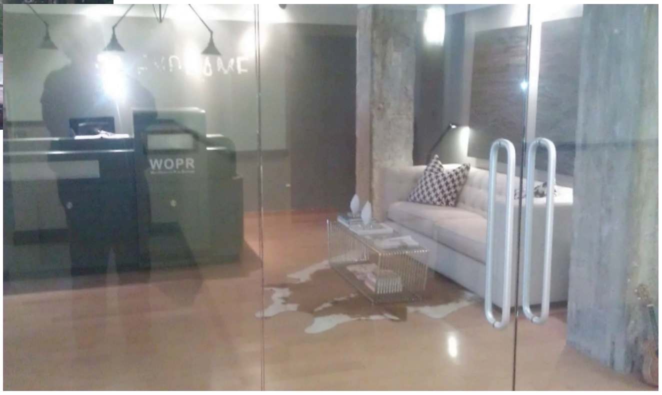
Black Hat Versus White Hat:
The Other Side Of The Snowden/Hastings/Barrett Brown Cases

By Jill Simpson and Jim March – June 24th 2013

Left: front of the Biltmore office building (formerly a hotel) in Atlanta GA containing "Endgame", an obscure private offshoot of the US intelligence community.



Right: Endgame's lobby at the 7th floor. Note the strange font on the word "Endgame" behind the receptionist's desk – unless you knew about the word "Endgame" as the company name you would be unlikely to successfully read it. They are also missing from the directory in the downstairs lobby. Weirdest of all we see the words "WOPR" on a computer of some sort – a reference to the sentient fictional computer called "War Operation Planned Response" in the movie "Wargames" (the first "hacker movie") which attempted to start a nuclear war before "thinking" better of it. The general theme of the lobby and visible meeting areas is "Google-ish" - bean bag chairs and other casual touches surrounded by near-total paranoia.

NOTE: all data in this report is from publicly available sources as of Monday June 24th 2013 and will be footnoted as to origins wherever possible. It will not be possible to label us as "hackers" based on this report or anything else.

The final moves in a chess game are called the "endgame". It has come to the attention of American whistleblowers and election integrity specialists that the CIA, NSA and White House have designed the ultimate final "endgame" for the free world as we know it - with a group of computer "security specialists".

One key component of this is a corporate office called Endgame[1] based in Atlanta Georgia (at the old Biltmore Hotel building, 817 W. Peachtree NW suite 770).[2] This company is a private spin-off from the major intelligence source X-Force that was founded originally by Chris Klaus whose career dates to at least 1994 when he founded Internet Security Systems, a private "white hat" counter-hacker group.[3]

[1] http://www.endgamesystems.com

[2] http://www.superpages.com/bp/Atlanta-GA/Endgame-Systems-LLC-L2239339339.htm

[3] http://news.google.com/newspapers?nid=1696&dat=19981110&id=UxsbAAAAIBAJ&sjid=FEkEAAAAIBAJ&pg=4219,1551099 – this shows that as of 1998 the "X-Force" was an elite division of ISS.

The X-Force was a team of elite cyber-security specialists who operated within ISS in an Atlanta office and made daily reports to the intelligence community and White House about Internet security and malicious software threats. They were allegedly defensive in nature, at least when they started out, and protective of US security. One of their members was Christopher Rouland who was a famous hacker who got caught attacking the Pentagon's systems by US Airforce cyber-cop Jim Christy who gave him a "break" so long as he would work from then forward as a "white hat" cybersleuth for the US government.[4]

"White hat" in this context means defensive Internet security - fighting the "black hat" attackers. We write this in part to show that Rouland and his company Endgame have in fact gone back to "black hat" with the approval of the Federal government, doing (and facilitating for others) the sorts of attacks that the Pentagon, the NSA and the like don't want their fingers found in.

For a quick look at just how paranoid Endgame seems to be, this video taken from a micro-camera mounted on glasses showed what happened when we went to take a look:
http://www.youtube.com/watch?v=Vr5LIgZvx_8

Rouland took over the X-Force and ISS operations from Klaus for a period of time until ISS and X-Force were bought out as a package by IBM.[5] Rouland either decided not to continue with IBM or his criminal record excluded him; for whatever reason he switched a few years ago and co-founded a new private corporation called "Endgame" with the generous funding of Chris Darby who is the CEO of In-Q-Tel, an independent strategy investment firm that supports the missions of the Central Intelligence Agency and the broader intelligence community.[6] Darby still sits on Endgame's board of directors.[7]

One key member of the board of directors at Endgame is retired Lt. General Kenneth A. Minihan[8] whose claim to fame is that he was the 14th director of the National Security Agency/Central Security Service. He is a former director of the Defense Intelligence Agency and a founder of the National Information Assurance Program which is a United States government initiative to meet the security testing needs for information technology for both consumers and producers that is operated by the NSA and was originally a joint effort between the NSA and NIST (National Institute of Standards and Technology). The goal of the National Information Assurance Program (NIAP) was to ensure that consumer and business software products comply with the "Common Criteria Evaluation Standard". In 1994 the Federal government had already passed "CALEA" ("Communications Assistance to Law Enforcement Act") which mandated back-door intelligence access to consumer and business internet systems and products.[9] This back-door access could then be "double checked" by the updates that Minihan oversaw under NIAP and/or the "Common Criteria" and we strongly suspect they are privately used by Endgame and created by Klaus' boys under X-Force.

In a 2003 interview Chris Klaus started by saying that attacks against Linux would be an increasing area of concern before devoting the rest of the interview to threats against Microsoft Windows. Microsoft had by that time been deep enough "in bed" with the NSA to put back doors into the Microsoft Windows NT

[4] http://attrition.org/errata/media/pd.008.html

[5] www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html#p4

[6] http://www.crunchbase.com/person/chris-darby

[7] http://www.endgamesystems.com/about-us/ - or if that page disappears we have a PDF printout of it as of June 23rd 2013 archived at: https://docs.google.com/file/d/0B6Fh3F6hufhDRmt1WFdGZnNrcFk/edit?usp=sharing

[8] See footnote 7 where he is referenced...

[9] The "Communications Assistance to Law Enforcement Act" mandates that "ISPs" (Internet Service Providers) install taps for law enforcement. What most people don't realize is that any website that stores information for you is an "ISP" by the Federal Government's definitions, so that includes Gmail, Google Docs, Youtube, Facebook, Yahoo and many more we don't usually think of as "ISPs". Put another way: the definition of "ISP" has grown significantly since 1994 to include online services not even considered plausible in 1994, such as Facebook.

operating system, the ancestor of all subsequent versions including those in use now.[10] Klaus was, by 2003, attempting to steer people away from Linux knowing it would be harder to plant "software taps" into Linux due to the open-source nature of the code – basically geeks can peer under the hood of Linux and might detect data taps.[11] Microsoft keeps the innards of Windows secret via trade secret and copyright laws and hence taps can go undetected longer which has allowed Endgame, ISS and X-Force to write reports and software tools to exploit foreign governments around the world. This interview in 2003 is therefore indicative of where Klaus' head was at – he was already a partner with the NSA, involved in the X-Force and reporting to the White House daily – and wanted to make sure US/NSA access to foreign and domestic online systems remained available by panning Linux in 2003 when it was in it's infancy but clearly an up-and-coming "threat" to the intelligence communities around the world.[12]

Klaus had dreamed this up while serving on the National Common Criteria task force. This set of software back doors allowed him and his ISS to continue their leadership roles in President George W. Bush's National Infrastructure Advisory Council and the FBI's "Infraguard" program along with their cyber-protection and information warfare contracts with the Department of Defense and the US Department of Justice. Klaus was selected for this job as co-chair of the NCC by the Business Software Alliance (a trade group with Microsoft as the largest and leading "partner"), the Information Technology Association of America, the US Chamber of Commerce, TechNet and Tom Ridge, then-Secretary of the Department of Homeland Security. As co-chair of the Technical Standards and Common Criteria task force in 2003 it was Klaus' job to bring together experts from government, the private sector and academia to provide a national strategy to "secure cyberspace" for President George W. Bush so that the Department of Homeland Security could implement a plan to protect the United States from domestic and foreign threats, online or otherwise.[13]

Klaus testified in 2003 before the House Government Reform, Subcommittee on Technology, Inter-government Relations and the Census committee about his industry experience as being the first commercial vulnerability assessment inventor and the first inventor of intrusion detection products, and how it would be cost-effective to develop a "criteria and certification" process for software products to help defend against threats.[14] This federal control thereby allowing the insertion of back doors into that software at the same time via federal control over certification so that the US could spy on every foreign and domestic person, government or organization in the world.

This is also where Klaus and his X-Force boys including Mr. Rouland made their funding connections with the Intelligence community including the director of the DIA, Gen. Minihan, and why In-Q-Tel chose these folks to run a private version of all this in Endgame.

It might be added that Mr. Rouland was the designer of the www.senate.gov website and infrastructure

[10] http://www.washingtonsblog.com/2013/06/microsoft-programmed-in-nsa-backdoor-in-windows-by-1999.html and http://techrights.org/2013/06/15/nsa-and-microsoft/ - this is not a deep secret although Snowden may have succeeded in getting people to pay attention...

[11] Linux is "open source". In 1993 a Finnish computer science student by the name of Linus Torvalds wrote the first "kernel" (think "core") of what came to be called "Linus' Unix" or "Linux". He gave it away free so long as anybody doing modifications or extensions of it also gave those aware free – including the human readable "source code" showing how it was done. It basically spiraled out of control from there and now has tens of thousands of contributors who all have access to the "how it works" info; Linus still manages the key Kernel component, screening and approving (and occasionally writing) modifications. With that many eyes on the ball, pulling a fast one isn't easy. In comparison, as few as one product manager and one coder can slip something ugly into Windows. For those curious about the details and permutations see generally http://www.gnu.org/licenses – and also the "Creative Commons" movement: http://creativecommons.org

[12] http://www.technewsworld.com/story/32288.html – note the opening paragraph in particular regarding Linux.

[13] http://www.technewsworld.com/story/32288.html

[14] http://www.thefreelibrary.com/Internet+Security+Systems%27+Founder+and+Chief+Technology+Officer,...-a0131654799

which would have potentially allowed him to plant taps.[15] Let us be clear: the senate.gov site is more than a website, it is a communication infrastructure for the Senators and their staffers and taps into that by somebody we know for a fact started out as a criminal should be of serious concern to all. We know that another contractor by the name of Mike Connell did work on the equivalent House side (doing portions for various committees and individual Republican house member websites)[16] and Connell died in a plane crash shortly after being called to testify in an Ohio electronic voting case.[17] So there's a pattern of sketchy people doing things to the most important computers in the nation.

The “services” offered by Endgame include offensive and defensive vulnerability research including software called Bonesaw supporting the detection and mitigation of cyber threats. This basically means that they cover both offensive and defensive aspects of computer security. What they can do is show what computers exist at specific locations and show the user of “Bonesaw” what software vulnerabilities are on those computers, making attacks easy against citizen, business or government systems across the planet.[18] Bonesaw has information in it about both threats and targets and can connect the two, for the low, low price of $2.5million per customer per 25 exploits according to Emails found by Anonymous in 2011.[19] What an “exploit” allows is either reading from or alteration of an online system, which could even possibly blow up a power plant or other critical physical infrastructure.

“Zero day” exploits (meaning “security holes” or “flaws in a given system” are particularly dangerous because they haven't yet been reported to (or discovery by) anybody who has the job of patching them. So the people who can defend against the attack have “zero days” in which to do something about it. Ethical “white hat” hacking behavior on encountering any such flaw is to report it to whoever needs to fix it – say, Cisco for a flaw in their large routers. If Cisco doesn't respond or doesn't do anything significant about the issue, a public release is warranted because that is the action most likely to make Cisco (in this example) managers wake up and do something – at which point it is no longer a “zero day” exploit. Anybody who continues to hide and either exploits or facilitates the usage of a zero day exploit cannot portray themselves as “one of the good guys” - period, end of discussion.[20]

In this context Endgame long ago “went over to the dark side” of the computer security world.

This was first brought to light by Barrett Brown, the journalist and alleged leader of Anonymous who is currently being prosecuted by the US government for “hacking”. It is contended in recent reports that he was arrested shortly after looking into the Endgame operation in Atlanta and exposing what Bonesaw is and can do.[21]

The organization “Free Barrett Brown” consisting of Brown’s supporters wrote a condolence message on the recent death of intelligence reporter Michael Hastings that also confirms that Hastings was working on the

[15] http://www.zoominfo.com/p/Chris-Rouland/6976439

[16] http://www.sourcewatch.org/index.php/Mike_Connell – third paragraph

[17] http://rawstory.com/news/2008/Republican_IT_consultant_subpoenaed_in_case_0929.html

[18] http://www.defensenews.com/article/20130115/C4ISR01/301150007/Nathaniel-Fick-Former-CNAS-Chief-Heads-Cyber-Targeting-Firm

[19] http://www.slate.com/articles/technology/future_tense/2013/01/zero_day_exploits_should_the_hacker_gray_market_be_regulated.html and www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html#p4

[20] http://www.zerodayinitiative.com/about/ - this is a good overview of the process for “ethical hacking” and the reporting of major exploits including zero day security holes. However, while they claim that for-profit use of zero-day exploits is limited to “a very small minority” of security researchers, the kind of cash Endgame and their competitors can throw at the people who can find exploits has possibly affected the percentage who have “turned black hat”.

[21] http://www.thenation.com/article/174851/strange-case-barrett-brown#axzz2XBSWGd2B

Brown case, including Brown's initial (aborted by arrest) reporting on Endgame.[22] Hastings, prior to his untimely death, posted on his Twitter account to his friend Ron Brynaert that he was going to be working on Barrett Brown's story and to "get ready for your mind to be blown".[23]

However, before going underground Michael Hastings' car exploded and his engine was blown sixty feet in a fiery crash in Los Angeles. Many journalists on the left in the US have assumed foul play in the Hastings crash and recently an Email was released by one of Hastings' friends in the military that suggests Hastings was onto a major case and about to go underground after learning he was being investigated and under surveillance by people he assumed were FBI.

Clearly the FBI worked with the creators of Bonesaw and their supporters in the intelligence infrastructure who had no desire to see any of this come to light. In fact, when HBGary was researching people on the left who were writing about misconduct at the US Chamber of Commerce, Christopher Rouland ordered an Endgame employee to write an Email to HBGary that stated "please let HBGary know we don't want to see our name in an Email" as was recently reported by Nation magazine in an article about Barrett Brown. Brown, according to Nation magazine, published as a reporter the Email from the Stratfor data dump that Anonymous made available. Brown and his "Project PM" which Michael Hastings was also a part of became fascinated with Endgame.

It appears Endgame desired to remain under the radar as was exhibited by an exchange between HBGary's Aaron Barr and Brian Masterson at Xteron brought to light by Barrett Brown's reporting where he reproduced these Email exchanges:

> Aaron Barr to Brian Masterson of Xetron: "But they are awfully cagey about their data. They keep telling me that if their name gets out in the press they are done. Why?"
>
> CEO Chris Rouland to employee John Farrell: "Please let HBgary know we don't ever want to see our name in a press release."
>
> John Farrell to Aaron Barr: "Chris wanted me to pass this along. We've been very careful NOT to have public face on our company. Please ensure Palantir and your other partners understand we're purposefully trying to maintain a very low profile. Chris is very cautious based on feedback we've received from our government clients. If you want to reconsider working with us based on this, we fully understand."
>
> Aaron Barr to John Farrell: "I will make sure your [sic] a 'silent' partner and will ensure we are careful about such sensitivities going forward." http://wiki.echelon2.org/wiki/Endgame_Systems

Clearly this reporting by Brown showed Endgame to be particularly secretive even by the standards of private intelligence community corporations. This set of exchanges by Email show that Endgame was working with HBGary's Aaron Barr who became famous for attempting to "out" Anonymous, who then in turn dumped and spread data from HBGary, Stratfor and others, but did not successfully raid Endgame, to show that HBGary and the like were investigating individuals who were trying to show that the US Chamber of Commerce was working with foreign countries, corporations and promoting them through foreign "American Chamber of Commerce" (AmCham) branches over actual American businesses. This is not

[22] http://freebarrettbrown.org/michael-hastings-death-barrett-brown/ - this message references Hastings' work on "Project PM" which included Endgame: http://wiki.echelon2.org/wiki/Endgame_Systems

[23] https://twitter.com/mmhastings/status/294534049094053888 – in context, this was about "minds blowing" over Hastings' review of the Barrett Brown situation and Project PM, of which Endgame was a major part: http://wiki.echelon2.org/wiki/Main_Page – note highlighting of Endgame entry towards the bottom of the screen.

surprising considering that Chris Klaus served on a board with the US Chamber of Commerce, and Barrett Brown attempted to expose the whole rotten mess which has come to be known as “Team Themis” made up of HBGary, Palantir and Berico, with Endgame providing “unusually accurate report on WikiLeaks and Anonymous”.[24]

What is at stake here is that the United States government has outsourced the most evil elements of national security: the ability to hack into computer systems across the world, foreign and domestic, private or government owned. The organizations they outsourced this to then set about monetizing the process, selling it to the highest bidder. This process could also allow corporations and the financial and political elites to create acts of war that appear to have come from the US Government due to the severely interconnected nature of the intelligence community, split between private companies and actual government agencies with alleged oversight of sorts. Edward Snowden's access to NSA data while an employee of a private company for only four months (Booz Allen Hamilton, owned in large part by the Carlyle group which has long ties to the Bush family) illustrates the extent of the problem.

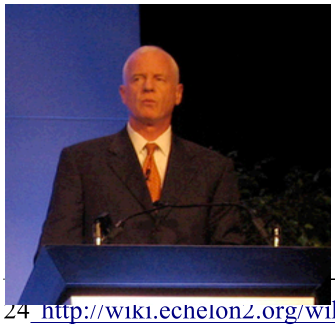
While Snowden was in Hong Kong he stated that the US Government had been attacking foreign systems of governments we are allegedly at peace with. Clearly these systems and exploits have their roots in the NSA and CIA and the private firm Endgame. What is interesting to progressive civil libertarians in the United States is that the “white hats” may have become “black hats” while nobody was watching (or able to watch until now). The question becomes: are Barrett Brown, Julian Assange and Eric Snowden the “white hats” who have been exposing criminal activities of the “black hats” at Endgame and their allies? It is clear that the political chess game is indeed in play and that the Endgame team currently is ahead on points but being exposed.

Since pictures of Snowden, Assange. Bradley Manning and Barrett Brown have been shown all over the world, it is now time to expose the black hat chess players with the same degree of publicity.

Christopher Klaus

Christopher Rouland

Aaron Barr (HBGary)



(Right) Lt. General Kenneth A. Minihan

(Left) Chris Darby

[24] http://wiki.echelon2.org/wiki/Endgame_Systems

In conclusion:

Who is actually being protected, the citizens or the "security state" or the multi-national corporations?

Endgame is admitting to facilitating computer crime against overseas targets at a minimum (and likely domestic) – even the foreign attacks violate US law and if you and I did it we would be prosecuted under a number of federal statutes that prohibit, among other things, attacks against "those computers used in or affecting interstate or foreign commerce or communication" including overseas.

The US Department of Justice has a good overview of federal computer crimes and their possible prosecutions at http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf – by their own marketing materials Endgame, HBGary and the rest of the privatized intelligence services violate enormous sections of it on a daily basis or conspire to facilitate (for profit) violations by others. Reporters, critics and at least some members of congress have called for the investigation and prosecution of HBGary[25] and we think it obvious that investigating Endgame is even more vital. Endgame has contracts with various elements of the US federal government's intelligence infrastructure including the US DOJ's "National Security Division – Counterespionage Section".[26] Among other problems, part of what Endgame does can be described as acts of war (hence their own reference to "WOPR"?), without even the minimal oversight that the NSA and other actual government agents and agencies are subjected to. It is time for President Obama to appoint a special prosecutor to determine if the NSA and CIA have outsourced criminal activities to private "hacker groups" such as Endgame since the DOJ has a clear conflict of interest as an employer of Endgame. It is also time for Congress to investigate whether government contractors such as Endgame who are tied to the intelligence community are selling computer exploits against foreign and domestic targets to the highest bidder.

Jill Simpson is a practicing attorney in rural Northern Alabama and a noted whistleblower in several political/legal scandals including the political prosecution of AL Gov. Don Siegelman. She is also a seminary student and social justice activist with a focus on election reform and the reforms needed to end political prosecutions once and for all at the US Department of Justice.

Jim March is a computer technical support/system administration/technical writing professional with a long history of interest and activism in electronic voting issues. He has previously served on the board of the Southern Arizona ACLU and is now living in Northern Alabama.

Simpson and March researched the "Orca" Republican election monitoring process, the Scytl election systems relating to military overseas voting and the "OpSec" PR program last year for a coalition of California progressives, traveling across the country to various places where election misdeeds were occurring. Their research on the problems with the Military Overseas Voting Act ("MOVE") are summarized at:
http://electionprotectionaction.org/uploads/MOVE%20Act%20nov%205th%20article.pdf

[25] http://www.forbes.com/sites/parmyolson/2011/03/17/congress-opens-investigation-into-hbgary-scandal

[26] http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf – Note page 12 (PDF page 18) for the reference to this DOJ unit. There's even a phone number for them (202-514-1187) and a description there of how prosecutions of certain classes of computer crime must be "pre-cleared" by that division – is that to ensure that the crimes in question are not committed by a sanctioned agency, person or company? Additionally, many activists are now questioning whether the DOJ refused to prosecute HBGary and the other "Team Themis" companies for crimes they committed because their partner Endgame worked with HBGary to target Glenn Greenwald, members of Anonymous and various other activists.