GlobalResearch
Center for Research on Globalization

Security Grifters Partner-Up on Sinister Cyber-Surveillance Project

By Tom Burghardt
Global Research, July 04, 2011
Antifascist Calling... 3 July 2011

Region: USA
Theme: Police State & Civil Rights

Last week, the White House released its National Strategy for Counterterrorism, a macabre document that places a premium on "public safety" over civil liberties and constitutional rights.

Indeed, "hope and change" huckster Barack Obama had the temerity to assert that the President "bears no greater responsibility than ensuring the safety and security of the American people."

Pity that others, including CIA "black site" prisoners tortured to death to "keep us safe" (some 100 at last count) aren't extended the same courtesy as The Washington Post reported last week.

As Secrecy News editor Steven Aftergood correctly points out, the claim that the President "has no greater responsibility than 'protecting the American people' is a paternalistic invention that is historically unfounded and potentially damaging to the political heritage of the nation."

Aftergood avers, "the presidential oath of office that is prescribed by the U.S. Constitution (Art. II, sect. 1) makes it clear that the President's supreme responsibility is to '…preserve, protect, and defend the Constitution of the United States.' There is no mention of public safety. It is the constitutional order that the President is sworn to protect, even if doing so entails risks to the safety and security of the American people."

But as our former republic slips ever-closer towards corporate dictatorship, Obama's mendacious twaddle about "protecting the American people," serves only to obscure, and reinforce, the inescapable fact that it's a rigged game.

Rest assured, "what happens in Vegas," Baghdad, Kabul or Manama–from driftnet spying to political-inspired witchhunts toillegal detention–won't, and hasn't, "stayed in Vegas."

Cyber Here, Cyber There, Cyber-Surveillance Everywhere

Last month, researcher Barrett Brown and the OpMetalGearnetwork lifted the lid on a new U.S. Government-sponsored cyber-surveillance project, Romas/COIN, now Odyssey, a multiyear, multimillion dollar enterprise currently run by defense and security giant Northrop Grumman.

With some $10.8 billion in revenue largely derived from contracts with the Defense Department, Northrop Grumman was No. 2 on the Washington Technology 2011 Top 100

List of Prime Federal Contractors.

“For at least two years,” Brown writes, “the U.S. has been conducting a secretive and immensely sophisticated campaign of mass surveillance and data mining against the Arab world, allowing the intelligence community to monitor the habits, conversations, and activity of millions of individuals at once.”

Information on this shadowy program was derived by scrutinizing hundreds of the more than 70,000 HBGary emails leaked onto the web by the cyber-guerrilla collective Anonymous.

Brown uncovered evidence that the “top contender to win the federal contract and thus take over the program is a team of about a dozen companies which were brought together in large part by Aaron Barr–the same disgraced CEO who resigned from his own firm earlier this year after he was discovered to have planned a full-scale information war against political activists at the behest of corporate clients.”

Readers will recall that Barr claimed he could exploit social media to gather information about WikiLeaks supporters in a bid to destroy that organization. Earlier this year, Barr told theFinancial Times he had used scraping techniques and had infiltrated WikiLeaks supporter Anonymous, in part by using IRC, Facebook, Twitter and other social media sites.

According to emails subsequently released by Anonymous, it was revealed that the ultra rightist U.S. Chamber of Commerce had hired white shoe law firm Hunton & Williams, and that Hunton attorneys, upon recommendation of an unnamed U.S. Department of Justice official, solicited a set of private security contractors–HBGary, HBGary Federal, Palantir and Berico Technologies (collectively known as Team Themis)–and stitched-up a sabotage campaign against WikiLeaks, journalists, labor unions, progressive political groups and Chamber critics.

Amongst the firms who sought to grab the Romas/COIN/Odyssey contract from Northrop when it came up for a “recompete” wasTASC, which describes itself as “a renowned provider of advanced systems engineering, integration and decision-support services across the intelligence, defense, homeland security and federal markets.”

According to Bloomberg BusinessWeek, TASC’s head of “Cybersecurity Initiatives,” Larry Strang, was formerly a Vice President with Northrop Grumman who led that firm’s Cybersecurity Group and served as Northrop’s NSA Account Manager. Prior to that, Strang, a retired Air Force Lt. Colonel, was Vice President for Operations at the spooky Science Applications International Corporation (SAIC).

Brown relates that emails between TASC executives Al Pisani, John Lovegrow and former HBGary Federal CEO Aaron Barr, provided details that they “were in talks with each other as well as Mantech executive Bob Frisbie on a ‘recompete’ pursuant to ‘counter intelligence’ operations that were already being conducted on behalf of the federal government by another firm, SAIC, with which they hoped to compete for contracts.”

In fact, HBGary Federal and TASC may have been cats-paws for defense giant ManTech International in the race to secure U.S. Government cyber-surveillance contracts. Clocking in at No. 22on Washington Technology’s “2011 Top 100 list,” ManTech earned some $1.46 billion in 2010, largely derived from work in “systems engineering and integration, technology and software development, enterprise security architecture, intelligence

operations support, critical infrastructure protection and computer forensics." The firm's major customers include the Defense Department, Department of Homeland Security, the Justice Department and the Defense Advanced Research Projects Agency (DARPA), the Pentagon's geek squad that is busily working to develop software for their Cyber Insider Threat (CINDER) program.

Both HBGary Federal and parent company HBGary, a California-based security firm run by the husband-wife team, Greg Hoglund and Penny Leavy, had been key players for the design of malware, undetectable rootkits and other "full directory exfiltration tools over TCP/IP" for the Defense Department according to documents released by the secret-shredding web site Public Intelligence.

Additional published documents revealed that they and had done so in close collaboration with General Dynamics (Project Cand Task Z), which had requested "multiple protocols to be scoped as viable options … for VoIP (Skype) protocol, BitTorrent protocol, video over HTTP (port 80), and HTTPS (port 443)" for unnamed secret state agencies.

According to Brown, it appears that Romas/COIN/Odyssey was also big on social media surveillance, especially when it came to "Foreign Mobile" and "Foreign Web" monitoring. Indeed, documents published by Public Intelligence (scooped-up by the HBGary-Anonymous hack) was a ManTech International-HBGary collaboration describing plans for Internet Based Reconnaissance Operations. The October 2010 presentation described plans that would hand "customers," presumably state intelligence agencies but also, as revealed by Anonymous, corporate security entities and public relations firms, the means to perform "native language searching" combined with "non-attributable architecture" and a "small footprint" that can be "as widely or narrowly focused as needed."

ManTech and HBGary promised to provide customers the ability to "Locate/Profile Internet 'Points of Interest'" on "individuals, companies, ISPs" and "organizations," and would do so through "detailed network mapping" that will "identify registered networks and registered domains"; "Graphical network representation based on Active Hosts"; "Operating system and network application identification"; "Identification of possible perimeter defenses" through "Technology Research, Intelligence Gap Fill, Counterintelligence Research" and "Customer Public Image Assessment."

The presentation described the social media monitoring process as one that would "employ highly skilled network professionals (read, ex-spooks and former military intelligence operatives) who will use "Non-attributable Internet access, custom developed toolsets and techniques, Native Language and in-country techniques" that "utilize foreign language search engines, mapping tools" and "iterative researching methodologies" for searching "Websites, picture sites, mapping sites/programs"; "Blogs and social networking sites"; "Forums and Bulletin Boards"; "Network Information: Whois, Trace Route, NetTroll, DNS"; "Archived and cached websites."

Clients who bought into the ManTech-HBGary "product" were promised "Rapid Non-attributable Open Source Research Results"; "Sourced Research Findings"; "Triage level Analysis"; "Vulnerability Assessment" and "Graphical Network and Social Diagramming" via data mining and extensive link analysis.

Undoubtedly, readers recall this is precisely what the National Security Agency has been

doing since the 1990s, if not earlier, through their electronic communications intercept program Echelon, a multibillion Pentagon project that conducted corporate espionage for American multinational firms as researcher Nicky Hager revealed in his 1997 piece forCovertAction Quarterly.

Other firms included in Lovegrove's email to Barr indicate that the new Romas/COIN/Odyssey "team" was to have included: "TASC (PMO [Project Management Operations], creative services); HBGary (Strategy, planning, PMO); Akamai (infrastructure); Archimedes Global (Specialized linguistics, strategy, planning); Acclaim Technical Services (specialized linguistics); Mission Essential Personnel (linguistic services); Cipher (strategy, planning operations); PointAbout (rapid mobile application development, list of strategic partners); Google (strategy, mobile application and platform development–long list of strategic partners); Apple (mobile and desktop platform, application assistance–long list of strategic partners). We are trying to schedule an interview with ATT plus some other small app developers."

Recall that AT&T is the NSA's prime telecommunications partner in that agency's illegal driftnet surveillance program and has been the recipient of "retroactive immunity" under the despicable FISA Amendments Act, a law supported by then-Senator Barack Obama. Also recall that the giant tech firm Apple was recently mired in scandal over reports that their mobile phone platform had, without their owners' knowledge or consent, speared geolocational data from the iPhone and then stored this information in an Apple-controlled data base accessible to law enforcement through various "lawful interception" schemes.

"Whatever the exact nature and scope of COIN," Brown writes, "the firms that had been assembled for the purpose by Barr and TASC never got a chance to bid on the program's recompete. In late September, Lovegrove noted to Barr and others that he'd spoken to the 'CO [contracting officer] for COIN'." The TASC executive told Barr that "the current procurement approach" was cancelled, citing "changed requirements."

Apparently the Pentagon, or other unspecified secret state satrapy told the contestants that "an updated RFI [request for information]" will be issued soon. According to a later missive from Lovegrove to Barr, "COIN has been replaced by a procurement called Odyssey." While it is still not entirely clear what Romas/COIN or the Odyssey program would do once deployed, Brown claims that "mobile phone software and applications constitute a major component of the program."

And given Barr's monomaniacal obsession with social media surveillance (that worked out well with Anonymous!) the presence of Alterian and SocialEyez on the procurement team may indicate that the secret state is alarmed by the prospect that the "Arab Spring" just might slip from proverbial "safe hands" and threaten Gulf dictatorships and Saudi Arabia with the frightening specter of democratic transformation.

Although the email from TASC executive Chris Clair to John Lovegrow names "Alterion" as a company to contact because of their their "SM2 tool," in all likelihood this is a typo given the fact that it is the UK-based firm "Alterian" that has developed said SM2 tool, described on their web site as a "business intelligence product that provides visibility into social media and lets you tap into a new kind of data resource; your customers' direct thoughts and opinions."

This would be a highly-profitable partnership indeed for enterprising intelligence agencies

and opaque corporate partners intent on monitoring political developments across the Middle East.

In fact, a 2010 press release, announced that Alterian had forged a partnership with the Dubai-based firm SocialEyez for "the world's first social media monitoring service designed for the Arab market."

We're informed that SocialEyez, a division of Media Watch Middle East, described as "the leading media monitoring service in the Middle East," offers services in "television, radio, social media, online news and internet monitoring across most sectors including commercial, government and PR."

That Barr and his partners were interested in bringing these firms to the Romas/COIN table is not surprising considering that the Alterian/SocialEyez deal promises "to develop and launch an Arabic language interface for Alterian SM2 to make it the world's first Arab language social media monitoring tool." Inquiring minds can't help but wonder which three-lettered American agencies alongside a stable of "corporate and government clients, including leading Blue Chips" might be interested in "maximising their social media monitoring investment"?

Pentagon "Manhunters" in the House

On an even more sinister note, the inclusion of Archimedes Global on the Romas/COIN team should set alarm bells ringing.

Archimedes is a small, privately-held niche security firm headquartered in Tampa, Florida where, surprise, surprise, U.S. Central Command (USCENTCOM) has it's main headquarters at the MacDill Air Force Base. On their web site, Archimedes describes itself as "a diversified technology company providing energy and information solutions to government and businesses worldwide." The firm claims that it "delivers solutions" to its clients by "combining deep domain expertise, multi-disciplinary education and training, and technology-enabled innovations."

While short on information regarding what it actually does, evidence suggests that the firm is chock-a-block with former spooks and Special Forces operators, skilled in the black arts of counterintelligence, various information operations, subversion and, let's be frank, tasks euphemistically referred to in the grisly trade as "wet work."

According to The Washington Post, the firm was established in 2005. However, although the Post claims in their "Top Secret America" series that the number of employees and revenue is "unknown," Dana Priest and William M. Arkin note that Archimedes have five government clients and are have speared contracts relating to "Ground forces operations," "Human intelligence," Psychological operations," and "Specialized military operations."

Brown relates that Archimedes was slated to provide "Specialized linguistics, strategy, planning" for the proposed Romas/COIN/Odyssey project for an unknown U.S. Government entity.

Based on available evidence however, one can speculate that Archimedes may have been chosen as part of the HBGary Federal/TASC team precisely because of their previous work as private contractors in human intelligence (HUMINT), running spies and infiltrating assets into organizations of interest to the CIA and Joint Special Operations Command (JSOC)

throughout the Middle East, Central- and South Asia.

In 2009, Antifascist Calling revealed that one of Archimedes Global's senior directors, retired Air Force Lt. Colonel George A. Crawford, published a chilling monograph, Manhunting: Counter-Network Organizing for Irregular Warfare, for the highly-influential Joint Special Operations University (JSOU) at MacDill Air Force Base in Tampa.

JSOU is the "educational component" of United States Special Operations Command (USSOCOM). With a mission that touts its ability to "plan and synchronize operations" against America's geopolitical adversaries and rivals, JSOU's Strategic Studies Department "advances SOF strategic influence by its interaction in academic, interagency, and United States military communities."

Accordingly, Archimedes "information and risk" brief claim they can solve "the most difficult communication and risk problems by seeing over the horizon with a blend of art and science." And with focus areas that include "strategic communications, media analysis and support, crisis communications, and risk and vulnerability assessment and mitigation," it doesn't take a rocket scientist to infer that those well-schooled in the dark art of information operations (INFOOPS) would find a friendly home inside the Romas/COIN contract team.

With some 25-years experience "as a foreign area officer specializing in Eastern Europe and Central Asia," including a stint "as acting Air and Defense Attaché to Kyrgyzstan," Crawford brings an interesting skill-set to the table. Crawford writes:

Manhunting–the deliberate concentration of national power to find, influence, capture, or when necessary kill an individual to disrupt a human network–has emerged as a key component of operations to counter irregular warfare adversaries in lieu of traditional state-on-state conflict measures. It has arguably become a primary area of emphasis in countering terrorist and insurgent opponents. (George A. Crawford, Manhunting: Counter-Network Organization for Irregular Warfare, JSOU Report 09-7, The JSOU Press, Hurlburt Field, Florida, September 2009, p. 1)

Acknowledged manhunting masters in their own right, the Israeli settler-colonial security apparat have perfected the art of "targeted killing," when they aren't dropping banned munitions such as white phosphorus on unarmed, defenseless civilian populations or attacking civilian vessels on the high seas.

Like their Israeli counterparts who come highly recommended as models of restraint, an American manhunting agency will employ similarly subtle, though no less lethal, tactics. Crawford informs us:

When compared with conventional force-on-force warfare, manhunting fundamentally alters the ratio between warfare's respective firepower, maneuver, and psychological elements. Firepower becomes less significant in terms of mass, while the precision and discretion with which firepower is employed takes on tremendous significance, especially during influence operations. Why drop a bomb when effects operations or a knife might do? (Crawford, op. cit., p. 11, emphasis added)

Alongside actual shooters, "sensitive site exploitation (SSE) teams are critical operational components for Pentagon "manhunters." We're told that SSE teams will be assembled and able to respond on-call "in the event of a raid on a suspect site or to conduct independent

‘break-in and search’ operations without leaving evidence of their intrusion.” Such teams must possess “individual skills” such as “physical forensics, computer or electronic exploitation, document exploitation, investigative techniques, biometric collection, interrogation/debriefing and related skills.”

As if to drive home the point that the target of such sinister operations are the American people and world public opinion, Crawford, ever the consummate INFOOPS warrior, views “strategic information operations” as key to this murderous enterprise. Indeed, they “must be delicately woven into planned kinetic operations to increase the probability that a given operation or campaign will achieve its intended effect.”

Personnel skilled at conducting strategic information operations–to include psychological operations, public information, deception, media and computer network operations, and related activities–are important for victory. Despite robust DoD and Intelligence Community capabilities in this area, efforts to establish organizations that focus information operations have not been viewed as a positive development by the public or the media, who perceive government-sponsored information efforts with suspicion. Consequently, these efforts must take place away from public eyes. Strategic information operations may also require the establishment of regional or local offices to ensure dissemination of influence packages and assess their impact. Thus manhunting influence may call for parallel or independent structures at all levels…” (Crawford, op. cit., pp. 27-28, emphasis added)

While we do not as yet have a complete picture of the Romas/COIN/Odyssey project, some preliminary conclusions can be drawn.

“Altogether, then,” Brown writes, “a successful bid for the relevant contract was seen to require the combined capabilities of perhaps a dozen firms–capabilities whereby millions of conversations can be monitored and automatically analyzed, whereby a wide range of personal data can be obtained and stored in secret, and whereby some unknown degree of information can be released to a given population through a variety of means and without any hint that the actual source is U.S. military intelligence.”

Although Brown’s initial research concluded that Romas/COIN/Odyssey will operate “in conjunction with other surveillance and propaganda assets controlled by the U.S. and its partners,” with a firm like Archimedes on-board, once information has been assembled on individuals described in other contexts as “radicals” or “key extremists,” will they subsequently be made to “disappear” into the hands of “friendly” security services such as those of strategic U.S. partners Bahrain and Saudi Arabia?

We’re reminded that “Barr was also at the center of a series of conspiracies by which his own company and two others hired out their collective capabilities for use by corporations that sought to destroy their political enemies by clandestine and dishonest means.”

Indeed, “none of the companies involved,” Brown writes, have been investigated; a proposed Congressional inquiry was denied by the committee chair, noting that it was the Justice Department’s decision as to whether to investigate, even though it was the Justice Department itself that made the initial introductions. Those in the intelligence contracting industry who believe themselves above the law are entirely correct.”

Brown warns that “a far greater danger is posed by the practice of arming small and unaccountable groups of state and military personnel with a set of tools by which to achieve

better and better ‘situational awareness’ on entire populations” while simultaneously manipulating “the information flow in such a way as to deceive those same populations.”

Beginning, it should be noted, right here at home…

Articles by: **Tom Burghardt**
http://antifascist-calling.blogspot.com/