GlobalResearch
Center for Research on Globalization

Orwell 2011: Towards a Pervasive “Surveillance State” in America

Biometrics, Facial Mapping, "Computer-Aided ID"....

By Tom Burghardt
Global Research, March 28, 2011
Antifascist Calling... 28 March 2011
Region: USA
Theme: Police State & Civil Rights

Not since AT&T whistleblower Marc Klein’s 2006 revelations that U.S. telecommunications giants were secretly collaborating with the government to spy on Americans, has a story driven home the point that we are confronted by a daunting set of invisible enemies: the security and intelligence firms constellating the dark skies of the National Security State.

As echoes from last month’s disclosures by the cyber-guerrilla collective Anonymous continue to reverberate, leaked HBGary emails and documents are providing tantalizing insight into just how little daylight there is between private companies and the government.

The latest front in the ongoing war against civil liberties and privacy rights is the Pentagon’s interest in “persona management software.”

A euphemism for a suite of high-tech tools that equip an operative–military or corporate, take your pick–with multiple avatars or sock puppets, our latter day shadow warriors hope to achieve a leg up on their opponents in the “war of ideas” through stealthy propaganda campaigns rebranded as “information operations.”

A Pervasive Surveillance State

The signs of a pervasive surveillance state are all around us. From the “persistent cookies” that track our every move across the internet to indexing dissidents already preemptively detained in public and private data bases: threats to our freedom to speak out without harassment, or worse, have never been greater.

As constitutional scholar Jack Balkin warned, the transformation of what was once a democratic republic based on the rule of law into a “National Surveillance State,” feature “huge investments in electronic surveillance and various end runs around traditional Bill of Rights protections and expectations about procedure.”

“These end runs,” Balkin wrote, “included public private cooperation in surveillance and exchange of information, expansion of the state secrets doctrine, expansion of administrative warrants and national security letters, a system of preventive detention, expanded use of military prisons, extraordinary rendition to other countries, and aggressive interrogation techniques outside of those countenanced by the traditional laws of war.”

Continuing the civil liberties’ onslaught, The Wall Street Journal reported last week that Barack Obama’s “change” regime has issued new rules that “allow investigators to hold

domestic-terror suspects longer than others without giving them a Miranda warning, significantly expanding exceptions to the instructions that have governed the handling of criminal suspects for more than four decades."

The Journal points out that the administrative "revision" of long-standing rules and case law "marks another step back from [Obama's] pre-election criticism of unorthodox counterterror methods."

Also last week, The Raw Story revealed that the FBI has plans to "embark on a $1 billion biometrics project and construct an advanced biometrics facility to be shared with the Pentagon."

The Bureau's new biometrics center, part of which is already operating in Clarksburg, West Virginia, "will be based on a system constructed by defense contractor Lockheed Martin."

"Starting with fingerprints," The Raw Story disclosed, the center will function as "a global law enforcement database for the sharing of those biometric images." Once ramped-up "the system is slated to expand outward, eventually encompassing facial mapping and other advanced forms of computer-aided identification."

The transformation of the FBI into a political Department of Precrime is underscored by moves to gift state and local police agencies with electronic fingerprint scanners. Local cops would be "empowered to capture prints from any suspect, even if they haven't been arrested or convicted of a crime."

"In such a context," Stephen Graham cautions in Cities Under Siege, "Western security and military doctrine is being rapidly imagined in ways that dramatically blur the juridical and operational separation between policing, intelligence and the military; distinctions between war and peace; and those between local, national and global operations."

This precarious state of affairs, Graham avers, under conditions of global economic crisis in the so-called democratic West as well as along the periphery in what was once called the Third World, has meant that "wars and associated mobilizations ... become both boundless and more or less permanent."

Under such conditions, Dick Cheney's infamous statement that the "War on Terror" might last "decades" means, according to Graham, that "emerging security policies are founded on the profiling of individuals, places, behaviours, associations, and groups."

But to profile more effectively, whether in Cairo, Kabul, or New York, state security apparatchiks and their private partners find it necessary to squeeze ever more data from a surveillance system already glutted by an overabundance of "situational awareness."

"Last October," Secrecy News reported, "the DNI revealed that the FY2010 budget for the National Intelligence Program (NIP) was $53.1 billion. And the Secretary of Defense revealed that the FY2010 budget for the Military Intelligence Program (MIP) was $27.0 billion, the first time the MIP budget had been disclosed, for an aggregate total intelligence budget of $80.1 billion for FY 2010."

This excludes of course, the CIA and Pentagon's black budget that hides a welter of top secret and above Special Access Programs under a dizzying array of code names and acronyms. In February, Wired disclosed that the black budget "appears to be about $56

billion, the same as last year," but this "may only be the tip of an iceberg of secret funds."

While the scandalous nature of such outlays during a period of intense economic and social attacks on the working class are obvious, less obvious are the means employed by the so-called "intelligence community" to defend an indefensible system of exploitation and corruption.

Which brings us back to the HBGary hack.

"Operation MetalGear"

While media have focused, rightly so, on the sleazy campaign proposed to Bank of America and the U.S. Chamber of Commerce by the high-powered law firm and lobby shop Hunton & Williams (H&W) to bring down WikiLeaks and tar Chamber critics, the treasure trove of emails leaked by Anonymous also revealed a host of Pentagon programs pointed directly at the heart of our freedom to communicate.

In fact, The Tech Herald revealed that while Palantir and Berico sought to distance themselves from HBGary and Hunton & William's private spy op, "in 2005, Palantir was one of countless startups funded by the CIA, thanks to their venture funding arm, In-Q-Tel."

"Most of In-Q-Tel's investments," journalist Steve Ragan wrote, "center on companies that specialize in automatic collection and processing of information."

In other words Palantir, and dozens of other security start-ups to the tune of $200 million since 1999, was a recipient of taxpayer-funded largess from the CIA's venture capitalist arm for products inherently "dual-use" in nature.

"Palantir Technologies," The Tech Herald revealed, was "the main workhorse when it comes to Team Themis' activities."

In proposals sent to H&W, a firm recommended to Bank of America by a Justice Department insider, "Team Themis said they would 'leverage their extensive knowledge of Palantir's development and data integration environments' allowing all of the data collected to be 'seamlessly integrated into the Palantir analysis framework to enhance link and artifact analysis'."

Following the sting of HBGary Federal and parent company HBGary, Anonymous disclosed on-going interest and contract bids between those firms, Booz Allen Hamilton and the U.S. Air Force to develop software that will allow cyber-warriors to create fake personas that help "manage" Pentagon interventions into social media platforms like Facebook, Twitter and blogs.

As Ragan points out, while the "idea for such technology isn't new," and that "reputation and persona management techniques have been used by the government and the private sector for years," what makes these disclosures uniquely disturbing are apparent plans by the secret state to use the software for propaganda campaigns that can just as easily target an American audience as one in a foreign country.

While neither HBGary nor Booz Allen secured those contracts, interest by HBGary Federal's disgraced former CEO Aaron Barr and others catering to the needs of the militarist state

continue to drive development forward.

Dubbed "Operation MetalGear", Anonymous believes that the program "involves an army of fake cyber personalities immersed in social networking websites for the purposes of manipulating the mass population via influence, crawling information from major online communities (such as Facebook), and identifying anonymous personalities via correlating stored information from multiple sources to establish connections between separate online accounts, using this information to arrest dissidents and activists who work anonymously."

As readers recall, such tools were precisely what Aaron Barr boasted would help law enforcement officials take down Anonymous and identify WikiLeaks supporters.

According to a solicitation (RTB220610) found on the FedBizOpps.Gov web site, under the Orwellian tag "Freedom of Information Act Support," the Air Force is seeking software that "will allow 10 personas per user, replete with background, history, supporting details, and cyber presences that are technically, culturally and geographacilly [sic] consistent."

We're informed that "individual applications will enable an operator to exercise a number of different online persons from the same workstation and without fear of being discovered by sophisticated adversaries."

Creepily, "personas must be able to appear to originate in nearly any part of the world and can interact through conventional online services and social media platforms. The service includes a user friendly application environment to maximize the user's situational awareness by displaying real-time local information."

Aiming for maximum opacity, the RFI demands that the licence "protects the identity of government agencies and enterprise organizations." An "enterprise organization" is a euphemism for a private contractor hired by the government to do its dirty work.

The proposal specifies that the licensed software will enable "organizations to manage their persistent online personas by assigning static IP addresses to each persona. Individuals can perform static impersonations, which allow them to look like the same person over time. Also allows organizations that frequent same site/service often to easily switch IP addresses to look like ordinary users as opposed to one organization."

While Barr's premature boasting may have brought Team Themis to ground, one wonders how many other similar operations continue today under cover of the Defense Department's black budget.

Corporate Cut-Outs

Following up on last month's revelations, The Guardian disclosed that a "Californian corporation has been awarded a contract with United States Central Command (Centcom), which oversees US armed operations in the Middle East and Central Asia, to develop what is described as an 'online persona management service' that will allow one US serviceman or woman to control up to 10 separate identities based all over the world."

That firm, a shadowy Los Angeles-based outfit called Ntrepid is devoid of information on its corporate web site although a company profile avers that the firm "provides national security and law enforcement customers with software, hardware, and managed services for cyber operations, analytics, linguistics, and tagging & tracking."

According to Guardian reporters Nick Fielding and Ian Cobain, Ntrepid was awarded a $2.76M contract by CENTCOM, which refused to disclose "whether the multiple persona project is already in operation or discuss any related contracts."

Blurring corporate lines of accountability even further, The Tech Herald revealed that Ntrepid may be nothing more than a "ghost corporation," a cut-out wholly owned and operated by Cubic Corporation.

A San Diego-based firm describing itself as "a global leader in defense and transportation systems and services" that "is emerging as an international supplier of smart cards and RFID solutions," Cubic clocks in at No. 75 on Washington Technology's list of 2010 Top Government Contractors.

Founded by Walter J. Zable, the firm's Chairman of the Board and CEO, Cubic has been described as one of the oldest and largest defense electronics firms on the West Coast.

Chock-a-block with high-level connections to right-wing Republicans including Darrell Issa, Duncan Hunter and Dan Coates, during the 2010 election cycle Cubic officers donated some $90,000 to Republican candidates, including $25,000 to the National Republican Congressional Committee and some $30,000 to the National Republican Senatorial Committee, according to the Center for Responsive Politics' OpenSecrets.org.

With some $1 billion in 2009 revenue largely derived from the Defense Department, the company's "Cyber Solutions" division "provides specialized cyber security products and solutions for defense, intelligence and homeland security customers."

The RFI for the Air Force disclosed by Anonymous Ragan reports, "was written for Anonymizer, a company acquired in 2008 by intelligence contractor Abraxas Corporation. The reasoning is that they had existing persona management software and abilities."

In turn, Abraxas was purchased by Cubic in 2010 for $124 million, an acquisition which Washington Technology described as one of the "best intelligence-related" deals of the year.

As The Tech Herald revealed, "some of the top talent at Anonymizer, who later went to Abraxas, left the Cubic umbrella to start another intelligence firm. They are now listed as organizational leaders for Ntrepid, the ultimate winner of the $2.7 million dollar government contract."

Speculation is now rife that since "Ntrepid's corporate registry lists Abraxas' previous CEO and founder, Richard Helms, as the director and officer, along with Wesley Husted, the former CFO, who is an Ntrepid officer as well," the new firm may be little more than an under-the-radar front for Cubic.

Amongst the Security Services offered by the firm we learn that "Cubic subsidiaries are working individually and in concert to develop a wide range of security solutions" that include: "C4ISR data links for homeland security intelligence, surveillance and reconnaissance missions;" a Cubic Virtual Analysis Center which promises to deliver "superior situational awareness to decision makers in government, industry and nonprofit organizations," human behavior pattern analysis, and other areas lusted after by securocrats.

The Guardian informs us that the “multiple persona contract is thought to have been awarded as part of a programme called Operation Earnest Voice (OEV), which was first developed in Iraq as a psychological warfare weapon against the online presence of al-Qaida supporters and others ranged against coalition forces.”

“Since then,” Fielding and Cobain wrote, “OEV is reported to have expanded into a $200m programme and is thought to have been used against jihadists across Pakistan, Afghanistan and the Middle East.”

While CENTCOM’s then-commander, General David Petraeus told the Senate Armed Services Committee last year that the program was designed to “counter extremist ideology and propaganda,” in light of HBGary revelations, one must ask whether firms involved in the dirty tricks campaign against WikiLeaks have deployed versions of “persona management software” against domestic opponents.

While we cannot say with certainty this is the case, mission creep from other “War on Terror” fronts, notably ongoing NSA warrantless wiretapping programs and Defense Department spy ops against antiwar activists, also involving “public-private partnerships” amongst security firms and the secret state, should give pause.

Tom Burghardt is a researcher and activist based in the San Francisco Bay Area. In addition to publishing in Covert Action Quarterly and Global Research, he is a Contributing Editor with Cyrano’s Journal Today. His articles can be read on Dissident Voice, The Intelligence Daily, Pacific Free Press, Uncommon Thought Journal, and the whistleblowing website WikiLeaks. He is the editor of Police State America: U.S. Military “Civil Disturbance” Planning, distributed by AK Press and has contributed to the new book from Global Research, The Global Economic Crisis: The Great Depression of the XXI Century.

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

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