GlobalResearch
Center for Research on Globalization

“Secrets R US”: America’s Spying Apparatus, Echelon, NSA Eavesdropping and the Outsourcing of Intelligence Operations

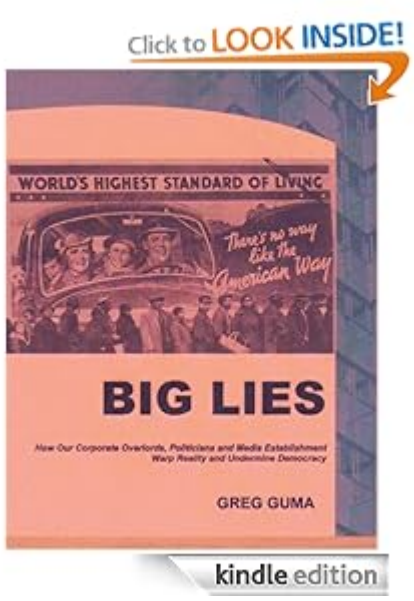
By Greg Guma
Global Research, October 29, 2013

Region: USA
Theme: Intelligence, Police State & Civil Rights, US NATO War Agenda

This essay is an excerpt from Big Lies: How Our Corporate Overlords, Politicians and Media Establishment Warp Reality and Undermine Democracy. Greg Guma’s latest book, Dons of Time, is a sci-fi look at the control of history as power.

Despite 24-hour news and talk about transparency, there’s a lot we don’t know about our past, much less current events. What’s worse, some of what we think we know isn’t true.

The point is that it’s no accident.



Consider, for example, the circumstances that led to open war in Vietnam. According to official history, two US destroyers patrolling in the Gulf of Tonkin off North Vietnam were victims of unprovoked attacks in August 1964, leading to a congressional resolution giving President Johnson the power “to take all necessary measures.”

In fact, the destroyers were spy ships, part of a National Security Agency (NSA) eavesdropping program operating near the coast as a way to provoke the North Vietnamese into turning on their radar and other communications channels. The more provocative the maneuvers, the more signals that could be captured. Meanwhile, US raiding parties were shelling mainland targets. Documents revealed later indicated that the August 4 attack on the USS Maddox – the pretext for passing the Gulf of Tonkin Resolution – may not even have taken place.

But even if it did, the incident was still stage managed to build up congressional and public support for the war. Evidence suggests that the plan was based on Operation Northwoods, a scheme developed in 1962 to justify an invasion of Cuba. Among the tactics the Joint Chiefs of Staff considered then were blowing up a ship in Guantanamo Bay, a phony "communist Cuba terror campaign" in Florida and Washington, DC, and an elaborate plan to convince people that Cuba had shot down a civilian airliner filled with students. That operation wasn't implemented, but two years later, desperate for a war, the administration's military brass found a way to create the necessary conditions in Vietnam.

NSA and Echelon

For more than half a century, the eyes and ears of US power to monitor and manipulate information (and with it, mass perceptions) has been the NSA, initially designed to assist the CIA. Its original task was to collect raw information about threats to US security, cracking codes and using the latest technology to provide accurate intelligence on the intentions and activities of enemies. Emerging after World War II, its early focus was the Soviet Union. But it never did crack a high-level Soviet cipher system. On the other hand, it used every available means to eavesdrop on not only enemies but also allies and, sometimes, US citizens.

In Body of Secrets, James Bamford described a bureaucratic and secretive behemoth, based in an Orwellian Maryland complex known as Crypto City. From there, supercomputers linked it to spy satellites, subs, aircraft, and equally covert, strategically placed listening posts worldwide. As of 2000, it had a $7 billion annual budget and directly employed at least 38,000 people, more than the CIA and FBI. It was also the leader of an international intelligence club, UKUSA, which includes Britain, Canada, Australia, and New Zealand. Together, they monitored and recorded billions of encrypted communications, telephone calls, radio messages, faxes, and e-mails around the world.

Over the years, however, the line between enemies and friends blurred, and the intelligence gatherers often converted their control of information into unilateral power, influencing the course of history in ways that may never be known. No doubt the agency has had a hand in countless covert operations; yet, attempts to pull away the veil of secrecy have been largely unsuccessful.

In the mid-1970s, for example, just as Congress was attempting to reign in the CIA, the NSA was quietly creating a virtual state, a massive international computer network named Platform. Doing away with formal borders, it developed a software package that turned worldwide Sigint (short for "signal intelligence": communication intelligence, eavesdropping, and electronic intelligence) into a unified whole. The software package was code named Echelon, a name that has since become a synonym for eavesdropping on commercial communication.

Of course, the NSA and its British sister, the Government Communications Headquarters (GCHQ), refused to admit Echelon existed, even though declassified documents appeared on the Internet and Congress conducted an initial investigation. But a European Parliament report also confirmed Echelon's activities, and encouraged Internet users and governments to adopt stronger privacy measures in response.

In March 2001, several ranking British politicians discussed Echelon's potential impacts on civil liberties, and a European Parliament committee considered its legal, human rights, and

privacy implications. The Dutch held similar hearings, and a French National Assembly inquiry urged the European Union to embrace new privacy enhancing technologies to protect against Echelon's eavesdropping. France launched a formal investigation into possible abuses for industrial espionage.

When Allies Compete

A prime reason for Europe's discontent was the growing suspicion that the NSA had used intercepted conversations to help US companies win contracts heading for European firms. The alleged losers included Airbus, a consortium including interests in France, Germany, Spain, and Britain, and Thomson CSF, a French electronics company. The French claimed they had lost a $1.4 billion deal to supply Brazil with a radar system because the NSA shared details of the negotiations with Raytheon. Airbus may have lost a contract worth $2 billion to Boeing and McDonnell Douglas because of information intercepted and passed on by the agency.

According to former NSA agent Wayne Madsen, the US used information gathered from its bases in Australia to win a half share in a significant Indonesian trade contract for AT&T. Communication intercepts showed the contract was initially going to a Japanese firm. A bit later a lawsuit against the US and Britain was launched in France, judicial and parliamentary investigations began in Italy, and German parliamentarians demanded an inquiry.

The rationale for turning the NSA loose on commercial activities, even those involving allies, was provided in the mid-90s by Sen. Frank DeConcini, then chairman of the Senate Intelligence Committee. "I don't think we should have a policy where we're going to invade the Airbus inner sanctum and find out their secrets for the purpose of turning it over to Boeing or McDonnell Douglas," he opined. "But if we find something, not to share it with our people seems to me to be not smart."

President Bill Clinton and other US officials buttressed this view by charging that European countries were unfairly subsidizing Airbus. In other words, competition with significant US interests can be a matter of national security, and private capitalism must be protected from state-run enterprises.

The US-Europe row about Airbus subsidies was also used as a "test case" for scientists developing new intelligence tools. At US Defense Department conferences on "text retrieval," competitions were staged to find the best methods. A standard test featured extracting protected data about "Airbus subsidies."

Manipulating Democracy

In the end, influencing the outcome of commercial transactions is but the tip of this iceberg. The NSA's ability to intercept to virtually any transmitted communication has enhanced the power of unelected officials and private interests to set covert foreign policy in motion. In some cases, the objective is clear and arguably defensible: taking effective action against terrorism, for example. But in others, the grand plans of the intelligence community have led it to undermine democracies.

The 1975 removal of Australian Prime Minister Edward Whitlam is an instructive case. At the time of Whitlam's election in 1972, Australian intelligence was working with the CIA against the Allende government in Chile. The new PM didn't simply order a halt to

Australia's involvement, explained William Blum in Killing Hope, a masterful study of US interventions since World War II. Whitlam seized intelligence information withheld from him by the Australian Security and Intelligence Organization (ASIO), and disclosed the existence of a joint CIA-ASIO directorate that monitored radio traffic in Asia. He also openly disapproved of US plans to build up the Indian Ocean Island of Diego Garcia as a military-intelligence-nuclear outpost.

Both the CIA and NSA became concerned about the security and future of crucial intelligence facilities in and near Australia. The country was already key member of UKUSA. After launching its first space-based listening post-a microwave receiver with an antenna pointed at earth-NSA had picked an isolated desert area in central Australia as a ground station. Once completed, the base at Alice Springs was named Pine Gap, the first of many listening posts to be installed around the world. For the NSA and CIA, Whitlam posed a threat to the secrecy and security of such operations.

An early step was covert funding for the political opposition, in hopes of defeating Whitlam's Labor Party in 1974. When that failed, meetings were held with the Governor-General, Sir John Kerr, a figurehead representing the Queen of England who had worked for CIA front organizations since the 50s. Defense officials warned that intelligence links would be cut off unless someone stopped Whitlam. On November 11, 1975, Kerr responded, dismissing the prime minister, dissolving both houses of Parliament, and appointing an interim government until new elections were held.

According to Christopher Boyce (subject of The Falcon and the Snowman, a fictionalized account), who watched the process while working for TRW in a CIA-linked cryptographic communications center, the spooks also infiltrated Australian labor unions and contrived to suppress transportation strikes that were holding up deliveries to US intelligence installations. Not coincidentally, some unions were leading the opposition to development of those same facilities.

How often, and to what effect, such covert ops have succeeded is another of the mysteries that comprise an unwritten history of the last half century. Beyond that, systems like Echelon violate the human right to individual privacy, and give those who control the information the ability to act with impunity, sometimes destroying lives and negating the popular will in the process.

Hiding the Agenda in Peru

In May 1960, when a U-2 spy plane was shot down over Soviet territory, President Dwight Eisenhower took great pains to deny direct knowledge or authorization of the provocative mission. In reality, he personally oversaw every U-2 mission, and had even riskier and more provocative bomber overflights in mind.

It's a basic rule of thumb for covert ops: When exposed, keep denying and deflect the blame. More important, never, never let on that the mission itself may be a pretext, or a diversion from some other, larger agenda.

Considering that, the April 20, 2001, shoot down of a plane carrying missionaries across the Brazilian border into Peru becomes highly suspicious. At first, the official story fed to the press was that Peruvian authorities ordered the attack on their own, over the pleas of the CIA "contract pilots" who initially spotted the plane. But Peruvian pilots involved in that

program, supposedly designed to intercept drug flights, insist that nothing was shot down without US approval.

Innocent planes were sometimes attacked, but most were small, low flying aircraft that didn't file flight plans and had no radios. This plane maintained regular contact and did file a plan. Still, even after it crash-landed, the Peruvians continued to strafe it, perhaps in an attempt to ignite the plane's fuel and eliminate the evidence.

> "I think it has to do with Plan Colombia and the coming war," said Celerino Castillo, who had previously worked in Peru for Drug Enforcement Agency. "The CIA was sending a clear message to all non-combatants to clear out of the area, and to get favorable press." The flight was heading to Iquitos, which "is at the heart of everything the CIA is doing right now," he added. "They don't want any witnesses."

Timing also may have played a part. The shoot down occurred on the opening day of the Summit of the Americas in Quebec City. Uruguay's President Jorge Ibanez, who had proposed the worldwide legalization of drugs just weeks before, was expected to make a high-profile speech on his proposal at the gathering. The downing of a drug smuggling plane at this moment, near territory held by Colombia's FARC rebels, would help to defuse Uruguay's message and reinforce the image of the insurgents as drug smugglers.

If you doubt that the US would condone such an operation or cover it up, consider this: In 1967, Israel torpedoed the USS Liberty, a large floating listening post, as it was eavesdropping on the Arab-Israeli war off the Sinai Peninsula. Hundreds of US sailors were wounded and killed, probably because Israel feared that its massacre of Egyptian prisoners at El Arish might be overheard. How did the Pentagon respond? By imposing a total news ban, and covering up the facts for decades.

Will we ever find out what really happened in Peru, specifically why a missionary and her daughter were killed? Not likely, since it involves a private military contractor that is basically beyond the reach of congressional accountability.

In 2009, when the Peru shoot down became one of five cases of intelligence operation cover up being investigated by the US House Intelligence Committee, the CIA inspector general concluded that the CIA had improperly concealed information about the incident. Intelligence Oversight and Investigations Subcommittee Chairwoman Jan Schakowsky, who led the investigation, didn't rule out referrals to the Justice Department for criminal prosecutions if evidence surfaced that intelligence officials broke the law. But she couldn't guarantee that the facts would ever come to light, since the Committee's report of its investigation would be classified.

The most crucial wrinkle in the Peruvian incident is the involvement of DynCorp, which was active in Colombia and Bolivia under large contracts with various US agencies. The day after the incident, ABC news reported that, according to "senior administration officials," the crew of the surveillance plane that first identified the doomed aircraft "was hired by the CIA from DynCorp." Within two days, however, all references to DynCorp were scrubbed from ABC's Website. A week later, the New York Post claimed the crew actually worked for Aviation Development Corp., allegedly a CIA proprietary company.

Whatever the truth, State Department officials refused to talk on the record about DynCorp's activities in South America. Yet, according to DynCorp's State Department

contract, the firm had received at least $600 million over the previous few years for training, drug interdiction, search and rescue (which included combat), air transport of equipment and people, and reconnaissance in the region. And that was only what they put on paper. It also operated government aircraft and provided all manner of personnel, particularly for Plan Colombia.

Outsourcing Defense

DynCorp began in 1946 as the employee-owned air cargo business California Eastern Airways, flying in supplies for the Korean War. This and later government work led to charges that it was a CIA front company. Whatever the truth, it ultimately became a leading PMC, hiring former soldiers and police officers to implement US foreign policy without having to report to Congress.

The push to privatize war gained traction during the first Bush administration. After the first Gulf War, the Pentagon, then headed by Defense Secretary Dick Cheney, paid a Halliburton subsidiary nearly $9 million to study how PMCs could support US soldiers in combat zones, according to a Mother Jones investigation. Cheney subsequently became CEO of Halliburton, and Brown & Root, later known as Halliburton KBR, won billions to construct and run military bases, some in secret locations.

One of DynCorp's earliest "police" contracts involved the protection of Haitian President Jean-Bertrand Aristide, and, after he was ousted, providing the "technical advice" that brought military officers involved in that coup into Haiti's National Police. Despite this dodgy record, in 2002 it won the contract to protect another new president, Afghanistan's Hamid Karzai. By then, it was a top IT federal contractor specializing in computer systems development, and also providing the government with aviation services, general military management, and security expertise.

Like other private military outfits, the main danger it has faced is the risk of public exposure. Under one contract, for example, DynCorp sprayed vast quantities of herbicides over Colombia to kill the cocaine crop. In September 2001, Ecuadorian Indians filed a class action lawsuit, charging that DynCorp recklessly sprayed their homes and farms, causing illnesses and deaths and destroying crops. In Bosnia, private police provided by DynCorp for the UN were accused of buying and selling prostitutes, including a 12-year-old girl. Others were charged with videotaping a rape.

In the first years of the 21st century, DynCorp's day-to-day operations in South America were overseen by State Department officials, including the Narcotic Affairs Section and the Air Wing, the latter a clique of unreformed cold warriors and leftovers from 80s operations in Central America. It was essentially the State Department's private air force in the Andes, with access to satellite-based recording and mapping systems.

In the 1960s, a similar role was played by the Vinnell Corp., which the CIA called "our own private mercenary army in Vietnam." Vinnell later became a subsidiary of TRW, a major NSA contractor, and employed US Special Forces vets to train Saudi Arabia's National Guard. In the late 1990s, TRW hired former NSA director William Studeman to help with its intelligence program.

DynCorp avoided the kind of public scandal that surrounded the activities of Blackwater. In Ecuador, where it developed military logistics centers and coordinated "anti-terror" police

training, the exposure of a secret covenant signed with the Aeronautics Industries Directorate of the Ecuadorian Air Force briefly threatened to make waves. According to a November 2003 exposé in Quito's El Comercio, the arrangement, hidden from the National Defense Council, made DynCorp's people part of the US diplomatic mission.

In Colombia, DynCorp's coca eradication and search-and-rescue missions led to controversial pitched battles with rebels. US contract pilots flew Black Hawk helicopters carrying Colombian police officers who raked the countryside with machine gun fire to protect the missions against attacks. According to investigative reporter Jason Vest, DynCorp employees were also implicated in narcotics trafficking. But such stories didn't get far, and, in any case, DynCorp's "trainers" simply ignored congressional rules, including those that restrict the US from aiding military units linked to human rights abuses.

In 2003, DynCorp won a multimillion-dollar contract to build a private police force in post-Saddam Iraq, with some of the funding diverted from an anti-drug program for Afghanistan. In 2004, the State Department further expanded DynCorp's role as a global US surrogate with a $1.75 billion, five year contract to provide law enforcement personnel for civilian policing operations in "post-conflict areas" around the world. That March, the company also got an Army contract to support helicopters sold to foreign countries. The work, described as "turnkey" services, includes program management, logistics support, maintenance and aircrew training, aircraft maintenance and refurbishment, repair and overhaul of aircraft components and engines, airframe and engine upgrades, and the production of technical publications.

In short, DynCorp was a trusted partner in the military-intelligence-industrial complex. "Are we outsourcing order to avoid public scrutiny, controversy or embarrassment?" asked Rep. Schakowsky upon submitting legislation to prohibit US funding for private military firms in the Andean region. "If there is a potential for a privatized Gulf of Tonkin incident, then the American people deserve to have a full and open debate before this policy goes any further."

If and when that ever happens, the discussion will have to cover a lot of ground. Private firms, working in concert with various intelligence agencies, constitute a vast foreign policy apparatus that is largely invisible, rarely covered by the corporate press, and not currently subject to congressional oversight. The Freedom of Information Act simply doesn't apply. Any information on whom they arm or how they operate is private, proprietary information.

The US government downplays its use of mercenaries, a state of affairs that could undermine any efforts to find out about CIA activities that are concealed from Congress. Yet private contractors perform almost every function essential to military operations, a situation that has been called the "creeping privatization of the business of war." By 2004, the Pentagon was employing more than 700,000 private contractors.

The companies are staffed by former generals, admirals, and highly trained officers. Name a hot spot and some PMC has people there. DynCorp has worked on the Defense Message System Transition Hub and done long-range planning for the Air Force. MPRI had a similar contract with the Army, and for a time coordinated the Pentagon's military and leadership training in at least seven African nations.

How did this outsourcing of defense evolve? In 1969, the US Army had about 1.5 million active duty soldiers. By 1992, the figure had been cut by half. Since the mid-1990s,

however, the US has mobilized militarily to intervene in several significant conflicts, and a corporate "foreign legion" has filled the gap between foreign policy imperatives and what a downsized, increasingly over-stretched military can provide.

Use of high technology equipment feeds the process. Private companies have technical capabilities that the military needs, but doesn't always possess. Contractors have maintained stealth bombers and Predator unmanned drones used in Afghanistan and Iraq. Some military equipment is specifically designed to be operated and maintained by private companies.

In Britain, the debate over military privatization has been public, since the activities of the UK company Sandline in Sierra Leone and Papua New Guinea embarrassed the government in the late 1990s. But no country has clear policies to regulate PMCs, and the limited oversight that does exist rarely works. In the US, they have largely escaped notice, except when US contract workers in conflict zones are killed or go way over the line, as in the case of Blackwater.

According to Guy Copeland, who began developing public-private IT policy in the Reagan years, "The private sector must play an integral role in improving our national cybersecurity." After all, he has noted, private interests own and operate 85 percent of the nation's critical IT infrastructure. He should know. After all, Copeland drafted much of the language in the Bush Administration's 2002 National Strategy to Secure Cyberspace as co-chair of the Information Security Committee of the Information Technology Association of America.

Nevertheless, when the federal government becomes dependent on unaccountable, private companies like DynCorp and Blackwater (later renamed Xe Services) for so many key security services, as well as for military logistics, management, strategy, expertise and "training," fundamental elements of US defense have been outsourced. And the details of that relationship are matters that the intelligence community will fight long and hard to keep out of public view.

Corporate Connections and "Soft Landings"

Although the various departments and private contractors within the military-intelligence-industrial complex occasionally have turf battles and don't always share information or coordinate strategy as effectively as they might, close and ongoing contact has long been considered essential. And it has expanded as a result of the information revolution. The entire intelligence community has its own secret Intranet, which pulls together FBI reports, NSA intercepts, analysis from the DIA and CIA, and other deeply covert sources.

Private firms are connected to this information web through staff, location, shared technology, and assorted contracts. Working primarily for the Pentagon, for example, L-3 Communications, a spinoff from major defense contractor Lockheed Martin, has manufactured hardware like control systems for satellites and flight recorders. MPRI, which was bought by L-3, provided services like its operations in Macedonia. L-3 also built the NSA's Secure Terminal Equipment, which instantly encrypts phone conversations.

Another private contractor active in the Balkans was Science Applications, staffed by former NSA and CIA personnel, and specializing in police training. When Janice Stromsem, a Justice Department employee, complained that its program gave the CIA unfettered access to

recruiting agents in foreign police forces, she was relieved of her duties. Her concern was that the sovereignty of nations receiving aid from the US was being compromised.

In 1999, faced with personnel cuts, the NSA offered over 4000 employees “soft landing” buy outs to help them secure jobs with defense firms that have major NSA contracts. NSA offered to pay the first year’s salary, in hopes the contractor would then pick up the tab. Sometimes the employee didn’t even have to move away from Crypto City. Companies taking part in the program included TRW and MPRI’s parent company, Lockheed Martin.

Lockheed was also a winner in the long-term effort to privatize government services. In 2000, it won a $43.8 million contract to run the Defense Civilian Personnel Data System, one of the largest human resources systems in the world. As a result, a major defense contractor took charge of consolidating all Department of Defense personnel systems, covering hiring and firing for about 750,000 civilian employees. This put the contractor at the cutting edge of Defense Department planning, and made it a key gatekeeper at the revolving door between the US military and private interests.

Invisible Threats

Shortly after his appointment as NSA director in 1999, Michael Hayden went to see the film Enemy of the State, in which Will Smith is pursued by an all-seeing, all hearing NSA and former operative Gene Hackman decries the agency’s dangerous power. In Body of Secrets, author Bamford says Hayden found the film entertaining, yet offensive and highly inaccurate. Still, the NSA chief was comforted by “a society that makes its bogeymen secrecy and power. That’s really what the movie’s about.”

Unlike Hayden, most people don’t know where the fiction ends and NSA reality begins. Supposedly, the agency rarely “spies” on US citizens at home. On the other hand, the Foreign Intelligence Surveillance Act allows a secret federal court to waive that limitation. The rest of the world doesn’t have that protection. Designating thousands of keywords, names, phrases, and phone numbers, NSA computers can pick them out of millions of messages, passing anything of interest on to analysts. One can only speculate about what happens next.

After 9/11 the plan was to go further with a project code named Tempest. The goal was to capture computer signals such as keystrokes or monitor images through walls or from other buildings, even if the computers weren’t linked to a network. One NSA document, “Compromising Emanations Laboratory Test Requirements, Electromagnetics,” described procedures for capturing the radiation emitted from a computer-through radio waves and the telephone, serial, network, or power cables attached to it.

Other NSA programs have included Oasis, designed to reduce audiovisual images into machine-readable text for easier filtering, and Fluent, which expanded Echelon’s multilingual capabilities. And let’s not forget the government’s Carnivore Internet surveillance program, which can collect all communications over any segment of the network being watched.

Put such elements together, combine them with business imperatives and covert foreign policy objectives, then throw PMCS into the mix, and you get a glimpse of the extent to which information can be translated into raw power and secretly used to shape events. Although most pieces of the puzzle remain obscure, enough is visible to justify suspicion,

outrage, and a campaign to pull away the curtain on this Wizard of Oz. But fighting a force that is largely invisible and unaccountable – and able to eavesdrop on the most private exchanges, that is a daunting task, perhaps even more difficult than confronting the mechanisms of corporate globalization that it protects and promotes.

The original source of this article is Global Research
Copyright © Greg Guma, Global Research, 2013

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: **Greg Guma**

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca