without noticing. There is, of course, the matter of the Israelis. Can't wage cyberwar with them, can't wage cyberwar without them, so you never know when some surprise code will show up. Heck, we even refuse to admit that they're stealing from us every bit as much as our rivals. Doing so might make us stop and think twice about whether we're prepared to play this game.

I'm most interested in what this entails for secrecy. The Sanger article, of course, is an egregious version of sanctioned leaks of classified information. The most intriguing bit, to me, is this suggestion we've found a way to bridge air gaps.

> In fact, thumb drives turned out to be critical in spreading the first variants of the computer worm; later, more sophisticated methods were developed to deliver the malicious code.

But the most amusing tidbit is this mention of the sabotage we've conducted in the past.

> For years the C.I.A. had introduced faulty parts and designs into Iran's systems — even tinkering with imported power supplies so that they would blow up — but the sabotage had had relatively

> little effect.

The fact that we introduced faulty designs into Iran's systems is, you'll note, precisely the information that Jeff Sterling is currently being prosecuted for, that James Risen is being subpoenaed for. But here it is, dropped into a sanctioned leak story, easily the least interesting nugget.

At this level, then, this story displays the height of the Bomb Power President's abuse of information asymmetry, permitting selected people to spread the same secrets that are criminalized from others.

But the larger tale—particularly the escape of StuxNet and its subsequent exposure—shows the lie of this arrogance. The Chinese, certainly, can take what they want. Bradley Manning allegedly can take what he wants too. And unless the code is perfect, and unless the Israelis refrain from toying with the code, eventually the code, the Bomb Power itself, will become available.

Obama's foolish embrace of these new technologies without considering the larger impact may lead to the decline of the Bomb Power President—of Presidents, generally. It may lead to something far more fearful.

But one thing is clear: he didn't really stop to think about all that before he set free his zoo animal.

SCOTUS CERT GRANT IN CLAPPER TAKES KEY 9TH CIRCUIT CASES

HOSTAGE

Marcy noted briefly Monday morning, the Supreme Court granted certiorari in *Clapper v. Amnesty International*:

> SCOTUS did, however, grant cert to Clapper v. Amnesty, which I wrote about here and here. On its face, Clapper is just about the FISA Amendments Act. But it also has implications for wiretap exceptions—and, I've argued—data mining exceptions to the Fourth Amendment. In any case, SCOTUS seems interested in reversing the 2nd Circuit opinion, which had granted standing to people whose work had been chilled by the passage of the FAA. Also, as I hope to note further today, SCOTUS' Clapper decision may also impact the *Hedges v. Obama* ruling from last week.

As Marcy indicated, there is nothing good afoot from SCOTUS taking cert in *Clapper*; if they wanted to leave the very nice decision of the 2nd Circuit intact, they simply leave it intact and don't grant review. Oh, and, yes, Marcy is quite right, it's a very safe bet that Clapper will "impact" the also very nice recent decision in Hedges, which is, itself, headed with a bullet to the 2nd Circuit.

There was, of course, much discussion of the significance of the *Clapper* cert grant yesterday on Twitter; one of the best of which was between Marcy, Lawfare's Steve Vladeck and, to a lesser extent, me. To make a long story a little shorter, I said (here and here):

> See, and I HATE saying this, I think Kennedy will do just that+then same 5 will kill al-Haramain once it gets to SCOTUS and then they will have capped the Bush wiretapping well completely and closed off standing significantly for the future.

Yikes, I did not contemplate just how true this statement was; the *Clapper* cert grant has already had a far deeper and more pernicious effect than even I suspected. This morning, in a move I do not believe anybody else has caught on to yet, the 9th Circuit quietly removed both *al-Haramain* and the CCR case encaptioned *In Re: NSA Telecommunications Litigation/CCR v. Obama* from the oral argument calendar that has long been set for June 1 in the old 9th Circuit Pasadena courthouse. The orders for both al-Haramain and CCR are identical, here is the language from the *al-Haramain* one:

> Argument in this case scheduled for June 1, 2012 in Pasadena, California, is vacated pending the Supreme Court's decision in *Clapper v. Amnesty Int'l*, No. 11- 1025. The court may order supplemental briefing following the Supreme Court's decision. Oral argument will be rescheduled.

Whoa. This is extremely significant, and extremely unfortunate. Also fairly inexplicable. Entering the order for *CCR* makes some sense, since it involves the same "fear of surveillance" standing issue as is at issue in *Clapper*; but doing it for *al-Haramain* makes no sense whatsoever, because *al-Haramain* is an "actual" surveillance standing case.

There simply is no issue of the claimed, putative, standing concern that permeates *Clapper* and *CCR*. Well, not unless the 9th Circuit panel thinks the Supreme Court might speak more broadly, and expand the parameters wildly, in *Clapper* just as they did in *Citizens United*. That would be a pretty ugly path for the Supreme beings to follow; but, apparently, not just a cynical bet on my part, but also a bet the 9th Circuit immediately placed as well.

To be fair, even positive forward thinking players, like Steve Vladeck, thought the lower courts might be copacetic, or that the Supremes might comply. Maybe not so much. I know,

shocking. Here is a glimpse, through Vladeck, of the situation:

> But at a more fundamental level, there's one more point worth making: Readers are likely familiar with Alex Bickel's Passive Virtues, and his thesis that, especially on such sensitive questions where constitutional rights intersect with national security, courts might do best to rely on justiciability doctrines to duck the issue—and to thereby avoid passing upon the merits one way or the other. [Think Joshua at the end of WarGames: "The only winning move is not to play."] And at first blush, this looks like the perfect case for Bickel's thesis, given the implications in either direction on the merits: recognizing a foreign intelligence surveillance exception and thereby endorsing such sweeping, warrantless interceptions of previously protected communications vs. removing this particular club from the government's bag…
>
> And yet, the foreign intelligence surveillance exception only exists because it has already been recognized by a circuit-level federal court, to wit, the FISA Court of Review. Whether the passive virtues might otherwise justify judicial sidestepping in such a contentious case, the fact of the matter is that this is a problem largely (albeit not entirely, thanks to the FISA Amendments Act) of the courts' making. To duck at this stage would be to let the FISA Court of Review—the judges of which are selected by the Chief Justice—have the last word on such a momentous question of constitutional law. In my view, at least, that would be unfortunate, and it's certainly not what Bickel meant…

Back to al-Haramain and the effects in the 9th

Circuit. Here is the latest, taken from the Motion for Reconsideration filed late yesterday by al-Haramain, Wendell Belew and Asim Ghafoor:

> The question presented in Clapper is thus wholly unrelated to the issues presented on the defendants' appeal in the present case. The Supreme Court's decision in Clapper will have no effect on the disposition of the present case. Thus, there is no reason to delay the adjudication of this appeal pending the decision in Clapper, which would only add another year or more to the six-plus years that this case has been in litigation.
>
> It makes sense for the Court to have vacated the oral argument date for Center for Constitutional Rights v. Obama, No. 11-15956, which involves theories of Article III standing similar to those in Clapper. It does not, however, make sense in the present case, where Article III standing is based on proof of actual past surveillance rather than the fear of future surveillance and expenditures to protect communications asserted in Clapper.

Yes, that is exactly correct.

And, therein, resides the problem with Vladeck's interpretation of what is going on with the *Clapper case*. Steve undersold, severely, just how problematic *Clapper* is. Both the discussion herein, and the knee jerk action of the 9th Circuit, the alleged liberal scourge of Democratic Federal Appellate Courts, demonstrate how critical this all is and why *Clapper* is so important.

Clapper has not only consumed its own oxygen, it has consumed that of independent, and important, nee critical, elements of the only reductive cases there are left in the United States judicial system in regards to these ends. That

would be, at an irreducible minimum, *al-Haramain* in the 9th Circuit.

If you have forgotten about *al-Haramain*, and the proceedings that took place in the inestimable Vaughn Walker's, court, here it is. Of all the attempts to attack the Bush/Cheney wiretapping crimes, *al-Haramain* is the only court case that, due to its unique circumstances, has been successful. It alone stands for the proposition that mass crimes were, in fact, committed. *al-Haramain* had a tough enough road ahead of it on its own, the road has become all the more treacherous now because of *Clapper*.

The 9th Circuit should grant the motion for reconsideration and reinstate *al-Haramain* on the oral argument calendar, but that is quite likely a longshot at this point. Expect the DOJ to file a very aggressive response, they are undoubtedly jumping for joy at this stroke of good fortune and will strive to protect it.

REMEMBER WHEN RUSSIA'S ENEMY HELPED THE MUJAHADEEN NEUTRALIZE RUSSIA'S MOST EFFECTIVE WEAPON?

"Bluster"! "Exaggeration"!

Those are some of the words Joe Lieberman and some more credible people are using to dismiss Iran's claim that it has accessed the data from the Sentinel drone it brought down last year.

Aside from "independent experts" pointing out

the obvious fact that Iran could have gotten details about the Sentinel's use to surveil Osama bin Laden's compound from public reports (though how would it have gotten the specific dates?), the US security establishment has offered no detailed explanation of how Iran got the data it claims to have taken from the drone.

> General Hajizadeh cited as evidence data that he said was extracted from the drone's computer hard drives revealing its operations in the months before it went down in Iran — either because it was shot down, as Iranian officials have claimed, or because it experienced a technical failure, as the Americans have said.
>
> The drone, he said, had undergone repairs in California in October 2010 and returned to Afghanistan in November 2010, where American officials have acknowledged it operated, though without specifying where its missions took it. He added that the drone's computer memory revealed that it had flown over the compound in Pakistan where Osama bin Laden was killed in an American raid in May 2011.
>
> "Had we not accessed the plane's softwares and hard disks, we wouldn't have been able to achieve these facts," General Hajizadeh said, according to the news agency Fars.
>
> The White House and American intelligence officials declined Sunday to comment on the new claims, though independent experts expressed skepticism. They noted that the information about the drone's activities — including its use in the Bin Laden raid — could have been drawn from public reports about the sophisticated aircraft.

That may not entirely confirm that the data cited by Iran is accurate, but it sure doesn't refute it.

That said, all these experts bewailing "bluster" have not mentioned the more obvious explanation behind Iran's claim—even though just three days ago the news was filled with reports of Russia and China asking for information on the drone and much of the coverage of this latest fact acknowledges that in their stories.

Consider: while the OBL surveillance (though not the timing) was publicly reported, the maintenance records cited by the Iranians probably aren't. But those details are more likely to be available not in the drone itself, but on Lockheed's networks, which were hacked (though Lockheed claims no data was compromised) last year; everyone blames China for that hack. And if China has been able to access drone data off our networks like they've been able to access all our other weapons development data, then it would presumably make it a lot easier to break the encryption on the Sentinel drone itself.

Our fear-mongering about Iran, as well as our overthrow of Qaddafi and efforts to overthrow Assad, has far more to do with efforts to shore up Saudi—and therefore US—hegemony in the key oil-producing region of the world than nukes. And while China has been cozying up to the Saudis in ways that ought to make us rethink our unquestioning pursuit of Saudi goals, our efforts to eliminate any counter-weight to Saudi power in the region is a real threat to China (not to mention our ability to wage war in the African countries China has spent a decade cultivating by pressing a few buttons in Nevada). Precisely the same kind of threat we judged Russian expansion into Afghanistan to be in 1979 when we started funneling money—and ultimately, some years later, Stinger missiles—to the mujahadeen. The Stinger missiles took away Russia's air superiority and with it their ambitions to keep Afghanistan and

ultimately, their commitment to empire more generally.

So while it may comfort the public to be told Iran could never manage to reverse engineer our drone, the possibility that China and Iran may be making real progress in neutralizing our favorite new weapon would presumably worry the national security establishment. Just in time for Iran to enter negotiations and in such a way that the implicit threat from China is understood.

These blustery experts should have listened to me when I warned that China's ability to access our defense networks with ease was far more dangerous than Bradley Manning and his Lady Gaga CD.

AT WHAT POINT DO OUR CYBERWAR TOYS BECOME WMD?

The other day, Ellen Nakashima reported on new cyberwar acquisition guidelines that will allow DOD, under certain circumstances, to deploy targeted exploits without the regular testing or oversight process.

> The rapid process will take advantage of existing or nearly completed hardware and software developed by industry and government laboratories. This approach could take several months in some cases, or a few days in others.
>
> [snip]
>
> Under the rapid plan, weapons can be financed through the use of operational funds, in "days to months," and some steps that ordinarily would be required

> would be eliminated. These include some planning documents and test activities, according to the report.
>
> The weapons may be designed for a single use or for some other limited deployment, and they would be used in offensive cyber operations or to protect individual computer systems against specific threats, said the report.

As she describes it, this rapid development will (is supposed to?) only be used in fairly targeted cases.

But what are the chances the speed and limited oversight lead to mistakes? What are the chances that our rush to roll out exploits leads us to set off some unintended consequences?

Consider Richard Clarke's explanation for how StuxNet escaped the narrow confines of the Natanz centrifuge facility it targeted.

> "It got loose because there was a mistake," [Clarke] says. "It's clear to me that lawyers went over it and gave it what's called, in the IT business, a TTL."
>
> "What's that?"
>
> "If you saw *Blade Runner* [in which artificial intelligence androids were given a limited life span—a "time to die"], it's a 'Time to Live.'" Do the job, commit suicide and disappear. No more damage, collateral or otherwise.
>
> "So there was a TTL built into Stuxnet," he says [to avoid violating international law against collateral damage, say to the Iranian electrical grid]. And somehow it didn't work."
>
> "Why wouldn't it have worked?"
>
> "TTL operates off of a date on your computer. Well, if you are in China or

> Iran or someplace where you're running bootleg software that you haven't paid for, your date on your computer might be 1998 or something because otherwise the bootleg 30-day trial TTL software would expire.
>
> "So that's one theory," Clarke continues. "But in any event, you're right, it got out. And it ran around the world and infected lots of things but didn't do any damage, because every time it woke up in a computer it asked itself those four questions. Unless you were running uranium nuclear centrifuges, it wasn't going to hurt you."
>
> "So it's not a threat anymore?"
>
> "But you now have it, and if you're a computer whiz you can take it apart and you can say, 'Oh, let's change this over here, let's change that over there.' Now I've got a really sophisticated weapon. [first brackets mine, all others original]

Here's a cyberweapon presumably developed under the existing "deliberate" process, with full testing and oversight. If Clarke's description of the problem is correct, it's not so much a testing problem as an inadequate understanding of the environment—a failure to account for all those computers on which, because their clocks were not set properly, the TTL orders malfunctioned. And while StuxNet itself may not have done collateral damage, who knows what hackers who have gotten the code did with it?

So while StuxNet, with the benefit of time and testing, didn't do excessive damage when DOD's plans proved to be inadequate, who's to say that an exploit deployed with far less time—purchased for use—won't do more damage?

Also, note how much more quickly DOD appears to be moving to make sure it has lots of cyberweapons to deploy than it has moved to make

sure it has the most rudimentary defenses against exploitation. Probably, when our cyberwar toys turn into a WMD, they'll hurt people in the Middle East or China. But given our rush into offensive cyberwar before we've protected ourselves, who knows?