Updated: 4/16/2011

U.S. Chamber of Commerce & HBGary Spying

The HBGary Federal intrusion resulted in the publishing of over 70,000 internal emails. We provided an initial assessment on 3/9/2011 and have settled in to providing updates as we further digest the evidence.

We have gathered a team to perform a detailed, structured analysis of the contents. We discovered a **significant error** in reports dated 4/08/2011 and prior regarding the interpretation of the **COIN** acronym. We identified a significant player we had missed, **William Luti,** and his presence coupled with the correction regarding **COIN** make for a significantly different interpretation than we have previously offered.

Initial Updates of 3/9/2011 & 3/27/2011

The world's initial response was based almost entirely on the content of a presentation which detailed a planned Corporate Information Reconnissance Cell and attendant Information Operation (psyops) aimed at the SEIU and a number of Progressive organizations. The actors were to be HBGary Federal, Palantir, and Berico. The customer for this was the Chamber of Commerce and the law firm Hunton Williams was to be the middle man.

Executive Summary

There exists an intelligence program known as Romas/**COIN,** which is short for **Counter Insurgecy,** and this appears to be largely run by Northrop Grumman. We had initially erred significantly, interpreting the frequent references of domestic spying and the similarity between **COIN** and **COINTELPRO** to mean that there were related, sanctioned domestic efforts using the same systems. Now our reading indicates that there are domestic spying operations being offered to various government agencies, but they are not directly connected with the Romas/COIN discussions.

HBGary CEO Aaron Barr in conjunction with NG executive Tom Conroy were attempting to strip the Romas/COIN business to the benefit of former NG subsidiary TASC. It should be noted that Conroy originally came to Northrop Grumman with the TASC acqusition.

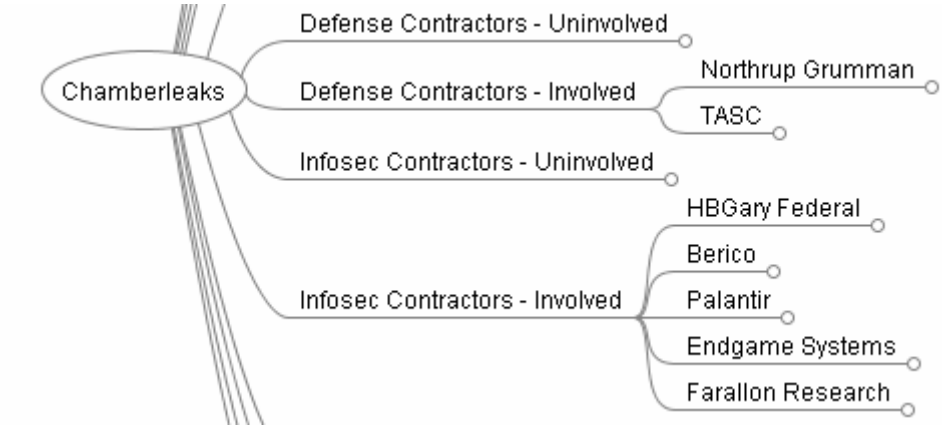
HBGary engaged in an abortive attempt to get the **Office of the Secretary of Defense** to fund a program known as **Magpii**. Short for Magnifying PII (personally identifying information), this was to be a location-centric social media startup company – basically opt-in spying on the American people.

Since our last update we've added a pair of people to our analysis effort who know a bit of **William Luti**'s history.

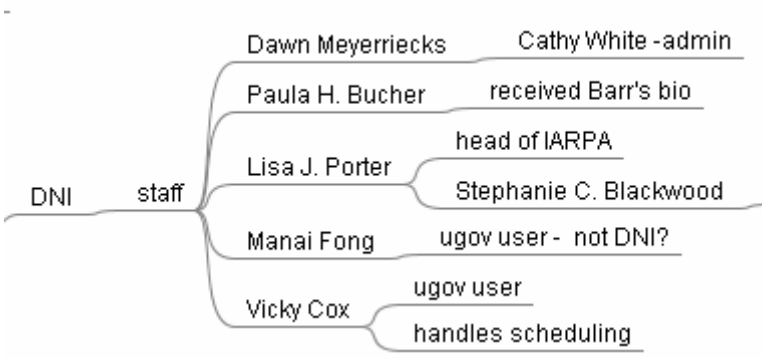
Structured Analysis

We undertook an initial reading of the email, creating a mind map with the names of all the players and a timeline. We are sorting them by major categories and then into those who are involved or not involved. There was much basic business development as well as the actual scheme, so there are many innocent parties named as well.

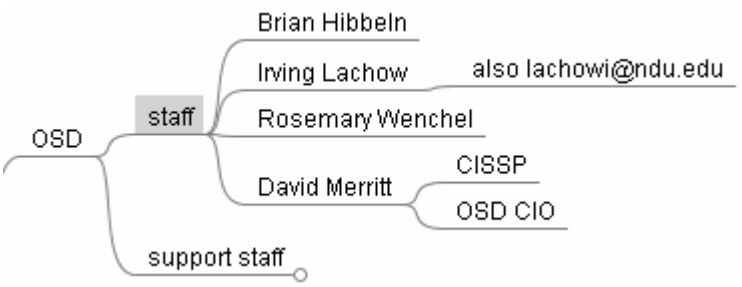
Having read several thousand of the emails our investigation focuses on the efforts of HBGary Federal CEO, working in conjunction with Northrop Grumman executives Tom Conroy and William Luti, to strip the Romas/COIN business to benefit TASC, HBGary, and a number of other related entities.



There are many interactions with various military and intelligence agencies but one of the most interesting thus far has been the discussions between the contractors and IARPA head Lisa J. Porter in the office of the Director of National Intelligence. There was obviously something significant happening, but our earlier assessment that this was part of **COINTELPRO** reborn was obviously incorrect.



Lloyd Lachow and CIO David Merrit from the Office of the Secretary of Defense were deeply involved in introducing HBGary to another contractor, Farallon, and a group of similar size to those driving Team Themis were working on obtaining funding for the **Magpii** concept – opt-in spying on the American people, luring them in with location aware social media services.



Specific Email Threads

The 70,000 email collection is initially intimidating, but with a little assistance that helped identify who the key players were in the mix it is a manageable problem. These are just the ones we've digested thus far. Our feeling is that we're perhaps 75% complete and further sense making is starting to depend on outside inputs from those who know the history and players in this field.

Aaron Barr & Tom Conroy

Barr was Conroy's "go to guy" at Northrop Grumman but it's unclear if this dates back to before 2001, when TASC was acquired, or if it was after NG divested themselves of TASC. Barr characterizes Conroy as a mentor. The emails presented show the developing plan to strip NG of the Romas/COIN business.

Aaron Barr & Al Pisani

Pisani is an executive at TASC and seems to be the top level contact, first for the stripping of the Romas/COIN business, and later for the acquisition of the struggling HBGary Federal.

Codename: Romas

Barr and Conroy worked together on Romas, the overseas intelligence collection project. The contract officer for the military unit running this is named. The domestic groups to be targeted for the Chamber of Commerce are revealed.

NSA spearfishing

NSA staffer Raplh Ghent and Aaron Barr discuss a top level initiative for HBGary Federal. They plan to use their social media reconnissance capability to idenitfy high value targets, then they will take control of their computers using malware. The malware would come from HBGary founder Greg Hoglund's efforts. This highly targeted intrusion behavior is known as "sprearfishing", derived from the broader, automated phishing attacks we've all experienced.

Aaron Barr & Lisa Porter

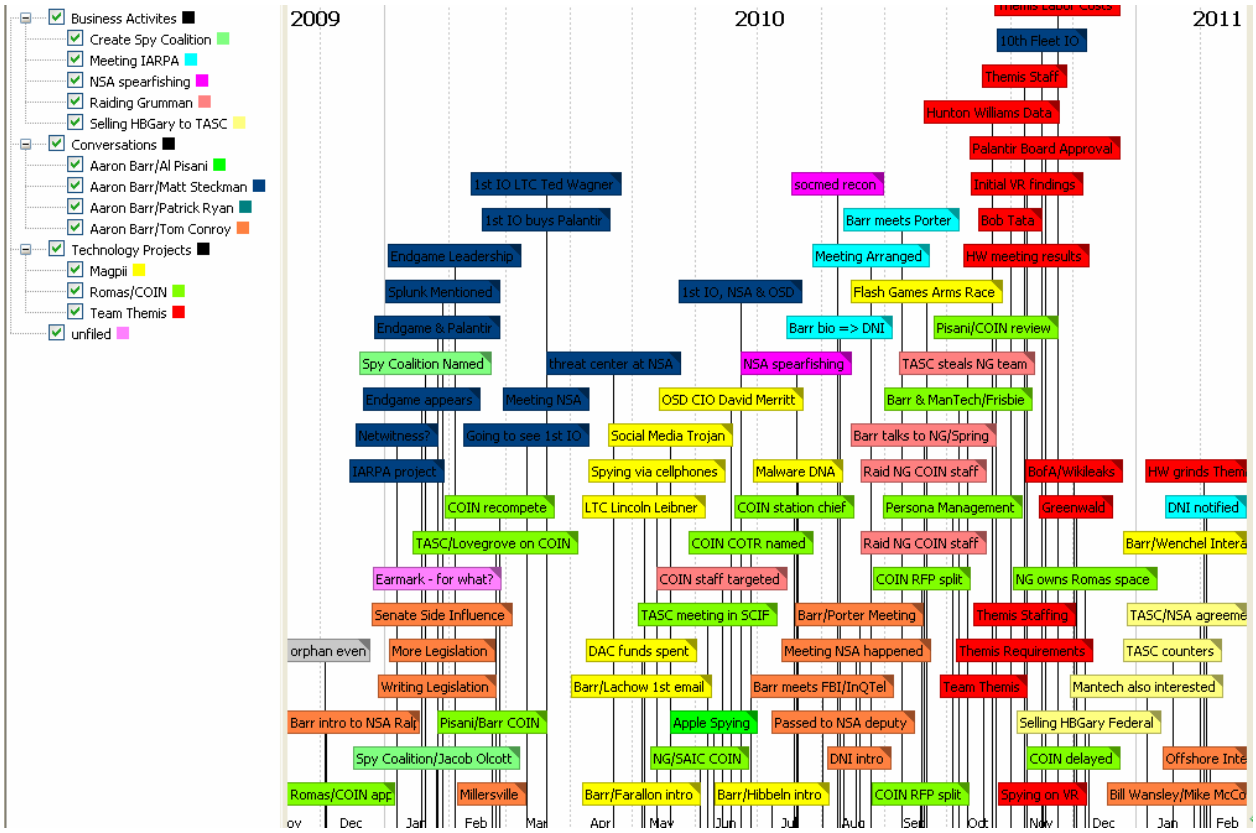
Barr sought and received a meeting with Intelligence Advanced Research Project Agency head Lisa J. Porter. There is no explicit information as to what they were discussing, We suspect that the Stuxnet worm was at least a portion of the conversation based on the urgency noted on certain dates.

Aaron Barr & Matthew Steckman

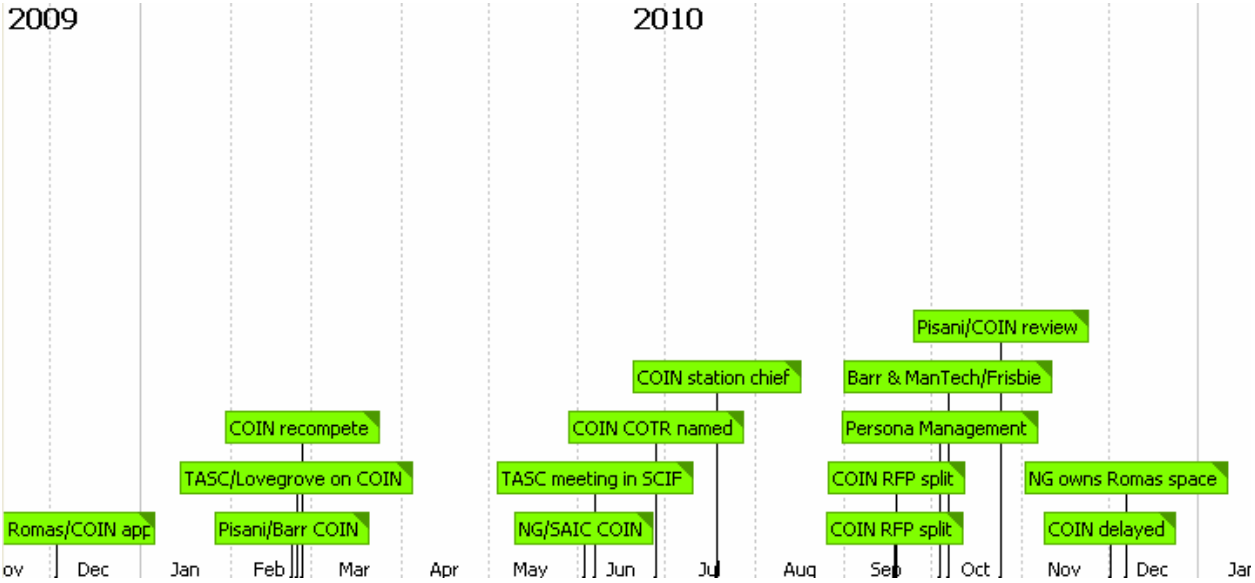
Barr and Steckman were very chatty so we left this for later in the process. We found the original message which indicates that Team Themis was initiated because Hunton Williams contacted Palantir. HBGary's poor internal practices and arrogant, foolish CEO have put them in the hot seat due to their intrusion, but they are not alone nor do they seem to be the prime mover for these schemes.

Time Lines

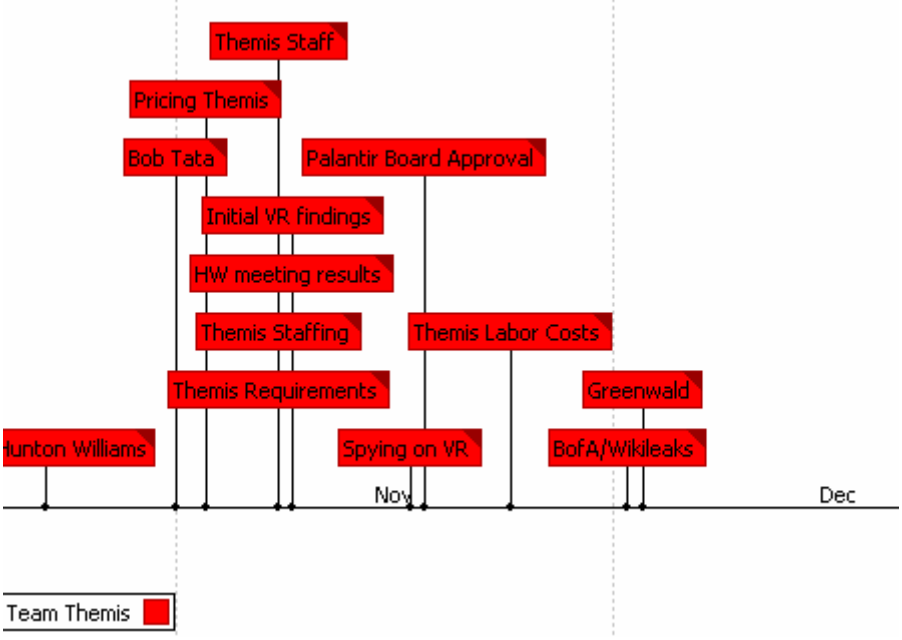
Based on the conversation threads we have analyzed we created the following timeline. A larger, more legible image has been attached with this document. The actual timeline data and directions for obtaining the program to read it are included if you receive the full analysis package.



The Romas/COIN timeline is specifically interesting for Northrop Grumman and for legislators. Banning companies and individuals found involved in domestic spying from government contracts would quickly clean up such behavior.



The Team Themis timeline is what the public knows, the interaction between the three visible contractors, HBGary, Berrico, and Palantir, with law firm Hunton Williams



HBGary was courting the Office of the Secretary of Defense for investment dollars to create something called Magpii – short for Magnifiying Personal Identifying Information. They didn't get funded, but the outstanding question is "Who did?"