Updated: 3/28/2011

U.S. Chamber of Commerce & HBGary Spying

The United States Chamber of Commerce retained law firm Hunton & Williams, intending to have them do opposition research on unions in general and in particular SEIU, liberal Netroots organizations, and turn up evidence of union funded astroturf aimed at Chamber interests. Hunton & Williams were entertaining an offer of the creation of a military intelligence style "fusion cell", conceived and built by HBGary Federal, with rapid startup assistance from project manager Berico and technology provider Palantir.

While awaiting word on the acceptance and funding of their proposed solution, HBGary Federal became aware that Bank of America would be the subject of Wikileaks' attention in the spring of 2011, and they drafted and shopped a speculative proposal for a similar operation aimed at Wikileaks. Barr preemptively began working on Wikileaks' partisans - the hacker collective known as "Anonymous", and he provided information to the Financial Times in an effort to publicize his company. This information included details on the alleged "leadership" of Anonymous.

Anonymous took note and responded in their usual fashion. They obtained and publicly dumped all of HBGary Federal's email, took over domains owned by the major players in HBGary's operation, broke in and defaced their web servers, and vandalized various social media and gaming profiles.

The HBGary email release is proving to be to the Chamber of Commerce and Bank of America what "Cablegate" was to the American government - a profound embarrassment, and a revelation of unethical and perhaps criminal conduct.

Actual Bank of America Response

Bank of America's previous attempt to bring down Wikileaks did not involve HBGary Federal, and presumably Hunton & Williams wasn't involved either, given that they were entertaining an offer of service from HBGary. The work appears to have gone to an entirely different security contractor. This effort was initially effective, breaking down Wikileaks primary site and financial arrangement, but then a different part of Anonymous involved themselves, distributing the Wikileaks infrastructure globally.

Original Assessment of Companies Involved

HBGary Federal is a startup that launched in the fall of 2010, and has begun bleeding money. CEO Aaron Barr, just 34 years old, engaged in unethical and perhaps criminal conduct in his latest pursuit of Anonymous, and their response will likely destroy his company and forever tarnish his career.

Palantir is an old, stable, well regarded player within the intelligence community. They promptly distanced themselves when this debacle began, citing their consistently ethical conduct in the past, their support for Progressive causes, and they explicitly apologized to journalist Glenn Greenwald, who had been instrumental in the Wikileaks transition from a centralized to a distributed operation. Rumour has it that Palantir's lead on this project was suspended by the company.

There is limited information on Berico, but they did distance themselves from the project, as Palantir did.

Updated Assesment of Companies Involved

Aaron Barr has exited HBGary Federal. Given the poor revenues and utterly ruined reputation we're sure something like a chapter 7 bankruptcy will be the final outcome.

Palantir did the right thing publicly but there now are what appear to be dramatic findings against them in the stolen email streams – indications that this spying on behalf of the Chamber was being built out with approval clear to the board level of their company and of Berico.

This supposed high level approval has been publicly presented in the form of incriminating messages but we want to vet it thoroughly before integrating it into the overall response. Part of the proposed strategy against the Chamber's enemies involved planting false documents. They and the companies involved are highly motivated to discredit these leaks

Analysis of Leaked Email

The leaked email corpus, some 70,000 items from five key players at HBGary, is massive. A thorough review during a formal investigation is needed but here are interesting things that we note thus far:

This thread from 1/31/2011 to 2/5/2011 reveals an interaction between Aaron Barr of HBGary, Bill Wansley of Booz Allen Hamilton, and John Woods of Hunton Williams. Booz Allen Hamilton has not been publicly mentioned but this is obviously a high level exchange right before everything blew up for HBGary.

2/5/2011 9:58 AM from John Woods of Hunton Williams

Good luck with the government. We look forward to seeing the paper when it is published.

From: Aaron Barr <aaron@hbgary.com>
To: Woods, John
Cc: Wansley, Bill [USA] <wansley_bill@bah.com>; Lashway, David; Way, Renee [USA] <way_renee@bah.com>; Howell, Lloyd [USA] <howell_lloyd@bah.com>; Oferrell, Chris [USA] <oferrell_chris@bah.com>
Sent: Sat Feb 05 10:46:01 2011
Subject: Re: Meeting at Booz Allen on Friday

John,

See link below. I have made significant progress on the group and have 80-90% of their leadership mapped out. Meeting with Govies next week. I have tight few weeks and have told the folks supporting our other effort that I will not be able to give them much support until my presentation is over on Feb. 14th. Sorry for the timing.

http://www.ft.com/cms/s/0/87dc140e-3099-11e0-9de3-00144feabdc0.html#axzz1D3oZIcTk

Aaron

On Jan 31, 2011, at 3:04 PM, Woods, John wrote:

Aaron - Please stand down. We should have a meeting.

From: Aaron Barr [mailto:aaron@hbgary.com]
Sent: Monday, January 31, 2011 3:03 PM
To: Wansley, Bill [USA]

Cc: Woods, John; Lashway, David; Way, Renee [USA]; Howell, Lloyd [USA]; Oferrell, Chris [USA]
Subject: Re: Meeting at Booz Allen on Friday

just a status. I started to look more carefully for wikileaks ties within anonymous...there are many. BTW, anonymous is looking for its next effort to get involved in and is looking to resurrect operation payback in support of wikileaks.

Aaron

On Jan 26, 2011, at 4:47 PM, Wansley, Bill [USA] wrote:

Aaron,

Nice talking to you today and I look forward to meeting you. We will plan a meeting this Friday at 10:30 at Booz Allen, 8283 Greensboro Drive, McLean, to discuss how you may be able to support our project.

Thanks,

Bill

William J. Wansley
Senior Vice President
Booz Allen Hamilton
(703) 902-6874 (o)
(703) 705-1483 (m)

A House Homeland Security Committee staffer named Jacob Olcott seems to have a strong connection to HBGary, presumably dating back to when Aaron Barr was employed by Northrup Grumman. This email is instructive and there are forty messages between the two throughout 2010. Olcott appears to have left the House and migrated to a similar position on the Senate side.

Hi Jake,

Thanks for the opportunity. I will take a look and provide what I can.

Aaron

On Jan 27, 2010, at 6:45 PM, Olcott, Jacob wrote:

One of the interesting things about working for Congress is that you can go long stretches of time where you never seem to have traction on an issue, and then suddenly a window of opportunity presents itself and you have a brief moment to take advantage of it. This is one of those moments for cybersecurity here in the House of Reps.

Several months ago, the Science and Technology Committee marked up a Cyber R&D bill. You can find the bill here: **http://www.rules.house.gov/111/LegText/111_hr4061_txt.pdf.** As you can tell, this was a fairly noncontroversial bill. The Speaker's office decided today that they want this bill on the floor **next week (likely Wednesday or Thursday)**.

Here's how the procedure works. Members are allowed to write amendments to the bill. They submit them to the Rules Committee. On Monday night, the Rules Committee will consider those amendments, and rule them either "in order" or "out of order." Amendments are supposed to be "germane" to the section of the bill that is being amended (there is a test for this, but basically an amendment has to relate to the subject matter under consideration). Amendments that are ruled "in order" can then be raised by that member on the floor – and put to a vote of the House.

As you can see from the text, the bill contains provisions on R&D, cyber workforce, strategic planning, social and behavioral cyber research, the focus of NSF grants, scholarship for service, NIST research, international standards, identity management, cyber awareness into legislation. Lots of good and interesting subjects that can be improved and enhanced through the amendment process. For those looking for an opportunity, **this is a great way to address some of these issues in a bill that will be voted on by the House of Representatives**.

Members have already been asking me for amendments, and I am busy drafting. You are a trusted ally, and I would really appreciate if you can take a look at this bill, see if you have some ideas about ways to improve it, and send them to me. **Please be creative!** I will take your submissions, turn them into amendment language, and send them to members who are interested in amending this bill.

Sorry for the late notice, but **I need your proposals by not later than FRIDAY at NOON**. If you're not comfortable drafting an amendment, feel free to submit an "idea" to me and I will do my best to turn it into legislative language that the members can use.

Thanks for your help.

Jake

Jacob Olcott
Subcommittee Director and Counsel
Emerging Threats, Cybersecurity, S&T Subcommittee
Committee on Homeland Security (Majority)
202-226-2623

This 9/17/2010 message from Aaron Barr to Aaron Spring, apparently still at Northrup Grumman, is a bit gossipy but it provides a great deal of information as to what is happening. Barr is later seen attempting to steer employment for Spring at TASC, a company that was purchased and later sold by Northrup Grumman. They, like Booz Allen Hamilton, have not received much public attention despite being deeply involved. We suspect this is due to the initial analysis focusing on the presentation provided by HBGary, Palantir, and Berico – there's no investigation required with that, they basically self-indicted by letting the slide show slip.

Aaron,

There is unfortunately in this circumstance no better way that I can do this. I know your in a tough spot, you all are. Your leadership has taken the fear and intimidation route instead of using better leadership through innovation and inspiration. I know we spoke a while back and you were on board, we have delayed in getting out offer letters waiting for the RFP and negotiating with the prime when and who to hire, the proposal is now imminent. Please know that none of the customer will question your loyalty to the mission if you sign a contingent offer, in fact it shows that no matter what you are trying to take care of yourself and want to stay with this mission. Government is not wedded to any specific company just a capability and your overall capability has been sagging. John doesn't care if you sign contingent offers with other teams, what he would not want you to do was do something that was detrimental to the mission, like what your current leadership is doing by using fear and intimidation. Your upper management knows how this drill works if your current ignorant local management doesn't. You always try to recruit key personnel form the incumbent to lower risk. Kathy and Dale have done that a 100 times. Your management is using fear and intimidation to try and keep people form talking with us and it is just sickening. Is SAIC/NG that insecure in their offering that is what they have to resort to? Following people to lunch, as if those people have no right to talk with me or Ted! It makes me very angry the position they are putting you all in. Bottom line I am going to win this contract and if you had a chance to see my team and strategy you would agree. Remember its not about size, its about innovation and focus on delivering the best capability for the customer.

You know me, you know what I am capable of, you also know your current team and its position with the customer. I can only imagine what they might tell you. I am not sure if you are aware but I have my badge back and speak with the customer regularly. I feel confident I know better than anyone how to make their mission more successful and how to tell that story in the proposal.

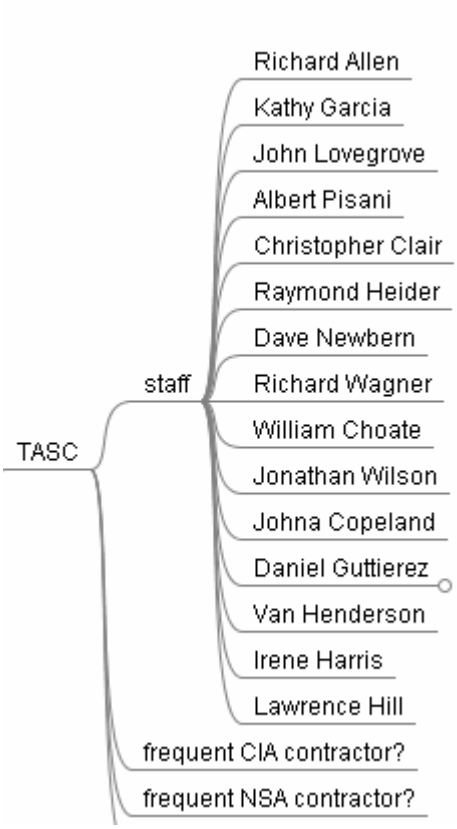
It is your choice. If you are still interested I will have a confidentiality agreement and contingent offer in your inbox by monday. This will secure you a leadership position on this amazing team (you will be amazed at this team). If I don't hear from you I will assume that I have missed my window and I will look elsewhere to fill the position. If I do hear from you we can exchange documents and we do not need to really communicate past that unless you want to. I am very sorry for your situation. I won't send you another email after this one unless requested.

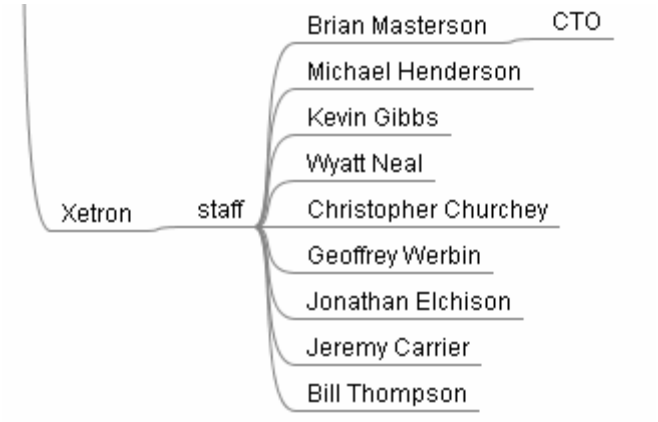
Aaron it has been a pleasure to work with you, and I truly wish you the best.

Aaron

P.S. Greg and I are working on a game that takes advantage of location, social, and virtual. He has a developer and artist working some of the first pieces now. Hopefully that will grow. its a great concept.

The following images were culled from the mindmap we're building as we examine the email. Northrup Grumman divisions Xetron and TASC were intimiately connected to HBGary and had some involvement in the overall plan, but the particulars are not yet clear.





The following email shows Northrup Grumman employee Jim "Torch" Hale greeting Barr as a member of the "Secret Squirrel Society". There exists in our intelligence/defense contractor community an informal back channel that facilitates things getting done and it would appear that Barr was being introduced to this group. Among his other correspondents are highly placed Northrup Grumman executives such as Tom Conroy.

From Aaron Barr 2/1/2010
Hey Good to hear from you (virtual secret handshake extended).

Sounds good. I am in the springs through wednesday. Get in the afternoon. We have meetings with Lawrence hill and comany tomorrow afternoon.

Aaron

From my iPhone

On Feb 1, 2010, at 9:16 AM, "Hale, Jim (AS)" <jim.hale@ngc.com> wrote:

<image002.gif>

Aaron,

Greetings from the Secret Squirrel Society. I'd like to have an informal discussion with you some time on what you're doing now. I suspect that it would be beneficial to both companies to for us to talk. Please let me know if you're interested. Thanks.

Torch

From: Shows, Bob (IS)
Sent: Friday, January 29, 2010 3:47 PM
To: Aaron Barr; Hale, Jim (AS)
Subject: 624th Ops Center--Next Steps
Importance: High

Aaron,

I spoke at length with Vickie Michaels of CyberSpace Operations Consulting, LLC. Fundamentally her company is interested, but wants NGC to pay her company upfront to consultant in bringing this business case together. I conveyed that was not going to work, but if she could get her boss to sign the NDA, I would work with her to see how they might fit.

Of note, she wasn't interested in investing 2-4 hours of her own time just tighten the shot pattern on this effort. We left it with her going to see her boss and present the case (for which she did not seem overly enthusiastic)—we'll see.

As I mentioned, CSOC would be nice to have on this team, but not essential. We have Tom Hobbins, Bob Hinson, Tim Peppe, Jim Hale, Mike Edwards, and others that you know to assist with senior customer interface.

Until we hear from Vickie, not sure we should plan to rendezvous in San Antonio—I'll stay on top of this and keep you in-the-loop.

Also, Jim Hale has some things in the work that he believes will be of interest to you. He'll be in touch soon.

Jim 'Torch' Hale

(719) 238-0763 (mobile)

Aaron Barr

(719) 510-8478 (mobile)

(301) 652-8885 x117

Best regards,

Robert 'Bob' Shows
USAF Account Team NGIS/DSD
Northrop Grumman Corporation
310.210.2549

The conditions in the Republican dominated House are such that they will attempt to sweep this under the rug as quickly as possible. House Select Intelligence Committee head Mike Rogers is amazingly vulnerable to pressure due to his public calls for the execution of Bradley Manning, coupled with the corruption that follows where ever he goes. We see signs that this is going to be an issue for the grassroots.

The hope for actual investigation will be in the hands of the Senate and Al Franken seems most likely to carry the ball.

There are great hazards if Northup Grumman is as deeply involved as they appear to be from this cursory examination. We have seen much information indicating that a division of General Dynamics is also involved, but we've not yet explored that. It's already public information that the Department of Justice engineered some of the connections, so it's deeply disingenuous for the GOP to dismiss this as a matter for the DoJ – they simply can't self police with something this explosive.

This update should be taken neither as complete nor well vetted. We must have a serious examination of the contents of the revealed emails to get to the bottom of this plot. Given that they're out in public the best thing to do is very likely going to be encouraging crowd sourced examination, then vetting and guiding the masses as they digest what has happened.