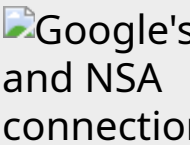
Google's deep CIA and NSA connections

by Eric Sommer



The Western media is currently full of articles reporting Google's denial that it cooperated in a government program to massively spy on American and foreign citizens by accessing data from Googles servers and those of other U.S. software companies.

The mainstream media has, however, almost completely failed to report that Google's denial, and its surface concern over 'human rights', is historically belied by its their deep involvement with some of the worst human rights abuses on the planet:

Google is, in fact, is a key participant in U.S. military and CIA intelligence operations involving torture; subversion of foreign governments; illegal wars of aggression; and military occupations of countries which have never attacked the U.S. and which have cost hundreds of thousands of lives in Afghanistan, Iraq, Pakistan, and elsewhere.

To begin with, as reported previously in the Washington Post and elsewhere, Google is the supplier of the customized core search technology for 'Intellipedia, a highly-secured online system

where 37,000 U.S. spies and related personnel share information and collaborate on their devious errands.

Agencies such as the so-called 'National Security Agency', or NSA, which is implicated in the current 'spying on Americans' scandal, have also purchased servers using Google-supplied search technology which processes information gathered by U.S. spies operating all over the planet.

In addition, Google is linked to the U.S. spy and military systems through its Google Earth software venture. The technology behind this software was originally developed by Keyhole Inc., a company funded by Q-Tel http://www.iqt.org/ , a venture capital firm which is in turn openly funded and operated on behalf of the CIA.

Google acquired Keyhole Inc. in 2004. The same base technology is currently employed by U.S. military and intelligence systems in their quest, in their own words, for "full-spectrum dominance" of the planet.

Moreover, Googles' connection with the CIA and its venture capital firm extends to sharing at least one key member of personnel. In 2004, the Director of Technology Assessment at In-Q-Tel, Rob Painter, moved from his old job directly serving the CIA to become 'Senior Federal Manager' at Google.

As Robert Steele, a former CIA case officer has put it: Google is "in bed with" the CIA.

Googles Friends spy on millions of Internet Users

Given Google's supposed concern with 'human rights' and with user-privacy, it's worth noting that Wired magazine reported some time ago that Google's friends at In-Q-Tel, the investment arm of the CIA, invested in Visible Technologies, a software firm specialized in 'monitoring social media'.

The 'Visible' technology can automatically examine more than a million discussions and posts on blogs, online forums, Flickr, YouTube, Twitter, Amazon, and so forth each day. The technology also 'scores' each online item, assigning it a positive, negative or mixed or neutral status, based on parameters and terms set by the technology operators. The information, thus boiled down, can then be more effectively scanned and read by human operators.

The CIA venture capitalists at In-Q-Tel previously said they will use the technology to monitor social media operating in other countries and give U.S. spies ¡°early-warning detection on how issues are playing internationally,¡± according to spokesperson

Donald Tighe. There is every possibility that the technology can also be used by the U.S. intellligence operatives to spy on domestic social movements and individuals inside the U.S.

Finally, Obama during his recent meeting with Chinese president Xi, again more-or-less accused China of cyber intrusions into U.S. government computers. There has, however, been a curious absence from the statements emanating from Google, from U.S. government sources, and from U.S. media reports of truely substantive evidence linking the Chinese government with the alledged break-in attempts. Words like 'sophisticated' and 'suspicion' have appeared in the media to suggest that the Chinese government is responsible for the break-ins. That may be so. But it is striking that the media has seemingly asked no tough questions as to what the evidence behind the 'suspicions' might be.

It should be noted that the U.S. government and its intelligence agencies have a long history of rogue operations intended to discredit governments or social movements with whom they happen to disagree. To see how far this can go, one need only recall the sordid history of disinformation, lies, and deceit used to frighten people into supporting the Iraq war.

Whether the past attacks on U.S. government systems, Google email, et al originated from the Chinese government, from the U.S. intelligence operatives, or from elsewhere, one thing is clear: A company that supplies the CIA with key intelligence technology; supplies mapping software which can be used for barbarous wars of aggression and drone attacks which kill huge numbers of innocent civilians; and which in general is deeply intertwined with the CIA and the U.S. military machines, which spy on millions, the company cannot be motivated by real

concern for the human rights and lives of the people in the U.S. and on the planet.

See more at http://www.pravdareport.com/opinion/columnists/17-06-2013/124841-google_cia_nsa-0/

Why Google Made the NSA

Inside the secret network behind mass surveillance, endless war, and Skynet

By Nafeez Ahmed

Read Part I

Mass surveillance is about control. It's promulgators may well claim, and even believe, that it is about control for the greater good, a control that is needed to keep a cap on disorder, to be fully vigilant to the next threat. But in a context of rampant political corruption, widening economic inequalities, and escalating resource stress due to climate change and energy volatility, mass surveillance can become a tool of power to merely perpetuate itself, at the public's expense.

A major function of mass surveillance that is often overlooked is that of knowing the adversary to such an extent that they can be manipulated into defeat. The problem is that the adversary is not just terrorists. It's you and me. To this day, the role of information warfare

as propaganda has been in full swing, though systematically ignored by much of the media.

Here, *INSURGE INTELLIGENCE* exposes how the Pentagon Highlands Forum's co-optation of tech giants like Google to pursue mass surveillance, has played a key role in secret efforts to manipulate the media as part of an information war against the American government, the American people, and the rest of the world: to justify endless war, and ceaseless military expansionism.

The war machine

In September 2013, the website of the Montery Institute for International Studies' Cyber Security Initiative (MIIS CySec) posted a final version of a paper on 'cyber-deterrence' by CIA consultant Jeffrey Cooper, vice president of the US defense contractor SAIC and a founding member of the Pentagon's Highlands Forum. The paper was presented to then NSA director Gen. Keith Alexander at a Highlands Forum session titled 'Cyber Commons, Engagement and Deterrence' in 2010.

MIIS CySec is formally partnered with the Pentagon's Highlands Forum through an MoU signed between the provost and Forum president Richard O'Neill, while the initiative itself is funded by George C. Lee: the Goldman Sachs executive who led the billion dollar valuations of Facebook, Google, eBay, and other tech companies.

Cooper's eye-opening paper is no longer available at the MIIS site, but a final version of it is available via the logs of a public national security conference hosted by the American Bar Association. Currently, Cooper is chief innovation officer at SAIC/Leidos, which is among a consortium of defense technology firms including Booz Allen Hamilton and others contracted to develop NSA surveillance capabilities.

The Highlands Forum briefing for the NSA chief was commissioned under contract by the undersecretary of defense for intelligence, and based on concepts developed at previous Forum meetings. It was presented to Gen. Alexander at a "closed session" of the Highlands Forum moderated by MIIS Cysec director, Dr. Itamara Lochard, at the Center for Strategic and International Studies (CSIS) in Washington DC.

Like Rumsfeld's IO roadmap, Cooper's NSA briefing described "digital information systems" as both a "great source of vulnerability" and "powerful tools and weapons" for "national security." He advocated the need for US cyber intelligence to maximize "in-depth knowledge" of potential and actual adversaries, so they can identify "every potential leverage point" that can be exploited for deterrence or retaliation. "Networked deterrence" requires the US intelligence community to develop "deep understanding and specific knowledge about the particular networks involved and their patterns of linkages, including types and strengths of bonds," as well as using cognitive

and behavioural science to help predict patterns. His paper went on to essentially set out a theoretical architecture for modelling data obtained from surveillance and social media mining on potential "adversaries" and "counterparties."

A year after this briefing with the NSA chief, Michele Weslander Quaid — another Highlands Forum delegate — joined Google to become chief technology officer, leaving her senior role in the Pentagon advising the undersecretary of defense for intelligence. Two months earlier, the Defense Science Board (DSB) *Task Force on Defense Intelligence* published its reporton *Counterinsurgency (COIN), Intelligence, Surveillance and Reconnaissance (IRS) Operations.* Quaid was among the government intelligence experts who advised and briefed the Defense Science Board Task Force in preparing the report. Another expert who briefed the Task Force was Highlands Forum veteran Linton Wells. The DSB report itself had been commissioned by Bush appointee James Clapper, then undersecretary of defense for intelligence — who had also commissioned Cooper's Highlands Forum briefing to Gen. Alexander. Clapper is now Obama's Director of National Intelligence, in which capacity he lied under oath to Congress by claiming in March 2013 that the NSA does not collect any data at all on American citizens.

Michele Quaid's track record across the US military intelligence community was to transition agencies into

using web tools and cloud technology. The imprint of her ideas are evident in key parts of the DSB Task Force report, which described its purpose as being to "influence investment decisions" at the Pentagon "by recommending appropriate intelligence capabilities to assess insurgencies, understand a population in their environment, and support COIN operations."

The report named 24 countries in South and Southeast Asia, North and West Africa, the Middle East and South America, which would pose "possible COIN challenges" for the US military in coming years. These included Pakistan, Mexico, Yemen, Nigeria, Guatemala, Gaza/West Bank, Egypt, Saudi Arabia, Lebanon, among other "autocratic regimes." The report argued that "economic crises, climate change, demographic pressures, resource scarcity, or poor governance could cause these states (or others) to fail or become so weak that they become targets for aggressors/insurgents." From there, the "global information infrastructure" and "social media" can rapidly "amplify the speed, intensity, and momentum of events" with regional implications. "Such areas could become sanctuaries from which to launch attacks on the US homeland, recruit personnel, and finance, train, and supply operations."

The imperative in this context is to increase the military's capacity for "left of bang" operations — before the need for a major armed forces commitment — to avoid insurgencies, or pre-empt them while still in incipient

phase. The report goes on to conclude that “the Internet and social media are critical sources of social network analysis data in societies that are not only literate, but also connected to the Internet.” This requires “monitoring the blogosphere and other social media across many different cultures and languages” to prepare for “population-centric operations.”

The Pentagon must also increase its capacity for “behavioral modeling and simulation” to “better understand and anticipate the actions of a population” based on “foundation data on populations, human networks, geography, and other economic and social characteristics.” Such “population-centric operations” will also “increasingly” be needed in “nascent resource conflicts, whether based on water-crises, agricultural stress, environmental stress, or rents” from mineral resources. This must include monitoring “population demographics as an organic part of the natural resource framework.”

Other areas for augmentation are “overhead video surveillance,” “high resolution terrain data,” “cloud computing capability,” “data fusion” for all forms of intelligence in a “consistent spatio-temporal framework for organizing and indexing the data,” developing “social science frameworks” that can “support spatio-temporal encoding and analysis,” “distributing multi-form biometric authentication technologies [“such as fingerprints, retina scans and DNA samples”] to the point of service of the

most basic administrative processes" in order to "tie identity to all an individual's transactions." In addition, the academy must be brought in to help the Pentagon develop "anthropological, socio-cultural, historical, human geographical, educational, public health, and many other types of social and behavioral science data and information" to develop "a deep understanding of populations."

A few months after joining Google, Quaid represented the company in August 2011 at the Pentagon's Defense Information Systems Agency (DISA) Customer and Industry Forum. The forum would provide "the Services, Combatant Commands, Agencies, coalition forces" the "opportunity to directly engage with industry on innovative technologies to enable and ensure capabilities in support of our Warfighters." Participants in the event have been integral to efforts to create a "defense enterprise information environment," defined as "an integrated platform which includes the network, computing, environment, services, information assurance, and NetOps capabilities," enabling warfighters to "connect, identify themselves, discover and share information, and collaborate across the full spectrum of military operations." Most of the forum panelists were DoD officials, except for just four industry panelists including Google's Quaid.

DISA officials have attended the Highlands Forum, too — such as Paul Friedrichs, a technical director and chief

engineer of DISA's Office of the Chief Information Assurance Executive.

Knowledge is Power

Given all this it is hardly surprising that in 2012, a few months after Highlands Forum co-chair Regina Dugan left DARPA to join Google as a senior executive, then NSA chief Gen. Keith Alexander was emailing Google's founding executive Sergey Brin to discuss information sharing for national security. In those emails, obtained under Freedom of Information by investigative journalist Jason Leopold, Gen. Alexander described Google as a "key member of [the US military's] Defense Industrial Base," a position Michele Quaid was apparently consolidating. Brin's jovial relationship with the former NSA chief now makes perfect sense given that Brin had been in contact with representatives of the CIA and NSA, who partly funded and oversaw his creation of the Google search engine, since the mid-1990s.

In July 2014, Quaid spoke at a US Army panel on the creation of a "rapid acquisition cell" to advance the US Army's "cyber capabilities" as part of the Force 2025 transformation initiative. She told Pentagon officials that "many of the Army's 2025 technology goals can be realized with commercial technology available or in development today," re-affirming that "industry is ready to partner with the Army in supporting the new paradigm." Around the same time, most of the media was trumpeting the idea that Google was trying

to distance itself from Pentagon funding, but in reality, Google has switched tactics to independently develop commercial technologies which would have military applications the Pentagon's transformation goals.

Yet Quaid is hardly the only point-person in Google's relationship with the US military intelligence community.

One year after Google bought the satellite mapping software Keyhole from CIA venture capital firm In-Q-Tel in 2004, In-Q-Tel's director of technical assessment Rob Painter — who played a key role in In-Q-Tel's Keyhole investment in the first place — moved to Google. At In-Q-Tel, Painter's work focused on identifying, researching and evaluating "new start-up technology firms that were believed to offer tremendous value to the CIA, the National Geospatial-Intelligence Agency, and the Defense Intelligence Agency." Indeed, the NGA had confirmed that its intelligence obtained via Keyhole was used by the NSA to support US operations in Iraq from 2003 onwards.

A former US Army special operations intelligence officer, Painter's new job at Google as of July 2005 was federal manager of what Keyhole was to become: Google Earth Enterprise. By 2007, Painter had become Google's federal chief technologist.

That year, Painter told the *Washington Post* that Google was "in the beginning stages" of selling advanced secret versions of its products to the US government. "Google has ramped up its sales force in the Washington area in

the past year to adapt its technology products to the needs of the military, civilian agencies and the intelligence community," the *Post* reported. The Pentagon was already using a version of Google Earth developed in partnership with Lockheed Martin to "display information for the military on the ground in Iraq," including "mapping out displays of key regions of the country" and outlining "Sunni and Shiite neighborhoods in Baghdad, as well as US and Iraqi military bases in the city. Neither Lockheed nor Google would say how the geospatial agency uses the data." Google aimed to sell the government new "enhanced versions of Google Earth" and "search engines that can be used internally by agencies."

White House records leaked in 2010 showed that Google executives had held several meetings with senior US National Security Council officials. Alan Davidson, Google's government affairs director, had at least three meetings with officials of the National Security Council in 2009, including White House senior director for Russian affairs Mike McFaul and Middle East advisor Daniel Shapiro. It also emerged from a Google patent application that the company had deliberately been collecting 'payload' data from private wifi networks that would enable the identification of "geolocations." In the same year, we now know, Google had signed an agreement with the NSA giving the agency open-ended access to the personal information of its users, and its hardware and software, in the name of cyber security — agreements

that Gen. Alexander was busy replicating with hundreds of telecoms CEOs around the country.

Thus, it is not just Google that is a key contributor and foundation of the US military-industrial complex: it is the entire Internet, and the wide range of private sector companies — many nurtured and funded under the mantle of the US intelligence community (or powerful financiers embedded in that community) — which sustain the Internet and the telecoms infrastructure; it is also the myriad of start-ups selling cutting edge technologies to the CIA's venture firm In-Q-Tel, where they can then be adapted and advanced for applications across the military intelligence community. Ultimately, the global surveillance apparatus and the classified tools used by agencies like the NSA to administer it, have been almost entirely made by external researchers and private contractors like Google, which operate outside the Pentagon.

This structure, mirrored in the workings of the Pentagon's Highlands Forum, allows the Pentagon to rapidly capitalize on technological innovations it would otherwise miss, while also keeping the private sector at arms length, at least ostensibly, to avoid uncomfortable questions about what such technology is actually being used for.

But isn't it obvious, really? The Pentagon is about war, whether overt or covert. By helping build the technological surveillance infrastructure of the NSA, firms like Google are complicit in what the military-industrial complex does best: kill for cash.

As the nature of mass surveillance suggests, its target is not merely terrorists, but by extension, 'terrorism suspects' and 'potential terrorists,' the upshot being that entire populations — especially political activists — must be targeted by US intelligence surveillance to identify active and future threats, and to be vigilant against hypothetical populist insurgencies both at home and abroad. Predictive analytics and behavioural profiles play a pivotal role here.

Mass surveillance and data-mining also now has a distinctive operational purpose in assisting with the lethal execution of special operations, selecting targets for the CIA's drone strike kill lists via dubious algorithms, for instance, along with providing geospatial and other information for combatant commanders on land, air and sea, among many other functions. A single social media post on Twitter or Facebook is enough to trigger being placed on secret terrorism watch-lists solely due to a vaguely defined hunch or suspicion; and can potentially even land a suspect on a kill list.

The push for indiscriminate, comprehensive mass surveillance by the military-industrial complex — encompassing the Pentagon, intelligence agencies, defense contractors, and supposedly friendly tech giants like Google and Facebook — is therefore not an end in itself, but an instrument of power, whose goal is self-perpetuation. But there is also a self-rationalizing justification for this goal: while being great for the

military-industrial complex, it is also, supposedly, great for everyone else.