THE CHAMBERMAID'S REVENGE: IMF HACKED

Usually, the apparent purpose of hacks is fairly banal. To steal defense secrets. To profit organized crime. To embarrass a political opponent.

But a reported sophisticated hack on the IMF is far more intriguing.

> Because the fund has been at the center of economic bailout programs for Portugal, Greece and Ireland — and possesses sensitive data on other countries that may be on the brink of crisis — its database contains potentially market-moving information. It also includes communications with national leaders as they negotiate, often behind the scenes, on the terms of international bailouts. Those agreements are, in the words of one fund official, "political dynamite in many countries." It was unclear what information the attackers were able to access.
>
> The concern about the attack was so significant that the World Bank, an international agency focused on economic development, whose headquarters is across the street from the I.M.F. in downtown Washington, cut the computer link that allows the two institutions to share information.

The story mentions market-moving information, so I assume it could just be someone trying to play the bond markets.

But what is the scenario under which hackers compromise IMF's top secret files to get information on the deals signed between the banksters and debtor nations? While I'd like to see that information—and I'm sure the Greeks rioting in the streets and the Irish stoically

bearing down accepting their fate would like to see that information—I don't understand what entity would sponsor the hackers? Organized crime? China? Hacktivists? If it were the latter—which seems most plausible to me—wouldn't we already be looking at the demands German banksters made of Greek leaders?

I'm sure we'll learn more about this in the future. But for now, I'm really curious about who had the means and motive to hack the IMF.

Aside from a bunch of chambermaids, of course.

ANGLO-AMERICANS AT CYBERWAR: TWO WEEKS OF CUPCAKES

I've been meaning to return to this Ellen Nakashima story on our cyberwar efforts. As you recall, it lays out the turf war between the CIA and DOD over clandestine cyberops, partly by telling the story a fight over whether or not to disrupt the jihadist online magazine "Inspire."

> Last year, for instance, U.S. intelligence officials learned of plans by an al-Qaeda affiliate to publish an online jihadist magazine in English called Inspire, according to numerous current and senior U.S. officials. And to some of those skilled in the emerging new world of cyber-warfare, Inspire seemed a natural target.
>
> The head of the newly formed U.S. Cyber Command, Gen. Keith Alexander, argued that blocking the magazine was a legitimate counterterrorism target and would help protect U.S. troops overseas. But the CIA pushed back, arguing that it would expose sources and methods and

> disrupt an important source of intelligence. The proposal also rekindled a long-standing interagency struggle over whether disrupting a terrorist Web site overseas was a traditional military activity or a covert activity – and hence the prerogative of the CIA.
>
> The CIA won out, and the proposal was rejected. But as the debate was underway within the U.S. government, British government cyber-warriors were moving forward with a plan.
>
> When Inspire launched on June 30, the magazine's cover may have promised an "exclusive interview" with Sheik Abu Basir al-Wahishi, a former aide to Osama bin Laden, and instructions on how to "Make a Bomb in the Kitchen of Your Mom." But pages 4 through 67 of the otherwise slick magazine, including the bomb-making instructions, were garbled as a result of the British cyber-attack.
>
> It took almost two weeks for al-Qaeda in the Arabian Peninsula to post a corrected version, said Evan Kohlmann, senior partner at Flashpoint Global Partners, which tracks jihadi Web sites.

The Telegraph elaborated on that story by telling of the swell cupcake recipes MI6 replaced the bomb recipe with.

> The cyber-warfare operation was launched by MI6 and GCHQ in an attempt to disrupt efforts by al-Qaeda in the Arabian Peninsular to recruit "lone-wolf" terrorists with a new English-language magazine, the Daily Telegraph understands.
>
> When followers tried to download the 67-page colour magazine, instead of instructions about how to "Make a bomb in the Kitchen of your Mom" by "The AQ

> Chef" they were greeted with garbled computer code.
>
> The code, which had been inserted into the original magazine by the British intelligence hackers, was actually a web page of recipes for "The Best Cupcakes in America" published by the Ellen DeGeneres chat show.
>
> Written by Dulcy Israel and produced by Main Street Cupcakes in Hudson, Ohio, it said "the little cupcake is big again" adding: "Self-contained and satisfying, it summons memories of childhood even as it's updated for today's sweet-toothed hipsters."
>
> It included a recipe for the Mojito Cupcake – "made of white rum cake and draped in vanilla buttercream"- and the Rocky Road Cupcake – "warning: sugar rush ahead!"
>
> By contrast, the original magazine featured a recipe showing how to make a lethal pipe bomb using sugar, match heads and a miniature lightbulb, attached to a timer.

So apparently this operation against Inspire, which had government hackers and their bosses on two continents scheming and in-fighting, succeeded in delaying for two weeks the publication of a bomb recipe that probably existed elsewhere on the Internet already.

With cupcakes.

And these spooks are apparently impressed enough with themselves that they're boasting about it openly to journalists.

Dudes. Two weeks of cupcakes do not equate to Stuxnet.

I've been pondering the apparent self-congratulation over this op ever since I read this story, particularly in light of the seeming

similarity between this op and the WikiLeaks hack last year. Do our cyberwarriors consider it a legitimate "win" to simply delay the publication of a transnational internet operation for a week or so? At what cost? And by "cost," I mean both the tens of millions we're investing to develop, apparently, the capability to engage in juvenile pranks. And also the cost in credibility as a purported defender of free speech wastes its time harassing, but not preventing, the free speech of groups it doesn't like.

I mean, there must be more to our cyberwarfare than two weeks of cupcakes, isn't there?

Of course, there must be, if the CIA was concerned about sources and methods. Presumably, CIA was already monitoring who was reading Inspire. Which—whatever it says about the First Amendment in this country—is probably still a better use of cyberwar time and dollars than two weeks of cupcakes.

Or are we to believe that the Generals think we're going to win the GWOT by playing cyber-whack-a-mole with a group whose competitive advantage over us is in its nimbleness?

THE CRUX OF THE CISCO-US GOVERNMENT COLLABORATION

As I said in this comment, we're going to have to wait until the Canadian court releases more details on the failed extradition of Peter Alfred Adekeye to get a better sense of what the government did to piss off the court so badly. But this is my attempt to the crux of the matter.

The Adekeye deposition in Canada was set up in

April 2010 for a several day time period in May. On May 19 at the deposition, Adekeye admitted to accessing Cisco's website perhaps five times, though he said a Cisco employee had offered him that access. That part of his deposition was streamed back to Northern California. That same day—May 19—the arrest warrant was signed in the US (making it possible that Adekeye's deposition served to establish the probable cause to arrest him). And the Magistrate who signed the US arrest warrant was the same Magistrate overseeing discovery in this case. By the time Adekeye was arrested on May 20, his lawyers had not yet had an opportunity to question Adekeye. In effect, Cisco had gotten 14 hours of unrebutted deposition from Adekeye, after which he became unavailable to his lawyers.

In response, his lawyers requested that the civil procedure be stayed and that the judge order an accelerated discovery from Cisco with regards to its involvement in getting Adekeye extradited. As they described in their motion for a stay,

> Mr. Adekeye's deposition commenced in Vancouver, Canada on May 18, 2010. After Cisco spent nearly fourteen (14) full hours deposing Mr. Adekeye, the proceedings were interrupted by the Royal Canadian Mounted Police, who were accompanied by additional uniformed Vancouver Police Officers. The Mounted Police informed counsel and the Special Master appointed by the Court to oversee Mr. Adekeye's deposition, that they were there in order to effectuate the arrest of Mr. Adekeye. The Mounted Police presented to counsel and the Special Master a "Warrant For Provisional Arrest" issued pursuant to Section 13 of the Extradition Act, wherein the Honourable Mr. Justice Leask had executed a provisional arrest warrant for Mr. Adekeye. Attached to this provisional arrest warrant was a bench warrant issued by the Honorable Howard

> R. Lloyd—the assigned Magistrate Judge to this matter—for the arrest of Mr. Adekeye.
>
> [snip]
>
> At no point during these entire proceedings was there any mention to Mr. Adekeye or to his attorneys of a criminal investigation relating to the exact same facts underlying the instant civil lawsuit. Instead, Cisco insisted that the Court order Mr. Adekeye to be deposed, and proceeded to depose Mr. Adekeye for fourteen (14) hours. Despite having over three (3) days to do so, Cisco did not finish its questioning of Mr. Adekeye prior to his arrest. Mr. Adekeye's attorneys, moreover, were entirely unable to question their client in order to clarify or develop Mr. Adekeye's responses further. Because Mr. Adekeye is currently detained in Canada, without bail, he has not been able to review his testimony pursuant to Fed. R. Civ. P. 30, nor has he been able to otherwise summarize his testimony or prepare an affidavit to the Court requesting an extension of time to further brief the Underlying Motions.
>
> In addition to the very real Fifth Amendment issues now a part of this case, Multiven fears that in the event the Court does not vacate or continue the supplemental briefing deadline and the June 7 hearing, Cisco will present, as evidence in support of its Underlying Motion, incomplete deposition testimony of a party witness. Such incomplete, one-sided and out of context evidence is entirely prejudicial to Multiven, and the Court should not consider it.

The judge denied both motions, largely because in the interim both parties had submitted briefs based on Adekeye's deposition.

So in effect, the timing of the arrest accomplished two things. It gave Cisco an advantage in the civil case (insofar as Adekeye's lawyers didn't have a chance to depose him). But it also likely elicited evidence that supported Adekeye's arrest warrant.

Within 2 months of the arrest, the judge ruled on the summary judgments, basically ruling against Adekeye. Here's the logic he used to justify the claim that Adekeye got unauthorized access to Cisco's compuuters.

> Multiven admit that on one occasion Adekeye accessed secure areas of the Cisco network. They contend however, that a Cisco employee, Wes Olson, supplied Adekeye with his login and password, thus authorizing Adekeye to access the restricted website. (Multiven's Opposition at 7-12.) It is undisputed that Wes Olson provided Adekeye with his login and "external" password. Olsen declares that the password was given to Adekeye "to give him access to Cisco's network on one occasion, for a specific purpose."10 However, it is also undisputed that an employee's giving his login and password to Adekeye was a violation of Cisco's policies, and thus Olson's providing access to Adekeye in this manner did not constitute a valid authorization.

And here's how he dismissed the Fifth Amendment concerns about the deposition.

> On June 8, 2010, Multiven filed a Motion to Stay Counterclaims. (hereafter, "Motion to Stay," Docket Item No. 234.) Multiven contend that further litigation of the counterclaims will jeopardize Adekeye's Fifth Amendment privileges in parallel criminal proceedings arising out of the same factual circumstances. (Motion to Stay at 5-7.)

> [snip]
>
> Here, Adekeye has already voluntarily submitted declarations in support of Multiven's briefs regarding the parties' cross-motions for summary judgment and has been deposed extensively, including fourteen hours of deposition testimony that he voluntarily provided in Vancouver, Canada prior to his arrest. Without deciding whether Adekeye was sufficiently aware of the likelihood of criminal prosecution for his declarations and deposition testimony to effect a waiver of his Fifth Amendment rights,21 the Court finds that continuing the litigation will only minimally implicate Adekeye's Fifth Amendment rights, given the extensive testimony he has already provided in this
>
> case.

So that's the real background to the settlement: Cisco had largely already won on their substantive claim, using evidence from Adekeye's partial deposition. Which left Adekeye with the risk that continuing his anti-trust claim would expose him to ongoing risk on the criminal claims.

Now it does seem like Adekeye is vulnerable in the computer fraud charges (though presumably 5 of them, not 97). But at the same time, it does seem clear that the government used the deposition to set up—and probably collect evidence for—the arrest and with it the criminal case.

WHY DIDN'T WE ASK CHINA TO FIND SCOOTER LIBBY'S MISSING PLAME LEAK E-MAILS?

WSJ has an article reporting on the purportedly Chinese-launched GMail hacks that targeted top White House officials.

The article is interesting not because it claims the Chinese want to hack top officials. Who do you think they'd be most interested in hacking?

Rather, the article is interesting for some of the implications bandied about in the article. For example, Darrell Issa and CREW's Melanie Sloan suggest the only reason the Chinese would hack the GMail accounts of White House officials is if those people were improperly conducting official business on GMail.

> "If all White House officials were following rules prohibiting the use of personal email for official business, there would simply be no sensitive information to find," said Rep. Darrell Issa, Republican chairman of the House Oversight and Government Reform Committee, and a frequent thorn in the Obama administration's side. "Unfortunately, we know that not everyone at the White House follows those rules and that creates an unnecessary risk."
>
> Melanie Sloan, executive director of Citizens for Responsibility and Ethics in Washington, a watchdog group, said the hacking "suggests China believes government officials are using their personal accounts for official business, because I doubt they were looking for their weekend plans or a babysitter's

> schedule. Presumably, the Chinese wouldn't have done this if they weren't getting something."

More plausible is the suggestion that the Chinese were phishing for information they could then use to compromise other accounts.

> Stewart Baker, a former homeland security official in the Bush administration, said he suspects the ultimate goal of the hacking may have been to use the email accounts as a stepping stone to penetrate the officials' home computers.
>
> "If you can compromise that machine, you may well be able to access the communications they are having with the office," said Mr. Baker.

I'm most interested in all the assumptions here, that a bunch of Chinese hackers know precisely how the White House email system works. If that's true, why haven't we asked the Chinese to turn over the emails OVP deleted from the first days of the Plame leak investigation? And why haven't we asked the Chinese to turn over all those emails hidden on the RNC's server? Maybe they can also help us find all of John Yoo's torture emails?

Given how common it is, these days, for top officials to just delete their most inconvenient emails, I'm thinking American citizens ought to invite Chinese hackers to help us reclaim all the official records our overlords try to destroy.

THE CYBERWAR

CAMPAIGN AGAINST JIHADI LITERATURE AND WIKILEAKS

Ellen Nakashima has a piece following up on the WSJ story previewing DOD's cyberwar (which I posted on here). Before you read it, though, I wanted to suggest another reason we may be seeing this policy early (in addition to the hacking of all the defense contractors, now including L-3; and note, Nakashima references this legislation at the end of her article).

Last Thursday, the Defense Authorization bill passed the House. It retains Section 962, to which the Administration objected, which reads,

> SEC. 962. MILITARY ACTIVITIES IN CYBERSPACE.
>
> (a) AFFIRMATION.—Congress affirms that the Secretary of Defense is authorized to conduct military activities in cyberspace.
>
> (b) AUTHORITY DESCRIBED.—The authority referred to in subsection (a) includes the authority to carry out a clandestine operation in cyberspace—
>
> (1) in support of a military operation pursuant to the Authorization for Use of Military Force (50 U.S.C. 1541 note; Public Law 107–40) against a target located outside of the United States; or
>
> (2) to defend against a cyber attack against an asset of the Department of Defense.
>
> (c) BRIEFINGS ON ACTIVITIES.—Not later than 120 days after the date of the enactment of this Act, and quarterly thereafter, the Secretary of Defense shall provide a briefing to the Committees on Armed Services of the House of Representatives and the Senate

> on covered military cyberspace activities that the Department of Defense carried out during the preceding quarter.
>
> (d) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to limit the authority of the Secretary of Defense to conduct military activities in cyberspace.

So as you read Nakashima, remember that the Obama Administration objected to a section that authorized cyberwar in two circumstances—in support of an AUMF against a target outside of the US and in defense against a cyber attack on a DOD asset—and required quarterly briefings.

OK, now go read Nakashima.

Within the context of the Defense Authorization, a few points of DOD's campaign to describe what they believe their cyberwar policy to be stick out. First, it envisions preparatory actions—basically spying on a presumably non-belligerent adversary's infrastructure to map out how DOD would launch a cyberattack if the time came.

> The framework clarifies, for instance, that the military needs presidential authorization to penetrate a foreign computer network and leave a cyber-virus that can be activated later. The military does not need such approval, however, to penetrate foreign networks for a variety of other activities. These include studying the cyber-capabilities of adversaries or examining how power plants or other networks operate. Military cyber-warriors can also, without presidential authorization, leave beacons to mark spots for later targeting by viruses, the official said.

In other words, DOD is indicating that it will engage in cyberwar activities outside of those

authorized by Congress, activities which I'm sure they're claiming fall under their "preparing the battlefield" giant loophole they use to engage in spywork.

Then there's this:

> Last year, for instance, U.S. intelligence officials learned of plans by an al-Qaeda affiliate to publish an online jihadist magazine in English called Inspire, according to numerous current and senior U.S. officials. And to some of those skilled in the emerging new world of cyber-warfare, Inspire seemed a natural target.
>
> The head of the newly formed U.S. Cyber Command, Gen. Keith Alexander, argued that blocking the magazine was a legitimate counterterrorism target and would help protect U.S. troops overseas. But the CIA pushed back, arguing that it would expose sources and methods and disrupt an important source of intelligence. The proposal also rekindled a long-standing interagency struggle over whether disrupting a terrorist Web site overseas was a traditional military activity or a covert activity – and hence the prerogative of the CIA.
>
> The CIA won out, and the proposal was rejected. But as the debate was underway within the U.S. government, British government cyber-warriors were moving forward with a plan.

As Nakashima goes onto explain, the British attack on Inspire managed to delay the publication of a bomb-making article in the magazine for two weeks. But it did eventually get published.

The Inspire story is fascinating not just because it reveals the ongoing turf war between DOD and CIA—and makes clear Mac Thornberry

intends to let DOD win these battles.

But also, consider the cyberattack-which-shall-not-be-named: someone's successful effort to ensure WikiLeaks couldn't publish the State Department cables from a US server. The Inspire story makes it clear DOD is thinking in terms of take-downs of speech, which is precisely what the WL hack was.

And since WL was ultimately a compromise of DOD's networks, it would solidly fall under the congressionally-defined defense "against a cyber attack against an asset of the Department of Defense."

That is, it seems that Thornberry has authorized DOD to do things like hack WL. Congress seems to be in the business of helping the government exercise prior restraint.

That First Amendment sure was nice when we had it!

Though there's just one weird aspect to this: DOD didn't launch a cyberattack on WL when it compromised DOD resources: the Afghan and Iraq cables. Rather, it waited until all the DOD materials were already out, and then (we assume though don't know) started attacking free speech to protect the State Department's assets.

Anyway, all that prior restraint isn't good enough, it seems, and the Administration is going to campaign for more lenient guidelines allowing DOD to wade through other countries' infrastructure to figure out how to cyberattack them when the time comes.

I guess they can't very well complain about the Lockheed and L-3 hacks then.

RETALIATING AGAINST STATE-SPONSORED CYBER WAR

On the first news day after the holiday weekend reporting on Lockheed Martin, WSJ reports that the US is moving towards making cyberattacks an act of war.

> The Pentagon has concluded that computer sabotage coming from another country can constitute an act of war, a finding that for the first time opens the door for the U.S. to respond using traditional military force.

And they're building into this policy an assumption that the biggest attacks must have state sponsorship.

> Pentagon officials believe the most-sophisticated computer attacks require the resources of a government. For instance, the weapons used in a major technological assault, such as taking down a power grid, would likely have been developed with state support, Pentagon officials say.

This new policy won't be subject to intelligence manipulation at all, nosiree!

The next time someone wants to invent a casus belli against Iran, they can just point to a particularly successful hack and (ignoring all questions about appropriate retaliation for Stuxnet…) claim the Iranians have done it and say it, like evidence of WMD, is classified.

They already presumably fabricated one Laptop of Death for Iran, why not another?

And then, declaring ourselves incompetent to retaliate via cyberspace (Stuxnet notwithstanding), they'll have their excuse to

roll out the war machine.

ABOUT THE LOCKHEED MARTIN HACK

As first started leaking last week, Lockheed Martin seems to have been hacked.

> Last weekend was bad for a very large U. S. defense contractor that uses SecureID tokens from RSA to provide two-factor authentication for remote VPN access to their corporate networks. Late on Sunday all remote access to the internal corporate network was disabled. All workers were told was that it would be down for at least a week. Folks who regularly telecommute were asked to come into nearby offices to work. Then earlier today (Wednesday) came word that everybody with RSA SecureID tokens would be getting new tokens over the next several weeks. Also, everybody on the network (over 100,000 people) would be asked to reset their passwords, which means admin files have probably been compromised.

What seems to have happened is hackers used information gotten in the RSA Data Security hack to try to break Lockheed's own security—basically, Lockheed noticed that hackers were trying to use the keys they stole in March to open a bunch of locks at Lockheed. Lockheed appears to have discovered the effort and in response, started shutting down remote access on parts of its network.

> Lockheed Martin, the Pentagon's No. 1 supplier, is experiencing a major disruption to its computer systems that could be related to a problem with

> network security, a defense official and two sources familiar with the issue said on Thursday.
>
> Lockheed, the biggest provider of information technology to the U.S. government, is grappling with “major internal computer network problems,” said one of the sources who was not authorized to publicly discuss the matter.
>
> [snip]
>
> The slowdown began on Sunday after security experts for the company detected an intrusion to the network, according to technology blogger Robert Cringely. He said it involved the use of SecurID tokens that employees use to access Lockheed’s internal network from outside its firewall,
>
> [snip]
>
> Loren Thompson, chief operating officer of the Lexington Institute, and a consultant to Lockheed, said the company monitored every node on its vast global computer network from a large operations center in a Maryland suburb near Washington, D.C.
>
> “If it sees signs that the network is being compromised by outsiders it will shut down whole sectors of the network to protect information,” Thompson said.
>
> He said Lockheed had advanced networking monitoring tools that gave it a “much better understanding of their systems’ status than most other organizations, including the Department of Defense.”

In other words, Lockheed may have prevented a much bigger breach into their own systems. But the assumption of many is that other companies might not have noticed what Lockheed did. Stories on this hack all feature a list of other

defense contractors—like Boeing and Raytheon and Northrup Grumman—who "decline to comment," which might mean they're scrambling to address the same problem Lockheed is, only trying to do so without all the bad PR.

Now, most observers of this hack have suggested that the hackers—who might work for a state actors or some other sophisticated crime group—were after Lockheed's war toy information (which partly explains why you'd ask Lockheed's aerospace competitors if they'd been hacked too). But remember that Lockheed does a lot for the government besides build planes. Of particular note, they're a huge NSA contractor. Maybe the hackers were after info on jet fighters, or maybe they were after the data and data collection programs our own government hides from its own citizens.

Which is all a reminder that, amidst the sound and fury directed at WikiLeaks (which after all shared important information with citizens who deserved to know it), there's a whole lot more hacking we don't learn the results of, hacking that either might result in others adopting our lethal technologies, or in third parties stealing the data we're not even allowed to know.

Now, granted, Lockheed has far far better security than DOD's SIPRNet does. At least they're trying to protect their data. But it's not clear they—or their counterparts—are entirely successful.

OBAMA'S SECRET CYBERWARS

I sort of get the feeling that the entire legislative effort on cyberwar is going on in a classified annex.

Nevertheless, even from what we can see, we've got a dispute. As I noted a few weeks back, The House Armed Services Committee included a provision that explicitly granted DOD the power to conduct clandestine cyberwar activities in some situations, but required quarterly briefing on such activities.

> SEC. 962. MILITARY ACTIVITIES IN CYBERSPACE.
>
> (a) AFFIRMATION.—Congress affirms that the Secretary of Defense is authorized to conduct military activities in cyberspace.
>
> (b) AUTHORITY DESCRIBED.—The authority referred to in subsection (a) includes the authority to carry out a clandestine operation in cyberspace—
>
> (1) in support of a military operation pursuant to the Authorization for Use of Military Force (50 U.S.C. 1541 note; Public Law 107–40) against a target located outside of the United States; or
>
> (2) to defend against a cyber attack against an asset of the Department of Defense.
>
> (c) BRIEFINGS ON ACTIVITIES.—Not later than 120 days after the date of the enactment of this Act, and quarterly thereafter, the Secretary of Defense shall provide a briefing to the Committees on Armed Services of the House of Representatives and the Senate on covered military cyberspace activities that the Department of Defense carried out during the preceding quarter.
>
> (d) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to limit the authority of the Secretary of Defense to conduct military activities in cyberspace.

That seemed to be a response to earlier claims by DOD that it didn't have to brief such things to Congress.

As it happens, that's another of the sections of the Defense Authorization to which the Administration objects (though they did not issue a veto threat on it).

> Military Activities in Cyberspace: The Administration agrees that appropriate military operations in cyberspace are a vital component of national security, but objects to Section 962. The Administration has concerns about this provision and wants to work with Congress to ensure that any such legislation adds clarity and value to our efforts in cyberspace.

The choice by administrations to conduct cyberwar under DOD's auspices rather than CIA's as a way to avoid oversight is something that John Rizzo (!) warned about. And the bill has already given the Administration an extra three months of secret cyberwar before it has to start briefing Congress compared to the original bill.

What kind of war is Obama waging in cyberspace it refuses to tell Congress about?

DHS' TOP CYBERSECURITY OFFICER RESIGNS

As Marc Ambinder reports, the top cybersecurity guy at DHS, Phil Reitinger, announced his resignation today. Which is pretty odd, given that Obama just rolled out his cybersecurity strategy a few days ago. Though that's the excuse that Reitinger offered for the timing of

his departure.

> With significant progress having been made in activities across NPPD [National Protection and Programs Directorate], with growing recognition of DHS's roles and authorities, and the cybersecurity legislative proposal now delivered to the Hill, it's a logical point for me to leave the Department of Homeland Security and allow the team that we have developed together to carry our initiatives forward. [bracketed comment Ambinder's]

Okaaayyyy then. You finally win the pissing contest between NSA and DHS over who will lead cybersecurity and then you … leave? Leaving no one to lead the program you've fought so hard to lead, not to mention leaving no one to lobby for the legislative proposal just sent to Congress?

Though Reitinger isn't technically the CyberCzar, he makes at least the 10th top cybersecurity official to have left since 9/11.

Update: Here's how his job was described when he was hired.

> In addition to overseeing the department's mandate to protect government networks, Reitinger also will be responsible for coordinating Uncle Sam's outreach to private companies that own and operate the nation's most vital information assets. These digital assets power everything from water and electricity distribution systems to telecommunications and transportation networks.

As I described here, one of the most sensitive aspects of the cybersecurity legislation the Administration proposed (and, I think, one of its weakest parts), is the means by which critical infrastructure entities prove to the government that they have adequate

cybersecurity. It would seem really important to have continuity in this position to shepherd this part of the legislation through Congress.

Unless, of course, he's planning on representing the industry as the bill wends its way through Congress. Or, set up one of the auditing companies that will get rich off the way the legislation was written.

ERIC HOLDER CLAIMS RULE OF LAW EXISTS IN CYBERSPACE

Just days after asking Congress not to give the intelligence community a hard deadline to put a basic cybersecurity measure into place, the Obama Administration rolled out a cybersecurity strategy yesterday with great fanfare. The event itself seemed designed to bring as many Cabinet Secretaries into one place at one time—Hillary Clinton, Gary Locke, Janet Napolitano, and Eric Holder, along with DOD Deputy Secretary William Lynn and White House Cybersecurity Coordinator Howard Schmidt—to give the appearance of real cooperation on cyberspace issues.

The strategy itself is still mostly fluff, with paragraphs like this:

> This future promises not just greater prosperity and more reliable networks, but enhanced international security and a more sustainable peace. In it, states act as responsible parties in cyberspace—whether configuring networks in ways that will spare others disruption, or inhibiting criminals from using the Internet to operate from safe havens. States know that networked infrastructure must be protected, and they take measures to secure it from

> disruption and sabotage. They continue to collaborate bilaterally, multilaterally, and internationally to bring more of the world into the information age and into the consensus of states that seek to preserve the Internet and its core characteristics.

And loaded paragraphs like this, in the section on military goals:

> **Recognize and adapt to the military's increasing need for reliable and secure networks**. We recognize that our armed forces increasingly depend on the networks that support them, and we will work to ensure that our military remains fully equipped to operate even in an environment where others might seek to disrupt its systems, or other infrastructure vital to national defense. Like all nations, the United States has a compelling interest in defending its vital national assets, as well as our core principles and values, and we are committed to defending against those who would attempt to impede our ability to do so.

Lucky for DOD, there was no discussion of deadlines anywhere in the document, so they didn't have to admit their plan to "adapt to the military's increasing need for reliable and secure networks" was a long term project.

And then the strategy had a lot of language about norms, which places our cybersecurity strategy in the paradigm and language of international regime development from foreign relations (interestingly, Hillary started off the parade of Secretaries, further emphasizing this diplomatic approach).

But what struck me most about this dog and pony show, delivered on the day SCOTUS endorsed the executive branch's efforts to hide torture

behind the invocation of state secrets, was Eric Holder's discussion about rule of law in cyberspace.

> In recent months, the Justice Department has announced takedowns of significant criminal groups operating from Romania, Egypt, and elsewhere that had been victimizing American businesses and citizens – including children. We've also brought multiple criminal conspirators to justice for their roles in coordinated cybercrimes that, according to court documents, netted nearly 1.5 million dollars from U.S. victims. And, just a few weeks ago, we announced an operation to disable an international criminal network that had infected more than two million computers worldwide with malicious software. Until we stepped in – with the help of industry and security experts, as well as key international partners – this malware was allowing criminals to capture bank account numbers, user names, and other sensitive and financial information online.
>
> While we can all be encouraged by these and other successes, we cannot become complacent. As President Obama has repeatedly indicated – we must, and we will, take our global fight against cyber threats to the next level. The strategy that we are announcing today is an affirmation of that promise. **It reinforces our nation's support for the Budapest Convention –and for efforts to establish the rule of law in cyberspace**. It also reflects our ongoing commitment to prevent terrorists and other criminals from exploiting the Internet for operational planning or financing – or for the execution of attacks. [my emphasis]

We're going to build rule of law in cyberspace

apparently. Sort of like an extraterrestrial colony to preserve a way of life that used to exist on Earth (or at least in the US), but no longer does.

So rest assured, if this cyberstrategy is successful, we can expect rule of law in cyberspace as compensation for the fact that the government has destroyed rule of law in meatspace.

Oh, on that note, there was no discussion of any investigation into how it was that a media outlet, Wikileaks, was attacked with a sophisticated DDOS attack, ultimately damaging free speech.