Hal Berghel

CABLEGATE - SECURITY THEATER IN THREE ACTS (GIVE OR TAKE)

When I wrote my last column, the "Afghan War Diary" Wikileaks was only a few months old. As I write this column, it is taking on a new life. As fate would have it, U.S. diplomatic cables were also leaked. The leaks associated with the Army private just keep on coming. Maybe Wikileaks should create a spin off for this sort of thing - call it Wikiooze.

This latest twist, "cablegate," the anticipated release of 250,000 U.S. Embassy Diplomatic Cables, began in late November, 2010. According to Wikileaks, 15, 652 of them were classified "secret" and 101,748 were classified "confidential." At this writing, somewhere around 300 such messages have been posted on the Wikileaks' web sites, and an undisclosed number have been released to selective media outlets, the New York Times and the Manchester Guardian among them..

According to Wikipedia, Wikileaks first appeared in 2006, allegedly founded by a small international core of dissidents, journalists, and technologists. Since 2007, the name most commonly associated with Wikileaks has been Julian Assange who can't seem to stay out of the news at the moment.

In order to encourage the casual observer to focus on the main story line. We need a story board to follow the action. I offer the following modest example.

Act I: Protasis Character Development

As readers of this column know, the current Wikileak torrent (pun intended) began with the row over the release of 91,000 classified pentagon documents released by Wikileak last July. According to the U.S. government, right-wing commentators, and openers that seek opportunities to get their names in the news, the two main protagonists behind this would be act of treason are an Army private by the name of Manning, and Wikileak spokesman Julian Assange. Manning seems to be portrayed by the media as a Wikileaks whistleblower who sought to bring attention to war crimes and other heinous acts committed by Western militaries in Afghanistan and Iraq. Assange is less-favorably portrayed as a hacker-turned-cyber-anarchist who created the audience for Manning's derring-do. The antagonists, on the other hand, seem to come from the ranks of those who either were or might be outed by Manning's disclosures, and government officials who are deeply embarrassed by their inability to understand just what happened on their watch. On their account, Manning is a symbol of what is wrong with politics in the age of globalization and the Internet, and Assange is a self-promoting former computer hacker, sex offender and information warrior who seized the opportunity to morph Manning's revelations to personal fame. Act I ends with the principals all trying to fight their way onto the increasingly crowded moral high ground. Comparisons with Watergate are inescapable.

Commentary on Act I. As I argued in my last column, there's enough blame to splash around at least a healthy proportion of the military brass whose responsibility it is to secure their infrastructure, so the plot would be considerably improved if the cast of characters were suitably enlarged. During the opening run, however, most of the military brass and political types remain content to cast aspersions from stages left and right at both the cast and each other. At this writing the pentagon and diplomatic services have suggested that there may be some weaknesses in a few pertinent INFOSEC policies. There's a news flash for you. It goes without saying that no one in either camp holds themselves personally or professionally responsible for anything at all. Diplomats argue that good diplomacy can't exist without dissing unsavory foreign leaders behind their backs. Foreign leaders argue that such disrespect is the reason why the Western democracies have little to show for their largesse. Military brass attempt to distance themselves from all sides of the debacle with their usual mantra, "Mistakes happen. We have to try harder."

For those of you who are sympathetic to Private Manning's plight, I recommend downloading the Bob Dylan "Only a Pawn in their Game" ringtone on your cell phone; although I'm sure that he would prefer a donation to his defense fund (bradleymanning.org). For detractors, I recommend Stealer's Wheel "Stuck in the Middle with You."

Such were the events leading up to the last weeks of November, 2010. The real fireworks begin in Act II.

Act II: Epitasis - Tension and Chaos Reign Supreme

Act II begins in early December, 2010 after the initial release of a few hundred of U.S. diplomatic cables by Wikileaks. It was alleged that the source of these documents was the same Private Manning that released the Afghan War diaries in Act I. Fiber optic cables glowed with the thousands of downloads of these spicy morsels by curious netizens, first amendment enthusiasts, voyeurs, bureaucrats of

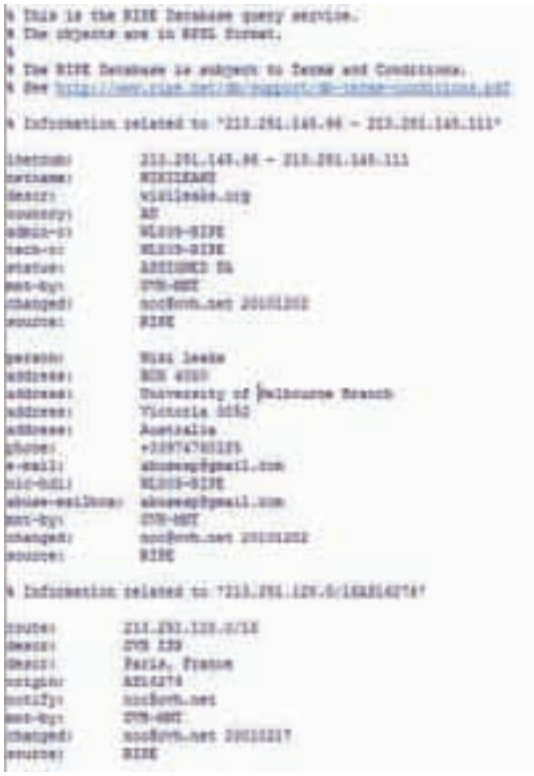


Figure 1: Wikileak Forensics?

every stripe, embarrassed diplomats,' vicarious jihadists, 'agendalistas', and of course, the media. Most of this entourage just can't quite seem to get the big picture. This act unfolds over several days.

Friday, December 2, 2010 was a day that will live in Wikinfamy. Over the previous Thursday evening, wikileaks.org's DNS service provider, EveryDNS.net, pulled the plug on Wikileaks' authoritative DNS records. Of course, DNS is the service that maps domain names onto IP addresses, so pulling the authoritative records means that after a short delay, the only way one could reach the host servers registered by EveryDNS would be to bypass the domain name and use the actual IP address as the URL in the browser location window - 204.236.131.131 in this case. According to EveryDNS:

"EveryDNS.net, a provider of free managed DNS services, supports nearly 500,000 web sites worldwide. At 10PM EST, on Wednesday December 1, 2010 a 24-hour termination notification email was sent to the email address associated with the wikileaks.org account. In addition to this email, notices were sent to wikileaks via Twitter and the chat function available through the wikileaks.org web site. Any downtime of the wikileaks.org web site has resulted from its failure to, with plentiful advance notice, use another DNS solution. Yesterday, pursuant to the EveryDNS.net Acceptable Use Policy the primary DNS hosted domains were disabled. Today, also in accordance with the EveryDNS.net Acceptable Use Policy, the secondary DNS hosted domains, including wikileaks.ch, were disabled. EveryDNS.net is not taking a position on the content hosted on the wikileaks.org or wikileaks.ch web site, it is following established policies. No one EveryDNS.net user has the right to put at risk, yesterday, today or tomorrow, the service that hundreds of thousands of other web sites depend on." According to Reuters, EveryDNS claimed that a 100 gigabit/second distributed denial of service attack against wikileaks was threatening the stability of their service to all of their other subscribers.

To further taunt our protagonists, Amazon Web Services, a primary host of the Wikileaks content in North America at 204.236.131.131, pulled the plug on the content-server as well. At this point, both the DNS records and the servers that serve the Wikileaks web content in North America were no longer accessible on the Internet. This is a first. Senator Joe Lieberman's staff apparently questioned Amazon about its relationship with Wikileaks prior to Amazon's decision to pull the plug, although Amazon denied that pulling the plug on Wikileaks was politically motivated. Whether politically motivated or not, it's most likely that Amazon treated this as a business decision, as hosting Wikileaks was probably seen as an unworthy annoyance by the time that Lieberman's staff got involved. In any event, Amazon's initial comment was: "Some of [Amazon Web Services] data is controversial, and that's perfectly fine. But, when companies or people go about securing and storing large quantities of data that isn't rightfully theirs, and publishing this data without ensuring it won't injure others, it's a violation of our terms of service, and folks need to go operate elsewhere." - which is exactly what Wikileaks did.

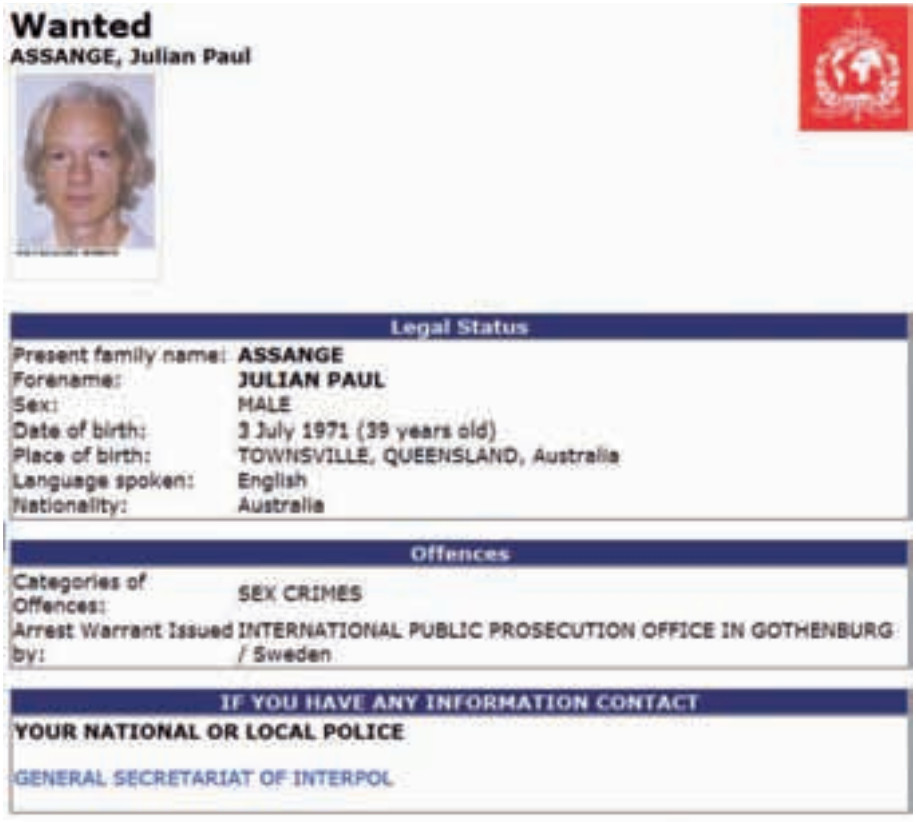


Figure 2: Interpol's Red Notice for Assange

Within a few hours after EveryDNS removed the authoritative DNS records for wikileaks.org, Wikileaks defiantly announced on Twitter that wikileaks.ch was created. Sure enough, a DNS entry for the domain wikileaks.ch was created in Switzerland by Piratenpartei Schweiz. That domain resolved to IP address 88.80.13.160 which is a part of a small class-B network cluster, not in Switzerland but in Sweden where ironically our second protagonist, Julian Assange, had an outstanding arrest warrant for alleged sex offenses. The Swedish server in turn redirected traffic to the French host, OVH ISP, at 213.251.145.96 (see Figure 1). This IP address was part of a 16-address server cluster located in France but registered in Melbourne, Australia. If you're getting the feeling that getting a hold of Wikileaks content on the Internet is like shoveling smoke into a bucket, the big picture is coming into focus.

But of course the matter couldn't end there. French Industry Minister Eric Besson asked for measures to bar wikileaks from France on the mirror site is hosted by Robaix (perhaps he didn't know about OVH ISP). Just prior to Besson's action, U.S. Senators Dianne Feinstein, chairman of the Senate Intelligence Committee, and vice-chairman Christopher Bond had called for Attorney General Eric Holder to prosecute wikileaks founder, Julian Assange. In the background one hears Ecuadorian officials arguing over the offer of asylum for Assange, while Evo Morales and Hugo Chaves laugh hysterically over Inca Pisco cocktails on the veranda of Morales' coca plantation.

But of course the matter couldn't end there. Paypal gets into the act by freezing the Wikileaks PayPal account they use for fundraising. Not to be outdone, the Swiss bank, Post Finance, froze Assange's account claiming that he opened it under false pretences.

But of course the matter couldn't end there, either. Interpol, the international paper tiger of law enforcement, enters the fray by issuing a "red notice" on Assange (see Figure 2) who was reported to be living in England. The extradition request from the European Union on behalf of Sweden regarding the latter's arrest warrant is binding on the UK, so under pressure Assange is forced to surrender to

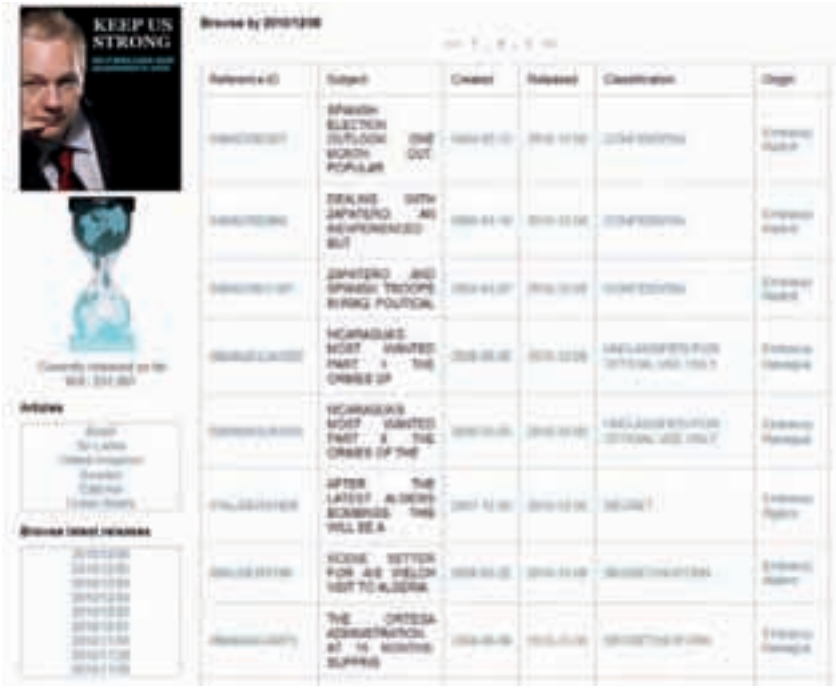


Figure 3: Assange may be stopped, but the Leaks Aren't The Big Picture?

English authorities while preparing a case to contest extradition to Sweden on the sex charge. This part of the script is reminiscent of James Cagney's role in Public Enemy.

Commentary: There is no question but that this protagonists' catastrophe is near at hand, though it is far from certain that it will end on the side of virtue. We sit through Act II overcome with bemused bewilderment. With all of the players claiming to be on the side of good and right, at this moment the plot is a bit imbalanced. As Act II developed, we were introduced to a dizzying array of players with increasing frequency. International diplomats covered their assets, politicians blamed everyone but themselves, all fingers pointed outward, no one shouldered responsibility for anything, and so it goes. And we haven't seen Private Manning since Act I! Who wrote this script, Yogi Berra? Denouement and resolution seem illusive at this point in time.

And all the while Wikileaks continues to post new cables (see Figure 3) and there was no shortage of European DNS and hosting services (e.g., wikileaks.nl, wikileaks.de, wikileaks.fi). What is remarkable in this cyber battle-of-wits was that it all unfolded so quickly. This is security theater at its best!

As this column goes to the publisher, Assange is an a British jail, Manning is in the Marine Corps Brig in Quantico, Virginia, Adrian Lamo, the hacker-turned-informant who outed Manning, is doing volunteer work in Northern California, U.S. military and State Department insiders are either in denial or waging an info war against Assange and Wikileaks, aggressive neoconservatives are calling for the execution of our protagonists, and all the while cablegate documents continue to float around cyberspace. One gets the sense that the U.S. government, and some of its allies, are of the opinion that Wikileaks can be stopped if only they put their collective minds to it. In one of life's greater ironies, the U.S. Government is sending emails to all employees and contractors instructing them not to look at the Wikileaks documents even on their personally owned computers. According to nextgov.com (http://www.nextgov.com/nextgov/ng_20101206_5274.php?oref=mostread), a Defense Department spokesperson wrote in an email that "Viewing or downloading still-classified documents from unclassified government computers creates a security violation." Duh. An official with the Library of Congress is reported to have said that "Unauthorized disclosures of classified documents do not alter the documents' classified status or automatically result in declassification of the documents." Double Duh. These bureaucrats don't seem to appreciate the motivational value of curiosity.

Let's face it; our government just doesn't get it. The toothpaste is out of the tube on cablegate, folks. These documents are etherial wisps in cyberspace at this point. The Internet isn't a thing; it's a dimensionless, virtual cloud with no physical features. There is no surface topology to the cloud, and no geographical features to orient us. You're not going to strangle it. The idea that once something gets on the Internet we can just reclaim it by pulling DNS records and suspending Web services is absurd, pure and simple. And the current kill-the-messenger psychosis is anal-retentive. This play is not written by Jules Verne and it won't end like Back to the Future. Get a grip.

Will Julian Assange be tried for sex crimes in Sweden? Will Bradley Manning ever be freed? Will Hamid Karzai ever forgive Karl Eikenberry for accusing him of being corrupt and his brother of being a narcotrafficker? Will the government of Iran ever forgive the Saudi King for suggesting that the U.S. "...kill the snake's head?" Will the Sunni's ever love the Shia? Will China ever stop ripping off IP? Will the Cubs win the pennant in 2011? I don't know. My crystal ball is a bit foggy on these points. But it's as clear as the air atop Everest on a few things. For one, anyone who wanted a copy of the Wikileaked documents by December 1, and who had the computer and networking skills of a kumquat, already had them. For another, if governments are to stand any chance of stemming the tsunami of stolen, secret documents into cyberspace, they're going to have to be far more selective about the people they put in charge of their IT departments! The PDOOMA approach to management and policy just doesn't port over to digital world very well.

Figure 4: TSA Body Scanners: The Latest Direction in Security Theater?

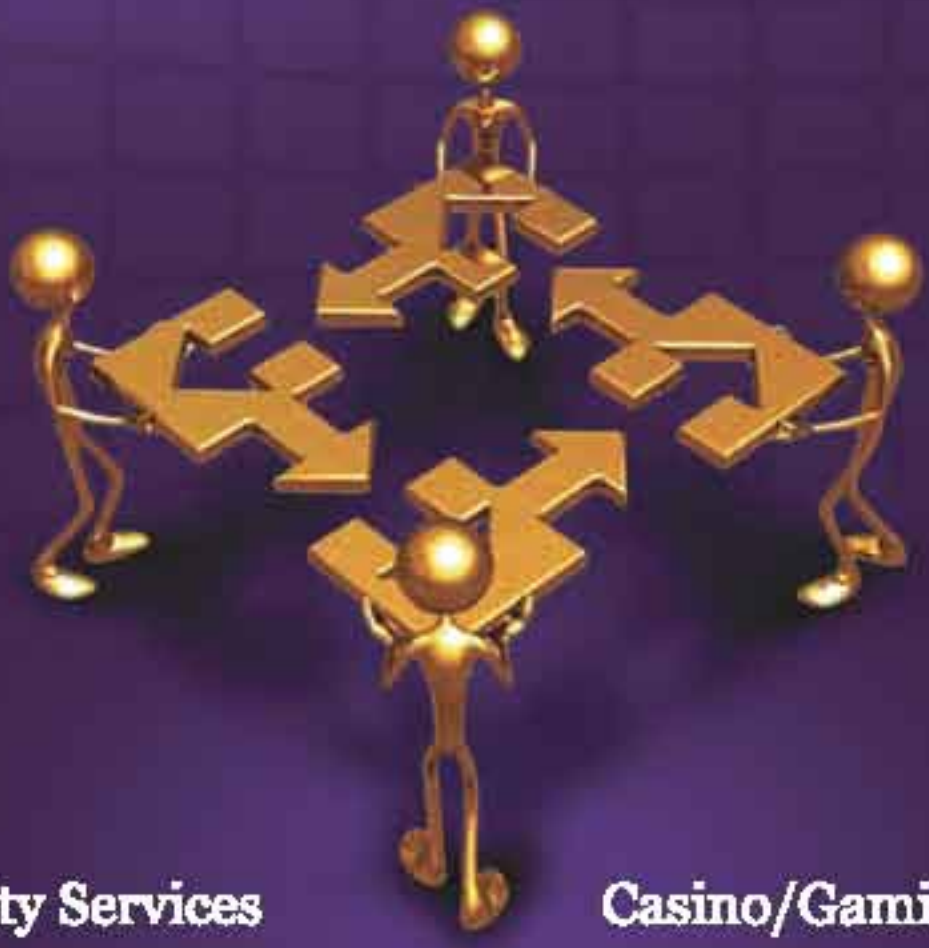
And just as a heads up, the new TSA advanced technology body scanners aren't going to cut it either. The lady with the insulin pump and 9mm pistol (see Figure 4) is going to find it a lot easier to get through security with a stolen TSA uniform and a phony ID. Wait until this security theater goes online!

Act III:

Stay Tuned

Hal Berghel is Director of both the UNLV School of Informatics and the Identity Theft and Financial Fraud Research and Operations Center (itffroc.org). His consultancy, Berghel.Net, provides security and management services to government and industry.

Linking Together Strong IT Experience with the Best Industry and Security Standards



IT Security Services

- Security and Compliance Assessment & GAP Analysis
- Governance, Risk Management
- Policy and Procedure Development
- Technical Control & Architecture Review
- Risk Assessment
- Security Architecture & Design

Casino/Gaming Services

- Apps/Web development and QA
- IGT Support
- Infinium Back Office Support
- Project Management
- Network and Help Desk Support
- Systems Integration

Link Technologies helps to ensure compliance of IT and data security requirements such as Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley (SOX) and Nevada Gaming Board Minimum Internal Control Standards (MICS). Link Technologies is an approved QSA company with certified staff. So we have proven to successfully help our clients meet the requirements set out by the PCI DSS mandates or other compliance requirements while helping them manage their security risks. Our expert consultants look to fully understand the clients business first and then determine the risks and appropriate mitigation.

LINK TECHNOLOGIES

Las Vegas Office
9500 Hillwood Drive Suite 112
Las Vegas, Nevada 89134
Phone: (702) 233-6703

Reno Office
995 Forest Street
Reno, Nevada 89509
Phone: (775) 624-4545

Additional Locations In:
Philadelphia
Washington D.C.
Los Angeles

Visit us online to learn more about what we can do for you!
www.LinkTechConsulting.com