Search Google™ Custom Search

THE TOWER OF BABEL RISES AGAIN ~ ITS CALLED THE UTAH DATA CENTER

Daneen G. Peterson, Ph.D.

May 2, 2013

The Tower of Babel Rises Again ~ It's Called the Utah Data Center

I know I said I retired, however there are significant issues that need to be revealed about what's happening under the guise of protecting us . . . **NOT!**

ALL semblance of privacy will be eliminated. Privacy has already been significantly eroded, however, you will not believe the total, complete control and invasiveness, that is planned for your future . . .

About five years ago, I was looking for a webmaster and tried out several people. One person was a high level IT person for New York City hospitals. He told me that they were recording **EVERYTHING** about a person who entered their hospital system. He believed that the controllers decided to gather such info at hospitals, "because, after all, **EVERYONE** eventually ends up in the hospital at one time or another. So what better time to collect very personal information about them". He felt that the data collection was **NOT** for just for hospital and doctor use, but for the government to have and assemble into huge databases, like the one they are building today, in Bluffdale, Utah.

In an effort to warn you of the coming Armageddon, a battle being pitched to reduce the minds, words and thoughts of mankind to a common computerized denominator . . . is a modern day 'Tower of Babel' reversed and ascending. The following information will let you understand what the communists are planning for your future.

The European Union attempted to re-create the **first** Tower of Babel, their Parliament Building in Strasbourg, France.

Yes, this is the FINISHED building!

The above information was taken from my article: ***The EU and the NAU ~ Two Peas in a Pod!*** found here.
Strasbourg is located in the Alsace Region of France on the German Border, and is regarded as the bridge of

unity between modern France and Germany. It is the first seat of the European Parliament and **the only place where the whole parliament regularly meets**. Some have likened the shape and unfinished look of the building to a **re-creation of the biblical 'Tower of Babel'**. A rather appropriate comment, considering the number of countries and languages spoken there.

It is the European Union's (EU) **first seat of Power** -- where the **SELECTED** and **UNACCOUNTABLE** 'leaders' regularly meet. The 'leaders' consist of the plutocratic oligarchy (a wealthy few) of communist leanings.

The faux parliament of **ELECTED** MEPs primarily meet and work in Brussels, Belgium, where the other two main institutions of the EU are headquartered for those who are **ELECTED** to it. The MEPs are required to 'rubber stamp' what their 'leaders' want.

The world's **SECOND** Tower of Babel is to reside in an innocuously named building called the '**Utah Data Center**' which will house massive computer data banks in a gigantic building covering an area more than FIVE times the size of the US Capitol building.

The boundaries of the town of Bluffdale, Utah where it is located, had to be expanded to encompass the facility.

What's a Yottabyte?

To understand the depth and breadth of the planned data capture and manipulation of that data . . . you need to understand the following computer terminology:

Eric Schmidt, Google's former CEO, once estimated that **the total of all human knowledge created from the dawn of man to 2003 totaled 5 EXABYTES**.

A recent report by Cisco, stated that the global Internet traffic will quadruple from 2010 to 2015, **reaching only 966 EXABYTES per year by 2015**.

A **MILLION EXABYTES** = **ONE YOTTABYTE**. 'They' are working secretly around the clock to create computers capable of routinely handling yottabytes. Get ready for the complete, total aggregation of your life, gathered, controlled and **USED** by the plutocratic oligarchs who run our communist government.

When the computers they are building to aggregate massive amounts of data will reach a magnitude of capacity such that you will be reduced to nothing more than a 'cipher', "a person or thing of no importance or value; a nonentity with a value of **ZERO**". They are secretly working **VERY HARD** to achieve that level of yottabyte computing capacity.

The NSA building is a 1-million-square-foot data storehouse, and **IF** the agency were to ever fill the Utah database with a **SINGLE YOTTABYTE** of information, it will be equal to about 500 quintillion (500,000,000,000,000,000,000) pages of text.

What will exist . . . when this massive computer complex gathers all the world's data and discourse, taken from **ALL** languages, and then decodes and translates that into a **SINGLE** coherent, intelligible computer language, which is then manipulated to gain knowledge and comprehension . . . will be to the complete detriment of all of us who are surveilled. **Thus God's punishment for the 'Tower of Babel' will be reversed!** Out of many languages . . . **ONE**!

A 'Real World' Example of Electronic Medical Records Violations . . .

Government-funded medical experiments on babies risked blindness and death, over 23 prestigious universities involved

The U.S. *Office for Human Research Protections* (OHRP's) . . . "**complacency in addressing the nationwide experiment involving electronic medical records. Such devices are now being widely used despite having never received approval by the U.S. *Food and Drug Administration* (FDA), which means they are in clear violation of the *Federal Food, Drug, and Cosmetic Act* (FD&C).**"

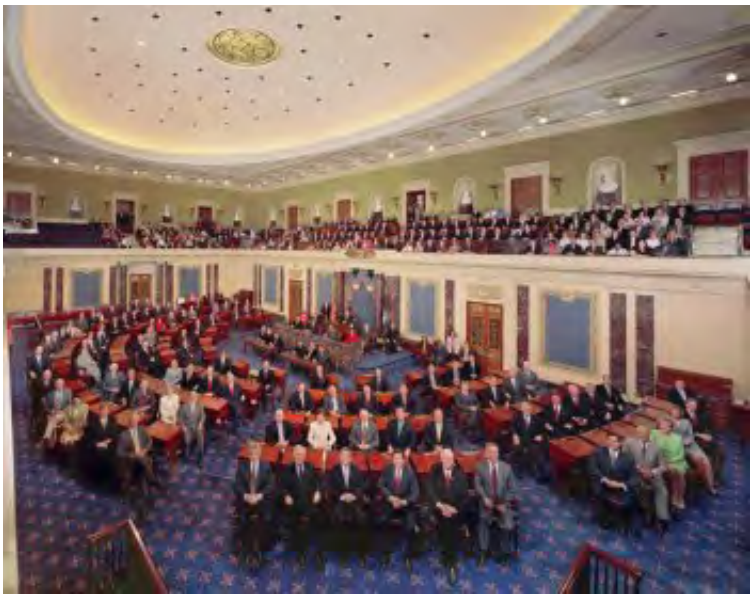
http://www.naturalnews.com/040057_medical_experiments_infants_universities.html

What's The CFR's Position?

What's the Council on Foreign Relations (CFR) talking about these days? The CFR have been in the driver's seat, running our foreign AND domestic affairs for decades. If you think they are just a 'think tank' . . . think again! Here's their latest push:

Bluffdale, Utah Cybersecurity Spy Building

The following information comes directly from the White House to you. If you can stomach it, carefully read the lies and deceit which consists of what I call '**information smothering**' below. I eventually stopped criticizing in **pink** because it became so obvious that the lies were redundant, lengthy and nothing but disgusting **gobbledygook**, and not worth any further effort to expose them.



http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

The Comprehensive National Cybersecurity Initiative **[CNCI]**

download as pdf

[The ILLEGAL, Marxist,] President Obama has identified cybersecurity as one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter. Shortly after taking office, the **[ILLEGAL, Marxist,]** President therefore ordered a thorough review of federal efforts to defend the U.S. information and communications infrastructure and the development of a comprehensive approach to securing America's digital infrastructure.

In May 2009, the **[ILLEGAL, Marxist,]** President accepted the recommendations of the resulting Cyberspace Policy Review, including the selection of an Executive Branch Cybersecurity Coordinator who will have regular

access to the **[ILLEGAL, Marxist,]** President. The Executive Branch was also directed to work closely with all key players in U.S. cybersecurity, **including state and local governments AND the private sector**, to ensure an organized and unified response to future cyber incidents; **strengthen public/private partnerships [fascism] to find technology solutions that ensure U.S. security and prosperity**; invest in the cutting-edge research and development necessary for the innovation and discovery to meet the digital challenges of our time; and begin a campaign to promote cybersecurity awareness and digital literacy from our boardrooms to our classrooms and begin to build the digital workforce of the 21st century. Finally, the **[ILLEGAL, Marxist,]** President directed that these activities be conducted in a way that is consistent with ensuring the privacy rights and civil liberties guaranteed in the Constitution and cherished by all Americans. **Liar, liar, pants of fire! If you believe that . . . then you'll believe ANYTHING!**

The activities under way to implement the recommendations of the Cyberspace Policy Review build on the Comprehensive National Cybersecurity Initiative (CNCI) **launched by President George W. Bush in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23) in January 2008 [which is covered in my article *Two 'Acts' of Tyranny on the Same Day!* found here]**. **[The ILLEGAL, Marxist,]** President Obama determined that the CNCI and its associated activities should evolve to become key elements of a broader, updated national U.S. cybersecurity strategy. These CNCI initiatives will play a key role in supporting the achievement of many of the key recommendations of **[The ILLEGAL, Marxist,]** President Obama's Cyberspace Policy Review.

The CNCI consists of a number of **mutually reinforcing initiatives** with the following major goals designed to help secure the United States in cyberspace:

- **To establish a front line of defense against today's immediate threats** by creating or enhancing shared situational awareness of network vulnerabilities, threats, and events within the Federal Government—and ultimately with state, local, and tribal governments and private sector partners—and the ability to act quickly to reduce our current vulnerabilities and prevent intrusions. **So that you understand . . . their reach will go way beyond the 'Federal Government' and will include 'private sector partners' which is, by definition, the combining of corporate and government . . . the very essence of fascism.**
- **To defend against the full spectrum of threats** by enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key information technologies.
- **To strengthen the future cybersecurity environment** by expanding cyber education; coordinating and redirecting research and development efforts across the Federal Government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace.

In building the plans for the CNCI, it was quickly realized that these goals could not be achieved without also strengthening certain key strategic foundational capabilities within the Government. Therefore, **the CNCI includes funding within the federal law enforcement, intelligence, and defense communities** to enhance such key functions as criminal investigation; intelligence collection, processing, and analysis; and information assurance critical to enabling national cybersecurity efforts. **What we have here is a description of the rising of a police state!**

The CNCI was developed with great care and attention to privacy and civil liberties concerns in close consultation with privacy experts across the government. Protecting civil liberties and privacy rights remain fundamental objectives in the implementation of the CNCI. **That statement is a complete lie. We already know that will not exist.**

In accord with President Obama's declared intent to make transparency a touchstone of his presidency, the Cyberspace Policy Review identified enhanced information sharing as a key component of effective cybersecurity. To improve public understanding of Federal efforts, the Cybersecurity Coordinator has directed the release of the following summary description of the CNCI. **There has been more secrecy, complete and TOTAL lack of 'transparency', and back room deals with Obama, than ALL prior presidents combined.**

CNCI Initiative Details **My question is . . . who or what IS this . . . 'Federal Enterprise'? Is it a police state? You decide . . .**

Initiative #1. Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet

Connections. The Trusted Internet Connections (TIC) initiative, headed by the Office of Management and Budget and the Department of Homeland Security, covers the consolidation of the Federal Government's external access points (including those to the Internet). This consolidation will result in a common security solution which includes: facilitating the reduction of external access points, establishing baseline security capabilities; and, validating agency adherence to those security capabilities. Agencies participate in the TIC initiative either as TIC Access Providers (a limited number of agencies that operate their own capabilities) **or by contracting with commercial Managed Trusted IP Service (MTIPS) providers through the GSA-managed NETWORX contract vehicle**.

Initiative #2. Deploy an intrusion detection system of sensors across the Federal enterprise. Intrusion Detection Systems using passive sensors form a vital part of U.S. Government network defenses by identifying when unauthorized users attempt to gain access to those networks. DHS is deploying, as part of its EINSTEIN 2 activities, signature-based sensors capable of inspecting Internet traffic entering Federal systems for unauthorized accesses and malicious content. The EINSTEIN 2 capability enables analysis of network flow information to identify potential malicious activity while conducting automatic full packet inspection of traffic entering or exiting U.S. Government networks for malicious activity using signature-based intrusion detection technology. Associated with this investment in technology is a parallel investment in manpower with the expertise required to accomplish DHS's expanded network security mission. EINSTEIN 2 is capable of alerting US-CERT in real time to the presence of malicious or potentially harmful activity in federal network traffic and provides correlation and visualization of the derived data. Due to the capabilities within EINSTEIN 2, US-CERT analysts have a greatly improved understanding of the network environment and an increased ability to address the weaknesses and vulnerabilities in Federal network security. As a result, US-CERT has greater situational awareness and can more effectively develop and more **readily share security relevant information with network defenders across the U.S. Government, as well as with security professionals in the private sector and the American public**. **[Fascism again]**The Department of Homeland Security's Privacy Office has conducted and published a Privacy Impact Assessment for the EINSTEIN 2 program. **Want to bet that Einstein is rolling over in his grave at the way they have co-opted his name to 'spin' their spy network.**

Initiative #3. Pursue deployment of intrusion prevention systems across the Federal enterprise. This Initiative represents the next evolution of protection for civilian Departments and Agencies of the Federal Executive Branch. This approach, called EINSTEIN 3, will draw on commercial technology and specialized government technology to conduct real-time full packet inspection and threat-based decision-making on network traffic entering or leaving these Executive Branch networks. The goal of EINSTEIN 3 is to identify and characterize malicious network traffic to enhance cybersecurity analysis, situational awareness and security response. It will have the ability to automatically detect and respond appropriately to cyber threats before harm is done, providing an intrusion prevention system supporting dynamic defense. EINSTEIN 3 will assist DHS US-CERT in defending, protecting and reducing vulnerabilities on Federal Executive Branch networks and systems.

The EINSTEIN 3 system will also support enhanced information sharing by US-CERT with Federal Departments and Agencies by giving DHS the ability to automate alerting of detected network intrusion attempts and, **when deemed necessary by DHS, to send alerts that do not contain the content of communications to the National Security Agency (NSA) so that DHS efforts may be supported by NSA exercising its lawfully authorized missions.** This initiative makes substantial and long-term investments to increase national intelligence capabilities to discover critical information about foreign cyber threats and use this insight to inform EINSTEIN 3 systems in real time. DHS will be able to adapt threat signatures determined by NSA in the course of its foreign intelligence and DoD information assurance missions for use in the EINSTEIN 3 system in support of DHS's federal system security mission. **Information sharing on cyber intrusions will be conducted in accordance with the laws and oversight for activities related to homeland security, intelligence, and defense in order to protect the privacy and rights of U.S. citizens. I guess they think if they repeat the lie often enough we'll believe it!**

DHS is currently conducting a exercise to pilot the EINSTEIN 3 capabilities described in this initiative based on technology developed by NSA and to solidify processes for managing and protecting information gleaned from observed cyber intrusions against civilian Executive Branch systems. **Government civil liberties and privacy officials are working closely with DHS and US-CERT to build appropriate and necessary privacy protections into the design and operational deployment of EINSTEIN 3. Believe that lie and I will offer**

you a chance to buy this bridge over here.

Initiative #4: Coordinate and redirect research and development (R&D) efforts. No single individual or organization is aware of all of the cyber-related R&D activities being funded by the Government. This initiative is developing strategies and structures for coordinating all cyber R&D sponsored or conducted by the U.S. government, both classified and unclassified, and to redirect that R&D where needed. This Initiative is critical to eliminate redundancies in federally funded cybersecurity research, and to identify research gaps, prioritize R&D efforts, and ensure the taxpayers are getting full value for their money as we shape our strategic investments.

Initiative #5. Connect current cyber ops centers to enhance situational awareness. There is a pressing need to ensure that government information security offices and strategic operations centers share data regarding malicious activities against federal systems, consistent with privacy protections for personally identifiable and other protected information and as legally appropriate, in order to have a better understanding of the entire threat to government systems and to take maximum advantage of each organization's unique capabilities to produce the best overall national cyber defense possible. This initiative provides the key means necessary to enable and support shared situational awareness and collaboration across six centers that are responsible for carrying out U.S. cyber activities. This effort focuses on key aspects necessary to enable practical mission bridging across the elements of U.S. cyber activities: foundational capabilities and investments such as upgraded infrastructure, increased bandwidth, and integrated operational capabilities; **enhanced collaboration, including common technology, tools, and procedures; and enhanced shared situational awareness through shared analytic and collaborative technologies**. **Who do they think they are kidding . . . they will hold those cards so close to their chest that there will be no daylight between the cards and their chest.**

The National Cybersecurity Center (NCSC) within the Department of Homeland Security will play a key role in securing **U.S. Government networks and systems under this initiative by coordinating and integrating information from the SIX centers to provide cross-domain situational awareness, analyzing and reporting on the state of U.S. networks and systems, and fostering interagency collaboration and coordination**.

What you will have will be a COMPLETE lockdown of the entire country managed by 'our friends' at the DHS and their goon types who have been working for the TSA.

Initiative #6. Develop and implement a [Federal] **government-wide cyber counterintelligence (CI) plan.** A government-wide cyber counterintelligence plan is necessary to **coordinate activities across all Federal Agencies to detect, deter, and mitigate the foreign-sponsored cyber intelligence threat to U.S. and private sector information systems.** To accomplish these goals, the plan establishes and expands cyber CI education and awareness programs and workforce development to integrate CI into all cyber operations and analysis, increase employee awareness of the cyber CI threat, and increase counterintelligence collaboration across the government. The Cyber CI Plan is aligned with the National Counterintelligence Strategy of the United States of America (2007) and supports the other programmatic elements of the CNCI. **Since when did "private sector information systems" become a part of the "government-wide cyber counterintelligence"? Isn't that a fascist state?**

Initiative #7. Increase the security of our classified networks. Classified networks house the Federal Government's most sensitive information and enable crucial war-fighting, diplomatic, counterterrorism, law enforcement, intelligence, and **homeland security operations**. Successful penetration or disruption of these networks could cause exceptionally grave damage to our national security. We need to exercise due diligence in ensuring the integrity of these networks and the data they contain. **Don't you wonder if all those naked scans from the airports will end up there?**

Initiative #8. Expand cyber education. While billions of dollars are being spent on new technologies to secure the U.S. Government in cyberspace, it is the people with the right knowledge, skills, and abilities to implement those technologies who will determine success. However there are not enough cybersecurity experts within the Federal Government or private sector to implement the CNCI, nor is there an adequately established Federal cybersecurity career field. Existing cybersecurity training and personnel development programs, while good, are limited in focus and lack unity of effort. In order to effectively ensure our continued technical advantage and future cybersecurity, we **must develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees**. It will take a national strategy, similar to the effort to upgrade science and mathematics education in the 1950's, to meet this challenge. **Why would anyone get a college education for those jobs when we ALL know that they will simply import foreigners for those jobs and pay them less than competent Americans. They've done it before, they're doing it now, they will do it in the future!**

Initiative #9. Snip . . .

Initiative #12. Define the Federal role for extending cybersecurity into critical infrastructure domains. The U.S. Government depends on a variety of privately owned and operated critical infrastructures to carry out the public's business. In turn, these critical infrastructures rely on the efficient operation of information systems and networks that are vulnerable to malicious cyber threats. This Initiative builds on the existing and ongoing partnership between the Federal Government and the public and private sector owners and operators of **Critical Infrastructure and Key Resources (CIKR)**. The Department of Homeland Security **and its private-sector partners** have developed a plan of shared action with an aggressive series of milestones and activities. It includes both short-term and long-term recommendations, specifically incorporating and leveraging previous accomplishments and activities that are already underway. It addresses security and information assurance efforts across the cyber infrastructure to increase resiliency and operational capabilities throughout the CIKR sectors. **It includes a focus on public-private sharing of information regarding cyber threats and incidents in both government and CIKR**. **aka . . . Facsism! Is it my imagination or does that acronym look rather . . . Russian????**

The Front and Back of America's 'Great Seal' ~ Get the Picture?

Who knew the Illuminati laid their evil stamp of ownership on the back of our 'Great Seal'? Did you?

Exposed: Massive New Spy Center Built to Track Your Emails and Phone Calls [And Much, Much More . . .]

http://www.alternet.org/story/154641/exposed%3A_massive_new_spy_center_built_to_track_your_emails_and_phone_calls?paging=off

JAMES BAMFORD: "So you have this massive agency that's collecting a tremendous amount of information every day **by satellites, by tapping into undersea cables, by picking up microwave links and tapping of cell phones and data links on your computer, email links, and so forth**. And then it has to store it someplace, and that's why they built Bluffdale. And then that acts as, in essence, like a cloud, a digital cloud, so that agency employees, analysts from around the country at NSA headquarters and their listening posts in different parts of the U.S.—in Georgia, Texas, Hawaii and Colorado—can all access that information held in Bluffdale in that data center. And that's pretty much a summary of what that data center is all about."

"**The NSA is much different from the CIA. First of all, it's about three times the size**. It costs far more. **It's tremendously more secret than the CIA**. And what it does is very different. It's focused on eavesdropping, on tapping into major communications links, on listening to what people around the world and, to some degree, in the United States say on telephones, email, communications . . . And **NSA is really the most powerful intelligence agency, not only in the U.S., but in the world today**."

". . . the other purpose, in addition to storing material, is it's a—it plays a major role in the codebreaking aspects of NSA. **NSA has several missions. One of them is intercepting communications. The other is breaking codes, because a lot of that information is encrypted. And the third function of NSA is making codes for the U.S., encrypting U.S. communications.** So Bluffdale will play a major role in the breaking of codes because, for breaking codes, you really need two key ingredients. One is a very large—a place where you can store a very large amount of material, because the more material you have, when you're going through it, using computers to go through it, what you're looking for is patterns. And the more material that you have—the more data, the more telephone calls, the more email, the more encrypted data that you have—the more patterns that you're likely to discover."

"And the second thing you need is a very, very powerful computer, a very fast computer that can go through enormous amounts of information very fast looking for those patterns. And so, **the NSA is now also building a very secret facility down in Tennessee at Oak Ridge, where during World War II the U.S., in great secrecy, developed the atomic bomb as part of the Manhattan Project.** So now, instead of an atomic bomb, you have a massive computer that the NSA is working on to be the fastest computer in the world, with speeds that are just beyond most people's comprehensions. And the reason for that is because they have to use these computers to do what they call "brute force" — in other words, take this data and just go through it as fast as possible just to look for these key patterns."

". . .the NSA has constantly denied that they're doing things, and then it turns out they are doing these things. **They denied they were doing domestic eavesdropping back in the '70s, and it turned out they had Operation SHAMROCK and Operation MINARET, and they've been reading every single telegram coming in or going out of the country for 30 years at that point**, and also eavesdropping on antiwar veterans. That came out during the Church Committee report. More recently, a few years ago, **President Bush said before camera that the United States is not eavesdropping on anybody without a warrant, and then it turns out that we had this exposure to all the warrantless eavesdropping in the New York Times article**. And so, you have this constant denial and parsing of words in terms of what he's saying." **Read that paragraph AGAIN so that you understand the lies they keep repeating about PRIVACY.**

"So, what I would like to do—I quote from a number of people in the article that are whistleblowers. They worked at NSA. They worked there many years. One of my key whistleblowers was the senior technical person on the largest eavesdropping operation in NSA. He was a very senior NSA official. He was in charge of basically automating the entire world eavesdropping network for NSA . . . **Bill Binney, the senior official I interviewed, had been with NSA for 40 years almost, and he left, saying that what they're doing is unconstitutional**."

What follows are two, nearly complete, articles by James Bamford which very succinctly reveals the breadth and depth of the massive computerized information storage building, currently under construction and scheduled for completion by September 2013.

NSA Utah Data Center Largest Spy Compound Ever - Part 1

---

http://www.virtualthreat.com/2012/06/01/nsa-utah-data-center-largest-spy-compound-ever-part-1/

Wired.com (Threat Level)

The spring air in the small, sand-dusted town has a soft haze to it, and clumps of green-gray sagebrush rustle in the breeze. Bluffdale sits in a bowl-shaped valley in the shadow of Utah's Wasatch Range to the east and the Oquirrh Mountains to the west. It's the heart of Mormon country, where religious pioneers first arrived more than 160 years ago. They came to escape the rest of the world, to understand the mysterious words sent down from their god as revealed on buried golden plates, and to practice what has become known as "the principle," marriage to multiple wives.

Today Bluffdale is home to one of the nation's largest sects of polygamists, the Apostolic United Brethren, with upwards of 9,000 members. The brethren's complex includes a chapel, a school, a sports field, and an archive. Membership has doubled since 1978—and the number of plural marriages has tripled—so the sect has recently been looking for ways to purchase more land and expand throughout the town. **Note: You may wonder as I did if the feeble token try for the presidency by Romney, after 'dropping out' in the '08 election . . . whether or not this spy complex was in the mix as the 'payoff'?**

But new pioneers have quietly begun moving into the area, secretive outsiders who say little and keep to themselves. Like the pious polygamists, they are focused on deciphering cryptic messages that only they have the power to understand. Just off Beef Hollow Road, less than a mile from brethren headquarters, thousands of hard-hatted construction workers in sweat-soaked T-shirts are laying the groundwork for the newcomers' own temple and archive, a massive complex so large that it necessitated expanding the town's boundaries. **Once built, it will be more than five times the size of the US Capitol.**

Photo: Name Withheld; Digital Manipulation: Jesse Lenz

Rather than Bibles, prophets, and worshippers, this temple will be filled with servers, computer intelligence experts, and armed guards. And instead of listening for words flowing down from heaven, these newcomers will be secretly capturing, storing, and analyzing vast quantities of words and images hurtling through the world's telecommunications networks. In the little town of Bluffdale, Big Love and Big Brother have become uneasy neighbors.

The NSA has become the largest, most covert, and potentially most intrusive intelligence agency ever.

Under construction by contractors with top-secret clearances, the blandly named Utah Data Center is

being built for the National Security Agency. A project of immense secrecy, it is the final piece in a complex puzzle assembled over the past decade. **Its purpose: to intercept, decipher, analyze, and store vast swaths of the world's communications as they zap down from satellites and zip through the underground and undersea cables of international, foreign, and domestic networks.** The heavily fortified $2 billion center should be up and running in September 2013. Flowing through its servers and routers and stored in near-bottomless databases will be all forms of communication, including **the complete contents of private emails, cell phone calls, and Google searches, as well as all sorts of personal data trails—parking receipts, travel itineraries, bookstore purchases, and other digital "pocket litter**." It is, in some measure, the realization of the "total information awareness" program created during the first term of the Bush administration—an effort that was killed by Congress in 2003 after it caused an outcry over its potential for invading Americans' privacy.

But "this is more than just a data center," says one senior intelligence official who until recently was involved with the program. The mammoth Bluffdale center will have another important and far more secret role that until now has gone unrevealed. **It is also critical, he says, for breaking codes. And code-breaking is crucial, because much of the data that the center will handle—financial information, stock transactions, business deals, foreign military and diplomatic secrets, legal documents, confidential personal communications—will be heavily encrypted.** According to another top official also involved with the program, the NSA made an enormous breakthrough several years ago in its ability to cryptanalyze, or break, unfathomably complex encryption systems employed by not only governments around the world but also many average computer users in the US. The upshot, according to this official: "Everybody's a target; everybody with communication is a target."

. . . In the process—and for the first time since Watergate and the other scandals of the Nixon administration—**the NSA has turned its surveillance apparatus on the US and its citizens.** It has established listening posts throughout the nation to collect and sift through billions of email messages and phone calls, whether they originate within the country or overseas. It has created a supercomputer of almost unimaginable speed to look for patterns and unscramble codes. Finally, **the agency has begun building a place to store all the trillions of words and thoughts and whispers captured in its electronic net**. And, of course, **it's all being done in secret**. To those on the inside, the old adage that NSA stands for Never Say Anything applies more than ever.

UTAH DATA CENTER

When construction is completed in 2013, the heavily fortified $2 billion facility in Bluffdale will encompass 1 million square feet.

Source: U.S. Army Corps of Engineers Conceptual Site plan

1. Visitor control center:

A $9.7 million facility for ensuring that only cleared personnel gain access.

2. Administration

Designated space for technical support and administrative personnel.

3. Data halls

Four 25,000-square-foot facilities house rows and rows of servers.

4. Backup generators and fuel tanks

Can power the center for at least three days.

5. Water storage and pumping

Able to pump 1.7 million gallons of liquid per day.

6. Chiller plant

About 60,000 tons of cooling equipment to keep servers from overheating.

7. Power substation

An electrical substation to meet the center's estimated 65-megawatt demand.

8. Security

Video surveillance, intrusion detection, and other protection will cost more than $10 million.

Source: U.S. Army Corps of Engineers Conceptual Site plan

A swath of freezing fog blanketed Salt Lake City **on the morning of January 6, 2011** . . . Accompanied by a

retinue of bodyguards, the man was NSA deputy director Chris Inglis, the agency's highest-ranking civilian and the person who ran its worldwide day-to-day operations.

A short time later, Inglis arrived in Bluffdale at the site of the future data center, a flat, unpaved runway on a little-used part of Camp Williams, a National Guard training site. There, in a white tent set up for the occasion, Inglis joined Harvey Davis, the agency's associate director for installations and logistics, and Utah senator **Orrin Hatch**, along with a few generals and politicians in a surreal ceremony. Standing in an odd wooden sandbox and holding gold-painted shovels, they made awkward jabs at the sand and thus officially broke ground on what the local media had simply dubbed "the spy center." Hoping for some details on what was about to be built, reporters turned to one of the invited guests, Lane Beattie of the Salt Lake **Chamber of Commerce**. Did he have any idea of the purpose behind the new facility in his backyard? "Absolutely not," he said with a self-conscious half laugh. "Nor do I want them spying on me."

For his part, Inglis simply engaged in a bit of double-talk, emphasizing the least threatening aspect of the center: "It's a state-of-the-art facility designed to support the intelligence community in its mission to, in turn, enable and protect the nation's cybersecurity." While cybersecurity will certainly be among the areas focused on in Bluffdale, what is collected, how it's collected, and what is done with the material are far more important issues. **Battling hackers makes for a nice cover—it's easy to explain, and who could be against it?** Then the reporters turned to **Hatch**, who proudly described the center as "**a great tribute to Utah**," then added, **"I can't tell you a lot about what they're going to be doing, because it's highly classified**."

And then there was this anomaly: Although this was supposedly the official ground-breaking for the nation's largest and most expensive cybersecurity project, **no one from the Department of Homeland Security, the agency responsible for protecting civilian networks from cyberattack, spoke from the lectern**. In fact, the official who'd originally introduced the data center, at a press conference in Salt Lake City in October 2009, had nothing to do with cybersecurity. It was Glenn A. Gaffney, deputy director of national intelligence for collection, a man who had **spent almost his entire career at the CIA.** As head of collection for the intelligence community, he managed the country's human and electronic spies.

Within days, the tent and sandbox and gold shovels would be gone and Inglis and the generals would be replaced by some 10,000 construction workers. "We've been asked not to talk about the project," Rob Moore, president of Big-D Construction, one of the three major contractors working on the project, told a local reporter. The plans for the center show an extensive security system: an elaborate $10 million antiterrorism protection program, **including a fence designed to stop a 15,000-pound vehicle traveling 50 miles per hour, closed-circuit cameras, a biometric identification system, a vehicle inspection facility, and a visitor-control center**. **Note: Don't you wonder if they constructed a similar fence along the Mexican border, as they promised, would there be 50 MILLION illegal aliens here in our country today?**

Inside, the facility will consist of four 25,000-square-foot halls filled with servers, complete with raised floor space for cables and storage. In addition, there will be more than 900,000 square feet for technical support and administration. The entire site will be self-sustaining, with fuel tanks large enough to power the backup generators for three days in an emergency, water storage with the capability of pumping 1.7 million gallons of liquid per day, as well as a sewage system and massive air-conditioning system to keep all those servers cool. Electricity will come from the center's own substation built by Rocky Mountain Power to satisfy the 65-megawatt power demand. Such a mammoth amount of energy comes with a mammoth price tag—about $40 million a year, according to one estimate. **Taxpayer dollars.**

Given the facility's scale and the fact that a terabyte of data can now be stored on a flash drive the size of a man's pinky, the potential amount of information that could be housed in Bluffdale is truly staggering. But so is the exponential growth in the amount of intelligence data being produced every day by the eavesdropping sensors of the NSA and other intelligence agencies. As a result of this "expanding array of theater airborne and other sensor networks," as a 2007 Department of Defense report puts it, the Pentagon is attempting to expand its worldwide communications network, known as the Global Information Grid, to handle yottabytes (10^{24} bytes) of data. (**A yottabyte is a septillion bytes—so large that no one has yet coined a term for the next higher magnitude**.)

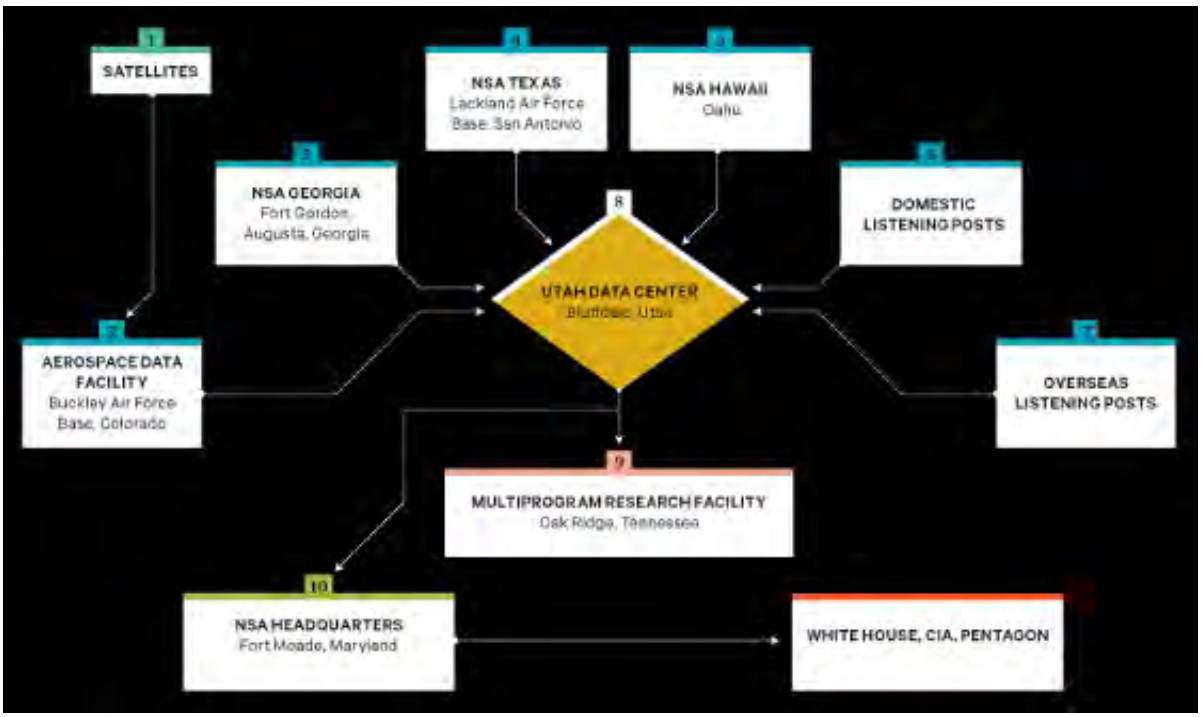
It needs that capacity because, according to a recent report by Cisco, global Internet traffic will quadruple from

2010 to 2015, reaching 966 exabytes per year. (**A million exabytes equal a yottabyte**.) In terms of scale, Eric Schmidt, Google's former CEO, once estimated that the total of all human knowledge created from the dawn of man to 2003 totaled 5 exabytes. And the data flow shows no sign of slowing. In 2011 more than 2 billion of the world's 6.9 billion people were connected to the Internet. By 2015, market research firm IDC estimates, there will be 2.7 billion users. Thus, the NSA's need for a 1-million-square-foot data storehouse. Should the agency ever fill the Utah center with a yottabyte of information, it would be equal to about 500 quintillion (500,000,000,000,000,000,000) pages of text.

The data stored in Bluffdale will naturally go far beyond the world's billions of public web pages. The NSA is more interested in the so-called invisible web, also known as the deep web or deepnet—data beyond the reach of the public. This includes password-protected data, US and foreign government communications, and noncommercial file-sharing between trusted peers. "**The deep web contains government reports, databases, and other sources of information of high value to DOD and the intelligence community**," according to a 2010 Defense Science Board report. "Alternative tools are needed to find and index data in the deep web … Stealing the classified secrets of a potential adversary is where the [intelligence] community is most comfortable." **With its new Utah Data Center, the NSA will at last have the technical capability to store, and rummage through, all those stolen secrets**. The question, of course, is how the agency defines who is, and who is not, "a potential adversary."

The NSA'S SPY NETWORK

Once it's operational, the Utah Data Center will become, in effect, the NSA's cloud. **The center will be fed data collected by the agency's eavesdropping satellites, overseas listening posts, and secret monitoring rooms in telecom facilities throughout the US. All that data will then be accessible to the NSA's code breakers, data-miners, China analysts, counterterrorism specialists, and others working at its Fort Meade headquarters and around the world. Here's how the data center appears to fit into the NSA's global puzzle**.—J.B.



Once it's operational, the Utah Data Center will become, in effect, the NSA's cloud.

1. Geostationary satellites

Four satellites positioned around the globe monitor frequencies carrying everything from walkie-talkies and cell phones in Libya to radar systems in North Korea. Onboard software acts as the first filter in the collection process, targeting only key regions, countries, cities, and phone numbers or email.

2. Aerospace Data Facility, Buckley Air Force Base, Colorado

Intelligence collected from the geostationary satellites, as well as signals from other spacecraft and overseas listening posts, is relayed to this facility outside Denver. About 850 NSA employees track the satellites, transmit target information, and download the intelligence haul.

3. NSA Georgia, Fort Gordon, Augusta, Georgia

Focuses on intercepts from Europe, the Middle East, and North Africa. Codenamed Sweet Tea, the facility has been massively expanded and now consists of a 604,000-square-foot operations building for up to 4,000 intercept operators, analysts, and other specialists.

4. NSA Texas, Lackland Air Force Base, San Antonio

Focuses on intercepts from Latin America and, since 9/11, the Middle East and Europe. Some 2,000 workers staff the operation. The NSA recently completed a $100 million renovation on a mega-data center here—a backup storage facility for the Utah Data Center.

5. NSA Hawaii, Oahu

Focuses on intercepts from Asia. Built to house an aircraft assembly plant during World War II, the 250,000-square-foot bunker is nicknamed the Hole. Like the other NSA operations centers, it has since been expanded: Its 2,700 employees now do their work aboveground from a new 234,000-square-foot facility.

6. Domestic listening posts

The NSA has long been free to eavesdrop on international satellite communications. But after 9/11, it installed taps in US telecom “switches,” gaining access to domestic traffic. An ex-NSA official says there are 10 to 20 such installations.

7. Overseas listening posts

According to a knowledgeable intelligence source, the NSA has installed taps on at least a dozen of the major overseas communications links, each capable of eavesdropping on information passing by at a high data rate.

8. Utah Data Center, Bluffdale, Utah

At a million square feet, this $2 billion digital storage facility outside Salt Lake City will be the centerpiece of the NSA’s cloud-based data strategy and essential in its plans for decrypting previously uncrackable documents.

9. Multiprogram Research Facility, Oak Ridge, Tennessee

Some 300 scientists and computer engineers with top security clearance toil away here, building the world’s fastest supercomputers and working on cryptanalytic applications and other secret projects.

10. NSA headquarters, Fort Meade, Maryland

Analysts here will access material stored at Bluffdale to prepare reports and recommendations that are sent to policymakers. To handle the increased data load, the NSA is also building an $896 million supercomputer center here.

Before yottabytes of data from the deep web and elsewhere can begin piling up inside the servers of the NSA’s new center, they must be collected. **To better accomplish that, the agency has undergone the largest building boom in its history, including installing secret electronic monitoring rooms in major US telecom facilities. Controlled by the NSA, these highly secured spaces are where the agency taps into the US communications networks**, a practice that came to light during the Bush years but was never acknowledged by the agency.

The broad outlines of the so-called warrantless-wiretapping program have long been exposed—how the NSA secretly and illegally bypassed the Foreign Intelligence Surveillance Court, which was supposed to oversee and authorize highly targeted domestic eavesdropping; **how the program allowed wholesale monitoring of millions of American phone calls and email**. In the wake of the program's exposure, Congress passed the FISA Amendments Act of 2008, which largely made the practices legal.

Telecoms that had agreed to participate in the illegal activity were granted immunity from prosecution and lawsuits. **What wasn't revealed until now, however, was the enormity of this ongoing domestic spying program**.

Sources of Information . . .

And . . . where will the information come from . . . here's only **ONE** of **MANY** sources of data from those 'eyes in the sky' that will be sent to the collection of yottabytes at the 'Utah Data Center'!

Workshop: Water Cycle Missions for the Next Decade http://www.crew-services.com/decadal/

(Workshop water cycle

Workshop Overview

Building on the first Earth Science Decadal Survey, NASA's Plan for a Climate-Centric Architecture for Earth Observations and Applications from Space , and the 2012 Chapman Conference on Remote Sensing of the Terrestrial Water Cycle, the objective of this workshop is to *gather wisdom and determine how to prepare for the next generation of water cycle missions in support of the second Earth Science Decadal Survey*.

Following a short plenary, we will discuss the intersection between science questions, technology readiness and satellite design optimization in a series of breakout group discussions designed to form the seeds of a set of water cycle mission formulation groups. **The workshop will formulate next-generation water cycle mission working groups and white papers, designed to identify capacity gaps and inform NASA**.

There are approximately 3,000 satellites operating in Earth orbit, according to the US National Aeronautics and Space Administration (NASA), out of roughly 8,000 man-made objects in total.
http://www.wisegeek.com/how-many-satellites-are-orbiting-the-earth.htm#

Terabyte, Petabyte, Exabyte, Zettabyte, Yottabyte

https://lists.apple.com/archives/dvdlist/2001/Apr/msg00231.html

NSA Utah Data Center Largest Spy Compound Ever – Part 2

http://www.virtualthreat.com/2012/06/02/nsa-utah-data-center-largest-spy-compound-ever-part-2/

For the first time, a former NSA official has gone on the record to describe the program, codenamed Stellar Wind, in detail. William Binney was a senior NSA crypto-mathematician largely responsible for automating the agency's worldwide eavesdropping network. A tall man with strands of black hair across the front of his scalp and dark, determined eyes behind thick-rimmed glasses, the 68-year-old spent nearly four decades breaking codes and **finding new ways to channel billions of private phone calls and email messages from around the world into the NSA's bulging databases**. As chief and one of the two cofounders of the agency's Signals Intelligence Automation Research Center, Binney and his team designed much of the infrastructure that's still likely used to intercept international and foreign communications.

He explains that the agency could have installed its tapping gear at the nation's cable landing stations—the more than two dozen sites on the periphery of the US where fiber-optic cables come ashore. If it had taken that route, the NSA would have been able to limit its eavesdropping to just international communications, which at the time was all that was allowed under US law. **Instead it chose to put the wiretapping rooms at key junction points throughout the country—large, windowless buildings known as switches—thus gaining access to not just international communications but also to most of the domestic traffic flowing through the US.** The network of intercept stations goes far beyond the single room in an AT&T building in San Francisco exposed by a whistle-blower in 2006. "I think there's 10 to 20 of them," Binney says. "That's not just San Francisco; they have them in the middle of the country and also on the East Coast."

WATCH THIS VIDEO . . .

http://www.youtube.com/watch?v=Elb80xou8Zg&feature=player_embedded

The eavesdropping on Americans doesn't stop at the telecom switches. To capture satellite communications in and out of the US, the agency also monitors AT&T's powerful earth stations, satellite receivers in locations that include Roaring Creek and Salt Creek. Tucked away on a back road in rural Catawissa, Pennsylvania, Roaring Creek's three 105-foot dishes handle much of the country's communications to and from Europe and the Middle East. And on an isolated stretch of land in remote Arbuckle, California, three similar dishes at the company's Salt Creek station service the Pacific Rim and Asia.

The former NSA official held his thumb and forefinger close together: "We are that far from a turnkey totalitarian state."

Binney left the NSA in late 2001, shortly after the agency launched its warrantless-wiretapping program. "They violated the Constitution setting it up," he says bluntly. "But they didn't care. They were going to do it anyway, and they were going to crucify anyone who stood in the way. When they started violating the Constitution, I couldn't stay." Binney says Stellar Wind was far larger than has been publicly disclosed and included not just eavesdropping on domestic phone calls but the inspection of domestic email. At the outset the program recorded 320 million calls a day, he says, which represented about 73 to 80

percent of the total volume of the agency's worldwide intercepts. The haul only grew from there. According to Binney—who has maintained close contact with agency employees until a few years ago—the taps in the secret rooms dotting the country are actually powered by highly sophisticated software programs that conduct "deep packet inspection," examining Internet traffic as it passes through the 10-gigabit-per-second cables at the speed of light.

The software, created by a company called Narus that's now part of Boeing, is controlled remotely from NSA headquarters at Fort Meade in Maryland and searches US sources for target addresses, locations, countries, and phone numbers, as well as watch-listed names, keywords, and phrases in email. Any communication that arouses suspicion, especially those to or from the million or so people on agency watch lists, are automatically copied or recorded and then transmitted to the NSA.

The scope of surveillance expands from there, Binney says. Once a name is entered into the Narus database, all phone calls and other communications to and from that person are automatically routed to the NSA's recorders. "Anybody you want, route to a recorder," Binney says. "If your number's in there? Routed and gets recorded." He adds, "The Narus device allows you to take it all." And when Bluffdale is completed, whatever is collected will be routed there for storage and analysis.

According to Binney, one of the deepest secrets of the Stellar Wind program—again, never confirmed until now—was that the NSA gained warrantless access to AT&T's vast trove of domestic and international billing records, detailed information about who called whom in the US and around the world. As of 2007, AT&T had more than 2.8 trillion records housed in a database at its Florham Park, New Jersey, complex.

Verizon was also part of the program, Binney says, and that greatly expanded the volume of calls subject to the agency's domestic eavesdropping. "That multiplies the call rate by at least a factor of five," he says. "So you're over a billion and a half calls a day." (Spokespeople for Verizon and AT&T said their companies would not comment on matters of national security.)

After he left the NSA, Binney suggested a system for monitoring people's communications according to how closely they are connected to an initial target. The further away from the target—say you're just an acquaintance of a friend of the target—the less the surveillance. But the agency rejected the idea, and, given the massive new storage facility in Utah, Binney suspects that it now simply collects everything. "The whole idea was, how do you manage 20 terabytes of intercept a minute?" he says. "The way we proposed was to distinguish between things you want and things you don't want." Instead, he adds, "they're storing everything they gather." And the agency is gathering as much as it can.

Once the communications are intercepted and stored, the data-mining begins. "You can watch everybody all the time with data-mining," Binney says. Everything a person does becomes charted on a graph, "financial transactions or travel or anything," he says. Thus, **as data like bookstore receipts, bank statements, and commuter toll records flow in, the NSA is able to paint a more and more detailed picture of someone's life**.

The NSA also has the ability to eavesdrop on phone calls directly and in real time. According to Adrienne J. Kinne, who worked both before and after 9/11 as a voice interceptor at the NSA facility in Georgia, in the wake of the World Trade Center attacks **"basically all rules were thrown out the window, and they would use any excuse to justify a waiver to spy on Americans."** Even journalists calling home from overseas were included. "A lot of time you could tell they were calling their families," she says, "incredibly intimate, personal conversations." Kinne found the act of eavesdropping on innocent fellow citizens personally distressing. "It's almost like going through and finding somebody's diary," she says.

In secret listening rooms nationwide, NSA software examines every email, phone call, and tweet as they zip by.

. . . Sitting in a restaurant not far from NSA headquarters, the place where he spent nearly 40 years of his life, Binney held his thumb and forefinger close together. "We are, like, that far from a turnkey totalitarian state," he says.

There is still one technology preventing untrammeled government access to private digital data: strong

encryption.

. . . The plan was launched in 2004 as a modern-day Manhattan Project. Dubbed the High Productivity Computing Systems program, its goal was to advance computer speed a thousandfold, **creating a machine that could execute a quadrillion (10^{15}) operations a second, known as a petaflop—the computer equivalent of breaking the land speed record**. And as with the Manhattan Project, the venue chosen for the supercomputing program was the town of Oak Ridge in eastern Tennessee, a rural area where sharp ridges give way to low, scattered hills, and the southwestward-flowing Clinch River bends sharply to the southeast. About 25 miles from Knoxville, it is the "secret city" where uranium- 235 was extracted for the first atomic bomb. A sign near the exit read: what you see here, what you do here, what you hear here, when you leave here, let it stay here. Today, not far from where that sign stood, Oak Ridge is home to the Department of Energy's Oak Ridge National Laboratory, and it's engaged in a new secret war. **But this time, instead of a bomb of almost unimaginable power, the weapon is a computer of almost unimaginable speed**.

. . . Known as the Multiprogram Research Facility, or Building 5300, the $41 million, five-story, 214,000-square-foot structure was built on a plot of land on the lab's East Campus and completed in 2006. Behind the brick walls and green-tinted windows, 318 scientists, computer engineers, and other staff work in secret on the cryptanalytic applications of high-speed computing and other classified projects. The supercomputer center was named in honor of George R. Cotter, the NSA's now-retired chief scientist and head of its information technology program. Not that you'd know it. "There's no sign on the door," says the ex-NSA computer expert.

At the DOE's unclassified center at Oak Ridge, work progressed at a furious pace, although it was a one-way street when it came to cooperation with the closemouthed people in Building 5300. Nevertheless, the unclassified team had its Cray XT4 supercomputer upgraded to a warehouse-sized XT5. Named Jaguar for its speed, it clocked in at 1.75 petaflops, officially becoming the world's fastest computer in 2009.

Meanwhile, over in Building 5300, the NSA succeeded in building an even faster supercomputer. "They made a big breakthrough," says another former senior intelligence official, who helped oversee the program.

Snip . . .

NSA believes it's on the verge of breaking a key encryption algorithm—opening up hoards of data.

That, he notes, is where the value of Bluffdale, and its mountains of long-stored data, will come in. **What can't be broken today may be broken tomorrow.** "Then you can see what they were saying in the past," he says. "By extrapolating the way they did business, it gives us an indication of how they may do things now." The danger, the former official says, is that it's not only foreign government information that is locked in weaker algorithms, **it's also a great deal of personal domestic communications, such as Americans' email intercepted by the NSA in the past decade**.

But first the supercomputer must break the encryption, and to do that, speed is everything. The faster the computer, the faster it can break codes. The Data Encryption Standard, the 56-bit predecessor to the AES, debuted in 1976 and lasted about 25 years. The AES made its first appearance in 2001 and is expected to remain strong and durable for at least a decade. But if the NSA has secretly built a computer that is considerably faster than machines in the unclassified arena, then the agency has a chance of breaking the AES in a much shorter time. **And with Bluffdale in operation, the NSA will have the luxury of storing an ever-expanding archive of intercepts until that breakthrough comes along**.

But despite its progress, the agency has not finished building at Oak Ridge, nor is it satisfied with breaking the petaflop barrier. Its next goal is to reach exaflop speed, one quintillion (10^{18}) operations a second, and eventually zettaflop (10^{21}) and yottaflop.

These goals have considerable support in Congress. Last November a bipartisan group of 24 senators sent

a letter to President Obama urging him to approve continued funding through 2013 for the Department of Energy's exascale computing initiative (the NSA's budget requests are classified). They cited the necessity to keep up with and surpass China and Japan. "The race is on to develop exascale computing capabilities," the senators noted. The reason was clear: By late 2011 the Jaguar (now with a peak speed of 2.33 petaflops) ranked third behind Japan's "K Computer," with an impressive 10.51 petaflops, and the Chinese Tianhe-1A system, with 2.57 petaflops.

Snip . . .

Yottabytes and exaflops, septillions and undecillions—the race for computing speed and data storage goes on. In his 1941 story "The Library of Babel," Jorge Luis Borges imagined a collection of information where the entire world's knowledge is stored but barely a single word is understood. **In Bluffdale the NSA is constructing a library on a scale that even Borges might not have contemplated. And to hear the masters of the agency tell it, it's only a matter of time until every word is illuminated.**

James Bamford (washwriter@gmail.com) is the author of:

The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America.

Related Links to the story above:

The NSA Is Building the Country's Biggest Spy Center NSA spy center: Unsettling details emerge, but director denies allegations NSA Building Massive `Cloud' Center in Utah Desert Utah Data Center Industry Day Presentation (download)

USACE Awards Contract to Build a Data Center at Camp Williams Utah

Balfour Beatty/DPR/Big-D Utah Data Center Project Website

2010 NSA budget request for Utah Data Center Phase One

State of Utah Approval Order: Installation of the New Utah Data Center

FY 2013 NSA Military Construction Budget Justification Documents

Video - Safety or surveillance: What is the NSA's Utah Data Center?

Utah Data Center Facility Support Contract - Sept 2012

NSA Construction Project Status as of 2/28/2013

Surprise Visitors Are Unwelcome At The NSA's Unfinished Utah Spy Center (Especially When They Take Photos)

Even Fox Faux News Reports . . .

NSA data center front and center in debate over liberty, security and privacy

James Bradford

By Catherine Herridge

http://www.foxnews.com/tech/2013/04/12/nsa-data-center-front-and-center-in-debate-over-liberty-security-and-privacy/# (Fox News Video of the Spy Center). Listen to the **NSA liar** say that they "don't hold data on American citizens, they take protecting your civil liberties and privacy as the most important thing that they do".

Snip . . . Twenty-five miles due south of Salt Lake City, a massive construction project is nearing completion. The heavily secured site belongs to the National Security Agency.

Because the Utah Data Center is a "secure facility" and you cannot go inside without the needed security clearances, Fox News rented a helicopter and took to the skies, where the depth and breadth of the Utah Center were stunning.

The aerial video footage is exclusive to the Fox News investigation and posted here. Two weeks after our filming, the helicopter pilot reported to our Fox News team that he had been visited by the FBI on a "national security matter."

The pilot said, according to the FBI agents, that the NSA had taken photos of the helicopter once it made several flyovers. These photos allowed the NSA to identify the make and manufacturer of the helicopter in California who, in turn, told the NSA who operates it in the Salt Lake City area.

The FBI wanted to know if we had the proper air space clearances to flyover the site, which the Fox News team did. Satisfied that the pilot was not flying "terrorists" over the site, the questioning concluded. While the pilot passed along the Fox News contact information, there was no further inquiries.

Binney said the helicopter incident **"showed the capability of the U.S. government to use information to trace people, their relationship to others and to raise suspicions about their activities and intentions."**

Lastly, Did You Know About . . .

The 20th Century: Talmudic triumph over Western civilization
http://www.john-friend.net/2013/04/the-20th-century-talmudic-triumph-over.html

Writing in ***Mein Kampf***, Adolf Hitler perfectly summarized the central theme of the twentieth century, a century

which amounted to a total Jewish triumph over and destruction of Western civilization. Hitler wrote, **"The ignorance of the broad masses as regards the inner character of the Jew, and the lack of instinct and insight displayed by our upper classes, are among the reasons which explain how it is that so many people fall an easy prey to the systematic campaign of falsehood which the Jew carries on."** Of course, Hitler was specifically describing the German nation, but his statement equally applies to all of Western civilization. The "ignorance of the broad masses as regards the inner character of the Jew" combined with "the lack of instinct and insight displayed by" the upper classes has led to a total destruction of our civilization, by and large, a fact most Westerners do ***not even recognize*** **because they cannot fathom the "systematic campaign of falsehood which the Jew carries on**," as Adolf Hitler explained.

In his book ***The Jewish Century***, Jewish author Yuri Slezkine **had this to say** on the very first page:
The Modern Age is the Jewish Age, and **the twentieth century**, in particular, **is the Jewish Century**... **Modernization, in other words, is about everyone becoming Jewish**.

Indeed, ***the Modern Age is the Jewish Age***, and the twentieth century most certainly was the Jewish Century. **Organized Jewry - a subversive, international criminal mafia operating all across the globe - came to dominate and largely control Western politics and governments, banking and international finance, media, academia and other aspects of Western society over the course of the past century**.

Talmudic Judaism's triumph over Western society - politically, culturally, and economically - was, for all intents and purposes, accomplished during the twentieth century. Of course, all students of history - real history, as opposed to the distorted, politically correct "history" students are taught in grade school and in college - recognize the destructive, parasitic nature of organized Jewry over time, no matter which nation they settle in.

Beginning in the 1600s at least, when Jews began to migrate and "assimilate" into non-Jewish, largely Christian societies in Europe, the **systematic assault upon and eventual subversion of Western civilization** began. **Jewish money-lenders corrupted various European courts and the traditional aristocracy, and Jewish agents infiltrated and largely took over Freemasonry and other secret societies -- primarily, the much-ballyhooed Illuminati -- in order to advance their international Talmudic agenda of world domination**.

Radical Jewish "intellectuals" formulated and advanced a variety of destructive and subversive political and cultural ideologies - primarily **international Communism** and **cultural Marxism** - as a means to control the societal reaction to the Industrial Revolution and its consequences **(international Communism)** and to critique and subvert traditional European society **(cultural Marxism)**, paving the way for the total annihilation of Western civilization and its social, cultural, religious, political, and economic norms. . .

Suggested reading: *The International Jew* series of books containing 'spot on' articles by Henry Ford.

How The Plutocratic Oligarchs Do It!

How the CIA Helped Disney Conquer Florida
http://www.thedailybeast.com/articles/2013/04/14/how-the-cia-helped-disney-conquer-florida.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+thedailybeast/articles+%28The+Daily+Beast+-+Latest+Articles%29

With advice from former CIA operatives and lawyers, Disney bought up the land for Florida's Disney World and orchestrated a unique legal situation—and set up an unconstitutional form of government.

What follows if and excerpt from TB Allman's ***Finding Florida***.

Starting in the mid-1960s when Disney set out to establish the Disney World Theme Park, they were **determined to get land at below market prices** and Disney operatives **engaged in a far-ranging conspiracy** to make sure sellers had no idea who was buying their Central Florida property. By resorting to such tactics **Disney acquired more than 40 square miles of land for less than $200 an acre**, but how to maintain control once Disney's empire had been acquired? The solution turned out to be cartoon-simple, thanks to the CIA.

Statue of Walt Disney and Mickey Mouse at Magic Kingdom Park in Walt Disney World in 1988. (Guido Cozzi/Atlantide Phototravel, via Corbis)

Disney's key contact was the consummate cloak-and-dagger operator, William "Wild Bill" Donovan. Sometimes called the "Father of the C.I.A," he was also the founding partner of Donovan, Leisure, Newton & Irvine, a New York law firm whose attorneys **included future C.I.A. director William Casey**. **Donovan's attorneys provided fake identities for Disney agents; they also set up a secret communications center, and orchestrated a disinformation campaign. In order to maintain "control over the overall development**," Disney and his advisers realized, "the company would have to **find a way to limit the voting power of the private residents**" even though, they acknowledged, **their efforts** "**violated the Equal Protection Clause**" **of the U.S. Constitution**.

Here again **the CIA was there to help**. Disney's principal legal strategist for Florida was a senior clandestine operative named Paul Helliwell. Having helped launch the C.I.A. secret war in Indochina, Helliwell relocated to Miami in 1960 in order to coordinate dirty tricks against Castro. At a secret "seminar" Disney convened **in May 1965 Helliwell** came up with the approach **that to this day allows the Disney organization to avoid taxation and environmental regulation as well as maintain immunity from the U.S. Constitution. It was the same strategy the C.I.A. pursued in the foreign countries. Set up a puppet government; then use that regime**

to do your bidding.

Though no one lived there, **Helliwell advised Disney to establish at least two phantom "cities," then use these fake governments to control land use and make sure the public monies the theme park generated stayed in Disney's private hands.** On paper Disney World's "cities" would be regular American home towns —**except their only official residents would be the handful of hand-picked Disney loyalists who periodically "elected" the officials who, in turn, ceded complete control to Disney executives.**

In early 1967, the Florida legislature created Hallowell's two "cities," both named for the artificial reservoirs Disney engineers created **by obstructing the area's natural water flow**. When you visit Disney's Magic Kingdom, you are visiting the City of Bay Lake, Florida. The other was the City of Lake Buena Vista. **In both "cities," in violation of both the U.S. and Florida Constitutions** the Disney-engineered legislation established a property qualification for holding elective office, requiring that each candidate for office there **"must be the owner, either directly or as a trustee, of real property situated in the City" in order "to be eligible to hold the office of councilman."**

Finding Florida By TD Allman 528 pages. Atlantic Monthly Press. $27.50.

Though enacted by the legislature, this and other crucial pieces of Disney-enabling legislation, which would reshape central Florida and affect the lives of tens of millions of people, was written by teams of Disney lawyers working in New York at the Donovan firm, and in Miami at Helliwell's offices. Disney lawyers in California signed off on the text before it was flown to Tallahassee where, without changing a word, Florida's compliant legislators enacted it into law. "**No one thought of reading it**," one ex-lawmaker later remarked. Later, after the houses there were sold, compliant legislatures excluded all the residents of Celebration from Disney's domain, to prevent them from voting.

Those who were there never forgot the day Disney inaugurated what truly would be a magic kingdom in Florida – **magically above the law**. The Governor and his Cabinet came down from Tallahassee. TV crews were in attendance, along with Florida's most eminent civic leaders. Right on schedule, the curtains parted. On the screen, Walt Disney gave his much beloved, self-deprecating smile, **then announced that in Florida he was going to create a new kind of America, not just a theme park**.

There would "be no landowners, and therefore no voter control," Disney responded, when asked how he planned to maintain control . . .

Last But Not Least . . . Some Final Tidbits

Ambush at the COMEX Corral http://www.fourwinds10.net/siterun_data/business/currency/news.php?q=1366246141

And the following from one of my favorite authors, John Kaminski:

The real terror is the law

http://www.fourwinds10.net/siterun_data/government/war/terrorism_war/news.php?q=1367185315

The New Welfare Map http://www.fourwinds10.net/siterun_data/business/economy/news.php?q=1365434795

These 11 States now have More People on Welfare than they do Employed!

Last month, the Senate Budget Committee reports that in fiscal year 2011, between food stamps, housing support, child care, Medicaid and other benefits, the average U.S. household below the poverty line received $168.00 a day in government support. What's the problem with that much support? Well, the median household income in America is just over $50,000, which averages out to $137.13 a day.

To put it another way, being on welfare now pays the equivalent of $30.00 an hour for a 40-hour week, while the average job pays $25.00 an hour.

Maryland Democratic Governor Martin O'Malley has instituted a tax on citizens for the amount of rain that falls on their property.

http://www.breitbart.com/Big-Government/2013/04/10/Maryland-governor-taxes-rain

The tax, officially known as a "**storm water management fee**," will be enforced in nine of the state's counties. The state legislature passed it in 2012 purportedly to "raise revenue to cleanup [sic] the Chesapeake Bay," according to MarylandReporter.com.

Former 2012 GOP U.S. Senate candidate Dan Bongino bashes the tax in a Wednesday afternoon press release. The law "**requires individuals, businesses, and even charitable organizations and houses of worship to pay a tax based on the amount of rain that falls on their property and the 'impervious surfaces' on their land**," he says. **Well folks . . . that's about as sick as it gets in this world of legislative tyranny!**

The tax, mandated by the EPA and enforced locally, will be calculated "through satellite surveillance of your property," the statement claims.

Bongino blasts "out of touch political aristocrats in Maryland will do anything to diminish your economic liberty and starve your wallet while padding theirs."

According to the conservative organization Change Maryland, the rain tax will cost Marylanders about $300 million annually.

Governor O'Malley famously tried increasing taxes to balance the state's budget with little success in 2007. The increase in the top marginal tax rate, known as a "millionaire's tax," cost Maryland $1.7 billion in lost tax revenue, according to Change Maryland. Between 2007 and 2010, the state population suffered a net loss of 31,000 people.

Photo: Capital News Service

About The 'Budget' Lie . . .

To understand why political 'budgets' are a **HOAX** . . . please watch at least the first 25 minutes of this film about:

How the Fascist (Corporate-Government) Syndicate who, while taxing you into oblivion, are stealing, pocketing and/or using your money as its 'power base'. Take the time to learn about America's REAL VAST HIDDEN wealth.

America's Enormous Hidden Wealth ~ How to Take Your Country Back
http://www.stopthenorthamericanunion.com/videos/AmericasHiddenWealthCAFR.html#Title (2:16:14)

If you are reading and sharing this information ~ you are part of the resistance!

Daneen G. Peterson, Ph.D.

Researcher, Author and Founder

http://www.StopTheNorthAmericanUnion.com