# WHY DOES DUQU MATTER?

The short answer is that if your PC got infected by Stuxnet last year, you were just collateral damage, unless you were operating a very specific set of uranium enrichment centrifuges. If you get Duqu this year, your network is under attack from a CIA/Mossad operation. They might seem a little outrageous, but bear with me while we get into the weeds of what Duqu is all about. I will lay out a set of assertions that lead to the conclusion that Duqu really is the "precursor to the next Stuxnet" as Symantec say in their whitepaper.

1. Stuxnet was created by the CIA and the Mossad

Although no one has officially claimed responsiblity for Stuxnet, both the U.S. and Israeli governments have done everything but take offical responsibility. Neither government has ever denied responsibilty, even when directly asked. In fact, officials in both governments have been reported as breaking out in big smiles when the subject comes up.

2. Duqu is from the same team that created Stuxnet.

The first clue that Duqu is from the Stuxnet team is the similarities between the rootkit components in both pieces of malware. The folks who have studied the two most closely are sure that Duqu is based on the Stuxnet component's source code. Despite what you may have read on the internet, the actual source code to Stuxnet is not publicly available. Some folks have reverse-engineered some of the Stuxnet source code from the binaries that are available, for various technical reasons, I'm sure that these don't serve as the basis for Duqu.

Duqu even has a fix for a bug in Stuxnet. Also, the only two pieces of malware in history to install themselves with as Windows device drivers with legitimate, but stolen, digital

certificates are Stuxnet and Duqu. Both Stuxnet and Duqu were active in the wild and managed to evade detection for many months. While that's not unheard of for malware, it is another point of similarity.

Stuxnet targeted a specific industrial control system (ICS) installation (the Siemens PLCs that were used to control the centrifuges at Natanz). Here's the lastest on what Duqu targets:

> Some of the companies affected or targeted by Duqu include the actual equipment that an ICS would control such as motors, pipes, valves and switches. To date, the vendors that make the PLC, controllers and systems/applications found in control centers are not yet affected, although this information could change as more variants are identified and these vendors look more closely at their systems.

There are no other instances of computer malware that target these sorts of installations.

3. Stuxnet was a worm, Duqu is not.

Stuxnet was a very aggressive computer worm. It had to be to jump the "air gap" that protects a secure ICS such as the system that ran the Natanz installation. When Stuxnet was discovered, the A-V vendors quickly discovered millions of computers had been (benignly) infected with Stuxnet. Duqu, on the other hand, has been found on only a handful of computers. Interestingly, no one has yet discovered the dropper, that is, the program used to place the Duqu rootkit on the infected machines. This is almost certainly because Duqu is being placed on these machines via a spear phishing attack. In spear phishing, specific targets are chosen and the attack is customized to the target.

4. Duqu is being used to download a RAT (Remote Access Trojan)

The rootkit component was used to download a standalone program designed to steal information from the computer that it has infected (including screenshots, keystrokes, lists of files on all drives, and names of open windows). Duqu is doing computer network reconnaissance. The information gathered by Duqu is very useful for planning future attacks. Before the command and control server was taken off-line, Symantec observed Duqu downloading three additional files to an infected machine.  The first was a module that could be injected into other processes running on the machine to gather some process-specific information as well as the computer's local and system times (including time zone and daylight savings time bias). Another downloaded module was used to extend the normal 36-day limitation on Duqu installations. The last downloaded module was a stripped down version of the standalone RAT, lacking the key logging and file exploration functionality.

5. Put it all together and it adds up to a well-executed, highly targeted covert operation

For the last ten months, Duqu has been quietly stalking a small number of industrial manufacturers. No one even noticed before early September and it wasn't until last week that the nature of the threat was clear to anyone. Duqu is spying on a handful of companies, gathering data that will be used for the design and development of the true Stuxnet 2.0. One thing we don't know is who the target of Stuxnet 2.0 will be. But I have a suspicion. Nothing indicates that the ultimate target (i.e., Iran) of the Stuxnet team has changed. In August of this year, Iran announced that it had activated its first pre-production set of his newer IR-2m and IR-4 centrifuges. These are the successors to the centrifuges that Stuxnet attacked. If you wanted to do these centrifuges what Stuxnet did to the earlier IR-1 centrifuges, you would need a lot of specific data about the safe operating specs of the various components that go into making advanced centrifuges. If you knew or suspected who was

supplying Iran with these components, you might want to gather some data from the internal networks of those suppliers. That's what I think the point of Duqu really is.

---

# DID DUQU FIX THE BUG THAT REVEALED STUXNET?

Duqu isn't Christopher Lee in *Attack of the Clones*, but it is the newest computer malware to hit mainstream consciousness. It's attracting attention mainly because it is based on the same software source code base as the Windows portion of Stuxnet. If you haven't heard about Duqu, check out the Wired article that first alerted me to its existence. If you are interested in the technical details, you need to read the excellent write-up by Symantec (pdf link).

Unfortunately, the twitterverse, blogosphere, and the computer security profession all seem to be caught up in a hype/debunking/speculation cycle that is spreading more heat than light. The primary significance of Duqu is what it tells us about the operation behind Stuxnet and Duqu, i.e. that it is an on-going enterprise conducting computer espionage and sabotage around the world. The fact that it is rather obviously (though not publicly) run by the U.S. intelligence community should concern everyone. I'll put up a more extensive post later (including a timeline!) detailing what the Duqu phase of the Stuxnet operation tells us about the cyberwarfare strategy of the U.S. and how it is endangering the safety and security of the U.S. and the whole industrialized world. But first, I want to remind everyone how Stuxnet was originally discovered:

> … the VirusBlokAda security firm in Minsk, received what seemed to be a relatively mundane email on June 17, 2010. An Iranian firm was complaining that its computers were behaving strangely, shutting themselves down and then rebooting. Ulasen and a colleague spent a week examining the machines. Then they found Stuxnet. VirusBlokAda notified other companies in the industry, including Symantec.

This incident became curiouser and curiouser as Symantec, Langner, and others took apart Stuxnet. There wasn't any obvious reason that Stuxnet would have caused that sort of behavior on an infected computer. I even wondered at the time whether or not Stuxnet's cover was blown intentionally since the perpetrators moved quickly to call further attention to themselves. But, thanks to the good work of the Symantec team, we can surmise something quite revealing about the initial discovery of Stuxnet.

The rootkit component of Duqu is quite similar to, but not exactly the same as, the one in Stuxnet. In both cases, if the infected computer gets rebooted while it is infected, the rootkit wants to make sure that it is running before the operating system is fully loaded. That's why this rootkit (both flavors, Stuxnet and Duqu) is packaged as a hardware device driver. Here's a feature of Duqu's driver that wasn't present in Stuxnet (as described by Symantec on page 4 of the pdf linked above):

> The driver then registers a DriverReinitializationRoutine and calls itself (up to 200 times) until it is able to detect the presence of the HAL.DLL file. This ensures the system has been initialized to a point where it can begin injecting the main DLL.

The bolded portion is the new functionality that wasn't present in Stuxnet. As a software developer, this detail tells me a lot. The driver is checking to make sure that the hardware abstraction layer (HAL.DLL) of Windows is loaded before it proceeds with the re-infection routine. The HAL is a portion of the Windows OS that really needs to be loaded before device drivers can function properly. Between the time that Stuxnet was deployed and this later version was compiled, the Stuxnet team identified a problem (a race condition) with their software being loaded before the HAL, probably only under the rarest of circumstances. So they modified their program to take this possible condition into account.
As I thought about this, I realized that the likely impact of the Stuxnet device driver being loaded before the HAL was properly initialized would almost certainly be that the machine would continuously crash and reboot. Look again at how Stuxnet was first discovered (remember it was in the wild for at least a full year before it was noticed by any anti-virus vendor):

> … the VirusBlokAda security firm in Minsk, received what seemed to be a relatively mundane email on June 17, 2010. An Iranian firm was complaining that its computers were behaving strangely, shutting themselves down and then rebooting. Ulasen and a colleague spent a week examining the machines. Then they found Stuxnet. VirusBlokAda notified other companies in the industry, including Symantec.

By November 3, 2010 (the compile date of the Duqu component), the Stuxnet team had fixed the bug that led to the discovery of Stuxnet last year. And then went almost another full year without being discovered by the anti-virus vendors. It is likely to be a lot harder to reconstruct what the Stuxnet team has been up to this time around, but it is clear that the operation is on-going and we can assume (unless

specific information turns up pointing in a different direction) that the primary target is still the Iranian nuclear program.

---

# STUXNET: THE CURIOUS INCIDENT OF THE SECOND CERTIFICATE

*"Is there any point to which you would wish to draw my attention?"*

"To the curious incident of the dog in the night-time."

"The dog did nothing in the night-time."

"That was the curious incident," remarked Sherlock Holmes.

Arthur Conan Doyle (Silver Blaze)

*[From ew: William Ockham, who knows a whole lot more about coding than I, shared some interesting thoughts with me about the Stuxnet virus. I asked him to share those thoughts it into a post. Thanks to him for doing so!]*

The key to unraveling the mystery of Stuxnet is understanding the meaning of a seemingly purposeless act by the attackers behind the malware. Stuxnet was first reported on June 17, 2010 by VirusBlokAda, an anti-virus company in Belarus. On June 24, VirusBlokAda noticed that two of the Stuxnet components, Windows drivers named MrxCls.sys and MrxNet.sys, were signed using the digital signature from a certificate issued to Realtek Semiconductor. VirusBlokAda immediately notified Realtek and on July 16, VeriSign revoked the Realtek certificate. The very next day, a new Stuxnet driver named jmidebs.sys appeared, but this one was signed with a certificate from JMicron Technology. This

new Stuxnet driver had been compiled on July 14. On July 22, five days after the new driver was first reported, VeriSign revoked the JMicron certificate.

The question I want to explore is why the attackers rolled out a new version of their driver signed with the second certificate. This is a key question because this is the one action that we know the attackers took deliberately after the malware became public. It's an action that they took at a time when there was a lot of information asymmetry in their favor. They knew exactly what they were up to and the rest of us had no clue. They knew that Stuxnet had been in the wild for more than a year, that it had already achieved its primary goal, and that it wasn't a direct threat to any of the computers it was infecting in July 2010. Rolling out the new driver incurred a substantial cost, and not just in monetary terms. Taking this action gave away a lot of information. Understanding why they released a driver signed with a second certificate will help explain a lot of other curious things in the Stuxnet saga.

It's easy to see why they signed their drivers the first time. Code signing is designed to prove that a piece of software comes from a known entity (using public key infrastructure) and that the software hasn't been altered. A software developer obtains a digital certificate from a "trusted authority". When the software is compiled, the certificate containing the developer's unique private key is used to "sign" the code which attaches a hash to the software. When the code is executed, this hash can be used to verify with great certainty that the code was signed with that particular certificate and hasn't changed since it was signed. Because drivers have very privileged access to the host operating system, the most recent releases of Microsoft Windows (Vista, Win7, Win2008, and Win2008 R2) won't allow the silent installation of unsigned drivers. The Stuxnet attackers put a lot of effort into developing a completely silent infection process. Stuxnet checked which

Windows version it was running on and which anti-virus software (if any) was running and tailored its infection process accordingly. The entire purpose of the Windows components of Stuxnet was to seek out installations of a specific industrial control system and infect that. To achieve that purpose, the Windows components were carefully designed to give infected users no sign that they were under attack.

The revocation of the first certificate by VeriSign didn't change any of that. Windows will happily and silently install drivers with revoked signatures. Believe it or not, there are actually good reasons for Windows to install drivers with revoked signatures. For example, Realtek is an important manufacturer of various components for PCs. If Windows refused to install their drivers after the certificate was withdrawn, there would be a whole lot of unhappy customers.

The release of a Stuxnet driver signed with a new certificate was very curious for several reasons. As Symantec recently reported [link to large pdf], no one has recovered the delivery mechanism (the Trojan dropper, in antivirus lingo) for this driver. We don't actually know how the driver showed up on the two machines (one in Kazakhstan and one in Russia) where it was found on July 17, 2010. This is significant because the driver is compiled into the Trojan dropper as resource. Without a new dropper, there's no way for that version of the virus to have infected additional computers. And there is no evidence that I'm aware of that Stuxnet with the new driver ever spread to any other machines.

The release of the newly signed driver did exactly one thing: Increase publicity about Stuxnet. The inescapable conclusion is that the Stuxnet attackers wanted to make headlines in July 2010. As Holmes says in *Silver Blaze*, "one true inference invariably suggests others". From this one inference, we can begin to understand

the most puzzling parts of the Stuxnet project. Who would publicize their secret cyber attack on an enemy? Why were there clues to the identity of the attackers left in the code? Why did the last version of Stuxnet use multiple 0-day exploits? Why did the attackers only take minimal steps to hide the true nature of the code? The answer to these questions is relatively simple. The Stuxnet project was never intended to stay secret forever. If it had been, there would never have been a new Stuxnet driver in July 2010. That driver helps put all the other pieces in context:  the clues left inside the code ("myrtus", "guava", and using May 9, 1979 as a magic value); the aspects of the code that have led various experts to label Stuxnet as amateurish, lame, and low quality; even the leak campaign by the U.S. and Israeli governments to unofficially take credit for Stuxnet. Rather than being mistakes, these were elements of the larger Stuxnet project.

Stuxnet was more than a cyber attack. It was a multi-pronged project. The design of the code supports the overall mission. The mission included a publicity campaign, or as the military and intelligence folks style it, a PSYchological OPeration (PSYOP). Unlike a typical malware attack, Stuxnet had (at least) two distinct phases. Phase 1 required a stealthy cyber attack against the Iranian nuclear program. Phase 2 required that the effects of that cyber attack become widely known while giving the perpetrators plausible deniability. That may seem a little strange at first, but if you put yourself in the shoes of the attackers, the strategy is more than plausible.

In fact, the attackers have explained it all. Take a look back at the story told in the New York Times article on January 15, 2011. According to the NYT, the Stuxnet project started as an alternative to an Israeli airstrike:

> Two years ago, when Israel still thought its only solution was a military one and

> approached Mr. Bush for the bunker-busting bombs and other equipment it believed it would need for an air attack, its officials told the White House that such a strike would set back Iran's programs by roughly three years. Its request was turned down.

Couple that statement with the reason the article appeared when it did:

> In recent days, American officials who spoke on the condition of anonymity have said in interviews that they believe Iran's setbacks have been underreported.

Imagine that you're an American policymaker who has to choose between launching a cyber attack and allowing a close ally to launch an actual military attack. If you choose the cyber attack option, how will anyone know that you've succeeded? If no one knows that you've successfully delayed the Iranian nuclear program, you'll be vulnerable to right-wing attacks for not doing enough to stop Iran and the pressure to bomb-bomb-bomb of Iran will grow. There's another reason to publicize the attack. If you're a superpower who starts a cyber war, you have to realize that your country contains a lot of very soft targets. You would want to make a big splash with this malware so that your industrial base starts to take the cyber war seriously. So, from the very beginning, the project included planning for the inevitable discovery and understanding of the Stuxnet malware. Just like the spread of the malware itself, the psyop will be impossible to directly control, but easy enough to steer in the appropriate direction. The attackers likely didn't know it would be Symantec and Ralph Langner who would start to unravel the exact nature of the Stuxnet malware, but they knew someone would. And they knew they would be able to get the New York Times to print the story they wanted to get out (I'm not demeaning the work of the reporters on this story, but I would

hope they realize that there is a reason they aren't being investigated for publishing a story about our efforts to undermine Iran's nuclear program and James Risen was).

---

# SARAH PALIN: GIBBERISH WE CAN BELIEVE IN?

Energy is supposed to be Sarah Palin's strong point, right? After all, she is the Governor of Alaska, and more to the point, was the chair of the Alaska Oil and Gas Conservation Commission, the agency that is supposed to "protect the public interest in exploration and development of oil and gas resources, while ensuring conservation practices, enhancing resource recovery, and protecting the health, safety, environment, and property rights of Alaskans." But when she was asked about ensuring that the fruits of domestic oil drilling would go to the domestic market, her answer was complete gibberish. By now, most of you have seen the video or read the transcript of her answer:

> Oil and coal? Of course, it's a fungible commodity and they don't flag, you know, the molecules, where it's going and where it's not. But in the sense of the Congress today, they know that there are very, very hungry domestic markets that need that oil first. So, I believe that what Congress is going to do, also, is not to allow the export bans to such a degree that it's Americans that get stuck to holding the bag without the energy source that is produced here, pumped here. It's got to flow into our domestic markets first.

Most people who've commented on this have just written it off as incomprehensible nonsense, especially the bit about flagging molecules, but I think 'flagging molecules' is the key to understanding what's going on inside Palin's brain. When I first heard this, I immediately noticed something that others had not. That answer is not just gibberish. It's gibberish from somebody whose grasp of the basic facts about energy markets is superficial and tenuous, at best.

Nine years ago, I was hired for my first software development job for an energy company. The company sent me to a short course covering the basics of the energy business. The very first page of the course materials was titled 'Fungible commodities' and described the worldwide market for energy industry raw materials (oil, coal, and natural gas). Palin started her answer with a very basic point that was actually germane to the question, albeit apparently contradictory to where she ended up. If oil is a fungible commodity, export bans are pointless. (I'm not necessarily endorsing the linked book's conclusion, it was just the first source I found that made the traditional argument.)

The second most memorable part of that course I took was the explanation of natural gas pipelines. The pipeline companies deliver gas from one place to another, but they don't necessarily 'ship' it. When a company pays to ship natural gas from Point A to Point B, it doesn't mean that the natural gas they put on the pipeline at Point A actually ends up at Point B. All natural gas is the same (i.e. it is fungible), so you don't necessarily get back the same stuff you put in. As the American Gas Association explains:

> Displacement transactions permit the lateral movement of gas through a transportation network. The configuration of many pipelines is such that it may not be apparent whether a

> given movement of gas is forward or backward from the point of receipt. It can be argued that all transportation service is performed by displacement as the physical delivery of the same molecules of gas is impossible.

Palin riffs from one aspect of fungibility to another before she starts her policy response to the question. That response is heavy with emotional terms (‘very, very hungry’, ‘holding the bag’, ‘got to flow to domestic markets first’) without any clear sense of what the policy is (Are export bans good or bad, who can tell from that answer?) This is the sort of answer you get from inexperienced people trying to hide their inability to apply the facts they know to a real situation. We saw the same thing in the Gibson interview (‘Charlie, don’t blink’ seemed to be the core theme there), but we expected it when she talked about foreign policy. For someone who John McCain claims "knows more about energy than probably anyone else in the United States of America", Sarah Palin’s energy policy gibberish seems suspiciously like the results of late-night test cramming, not the product of real experience.

---

# THE STRANGE CASE OF HIWA ABDUL RAHMAN RASHUL (PART 2)

In part 1, I laid out the facts surrounding the detention and illegal transfer of Hiwa Abdul Rahman Rashul. In this post, I want to demonstrate why this case matters. There is a pattern to the Bush/Cheney Administration’s illegal usurpation of executive power. Because the pattern broke down in this case, the strategy behind that power grab is laid bare.

The struggle within the administration over the disposition of Rashul and the way it was resolved helps to illuminate the true nature of the current regime. Perhaps this case creates an opening to unravel the authoritarian infrastructure that has been built within our country in the last eight years.

# Part 2: Why it matters

In the grand scheme of things, focusing on this case might seem a little like busting Al Capone for tax evasion. The Bush/Cheney Administration has institutionalized the most egregious extralegal executive abuses in our nation's history. As matters of policy, they've launched a war of aggression under false pretenses, violated the most basic human right treaties, trashed the Fourth Amendment, denied the right of habeas corpus to citizens and non-citizens alike, set up secret prisons, disappeared their presumed opponents around the world, tortured the innocent and presumed guilty alike, conducted sham military tribunals against the underage and the mentally ill, and, worst of all, claimed the power to indefinitely detain anyone in the world, including U.S. citizens, without any external check whatsoever. And that's just the stuff they have admitted to.

If we want to undo all this, and I very much do, we'll have understand how they were able to accomplish it. I'm not going to rehash the sociopolitical environmental conditions that the administration took advantage of. Folks here understand that the generalized fear and anger after the attacks of September 11, 2001, the fecklessness of the Democratic party, the docile and compliant traditional media, the tight discipline within the Republican party, and the latent authoritarian impulses of a sizeable minority of the country created the necessary conditions for what happened. I want to focus on how the administration manipulated secrecy, its own people's psychology, and the instinct

for institutional self-preservation to manage a shifting set of narratives that allowed them to follow a deliberate strategy of expanding executive power and upsetting the constitutional balance of government while evading responsibility and steam-rolling all opposition. Then, I hope to show how this case exposes some chinks in the rather substantial armor of these malefactors.

## Competing Narratives

One of the biggest problems in telling the full story of the Bush/Cheney Administration various illegal activities is distinguishing between the various narratives surrounding each episode. In every case, there is the story of the actual events are that always hidden behind a veil of secrecy. Then there is the momentary political scandal caused by a leak or leaks. The traditional media and the political opposition typically focus on that narrative only until there is an administration response. The administration responds with a modified limited hangout, selectively declassifying or leaking some information and augmenting it with false or misleading public statements to create an alternative narrative to defuse the political scandal. Later on, additional information comes out that contradicts the official narrative, but by that time, the issue is ‘old news’. Only after a series of scandals could anyone notice that there is a pattern to the actual events, the leaked narratives and the official narratives that help illuminate the strategy that the administration used. Keeping in mind that we always have to be alert to the unreliable narrator problem, let’s take a look at these narratives in the order they come into the public consciousness, the scandal, the hangout, and what really happened.

## Narrative 1:  The Scandal

The most easily overlooked, and most interesting, aspect of the scandal narrative is that it is almost always driven by institutional

self-preservation. In this instance, the confirmation of the existence of ghost detainees in Iraq was a side effect of Gen. Taguba's investigation of the Abu Ghraib scandal. The original leakers wanted to separate themselves from the Abu Ghraib scandal and prove they had explicit orders from higher-ups to hide Rashul. The first story about Rashul starts like this:

> The top U.S. commander in Iraq, Lt. Gen. Ricardo Sanchez, issued a classified order last November directing military guards to hide a prisoner, later dubbed "Triple X" by soldiers, from Red Cross inspectors and keep his name off official rosters. The disclosure, by military sources, is the first indication that Sanchez was directly involved in efforts to hide prisoners from the Red Cross, a practice that was sharply criticized by Maj. Gen. Antonio Taguba in a report describing abuses of detainees at the Abu Ghraib prison near Baghdad.

Whatever the triggering event, whether there's a whistleblower, an inadvertant disclosure, or just someone with a score to settle, the first big story in the mainstream press is usually shaped by a bureacracy trying to protect itself. Which mean the story always has one big revelation and it almost always points the finger at political appointees. That naturally leads to an official administration response.

## Narrative 2: The Modified Limited Hangout

This is where the Bush/Cheney team has shown real innovation. The typical script for goes like this. You put a Cabinet-level official (or if you do it on background, the infamous Senior Administration Official or SAO) out front, backed up by some guy in uniform. After the obligatory 'the terrorists are gonna kill us all' hand-wringing, the SAO confirms some of the

details from the scandal story and adds a few new juicy bits, but denies or ignores significant elements of the previous narrative. The situation is presented as perfectly normal, at least for a post 9/11 world, and besides, the lawyers signed off on the whole thing, so no one could possibly question the purity of the administration motives, except the partisan media and their anonymous sources who are obviously from the Democrat party. Any uncomfortable questions are avoided because the answers are, of course, classified. The main purpose of the new narrative is deflect attention away from the most damaging aspects of the story. A key function of the cover story is to allow the policymakers to hide behind the lawyers and the lawyers to disclaim any responsiblity for the policy.

## Narrative 3: What really happened

Of course, the cover narrative never satisfies everyone. For example, Philippe Sands' dogged investigation of torture at Guantanamo led him to uncover the facts behind the institutionalization of torture there. Sands' article for Vanity Fair exposing the false timeline was really the inspiration for my analysis of the Rashul case. Valtin's yeoman work in ferreting out the fact that SERE techniques were the first choice for interrogations by some in this administration provided another clue. Ultimately, I came to realize that there was a pattern, even in the actual narratives.

In a comment to my previous post, Ondelette gets this almost exactly right, so I'll quote that:

> I think your timeline on Rashul is probably quite correct and very devastating. But I tried to do the '*when did the document come and when did the illegal actions come*' thing several times now, and it turns out as information seeps out, every time line

> is similar to yours with Rashul.
>
> The conduct begins.
> The administration wishes to make the conduct the norm.
> They solicit an opinion from OLC, who is led to believe that the conduct is only being contemplated.
> The OLC writes a memorandum.
> Written policies flow from the memorandum.

The one thing I think Ondelette gets wrong is the bit about the OLC thinking that the conduct is only being contemplated. I think the available evidence points us in a different direction. In this case, Goldsmith clearly knew that Rashul was already in Afghanistan when Gonzales asked for the opinion. Even before he was confirmed, when Goldsmith gets the call from Philbin it's described as urgent. You don't make calls like that for contemplated action. Those issues become urgent after the fact when someone questions the legality of the action. Compare this to what we know about the warrantless wiretapping. The program was started, the FBI and others questioned the legality, and then the OLC opinion was issued to shut down the debate. If you look closely at Yoo's DOD torture memo, you find some very direct coorelation between what had already been done at Guantanamo and the specific actions he immunized. This coorelation goes beyond the techniques documented in the request from Diane Beaver to Rumsfeld to include 'unauthorized' techniques used on al-Qatani and others. Here's how I would alter Ondelette's outline:

- An illegal policy is adopted.
- The policy is implemented.
- The policy is challenged.
- The OLC is presented with the Hobson's choice of authorizing the policy as

already implemented.
- The OLC writes an opinion.
- The policy becomes ‘legal’.
- A select few in Congress are notified about the policy, but only in broad outlines and under strict secrecy.

The OLC was repeatedly confronted with being asked to come up with a legal justification for a ‘vital’ program in the so-called War on Terror. Goldsmith’s descriptions of his interactions with David Addington are revealing. On one occasion, he quotes Addington thusly:

> If you rule that way, the blood of the hundred thousand people who die in the next attack will be on your hands.

Waving the bloody shirt was even more effective for the administration internally than it was politically. Despite all of Cap’n Jack’s protestations to the contrary, he effectively caved to this pressure with his draft opinion of March 2004.

## Rashul: Frayed Narratives

The Bush/Cheney Administration has been remarkably effective in creating a consistent false narrative that disguises the true nature of their regime and protects the perpetrators from being held accountable. In the case of Hiwa Abdul Rahman Rashul, there are some interesting holes in the cover story and breakdowns in the Administration’s execution of their standard game plan that leave an opening for an effective investigation. The first failure of execution was Goldsmith’s initial unwillingness to bless the rather obvious breach of the Geneva Convention. By bringing Rashul back to Iraq and *hiding him from the ICRC,* the administration engaged in conspiratorial conduct. By renewing the program of disappearing Iraqis to Afghanistan on the basis of a DRAFT

opinion from Goldsmith, the administration showed that they considered legality nothing but a formality. Finally, the cleverest thing part of the Bush/Cheney Adminstration game plan for implementing their tyrannical policies was the way they implicated Congress in their actions by manipulating Congressional notifications. I suspect that Congress is in the clear on this one. During the Rumsfeld modified limited hangout presser there was this exchange:

> SEC. RUMSFELD: And as we get more information, we'll make it available. The Congress has been briefed extensively on this, as I understand it. No.
>
> MR. DELL'ORTO: Not this particular case, as far as I know.
>
> MR. DIRITA: Yes. No, we've done some notifications to the staff on the Hill, both us and the CIA, with respect to the details of this particular case. And as we get more, we will provide it.

That's clear as mud. If there were notifications, it's likely they were done in June 2004 rather than July 2003 when the deed was done.

In that same presser, Rumsfeld openly implicated himself and George Tenet in the coverup. The CIA OIG criminal referral implicates the highest levels in the DOJ. The available information leaves a number of avenues open for Congressional investigation. Might I suggest to Sen. Leahy that he add that criminal referral to the list of documents he's been asking for? Indeed, I will. At the same time, I'll remind the Obama camp of that promise they gave Will Bunch and that they will likely be in charge of all these records in a few months. I'll also remind the folks here that our duty as citizens includes keeping the pressure on 'our' guys to do the right thing. I'm not naive enough to

think that Obama will do much about any of this unless there's some pressure. In fact, I'm old enough to remember that the best conditions for limiting Executive Branch power are when there is a Dem President and Dem Congress. We need to help Leahy, Levin, Waxman, and the rest that they need to keep pushing.

Here's my bottom line. There's plenty of evidence of war crimes for an international tribunal to start an investigation of Bush, Cheney, Rumsfeld, and the whole crew in February 2009. I think an international tribunal, as unlikely as it seems, would be a disaster. It would ignite a jingoistic furor in this country. These guys are our criminals and our responsibility. It's time for America to face up to what we've allowed this country to become. Unraveling some this big has to start with a single thread. I think that thread just might be asking what happened to Hiwa Abdul Rahman Rashul and what are we going to do about it?

[UPDATE]

If you really want to understand what Cheney's been up to the last eight years, you need to go back read the Iran-Contra Congressional Minority Report that he and David Addington wrote. The goal has always been as much about expanding Executive Branch power as anything else. I'm sure that Bush and Cheney get off on the torture, but for Cheney at least, that's secondary to the effort to establish what is effectively an elected constitutional dictator. That's another thing Cap'n Jack never understood. It was never really about protecting America from terrorists. It was about using that as an excuse to push the real agenda.

[WilliamOckham makes an excellent, and absolutely critical, point in the update paragraph immediately above about the overarching plan of Cheney to retake, and expand further, Executive Branch power that was spelled out in the Iran-Contra Congressional Minority Report. And that is exactly what we have been witnessing in the announcement by the

Administration of last minute wild expansion of domestic spying and datamining capabilities, and as discussed in the two "FISA Redux" posts here and here. – bmaz]

---

# THE STRANGE CASE OF HIWA ABDUL RAHMAN RASHUL (PART 1)

[Today Emptywheel has a special treat in the form of a guest post from one of our very longtime commenters, William Ockham. Marcy alluded to this right before she left. WO really drilled deep into this story and has produced a great article. As the title suggests, there will also be a Part II that will delve into the implications. Give WO some love and participation in comments, and in light of the special nature of this post, please stay on topic for this one; if there are other issues, please feel free to use the previous post on the Bates Contempt Decision for those. Thank you. – bmaz]

In June 2004, Hiwa Abdul Rahman Rashul had his 15 minutes of fame when Secretary of Defense Donald Rumsfeld answered questions at a press conference about the detainee known to American soldiers only as Triple X, the first ghost detainee transferred from CIA custody to the U.S. military. Rashul was suspected of being a member of Ansar al-Islam, a violent Kurdish Sunni Islamist movement opposed to the dominant Kurdish groups of northeastern Iraq. The real story of Hiwa Abdul Rahman Rashul wasn’t his terrorist past or his time as a ghost detainee of the DOD, but his treatment by the CIA in between.

# Part 1: Did the DOJ cover up what its own OLC ruled was a war crime committed by the CIA?

The Office of Legal Counsel in the Bush Administration's Department of Justice has had a notoriously broad view of the Executive Branch's ability to define our obligations under the Geneva Conventions. But if the OLC under Goldsmith and Bradbury decided that the CIA had engaged in a grave breach of the Geneva Conventions (and even John Yoo agreed), and the CIA OIG had made a criminal referral to the DOJ, wouldn't you expect a prosecution? Recently released CIA documents suggest that such a referral was made, but no prosecution occurred. Perhaps the very public complicity of Donald Rumsfeld, Alberto Gonzales, and George Tenet played a role in the decision not to prosecute. But I'm getting ahead of myself. First, I want to make it clear that I'm using the term 'war crime' in the very narrow sense of a violation of U.S.C. § 2441.

## The Crime

Return with me now to those thrilling days of yester-year, that is, the summer of 2003. Dana Priest (in a story from October 2004) and Jane Mayer (The Dark Side) are our narrators. Mayer's account (in bold) appears to derive directly from Jack Goldsmith:

> Hiwa Abdul Rahman Rashul, a suspected member of the Iraqi Al-Ansar [sic] terrorist group, was captured by Kurdish soldiers in June or July of 2003 and turned over to the CIA, which whisked him to Afghanistan for interrogation.
>
> As he [Jack Goldsmith] awaited Senate confirmation in the summer of 2003, he

> received an urgent phone call from Patrick Philbin… Senior officials had to know right away if it was legal to move Iraqi terror suspects outside the country for interrogation… He was obliged to say he really wasn't sure what the answer was.
>
> In October, White House counsel Alberto R. Gonzales asked the Office of Legal Counsel to write an opinion on "protected persons" in Iraq and rule on the status of Rashul, according to another U.S. government official involved in the deliberations. [Mayer reports that the call from Gonzales came within the first two hours of Goldsmith's first day on the job and that he was given until the end of the week to answer the question.]
>
> Goldsmith, then head of the office, ruled that Rashul was a "protected person" under the Fourth Geneva Convention and therefore had to be brought back to Iraq, several intelligence and defense officials said.
>
> The CIA was not happy with the decision, according to two intelligence officials. It promptly brought Rashul back and suspended any other transfers out of the country.

Therein lies the tale. The U.S., as the Occupying Power of Iraq, was forbidden from transferring "protected persons" to locations outside of Iraq by Article 49 of GC-IV. Article 147 declares violations of Article 49 as 'grave breaches'. Any grave breach of the GC-IV committed by a U.S. national is a violation of the 1996 War Crimes Act (U.S.C 2441). These violations, unlike violations of Common Article 3, were not affected by the limitations and retroactive immunity provisions of the Military Commissions Act and the Detainee Treatment Act.

## The Cover-up

What happened when Rashul was returned to Iraq only made things worse for the U.S. When the existence of ‘ghost detainees’ in Iraq came to light in the aftermath of Abu Ghraib, Rashul’s story came out and the U. S. government chose to respond publicly. In the words of Donald Rumsfeld, speaking publicly on June 16, 2004:

> I was requested by the Director of Central Intelligence to take custody of an Iraqi national who was believed to be a high-ranking member of Ansar al-Islam. And we did so. We were asked to not immediately register the individual. And we did that… And we’re in the process of registering him with the ICRC at the present time.

Rumsfeld was being a little disingenuous about the process. Let’s pick up Rashul’s story as told by Edward T. Pound, writing for U.S. News and World Report:

> Rashul was returned to Iraq on October 29 [2003]. On November 18, Lt. Gen. Ricardo Sanchez, the top U.S. commander in Iraq, issued a classified order directing guards with the 800th Military Police Brigade to hide Rashul. The order was coded "Flash Red," meaning, says one military source, that it was "hot." It says that Sanchez’s command "accepts custody and detains Hiwa Abdul Rahman Rashul, a high-ranking Ansar al-Islam member." The order required extraordinary secrecy. Rashul’s name could not be disclosed to the Red Cross or to a foreign government. It prohibited the Army from entering Rashul’s name in any electronic prisoner database.
>
> Other requirements of the order include:
>
> Rashul will "remain segregated and

> isolated from the remainder of the detainee population. Under no circumstances will his presence be made known to the detainee population . . . "
>
> "Only military personnel and debriefers will have access to the detainee. . . . Knowledge of the presence of this detainee will be strictly limited on a need-to-know basis."
>
> "Any reports from interrogations or debriefings will contain only the minimum amount of source information . . . . No source reference will be made to identify [Rashul's] status, membership in Ansar al-Islam, or other terrorist group."
>
> Despite all this secrecy, Rashul has been interrogated only once—and then only briefly, a Pentagon official says.

Despite claims from administration officials that the CIA and DOD 'dropped the ball' by failing to register Rashul, it seems more likely that there was never any plan to register Rashul with ICRC and expose the fact that a grave breach of the Geneva Convention had occurred. Rumsfeld's statements (and those of his lackey Daniel Dell'Orto) implicate Rumsfeld and Tenet in a conspiracy to cover up this war crime. Unfortunately, Rashul's story seems to drop off the radar after June 2004 just as quickly as it burst on the scene the day before Rumsfeld's news conference. Even Dana Priest's story from October 2004 and Mayer's recent book don't deal with any fallout from this episode after June 2004.

The Consequences (or lack thereof)

We've been left wondering what, if anything, happened. Until now. Thanks to the FOIA efforts of the ACLU, the Center for Constitutional Justice, Amnesty International, and Washington Square Legal Services, the CIA has been forced to release over 100 documents, most of them

heavily redacted, about its ghost detention system. In addition, the CIA has released a Vaughn index of 250 representative documents (out of 7000) that they are withholding. Even with just this tip of the information iceberg, it is possible to trace the course of an internal investigation into the CIA's ghost detention activities in Iraq and, more importantly, the OIG's actions in the Rashul case.

The first document I want to highlight is an email from an OIG employee to John Helgerson, the CIA's Inspector General (and a huge, redacted, CC list). [Side note: The CIA uses Lotus Notes, but when I quote from the emails I'll use a standard format rather than trying to reproduce the idiosyncratic Notes interface. Also, the sender's department is generally not redacted, even when the name is.]

> Sent: 08/30/04 03:45 PM
>
> From: [redacted] OIG
>
> To: John L. Helgerson [other recipients redacted]
>
> Cc: [Many recipients redacted]
>
> Subject: Geneva Convention – Summary of relevant provisions
>
> John, et al. – attached is a collection of provisions drawn from the Geneva Convention that governs treatment of civilians in occupied territories that I thought most relevant based upon my limited understanding of the INV [Investigation] Staff's current work. I have included text from each of the selected provisions and explanations I thought useful drawn largely from a commentary published by the International Committee of the Red Cross a few years after the Convention was developed. I have tried to keep the summary short, but it is still imposing, and it is intended to be a starting

> point for understanding, discussion, and further research on the meaning and reach of the various provisions. [redacted] has been involved in researching the Convention and the two of us shall continue to develop background material for the investigations. Please let me know if you have specific questions that require further insight.
>
> [redacted]
>
> [Attachment – MS Word Icon]
>
> Geneva Convention IV Summary.doc

The attachment is exactly what it says. It is a thirteen-page document formatted as a table in landscape orientation. Both the email and attachment came from paper copies (i.e. they have handwritten markings). The attachment has only one marking. On the next to the last page, in the entry for Article 147, Grave Breaches, in the phrase "Unlawful deportation or transfer or unlawful confinement of a Protected Person", the second occurrence of the word "unlawful" is circled.

| | |
|---|---|
| | |

The next email I want to point out is also addressed to John Helgerson and sent 2 months later. It is probably by the same person as the first email, although the name is redacted on both.

> Sent: 10/29/04 04:08 PM
>
> From: [redacted] OIG
>
> To: John L. Helgerson
>
> Cc: [Many recipients redacted]
>
> Subject: Geneva Convention Summary
>
> John – At long last, I am sending you

> the attached memo in response to your request for a working summary relating the geneva convention to the matter of the ghost detainees. This may not look like much, but I have tried to keep it to bare minimum and avoid obscure Latin phrases, legal citations, etc. It may not stand up to scrutiny as more facts are developed, understanding increases, and the positions of OGC and the rest of the US Government become more clear. I am sure that [redaction of approximately ½ of a line] will be able to expand on and correct it, and to answer any follow-on questions you may have as a result. With that, and the soon-to-be-completed draft of an employee review policy, I will become a ghost employee.
>
> [Attachment – MS Word Icon]
> [Attachment – MS Word Icon]
>
> Geneva Convention Summary.doc Geneva Convention IV Matrix.doc

The Geneva Convention IV Matrix.doc is virtually identical to the file that was attached to the August email and is numbered with the same document tracking number as this email. Initially, I thought that the one page summary described in the email was missing, but it was included a few pages later in the document dump. All the issues raised by Rashul's treatment are covered and, as you can see in this image, the words 'individual' and 'mass transfers' are underlined in the sentence describing Article 49.

These two emails sent directly to Helgerson clearly indicate that the CIA IG is conducting a serious and consequential investigation. The synopsis of the Conventions is specific to the facts of Rashul's case.

The final piece of the puzzle is delivered by a CIA redactor's error. Two weeks after the second email to Helgerson, there was a heavily redacted email exchange between the CIA's Office of General Counsel (OGC), and lawyers in the Counter-Terrorism Center (CTC/LGL) and the Near East Division (NE/LGL). The exchange turns up a couple of different times within the document dump. The whole exchange would have been incomprehensible except for the fact that the subject of the email appears eight times and it is only redacted seven times. The subject was 'Hiwa Crimes Referral'. Hiwa is an unusual name so there is no doubt that this email exchange refers to Hiwa Abdul Rahman Rashul. Here's the exchange, in chronological order:

> 11/10/04 05:28pm
>
> From: [redacted] OGC
>
> To: [redacted]
>
> CC: [redacted]
>
> Subject: Hiwa Crimes Referral
>
> I have told the DCI and subsequently the DDO. I told them you would tell the CTC and NE management. I know that you will do it in a way that will be frank, realistic but not overly alarmist.
>
> 11/10/04 06:27pm (responding to the above)
>
> From: [redacted] CTC/LGL
>
> To: [redacted]
>
> CC: [redacted]
>
> [redacted] and I informed the D/CTC and DD/CTC.
>
> 11/11/04 10:49am (responding to initial email)
>
> From: [redacted] NE/LGL
>
> To: [redacted]

> CC: [redacted]
>
> Just want to sure that I have your okay to inform [redacted] of the matter. I think he is entitled to know, even though he is currently detailed outside the building.
>
> 11/12/04 08:07am (responding the request above)
>
> From: [redacted] OGC
>
> To: [redacted]
>
> CC: [redacted]
>
> OK.

There's no evidence that the DOJ ever took action on this referral even thought it was important enough the CIA's legal staff felt the need to personally notify, in a frank but not overly alarmist way, the new DCI (Porter Goss had just started less than 3 weeks before the referral), the DDO (head of the CIA covert operations directorate), the management of the Counter-Terrorism Center, and the head of the Near East division (the unit responsible for Iraq, Afghanistan, etc.). There's also no declination of prosecution for this case, although the document dump includes one for another referral from the CIA OIG.

This leaves us with one very important question: On what basis did the DOJ refuse prosecution? This is as clear-cut a case of a war crime as you can possibly get. Rashul was an Iraqi national taken into the custody the 'Occupying Power' in Iraq. That makes him a 'protected person'. There are no exceptions. Even spies and saboteurs have to be treated as 'protected persons' until they receive an administrative hearing. 'Protected Persons' can not be transferred to another country. To do so is a 'grave breach' and therefore a war crime under U.S. law. Under the Geneva Conventions, we have a positive duty to prosecute this crime.

Next up in Part 2, we’ll look at why this matters.