LOCK DOWN ON PRISON PLANET ALMOST COMPLETE
HOW THE US MILITARY CONTROL OF SOCIAL MEDIA HAS ALREADY IMPRISONED YOU AND THROWN AWAY THE KEY
Long before we could imagine the evil of the elite pedophile globalists of the world, they had already started locking down planet earth. They knew that humanity’s wakening consciousness would jeopardize their planetary reign so they had to find a way to imprison our minds, direct our thinking, and limit our expanding consciousness.

They did it right under our noses.

They did it with our own hard-earned money.

While we were busy rearing our children and tending our families, they were quietly implementing Alinsky’s rules and Soros’ regimes. They are evil people who prey on our children, profit from our blood, rape our women and countries, and control us with their money illusions. They don’t care about our national borders, cultural uniqueness, spiritual paths, or personal liberty. YOU are THEIRS to be “farmed” any way that brings them greater wealth, longer life, and wicked pleasures.

You have now awakened and realized that the nightmare is actually on the other side of your dreamy sleep. What do you do? First and foremost is to educate yourself on what has occurred since you stopped paying attention. The American Intelligence Media has been writing Citizens Intelligence Reports for several years now so that you can become highly informed patriots. Patriots need to know precisely who the enemy is, how they have weaponized the world, and what we can do to throw off our digital shackles.

The global elites know that education is the key to enlightenment. For this reason, you will find more and more outlets for self-education becoming censored and shut down by the planetary rulers. They simply can’t have us know what is going on as there are far too many of us and too few of them.

In this Citizens Intelligence Report we want to alert you to the grave dangers of the weaponization of the internet and social media. A new technological revolution is taking place that will affect all of us. They make it sound so cool and fun – the Internet of Things—but it is nothing more than a self-imposed prison that will eventually control you 24/7 once you connect into the network.
The more you participate in the automatic information fed directly to your devices that is personalizing your news, entertainment, business, and “life-patterns”, the more you will think you are free and fully informed. Actually, you will become more and more limited by what your pattern-of-life generates as your individualized algorithms. A mechanical virtual world will be created around you that becomes your personalized digital prison that, at first, may seem like digital heaven, but later rears its ugly head of control and enslavement. By then, it will be too late for any of us to break free.

Your new digital prison is being created every time you do an internet search, click a ‘like’ button on Facebook, type a phrase into your computer, choose something to watch on television, or speak a word into your phone. Every speck of “information” that you participate in is used to make your personalized digital life-pattern profile.

Even your bank account and everything you spend is being gathered in an NSA program called Marina [1] that knows so much about you that when you get into your car on a day you have a weekly appointment, your phone automatically pings the route and distance to your destination.

Your phone can also activate all your devices that are connected to the Internet of Things. As you approach your house with your phone, your garage door opens automatically as the lights in the house come on and the house alarm is turned off while your coffee maker starts and your TV comes on with your usual show as the heating pad in your easy chair turns on to your favorite setting.

There is no end to the “machine intelligence” support you can get from mechanically augmented reality. Now Facebook and its fake, phony, stooge inventor Mark Zuckerberg wants you to put on a 3-D visor and enter a self-created virtual reality world where it feels you are free to do as you please.

**HOW DID WE GET INTO DIGITAL PRISON?**

We have created this world by being lazy and not asking the hard questions—who owns and controls this technology, what is the ultimate goal of the Internet of Things, does this
technology serve or enslave humanity? Eric Schmidt, the CEO of Alphabet has bragged about this new system that claims it is ‘ready to go’.

Google, somehow, morphed into a "mother company" that is named **Alphabet which owns all 26 subsidiaries of Google**, including the only AI on the planet called **Google Deep Mind**. Alphabet seems to have unlimited money and unlimited technology patents that are supported wholesale by Wall Street and the U.S. military-industrial complex.

Essentially, Google has always been owned and operated by the dark side of our military-industrial complex. Like Cisco Systems, Inc. before them, Google (Alphabet) was incubated through the U.S. Defense Advance Research Project Agency (DARPA) and the CIA’s private corporate venture capital company called In-Q-Tel. (Ask yourself how it is that a government entity can hold private companies and enjoy private profits outside of Congressional oversight, but we digress.)

Google, Cisco, Facebook, Twitter, and most other search engines and social networks all run on allegedly “open source” code given out by DARPA/In-Q-Tel to universities and corporations to develop. Open source means free to the user without the need to pay royalties or fees to the inventor or creator. Basically, whoever is able to take this weaponized open source code (with encryption back door keys already built in) and develop it for the consumer wins the military contracts.

Then Wall Street (Goldman Sachs and JPMorgan Chase usually) sweeps in with venture capital, and in short time values the new tech company in the tens and hundreds of billions. After that, the banks loan whatever money these companies need to buy out all their competition. These newly acquired “Silicon Valley corporate stooges” then become front-men for even more weaponized military systems. This now includes Facebook, LinkedIn, Instagram, Pinterest, YouTube, Tumblr and Amazon.

Whether you know it or not, what is described above is already happening on a commercial level and soon will escalate to an overt military level while the innocent internet user is lulled into believing that he is simply having fun. Since most American and global businesses have some component on the internet, the militarization of the internet can be as powerful as the threat of global nuclear annihilation. Just imagine if the internet was turned off tomorrow – permanently, never to return.
Most of what we think of as modern life would end, and many people would never recover. Economies would collapse, wars would rage, and many of us wouldn’t know what to do or what to think. Modern life would collapse because the weapon of the internet already controls modern life. The life of the pygmy in Indonesia would go on uninterrupted, but American life would screech to a halt. We might not be able to “reboot” for years. This thought begs the question, “How did we let this happen?”

“We”, the users of the Internet and all things digital, were happy to use the new technology without asking basic questions like: Who actually owns the cables the Internet travels through? Can “they” turn it off? Why was so much power given over to the internet? At this point, is there an alternative or way out of this digital problem. But first we must see the internet and all of its “wonders” for exactly what they are – weapons of mass social manipulation. When we can see the evil plans of those who have advanced this technology without the moral compass necessary to guide such powerful tools, then perhaps we can change these innovations from weapons into the information tools that they were intended to be. Information was supposed to free humanity, not imprison it in a virtual world where education is replaced by nonsensical entertainment, religion is replaced by consumerism, and the real world by virtual reality.

PATENT THEFT AND WEAPONIZATION OF THE INTERNET

Not counting the social networking technology that was stolen, taxpayers of the United States, through the CIA’s private venture capital company In-Q-tel, largely funded the open source program that became Facebook, Google, Intel, Apple, and Microsoft. These companies have weaponized these devices and systems against the citizens of the world.

‘WE THE PEOPLE’ DEMAND THAT THESE COMPANIES, AND ANY OTHER LIKE THEM THAT HAVE BEEN FINANCIALLY SEEDED AND FUNDED BY U.S. TAXPAYERS, BE GIVEN TO THE PEOPLE AS A PUBLIC UTILITY AND THAT THE
FICTITIOUS OWNERS OF THESE COMPANIES BE PROSECUTED FOR PATENT INFRINGEMENT AND/OR THEFT.

In numerous articles from *Americans for Innovation*, the Anonymous Patriots have found unequivocal evidence that IBM’s Eclipse Foundation stole the original ideas and source code for Google and Facebook from Columbus, Ohio innovator Leader Technologies, Inc. through their *patent attorney James P. Chandler III. Chandler was mentor of Barack Obama, Eric Holder, Robert Mueller, James Comey and John Podesta, to name but a few.*

Chandler represented Leader Technologies, Inc. from the moment Leader realized their innovations were patentable in early 2000. But rather than file the patents immediately, Chandler suspiciously advised Leader to “reduce to practice” the invention before he would file them.

Hindsight shows that Chandler gave that advice in order to steal the actual source code when it was ready. Chandler bamboozled Leader into taking custody of a copy of the source code in 2002 which he immediately gave to the IBM Eclipse Foundation which then disseminated it to Zuckerberg/Facebook and other companies.

*David J. Kappos*, IBM’s attorney (who also served later as Obama’s Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office from 2009 to 2013) was also a student of Chandler at the time of the theft. This theft is one of if not the largest theft of intellectual property and trade secrets in history. It was clearly part of the weaponization of these digital platforms.

For more information, please see our Citizens Intelligence Reports on these subjects:
HOW DOES PATENT THEFT WORK?

Digital Prison Mechanisms

Once the Silicon Valley high-tech “dummy” companies are established by stooges who are pre-selected for their willingness to incorporate military “back doors” into all of their products, the NSA/CIA/FBI uses the information gleaned from those companies to surveil every American through every devise that broadcasts a signal – phone, computer, or any devise on the Internet of Things. Any intelligence agency can simply type in a query and access the metadata collected from every digital devise on the internet or that uses Wi-Fi or cell phone towers.
Among these spying tools is the RIOT (Rapid Information Overlay Technology) program by Raytheon which leaked to the public on Nov. 16, 2010.[2]

This information is used to target individuals for consumer behaviors as well as DoD intelligence collection. If an internet user is targeted, there are hundreds of ways to “attack” the user and manipulate his/her buying habits, personal life-pattern choices, and even the way the user thinks.

THE OBJECT OF THE INTELLIGENCE IS SIMPLE: **CONTROL THE USER. SOCIAL NETWORKS ON THE INTERNET ARE MILITARY EXPERIMENTS IN SOCIAL MANIPULATION. THIS IS WHAT IS CALLED PSYOPS – OR PSYCHOLOGICAL OPERATIONS.**

Another program used to gather the Internet metadata is **XKeyscore**, a secret computer system first used by the NSA for searching and analyzing global Internet data, which it collects on a daily basis. It enables almost unlimited surveillance of anyone anywhere in the world.

The NSA’s databank of collected communications allows its analysts to listen to the calls or read the emails of everything that the NSA has stored. It can also access your browsing histories or Google search terms that you’ve entered, and can alert them to any further activity that people connected to that email address or that IP address do in the future. XKeyscore consists of over 700 servers at approximately 150 sites where the NSA collects ALL data, on EVERYBODY, ALL THE TIME. [3]

Another component of NSA data collection is a program called Marina, a database and analysis tool set for intercepted internet metadata. The database stores metadata up to a year. The Marina metadata application tracks a user’s browser experience, gathers contact information/content and develops summaries of the target. It also has the capability to look back on the last 365 days’ worth of metadata seen by the collection system, whether or not the target was tasked for collection. The stored metadata is mainly used for pattern-of-life analysis.
AMERICANS ARE NOT EXEMPT BECAUSE METADATA IS NOT CONSIDERED DATA BY U.S. LAW. (SEE SECTION 702 OF THE FISA AMENDMENTS ACT).

Once the data is collected and can be queried and targeted, the data is then stored in an NSA program called Sentient World Simulation (SWS). This program is developing a parallel to Planet Earth, with billions of individual nodes (prisons) to reflect every man, woman, and child.

SWS will be a synthetic mirror of the real world with automated continuous calibration with respect to current real-world information. It provides an environment for testing psychological operations so that military leaders can develop and test multiple courses of action to anticipate and shape behaviors of adversaries, neutrals, and partners, including U.S. citizens. SWS also mimics financial institutions, utilities, media outlets, and street corner shops. By applying theories of economics and human psychology, its developers can predict how individuals and mobs will respond to various stressors.

These four programs — XKeyscore, Marina, RIOT, and Sentient World Simulation — create some of the environments which intend to imprison and control those who willingly enter into the digital virtual reality of the internet. The internet is a WARZONE according to the people who created and weaponized it. Notice that the description of SWS says that even “neutrals” are the target of these systems.

No one is safe from the surveillance, monitoring, targeting, and attacks of Facebook, Twitter, Google and Alphabet. Just look how President Donald Trump uses Twitter as a weapon against the corporate media. There is a battle for information and every person is in the middle of the battle whether they like it or not.

The largest domestic military exercises in US history happened in 2015. They were entitled: “Jade Helm 2015 — Master the Human Domain.” Just the very name of the exercise should show you where the U.S. military is focusing its time and energy — on U.S. citizens. It also clearly tells us the intent of the U.S. military is — to Master the Human Domain. So much for America freedom and liberty.

SOME HISTORY ABOUT DARPA/IN-Q-TEL “FRONT MEN”
The Defense Advanced Research Projects Agency (DARPA) has controlled technological innovation since 1958 when it was created by the military-driven Department of Defense. DARPA is the father of war-fighting, both conventional and digital. DARPA was controlled by a man they called “Yoda”, who leads a group called the Highlands Forum that directs all military research and development – the weaponization of every U.S. patent, over 4,000 of which have been stolen.

DARPA’s history is littered with death and destruction. DARPA and In-Q-Tel, through the Highlands Forum, have driven research and development for the military that has cost American taxpayers trillions. This same technology is also shared with countries throughout the world through open source sharing.

The U. S. military wants our enemies to have the technology so that it can spy upon them and keep up with them in weaponry. If both sides have the same technology and weapons, then more money needs to be spent on bigger and better weapons continually and the military industrial complex thrives and gets richer.

**THEIR BUSINESS PLAN IS SIMPLE:** MAKE SURE THE CUSTOMER HAS A NEED FOR MILITARY PRODUCTS AND SERVICES BY SUPPLYING THEIR ENEMIES WITH COMPETING PRODUCTS AND SERVICES, A BUSINESS CYCLE THAT NEVER STOPS AND GUARANTEES THAT THE MILITARY INDUSTRIAL COMPLEX WILL ALWAYS BE SELLING SOMETHING TO SOMEONE.

**History of In-Q-Tel – a CIA Venture Capital Investment Firm**

In 1999, the CIA created its own venture capital investment firm, In-Q-Tel, to fund promising start-ups that might create technologies useful for intelligence agencies. The inspiration for In-Q-Tel came earlier, when the Pentagon set up its own private sector
outfit. Known as the ‘Highlands Forum,’ this private network has operated as a bridge between the Pentagon and powerful American elites outside the military since the mid-1990s. Despite changes in civilian administrations, the unregulated and unconstitutional private military-industry network around the Highlands Forum has become increasingly successful in dominating U.S. defense policy.

Basically, the CIA needed to launder all of its stolen gold and set up many companies to wash its illegal money. Why do you think they call the CIA ‘The Company’?

In-Q-Tel also uses a company called SAIC, the U.S. defense firm Science Applications International Corporation, which changed its name to Leidos in 2013, now operating SAIC as a subsidiary. SAIC/Leidos is among the top 100 largest defense contractors in the U.S, and works closely with the U.S. intelligence community, especially the NSA. The agency is the company’s largest single customer and SAIC is the NSA’s largest contractor.

The Highlands Forum (Group)

Since 1973, Andrew Marshall has headed up one of the Pentagon’s most powerful agencies, the Office of Net Assessment (ONA), the U.S. defense secretary’s internal ‘think tank’ which conducts highly classified research on future planning for defense policy across the U.S. military and intelligence community. Out of Marshall’s work in the ONA came an independent group called the Highlands Forum.

Marshall, now 93 years old, is the DoD’s most elusive but one of its most influential officials. He created the Highlands Forum as a secret think tank for warfare innovation. All meetings are invitation-only, not open to the public, and no written records are kept, except for the snippets that participants reveal in their braggadocio and biographies, which are considerable.
Marshall created this type of secret platform so that no one could prove the Highland Forum exists or that it has the greatest power over high-tech warfare on the planet. Vice President Dick Cheney, Defense Secretary Donald Rumsfeld, and Deputy Secretary Paul Wolfowitz, who are widely considered the hawks of the neoconservative movement in American politics, were among Marshall’s star protégés.

The Highlands Forum’s influence on U.S. defense policy has operated through three main channels: its sponsorship by the Office of the Secretary of Defense; its direct link to Marshall’s ONA; and its direct link to DARPA/In-Q-Tel and the Highlands Forum.

The Highlands Forum has served as a two-way ‘influence bridge’: on the one hand, for the shadow network of private contractors to influence the formulation of information operations policy across U.S. military intelligence; and on the other, for the Pentagon to influence what is going on in the private sector.

There is no clearer evidence of this than the instrumental role of the Forum in incubating the idea of mass surveillance as a mechanism to dominate information on a global scale.

Around 1994, the Highlands Group was chaired by Richard O’Neill as an official Pentagon project at the appointment of Bill Clinton’s then defense secretary William Perry.
O’Neill’s own words, the group would function as the Pentagon’s ‘ideas lab.’

Total participants in the DoD’s Highlands Forum number over a thousand; although meetings and sessions largely consist of small closed workshop style gatherings of maximum 25–30 people, bringing together experts and officials depending on the subject.

The Forum has inside access to the chiefs of the main U.S. surveillance and reconnaissance agencies, as well as the directors and their assistants at DoD research agencies, from DARPA to the ONA, and is deeply plugged into the Pentagon’s policy research task forces. **In 2001, under the Total Information Awareness Program, President Bush secretly authorized the NSA’s domestic surveillance of Americans without court-approved warrants.**

From then on, Highlands Forum partner SAIC played a key role in the NSA roll out from inception. SAIC was then among a consortium receiving a $280 million contract to develop one of the NSA’s secret eavesdropping systems.

This was also the year that the Bush administration drew up its **Information Operations Roadmap.** Describing the internet as a “vulnerable weapons system,” Donald Rumsfeld’s IO roadmap had advocated that Pentagon strategy “should be based on the premise that the Department of Defense will ‘fight the net’ as it would an enemy weapons system.” The U.S. should seek “maximum control” of the “full spectrum of globally emerging communications systems, sensors, and weapons systems,” advocated the document.

As of 2006, SAIC had been awarded a multi-million dollar NSA contract to develop a big data-mining project called **ExecuteLocus,** despite the colossal $1 billion failure of its preceding contract, known as **Trailblazer.** Core components of **Total Information Awareness** were being quietly continued under new code names. The new surveillance program was then fully transitioned from DARPA’s jurisdiction to the NSA.
O’Neill said his job as Forum chairman was to scope case studies from real companies across the private sector, such as eBay and Human Genome Sciences, to figure out the basis of U.S. Information Superiority—how to dominate the information market—and leverage this for what the president and the secretary of defense wanted to do with regard to transformation of the Department of Defense.

Every project of DARPA and In-Q-Tel have been weaponized before they are shared with the companies who then are the “front” for a DARPA sponsored company. DARPA and In-Q-Tel keep the encryption codes and build in backdoor keys so that they can always control the military weapons that have been released into the corporate world for public use. According to DARPA and In-Q-Tel, innovation and technological advances must first be a weapon that can be controlled by its makers – the military.

The Highland Forum directed the creation of weapons of every sort that have been released into the corporate world and now control your laptop, phone, computer, and every other device with a “bugged” microprocessor inside. Intel microprocessors are found in most of our “private” digital devices and are, in fact, collecting “intelligence” for the Department of Defense, CIA, and NSA.

FOR MORE INFORMATION ON THIS TOPIC, SEE OUR CITIZENS INTELLIGENCE REPORT ENTITLED WHO REALLY OWNS THE MILITARY INDUSTRIAL COMPLEX: THE HIGHLANDS FORUM EXPOSED.

DARPA/In-Q-Tel and the Highlands Forum drive the process of continuous war from creating the devices that control all nuclear weapons to incubating the technologies that created the Internet, Intel microprocessors, Cisco routers, Google search engines,
Facebook social networks, the IBM Internet of Things, cellphones, Microsoft software, MacAfee security software, and all other commercial and military warfare devices using their source code.

The Highlands Forum has been the headquarters of weaponizing military patents, intellectual property and trade secrets for five decades. Andrew Marshall has the blood of millions on his hands, yet he is considered an America hero instead of a warlord criminal.

**INTEL (IN-Q-TEL) INSIDE**

Inside every Intel microprocessor is a smaller processor that lets Intel — who works for the Department of Defense — control every aspect of your computer remotely no matter what encryption codes or firewalls you use. All Intel microprocessor chips have a built-in backdoor that allows complete remote access to a PC through a second physical processor embedded within the main processor which has its own operating system embedded on the chip.

It is advertised as something that will allow IT professionals to remotely troubleshoot a PC. According to WikiLeaks, there is even secret diskless memory embedded on each chip that spies can use to store and retrieve data and instructions on each chip that is inaccessible to the user and supposedly only used for internal operations and maintenance. Intel’s latest x86 chips contain a secret backdoor with an embedded subsystem called the Management Engine (ME) that functions as a separate CPU and cannot be disabled, and the code is proprietary.

Even an encrypted hard drive can be monitored and controlled by the “processor within the processor” that already has your encryption key. There is more than just the NSA monitoring your calls, emails, and transmissions — there is Intel “Inside” your computer. Intel collects “intelligence” but it also provides a “back door” to control, or “turn off” your computer at will just like it has been demonstrated that Cisco routers have a “back door” open to the NSA. A backdoor is a method of bypassing normal authentication in a cryptosystem used for securing unauthorized remote access to a computer.
Samsung calls the on/off feature “Fake Off” meaning the TV looks like it is off, but is merely pretending to be off.

“I DON’T HAVE ANYTHING TO HIDE”

But why shouldn’t DARPA, through Intel, have open access to all your files and your computer? DARPA funded all the original development of microprocessors. **Intel is a front for DARPA and the military efforts to create, control, and weaponize all digital platforms through cyber-warfare.**

Just as the Internet was originally named after its founding group, DARPA, ARPARNET, microprocessors also were military creations that were permitted into the public marketplace only after the Department of Defense, and the CIA through In-Q-Tel, installed backdoors to control these powerful digital platforms of cyber warfighting.

Most semiconductor chips are made in Singapore, Taiwan, China, or Europe, but Intel designs and manufactures all their own chips in their own fabrication plants in America.

IN-Q-TEL IS WARFARE TECHNOLOGY – WEAPONIZED VENTURE CAPITAL & BANKING

Since Bill Clinton in 1999, In-Q-Tel funds promising start-ups that might create technologies useful for intelligence agencies just as the Department of Defense had
years earlier created DARPA. Both groups are controlled by the Highlands Forum. The Highlands Forum provides the ideas and funding for the scientific weaponization of new inventions through cooperation between the military and corporate contractors. Its biggest successes recently have been led by the CIA’s In-Q-Tel in the development of high-tech network-based cyber-warfare.

**The Highland Forum, DARPA, and In-Q-Tel are a secret multi-national high-tech think tank for inventing and controlling innovations that can be turned into weapons. In-Q-Tel is a bottomless source of funding for the CIA provided without any Congressional oversight.**

Military and information technology experts gather at the Highlands Forum meetings to consider the impacts of the globalization of IT on U. S. interests and warfare. The Forum developed the idea of “network-centric warfare” which is now a top concern of the military and the corporations that serve it.

Since 1999, there efforts have been supplemented by other quasi-secret organizations including The IBM Eclipse Foundation and the National Infrastructure Advisory Council.

---

**FOR MORE INFORMATION ON THIS TOPIC, SEE OUR CITIZENS INTELLIGENCE REPORT ENTITLED DARPA VADER AND THE EVIL INTEL EMPIRE INSIDE UNCOVERING THE DOD SITH LORDS THAT CONTROL YOUR LAPTOP**

**CISCO SYSTEMS MONOPOLY**

Once the ARPANET proved to be effective, routers were created that could handle exchanges between systems and computers. In 1998, virtually every internet exchange went through a Cisco router. In 2010, a researcher at IBM publicly revealed a flaw in a Cisco operating system that allowed a hacker to use a backdoor that was supposed to be available only to law enforcement agencies.

The intruder could hi-jack the Cisco device and use it to spy on all communications passing through it, including the content of e-mails, leaving products vulnerable to attack, particularly ubiquitous software programs like those produced by Microsoft. This
backdoor put millions of customers and their private information at risk and jeopardized
the security of electrical power facilities, public utilities, and transportation systems.

**Publicly, Cisco blamed the government for not telling them about this vulnerability, but
that was simply the pot calling the kettle black – the government was blaming itself
for the vulnerability, thus manipulating public opinion with a boldfaced deception.**

Cisco has been accused of remotely monitoring users’ connections through Cisco’s
Linksys E2700, E3500, E4500 devices. They have been reported to be remotely updated
to a firmware version that forces users to register for a cloud service which allows Cisco
to monitor their network use and ultimately shut down the cloud service account and
render the affected router unusable.

Cisco has also been accused of building a firewall backdoor developed by NSA into its
routers. The **Tailored Access Operations** (TAO) unit and other NSA employees intercept
servers, routers and other network gear being shipped to organizations targeted for
surveillance and install covert firmware onto them before they’re delivered. These Trojan
horse systems were described by an NSA manager as being “some of the most
productive operations in TAO because they pre-position access points into hard target
networks around the world.”

In fact, hiding in plain sight, Cisco registers the Dual_EC_DRBG NSA encryption back door
key with NIST (National Institute of Standards and Technology on all products for
export.) This key relies on an inbuilt flaw in the encryption standard which only the NSA
knows and can exploit at will to break in to any hardware, software or firmware.

**DARPA’S GOOGLE**

The U.S. intelligence community funded, nurtured and incubated Google as a military
weapon to control information. Seed-funded by the NSA (DARPA) and CIA (In-Q-Tel &
SAIC), Google was one among a group of private sector start-ups co-opted by U.S.
intelligence to control information warfare.

In 1994 two PhD students at Stanford University, Sergey Brin and Larry Page, made their
breakthrough on the first automated web crawling and page ranking application built
upon the source code given to them by DARPA/In-Q-Tel. That application remains the core component of what eventually became Google’s search service. Brin and Page had performed their work with funding from the Digital Library Initiative (DLI), a multi-agency program of the National Science Foundation (NSF), NASA and DARPA.

The NSA wanted to control and monitor digital information, particularly the data flowing over the internet. With its millions of customers around the world, Google is effectively a directory of people using the Internet. It has users’ e-mail addresses and knows where they are physically located, and what they are searching for on the web. Google has a “profile” on every user.

The government can “command” that any company, including Google, to turn over that information, and it does so as part of the NSA’s Prism program, which Google had been participating in for years by the time it signed the cooperative agreement with the NSA.

**Under Google’s terms of service, the company advises its users that it may share its “personal information” with outside organizations, including government agencies, in order to “detect, prevent, or otherwise address fraud, security or technical issues” and to “protect against harm to the rights, property or safety of Google.”**

**Google’s terms of service go further, they actually assume control of all user information with clever sleight of legal hand:** “When you upload, submit, store, send or receive content to or through our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content.”

The NSA partnered with Google, just one of hundreds of companies who have been brought into the NSA’s circle of secrecy. Starting in 2008, the agency began offering executives temporary security clearances, some good for only one day, so they could sit in on classified threat briefings. Several classified programs allow companies to share the designs of their products with the agency so it can inspect them for flaws and, in some instances, install backdoors or other forms of privileged access.
The NSA helps the companies find weaknesses in their products. But it also pays the companies not to fix some of them. Those weaknesses give the agency an entry point for spying or attacking foreign governments that install the products in their intelligence agencies, their militaries, and their critical infrastructure.

Essentially, the United States intelligence community funded, nurtured and incubated Google as part of a drive to dominate the world through control of information. Seed-funded by the NSA and CIA, Google was merely the first among a plethora of private sector start-ups co-opted by U.S. intelligence to retain ‘information superiority.’

The origins of this strategy trace back to Bill Clinton and the Highlands Forum which has functioned as a bridge between the U.S. government and elites across the business, industry, finance, corporate, and media sectors. The group has allowed some of the most powerful special interests in corporate America to systematically circumvent democratic accountability and the rule of law to influence government policies, as well as public opinion in the U.S. and around the world. The results have been catastrophic: mass surveillance and perception management amidst a permanent state of global war.

The U.S. intelligence community is implicated in nurturing today’s web platforms for the precise purpose of utilizing the technology as a mechanism to fight the global ‘information war’ - a war to legitimize the power of the few over the many. In reality, Google is a smokescreen behind which lurks the U.S. military-industrial complex.

**NSA’S MICROSOFT**

Microsoft shares zero day vulnerabilities in its products with the NSA before releasing a public alert or a software patch. McAfee, the Internet security company owned by Intel, provides the NSA, the CIA, and the FBI with network traffic flows, analysis of malware, and information about hacking trends.

Companies that promise to disclose holes in their products only to the spy agencies are paid for their silence. To an extent, these openings for government surveillance are required by law. Telecommunications companies in particular must build their equipment in such a way that it can be tapped by a law enforcement agency presenting a court order.
WHAT WE HAVE LEARNED SO FAR

- Microprocessors, the Internet, Cisco Systems, Google, and Intel were all DARPA/In-Q-Tel projects that flourished with new technologies created and funded by the military for cyberwarfare.

- **Most high-tech moguls are simply “front men”** selling DARPA and In-Q-Tel (the CIA’s DARPA) products that control our lives and spy on us continually.

- Intel processors have a backdoor built into the microprocessor that allows complete monitoring and control over your personal computer.

- Cisco Systems is a front for DARPA routers that were created with a backdoor for the NSA to spy on "virtually every exchange on the Internet."

- IBM hired many of Germany’s mind control scientists from WWII and carried on those experiments through the CIA that formed in 1947; those experiments took on many different names including MKUltra. Those German scientists had used IBM computers during the war to catalogue "undersirables" like Jews, gypsies, homosexuals, Poles and Russians and it organized the trains to the death camps for individuals marked for extermination and hideous experimentation.

- IBM/Cisco System’s "Internet of Things" plants net-bots in all devices under its control that can be activated remotely and used for cyber-attacks.

- The internet was first a DARPA project called the ARPANET which was created as an information technology weapon for cyberwarfare.

- The U. S. government has helped build, monitor, regulate, and control all physical aspects of Internet transmissions and broadcasts through the U. S. Board of Broadcasting Governors, which is a part of the Department of Defense. Every transmission through the internet or through cellphone towers is completely controlled by the U. S. government.

- The U. S. government can “turn off”, filter, manipulate, and control the Internet through the federally controlled transmission cables that span the world. If the U. S. wanted to turn off North Korea’s internet access, it is as simple as a keystroke. Thus, the U. S. government has been boldly lying about the Internet since its inception.

WHAT EVIL IS THE HIGHLANDS FORUM UP TO NOW?
By 2008, the NSA effectively resurrected the Total Information Awareness project with a focus on Internet data-mining via comprehensive monitoring of e-mails, text messages, and Web browsing. We also now know that the NSA’s XKeyscore ‘Digital Network Intelligence’ exploitation system was designed to allow analysts to search not just internet databases like emails, online chats and browsing history, but also telephone services, mobile phone audio, financial transactions and global air transport communications—essentially the entire global telecommunications grid. Highlands Forum partner SAIC played a key role, among other contractors, in producing and administering the NSA’s XKeyscore.

**Goldman Sachs is CIA**

Goldman Sachs (with JPMorgan in tow) is the investment firm responsible for creating the billion dollar fortunes of the tech sensations of the 21st century, from Google to Facebook, is intimately linked to the U.S. military intelligence community.

The convergence of these powerful financial and military interests around the Highlands Forum—through George Lee’s sponsorship of the Forum’s new partner, the MIIS Cybersec initiative—is revealing in itself. MIIS Cybersec’s director, Dr. Itamara Lochard, has long been embedded in Highlands.

Dr. Itamara Lochard is a senior Highlands Forum member and Pentagon information operations expert. She directs the MIIS CyberSec initiative that now supports the Pentagon Highlands Forum with funding from Goldman Sachs partner George Lee, who led the valuations of Facebook and Google.
Dr. Lochard maintains a comprehensive database of 1,700 non-state groups including insurgents, militias, terrorists, complex criminal organizations, organized gangs, malicious cyber actors and strategic non-violent actors, to analyze their organizational patterns, areas of cooperation, strategies and tactics.

Her views disclose much about what the Highlands Forum has been advocating all these years. In 2004, Lochard was co-author of a study for the U.S. Air Force’s Institute for National Security Studies on US strategy toward ‘non-state armed groups.’ The study on the one hand argued that non-state armed groups should be urgently recognized as a ‘tier one security priority,’ and on the other that the proliferation of armed groups provide strategic opportunities that can be exploited to help achieve policy goals.

There have and will be instances where the United States may find collaborating with armed group is in its strategic interests. But sophisticated tools must be developed to differentiate between different groups and understand their dynamics, to determine which groups should be countered, and which could be exploited for US interests.

In 2009, it also emerged from a Google patent application that the company had deliberately been collecting ‘payload’ data from private WI-fi networks that would enable the identification of “geolocations.” In the same year, 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.

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 U.S. 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.
Brainwashing 3.0

In 2011, the Forum hosted two DARPA-funded scientists, Antonio and Hanna Damasio, who are principal investigators in the ‘Neurobiology of Narrative Framing’ project at the University of Southern California. Evoking Zalman’s emphasis on the need for Pentagon psychological operations to deploy “empathetic influence,” the new DARPA-backed project aims to investigate how narratives often appeal “to strong, sacred values in order to evoke an emotional response,” but in different ways across different cultures.

The most disturbing element of the research is its focus on trying to understand how to increase the Pentagon’s capacity to deploy narratives that influence listeners in a way that overrides conventional reasoning in the context of morally-questionable actions.

The research is based on extracting narratives from millions of American, Iranian, and Chinese weblogs, and subjecting them to automated discourse analysis to compare them quantitatively across the three languages. The investigators then follow up using behavioral experiments with readers/listeners from different cultures to gauge their reaction different narratives “where each story makes an appeal to a sacred value to explain or justify a morally-questionable behavior of the author.” Finally, the scientists apply neurobiological fMRI scanning to correlate the reactions and personal characteristics of subjects with their brain responses.

DARPA’s goal is to mine millions of American weblogs as part of its ‘neurobiology of narrative framing’ research. As the Pentagon’s extensive funding of propaganda on Iraq and Afghanistan demonstrates, population influence and propaganda is critical not just in far-flung theatres abroad in strategic regions, but also at home, to quell the risk of domestic public opinion undermining the legitimacy of Pentagon policy.
U.S. PATENT OFFICE WORKS FOR DARPA/IN-Q-TEL

JUST AS LEADER TECHNOLOGIES WAS RIPPED OFF BY NSA/FBI/CIA ATTORNEY JAMES CHANDLER AND THE IBM ECLIPSE FOUNDATION FOR THEIR PATENTS THAT ARE ESSENTIAL TO FACEBOOK FOR SCALABILITY, SO TOO MANY INVENTORS HAVE HAD THEIR PATENTS STOLEN BY THE U.S. PATENT OFFICE.

This rip-off and theft is rationalized as legal once the patent committee determines that a patent may have some impact upon U.S. “national security.” Over five thousand patents have been legally confiscated (stolen) by the U. S. Patent Office, including many free energy patents that directly compete with oil and gas, and given to DARPA/In-Q-Tel for further development and weaponization. Once the patent is used to create a prototype, it has encrypted back-doors installed then it is given out as open source material for corporations and individuals to bring to the market place.

This national security rationalization for the theft of intellectual property fundamentally violates the Fifth Amendment Takings Clause which states that “private property [shall not] be taken for public use, without just compensation.”

If an inventor of a patent that is confiscated by the U. S. Patent Office tries to continue work on the patent, that inventor may end up in jail. The rules of this patent confiscation are located in 35 U.S. Code § 181 – Secrecy of certain inventions and withholding of patent, which provides that the government can take any patent and make it secret and use it at their discretion, or just make sure that it never gets developed.

THERE ARE STRICT PENALTIES IF THE INVENTOR EVEN SPEAKS OF THE PATENT AFTER IT HAS BEEN “CONFISCATED.”

Members of DARPA and In-Q-Tel provide the Defense Department and the CIA with these “secret” patents so that they might first be weaponized for military purposes. Often, patents are then given to fake companies, supported with U.S. tax dollars, who bring the patent to market.
This is what happened with the patent theft of Leader Technologies that was then used by the front companies Goggle and Facebook, which are actually directed by the Department of Defense and the CIA. Clearly the law the dark state chooses to ignore is Leader’s overarching property rights in the Fifth Amendment Takings Clause, which takes precedence.

The Patent Office did not withhold Leader’s patents, and therefore cannot rely on its confiscation six years earlier when Leader’s intellectual property was a trade secret disclose only to its duplicitous attorney James P. Chandler.

**Patent theft is only the tip of the iceberg.** Industrial espionage is common in all industries. Alphabet/Google and Facebook have seemingly endless money to “absorb” any competition through buying them and keeping competition at abeyance. There are many other ways to “suppress” technologies that threaten the “big” companies, whether oil, tech, pharmaceuticals, agriculture/food, energy production. Big corporations use governments, especially multi-national organizations, to do their bidding. Big corporations spend huge amounts of money on lobbying governments to “pay to play.”

**AND WHEN MONEY CAN’T ACCOMPLISH THE GOALS, THEY RESORT TO STEALING PATENTS AND KILLING INVENTORS.**

Suppression and sabotage of technologies has been the norm since the dawn of the twentieth century when fossil fuels and the petrodollar came to rule world economics. Over 5000 new patents have been “deemed” secret and have been suppressed by existing patent laws. There are U. S. patent laws permitting the government to steal and suppress any new technology (and imprison the inventor) which threatens “national security.”

Under Vice President Nixon, in the early 1950s, illegal, secret patent legislation was written, permitting the U.S. government to steal technology from inventors and/or suppress it should a case be made the technology might threaten the status quo.

**The shocked inventors also were informed that they could be jailed up to 20 years if they made the theft of their technology known to the public.**
35 U.S. CODE § 186 – PENALTY

Whoever, during the period or periods of time an invention has been ordered to be kept secret and the grant of a patent thereon withheld pursuant to section 181, shall, with knowledge of such order and without due authorization, willfully publish or disclose or authorize or cause to be published or disclosed the invention, or material information with respect thereto, or whoever willfully, in violation of the provisions of section 184, shall file or cause or authorize to be filed in any foreign country an application for patent or for the registration of a utility model, industrial design, or model in respect of any invention made in the United States, shall, upon conviction, be fined not more than $10,000 or imprisoned for not more than two years, or both.


VERY CLEARLY, THE PATENT SYSTEM IS MERELY A LURE FOR UNSUSPECTING INNOVATORS TO SHARE THEIR IDEAS SO THAT THE MILITARY-INDUSTRIAL COMPLEX CAN STEAL THEM AT WILL.

WANT TO KNOW ABOUT THE FREE ENERGY DEVICES THAT THIS CORRUPT PATENT SYSTEM IS SUPPRESSING FROM THE PEOPLE? SEE OUR CITIZENS INTELLIGENCE REPORT ENTITLED THE FREE ENERGY REVOLUTION HAS BEGUN
We have discussed the companies that you may already know have control over your life, but there are many, many more that we don’t know about. Many of us are reliant, even addicted, to these the internet, cellphones, and Facebook pages and groups. It has been shown that the internet creates different illnesses and some researchers say the internet is more addictive than drugs.

But what is worse is that DARPA/In-Q-Tel already has many programs that are not publicly known about and are being used right now to control U. S. citizens with cyberwarfare technologies. Let’s take a look at some of those other programs described by whistleblowers, like the Vault 7 Wiki-leaks, and see what those programs are intending to do for the U. S. military.

**Total Information Awareness** – Under the umbrella of a system known as Total Information Awareness, DARPA spearheaded many of the surveillance programs abused by the NSA. DARPA’s Total Information Awareness concept created a veritable buffet of advanced surveillance and data mining programs, many of which ultimately were folded into NSA’s PRISM. PRISM culled citizens’ personal data from companies like Microsoft, Google, and Facebook.

**PRISM** – A clandestine national security electronic surveillance program operated by the United States National Security Agency which can target customers of participating corporations outside or inside the United States.

**Sounds of Silence** – The Silent Subliminal Presentation System was developed for commercial use in 1992. A silent communications system in which non-aural carriers, in the very low (ELF) or very high audio-frequency (VHF) range or in the adjacent ultrasonic frequency spectrum are amplitude – or frequency- modulated with the desired intelligence and propagated acoustically or vibrationally, for inducement in to the brain, typically through the use of loudspeakers, earphones, or piezoelectric transducers. The modulated carriers may be transmitted directly in real time or may be recorded and stored on mechanical, magnetic, or optical media for delayed or repeated transmission to the listener. US Patent #5,159,703.

**ThinThread** – A U.S. National Security Agency program involved wiretapping and sophisticated analysis of the resulting data.
**Trailblazer Project** – U.S. National Security Agency program intended to develop a capability to analyze data carried on communications networks including cell phone networks and the Internet.

**Turbulence** – Turbulence is a National Security Agency information-technology project started circa 2005. It was developed in small, inexpensive “test” pieces rather than one grand plan like its failed predecessor, the Trailblazer Project. It also includes offensive cyberwarfare capabilities, like injecting malware into remote computers.

**Tailored Access Operations** – Intelligence-gathering unit of the NSA that is capable of harvesting approximately two petabytes of data per hour.

**Boundless Informant** – A system deployed by the NSA to analyze global electronic information. In March 2013, Boundless Informant gathered 14 billion data reports from Iran, 6.3 billion from India, and 2.8 billion from the United States.

**Bullrun** – A highly classified NSA program to preserve its ability to eavesdrop on encrypted communications by influencing and weakening encryption standards, by obtaining master encryption keys, and by gaining access to data before or after it is encrypted either by agreement, by force of law, or by computer network exploitation (hacking).

**Stuxnet** – Is the first discovered malware that spies on industrial systems, and it was used to attack Iran's nuclear facilities. It is believed to have originated from the United States under the Bush administration.

**Carnivore** – A system implemented by the Federal Bureau of Investigation that was designed to monitor email and electronic communications.

**DCSNet** – The Federal Bureau of Investigation’s point-and-click surveillance system that can perform instant wiretaps on any telecommunications device located in the United States.

**Fairview** – A mass surveillance program directed at foreign mobile phone users.
ICREACH – Surveillance front-end GUI that is shared with 23 government agencies, including the CIA, DEA, and FBI, to search illegally collected personal records.

Magic Lantern – A keystroke logging software deployed by the FBI in the form of an e-mail attachment. When activated, it acts as a trojan horse and allows the FBI to decrypt user communications.

Main Core – A personal and financial database storing information of millions of U.S. citizens believed to be threats to national security. The data mostly comes from the NSA, FBI, CIA, as well as other government sources.

MAINWAY – A NSA database containing metadata for hundreds of billions of telephone calls made through the four largest telephone carriers in the United States.

MUSCULAR – Overseas wiretapping of Google's and Yahoo's internal networks by the NSA.

MYSTIC – Is a voice interception program used by the National Security Agency.

Room 641A – A telecommunication interception facility operated by AT&T for the U.S. National Security Agency.

Sentry Eagle – It monitors and attacks an adversary's cyberspace through capabilities include SIGINT, Computer Network Exploitation, Information Assurance, Computer Network Defense, Network Warfare, and Computer Network Attack. The efforts included weakening U.S. commercial encryption systems.

Special Collection Service – A black budget program that is responsible for “close surveillance, burglary, wiretapping, breaking and entering.” It employs covert listening device technologies to bug foreign embassies, communications centers, computer facilities, fiber-optic networks, and government installations.

Terrorist Finance Tracking Program – A joint initiative run by the CIA and the Department of the Treasury to access the SWIFT (Society for Worldwide Interbank
Financial Telecommunication) transaction database as part of the Bush administration’s “Global War on Terrorism.”

Multi-state Anti-Terrorism Information Exchange (MATRIX) – A data mining system originally developed for the Florida Department of Law Enforcement.

Insight Program – It detects threat networks, irregular warfare, and terrorist operations by combining intelligence information from imaging sensors, crowd-source and other social network or text-based sensors, as well as from other sources for further analysis. Develops integrated human/machine reasoning into intelligence equipment to encompass operator knowledge and reasoning when dealing quickly with complex data from many different sensors.

EM Fields and Hidden Symbols – Uses techniques to incept thoughts and ideas into the mind. Once a mind has been programed with the memory patterns, words and symbols can trigger the programing without the need of the original device.

Nervous System Manipulation by Electromagnetic Fields from Monitors – US Patent and Trade Office, Patent #6,506,148 on subliminal behavior modification, 1/14/2003, United States Patent 6,506,148, Loos, January 14, 2003. Abstract: It is possible to manipulate the nervous system of a subject by pulsing images displayed on a nearby computer monitor or TV set. For the latter, the image pulsing may be imbedded in the program material, or it may be overlaid by modulating a video stream. Many computer monitors and TV tubes, when displaying pulsed images, emit pulsed electromagnetic fields of sufficient amplitudes to cause such excitation. It is therefore possible to manipulate the nervous system of a subject by pulsing images displayed on a nearby computer monitor or TV set. The image pulsing may be imbedded in the program material, or it may be overlaid by modulating a video stream, either as an RF signal or as a video signal. The image displayed on a computer monitor may be pulsed effectively by a simple computer program. For certain monitors, pulsed electromagnetic fields capable of exciting sensory resonances in nearby subjects may be generated even as the displayed images are pulsed with subliminal intensity. Inventors: Loos, Hendricus G. (3019 Cresta Way, Laguna Beach, CA 92651), Appl. No.: 872528 Filed: June 1, 2001

Narrative Networks Program – Developed classified techniques used to manipulate trust in humans. For its Narrative Networks program, DARPA collaborated with a CIA agency
called the Intelligence Advanced Research Projects Agency (IARPA) to develop methods of overwriting messages in the human mind.

**Mind Control Project** – Remotely disrupts political dissent and extremism by employing “Transcranial Magnetic Stimulation” (TMS) in tandem with sophisticated propaganda based on this technology. TMS stimulates the temporal lobe of the brain with electromagnetic fields. This research aims to stop individuals from thinking certain thoughts and make others believe things they normally would not believe. This research is being conducted by The Center for Strategic Communication at ASU and is entitled “Toward Narrative Disruptors and Inductors: Mapping the Narrative Comprehension Network and its Persuasive Effects.” Mechanical disruptions of narrative processing may be, ultimately, replicated through targeted strategic communication campaigns that approximate the narrative disruptions induced via magnetic stimulation. MIT neuroscientists have shown that they can plant false memories. Most of the research in this area currently revolves around how to induce and eliminate fear.

**CONTROLLING AMERICANS THROUGH THE INTERNET**

It is important to remember that since Barack Obama added new language in the National Defense Authorization Act of 2012, Americans are now seen as possible terrorists and are military targets and enemies of the state, unless proven otherwise. In essence, all of the above cyberwarfare programs are being used on Americans indiscriminately and with ill intent.

The Patriot Act, later called the U. S. Freedom Act is the exact opposite of its name – it takes away freedom from patriots and lets multi-national corporations and the "run-away military" use the American people as a cyberwarfare testing grounds.

**This fact is little known:** the U. S. military is now allowed to act within the borders of America and target Americans as hostile war-actors (as the military calls us). We are in an information war and the stacks are high – American freedom or military/corporate control. This battle wages while many people are complacent and perfectly happy with their digital experiences.
The internet is a weapon and it is our job to find out what the battle is all about and make sure that we retain our U.S. Civil Rights and American freedom and liberty. We must call out DARPA, In-Q-Tel, Highland Forum, and the U.S. Patent Office for their patent thefts, continuous lies, and cyberwarfare manipulations and demand that U.S. taxpayer dollars that funded these evil weaponized tools be acknowledged and that all cyber-tools be turned over to Americans without the spy systems and information control systems attached.

**HUMANITY MUST NOW FIGHT TO RESTORE FREEDOM AND PRIVACY BEFORE IT IS LOST FOREVER.**

To evolve as human beings into the next century, we need a free and private internet and social networks that are not manipulated as a tools to lock us inside the prison of our minds. Remember that the intent is to "master the human domain" via the mechanical domain controlled by ahrimanic warlords who wish to take our freedoms away.

[1] Katherine Losse, Mark Zuckerberg’s anathemized former speechwriter, revealed in her book *The Boy Kings* (2012) that the term at Facebook for Marina was "dark profiles."

http://www.fbcoverup.com/docs/cyberhijack/cyber-hijack-findings.html#katherine-losse


http://www.fbcoverup.com/docs/cyberhijack/cyber-hijack-findings.html#raytheon-riot


2 Comments

1  Barbara G Dailey on October 17, 2017 at 1:33 am  Reply
My God! I came to get other’s views, feeling myself not wise enough to form an opinion I suppose. Perhaps, others are just speechless, struck dumb, like me. Even in the hands of a benevolent master, this level of power cannot serve any of us well.

2  Our Spirit on October 17, 2017 at 7:47 am  Reply
Barbara, you might enjoy the podcasts that we do with “Betsy and Thomas”. We speak in everyday language to explain these things so that you can explain it to others. We will be recording a few audios on this subject in the next few days and you can find it all on our American Intelligence Media YouTube channel.

Like