GlobalResearch
Center for Research on Globalization

The NSA Is Building the Country's Biggest Spy Center, "Watch What You Say"

By James Bamford
Global Research, June 09, 2013
wired.com 3 March 2012

***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.

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.

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."

For the NSA, overflowing with tens of billions of dollars in post-9/11 budget awards, the cryptanalysis breakthrough came at a time of explosive growth, in size as well as in power. Established as an arm of the Department of Defense following Pearl Harbor, with the primary purpose of preventing another surprise assault, the NSA suffered a series of humiliations in the post-Cold War years. Caught offguard by an escalating series of terrorist attacks—the first World Trade Center bombing, the blowing up of US embassies in East Africa, the attack on the USS *Cole* in Yemen, and finally the devastation of 9/11—some began questioning the agency's very reason for being. In response, the NSA has quietly been reborn. And while there is little indication that its actual effectiveness has improved—after all, despite numerous pieces of evidence and intelligence-gathering opportunities, it missed the near-disastrous attempted attacks by the underwear bomber on a flight to Detroit in 2009 and by the car bomber in Times Square in 2010—there is no doubt that it has transformed itself into the largest, most covert, and potentially most intrusive intelligence agency ever created.

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.

<img src="/threatlevel/wp-content/gallery/20-04/ff_nsadatacenter2_f.jpg" alt="Utah Data Center">

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, mixing with a weeklong coating of heavy gray smog. Red air alerts, warning people to stay indoors unless absolutely necessary, had become almost daily occurrences, and the temperature was in the bone-chilling twenties. "What I smell and taste is like coal smoke," complained one local blogger that day. At the city's international airport, many inbound flights were delayed or diverted while outbound regional jets were grounded. But among those making it through the icy mist was a figure whose gray suit and tie made him almost disappear into the background. He was tall and thin, with the physique of an aging basketball player and dark caterpillar eyebrows beneath a shock of matching hair. 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.

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.

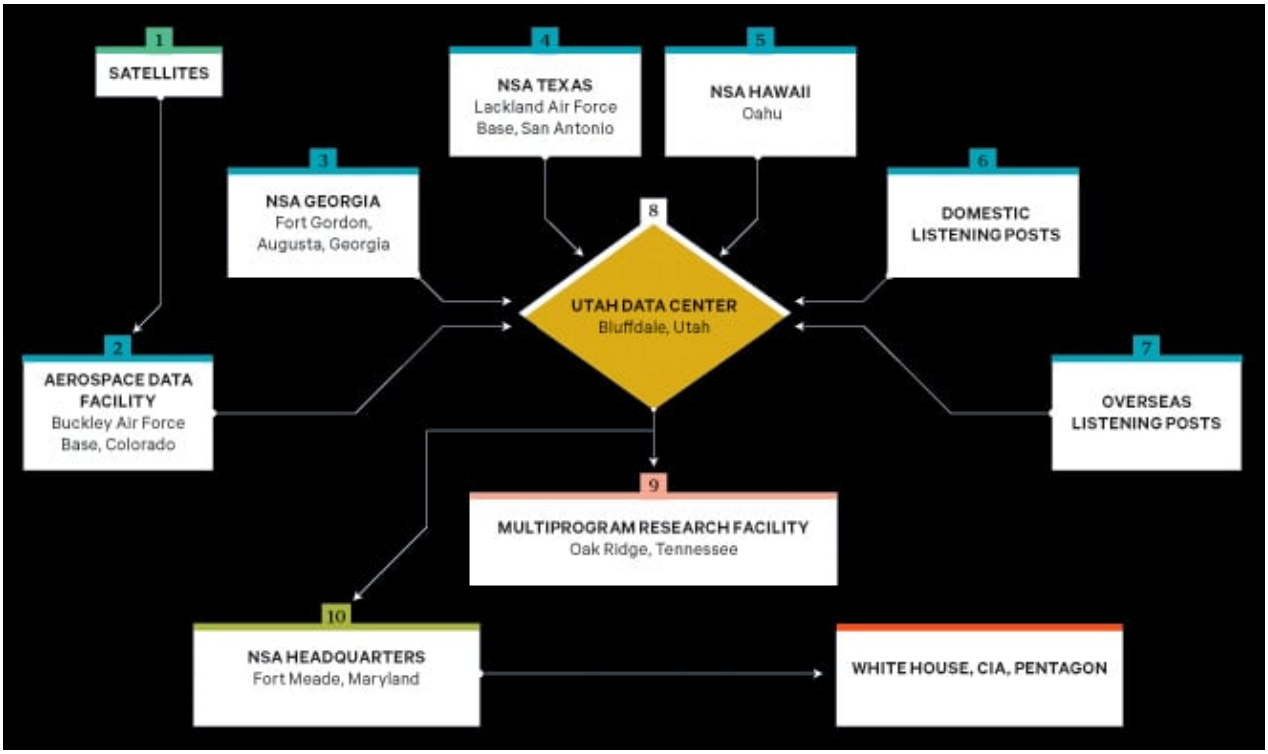
Given the facility's scale and the fact that a terabyte of data can now be stored on a flash drive the size of a man's pinky, the potential amount of information that could be housed in Bluffdale is truly staggering. But so is the exponential growth in the amount of intelligence

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 SPY NETWORK



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.

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 auto

mating 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.”

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.

But there is, of course, reason for anyone to be distressed about the practice. Once the door is open for the government to spy on US citizens, there are often great temptations to abuse that power for political purposes, as when Richard Nixon eavesdropped on his political enemies during Watergate and ordered the NSA to spy on antiwar protesters. Those and other abuses prompted Congress to enact prohibitions in the mid-1970s against domestic spying.

Before he gave up and left the NSA, Binney tried to persuade officials to create a more targeted system that could be authorized by a court. At the time, the agency had 72 hours to obtain a legal warrant, and Binney devised a method to computerize the system. "I had proposed that we automate the process of requesting a warrant and automate approval so we could manage a couple of million intercepts a day, rather than subvert the whole process." But such a system would have required close coordination with the courts, and NSA officials weren't interested in that, Binney says. Instead they continued to haul in data on a grand scale. Asked how many communications—"transactions," in NSA's lingo—the agency has intercepted since 9/11, Binney estimates the number at "between 15 and 20 trillion, the aggregate over 11 years."

When Barack Obama took office, Binney hoped the new administration might be open to reforming the program to address his constitutional concerns. He and another former senior

NSA analyst, J. Kirk Wiebe, tried to bring the idea of an automated warrant-approval system to the attention of the Department of Justice's inspector general. They were given the brush-off. "They said, oh, OK, we can't comment," Binney says.

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. Anyone—from terrorists and weapons dealers to corporations, financial institutions, and ordinary email senders—can use it to seal their messages, plans, photos, and documents in hardened data shells. For years, one of the hardest shells has been the Advanced Encryption Standard, one of several algorithms used by much of the world to encrypt data. Available in three different strengths—128 bits, 192 bits, and 256 bits—it's incorporated in most commercial email programs and web browsers and is considered so strong that the NSA has even approved its use for top-secret US government communications. Most experts say that a so-called brute-force computer attack on the algorithm—trying one combination after another to unlock the encryption—would likely take longer than the age of the universe. For a 128-bit cipher, the number of trial-and-error attempts would be 340 undecillion (10^{36}).

Breaking into those complex mathematical shells like the AES is one of the key reasons for the construction going on in Bluffdale. That kind of cryptanalysis requires two major ingredients: super-fast computers to conduct brute-force attacks on encrypted messages and a massive number of those messages for the computers to analyze. The more messages from a given target, the more likely it is for the computers to detect telltale patterns, and Bluffdale will be able to hold a great many messages. "We questioned it one time," says another source, a senior intelligence manager who was also involved with the planning. "Why were we building this NSA facility? And, boy, they rolled out all the old guys—the crypto guys." According to the official, these experts told then-director of national intelligence Dennis Blair, "You've got to build this thing because we just don't have the capability of doing the code-breaking." It was a candid admission. In the long war between the code breakers and the code makers—the tens of thousands of cryptographers in the worldwide computer security industry—the code breakers were admitting defeat.

So the agency had one major ingredient—a massive data storage facility—under way. Meanwhile, across the country in Tennessee, the government was working in utmost secrecy on the other vital element: the most powerful computer the world has ever known.

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.

In 2004, as part of the supercomputing program, the Department of Energy established its Oak Ridge Leadership Computing Facility for multiple agencies to join forces on the project. But in reality there would be two tracks, one unclassified, in which all of the scientific work would be public, and another top-secret, in which the NSA could pursue its own computer covertly. "For our purposes, they had to create a separate facility," says a former senior NSA computer expert who worked on the project and is still associated with the agency. (He is one of three sources who described the program.) It was an expensive undertaking, but one the NSA was desperate to launch.

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. The NSA's machine was likely similar to the unclassified Jaguar, but it was much faster out of the gate, modified specifically for cryptanalysis and targeted against one or more specific algorithms, like the AES. In other words, they were moving from the research and development phase to actually attacking extremely difficult encryption systems. The code-breaking effort was up and running.

The breakthrough was enormous, says the former official, and soon afterward the agency pulled the shade down tight on the project, even within the intelligence community and Congress. "Only the chairman and vice chairman and the two staff directors of each intelligence committee were told about it," he says. The reason? "They were thinking that this computing breakthrough was going to give them the ability to crack current public encryption."

In addition to giving the NSA access to a tremendous amount of Americans' personal data, such an advance would also open a window on a trove of foreign secrets. While today most sensitive communications use the strongest encryption, much of the older data stored by the NSA, including a great deal of what will be transferred to Bluffdale once the center is complete, is encrypted with more vulnerable ciphers. "Remember," says the former intelligence official, "a lot of foreign government stuff we've never been able to break is 128 or less. Break all that and you'll find out a lot more of what you didn't know—stuff we've already stored—so there's an enormous amount of information still in there."

The 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.

But the real competition will take place in the classified realm. To secretly develop the new exaflop (or higher) machine by 2018, the NSA has proposed constructing two connecting buildings, totaling 260,000 square feet, near its current facility on the East Campus of Oak Ridge. Called the Multiprogram Computational Data Center, the buildings will be low and wide like giant warehouses, a design necessary for the dozens of computer cabinets that will compose an exaflop-scale machine, possibly arranged in a cluster to minimize the distance between circuits. According to a presentation delivered to DOE employees in 2009, it will be an "unassuming facility with limited view from roads," in keeping with the NSA's desire for secrecy. And it will have an extraordinary appetite for electricity, eventually using about 200 megawatts, enough to power 200,000 homes. The computer will also produce a gargantuan amount of heat, requiring 60,000 tons of cooling equipment, the same amount that was needed to serve both of the World Trade Center towers.

In the meantime Cray is working on the next step for the NSA, funded in part by a $250 million contract with the Defense Advanced Research Projects Agency. It's a massively parallel supercomputer called Cascade, a prototype of which is due at the end of 2012. Its development will run largely in parallel with the unclassified effort for the DOE and other partner agencies. That project, due in 2013, will upgrade the Jaguar XT5 into an XK6,

codenamed Titan, upping its speed to 10 to 20 petaflops.

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.*
