IT WAS RAINING IN THE DATA CENTER

by
Everest Pipkin
Bachelor of Fine Art in Studio Art, University of Texas at Austin, 2013

Thesis
Submitted in Partial Fulfillment of the Requirements of the Degree of
MASTERS OF FINE ART
in
ART
at Carnegie Mellon University

Pittsburgh, Pennsylvania

Approved By:

_____
Rich Pell, Project Advisory Committee Chair

_____
Angela Washko, Project Advisory Committee Member

_____
Christopher Warren, Project Advisory Committee Member

_____
Jon Rubin, MFA Program Director

_____
Charlie White, Head of the School

_____
Dan Martin, Dean, College of Fine Arts

Date Degree Conferred: May, 2018

Abstract —

Stemming from a 2011 incident inside of a Facebook data facility in which hyper-cooled air formed a literal (if somewhat transient) rain cloud in the stacks, *It was raining in the data center* examines ideas of non-places and supermodernity applied to contemporary network infrastructure.

It was raining in the data center argues that the problem of the rain cloud is as much a problem of psychology as it is a problem of engineering. Although humidity-management is a predictable snag for any data center, the cloud was a surprise; a self-inflicted side-effect of a strategy of distance. The rain cloud was a result of the same rhetoric of ephemerality that makes it easy to imagine the inside of a data center to be both everywhere and nowhere.

This conceit of internet data being placeless shares roots with Marc Augé's idea of non-places (airports, highways, malls), which are predicated on the qualities of excess and movement. Without long-term inhabitants, these places fail to tether themselves to their locations, instead existing as a markers of everywhere. Such a premise allows the internet to exist as an other-space that is not conceptually beholden to the demands of energy and landscape. It also liberates the idea of 'the network' from a similar history of industry. However, the network is deeply rooted in place, as well as in industry and transit.

Examining the prevalence of network overlap in American fiber-optic cabling, it becomes easy to trace routes of cables along major US freight train lines and the US interstate highway system. The historical origin of this network technology is in weaponization and defense, from highways as a nuclear-readiness response to ARPANET's Pentagon-based funding. Such a linkage with the military continues today, with data centers likely to be situated near military installations— sharing similar needs electricity, network connectivity, fair climate, space, and invisibility.

We see the repetition of militarized tropes across data structures. Fiber-optic network locations are kept secret; servers are housed in cold-war bunkers; data centers nest next to military black-sites. Similarly, Augé reminds us that non-places are a particular target of terrorism, populated as they are with cars, trains, drugs and planes that turn into weapons. When the network itself is at threat of weaponization, the effect is an ambient and ephemeral fear; a paranoia made of over-connection.

Table of Contents

It was raining in the data center—

Prineville, Oregon, 2011—

In August of 2011, Jay Parikh, the Vice President of Infrastructure Engineering at Facebook received a call. As Parikh recounted to *The Register* in June of 2013, he remembered the conversation going something like this;

"'Jay, there's a cloud in the data centre,'

'What do you mean, outside?'

'No, inside.'

… It was raining in the data center."

Data centers house servers and other networked computer equipment in large warehouses, storing a large percentage of the information on the internet. They also provide the computational power necessary to support 'cloud computing', a system of distributed resources that lets a user off-load computational tasks. Predictably, data centers produce a remarkable amount of heat, with power use densities over 100 times that of a normal office building. The cost of air-conditioning alone can be immense, but without full-time climate control the racks of equipment would critically overheat in a matter of minutes.

The Prineville, Oregon Facebook facility was new, and had been built with a chiller-less air conditioning system, which promised to be more energy efficient than traditional cooling systems by using outside air.

From the official Facebook report:

“This resulted in cold aisle supply temperature exceeding 80°F and relative humidity exceeding 95%. The Open Compute servers that are deployed within the data center reacted to these extreme changes. Numerous servers were rebooted and few were automatically shut down due to power supply unit failure.”

Data centers are arranged in alternating ‘hot’ and ‘cold’ rows, with the cold rows generally serving as human-access points, where the hot rows are generally for fan exhaust. The ‘extreme changes’ described in the report above were caused by an accidental feedback loop of high temperature and low humidity air from the hot rows entering a water-based evaporative cooling system. When this air returned to the servers on the cold rows, it was so wet that it condensed. A cloud was raining on the cloud.

Parikh continued; “For a few minutes, you could stand in Facebook's data center and hear the pop and fizzle of Facebook's ultra-lean servers obeying the ultra-uncompromising laws of physics.”

There are multiple reasons for this formation of the cloud (and subsequent failure of servers), and Facebook went on to amend its official guidelines to guarantee a lower inside humidity, and recommended a rubber seal around all power-supplies— effectively water-proofing them from any future weather systems. But managing humidity in data centers has always been a puzzle, and Facebook’s complete oversight of the increased complexity that comes from using outside air seems unlikely.

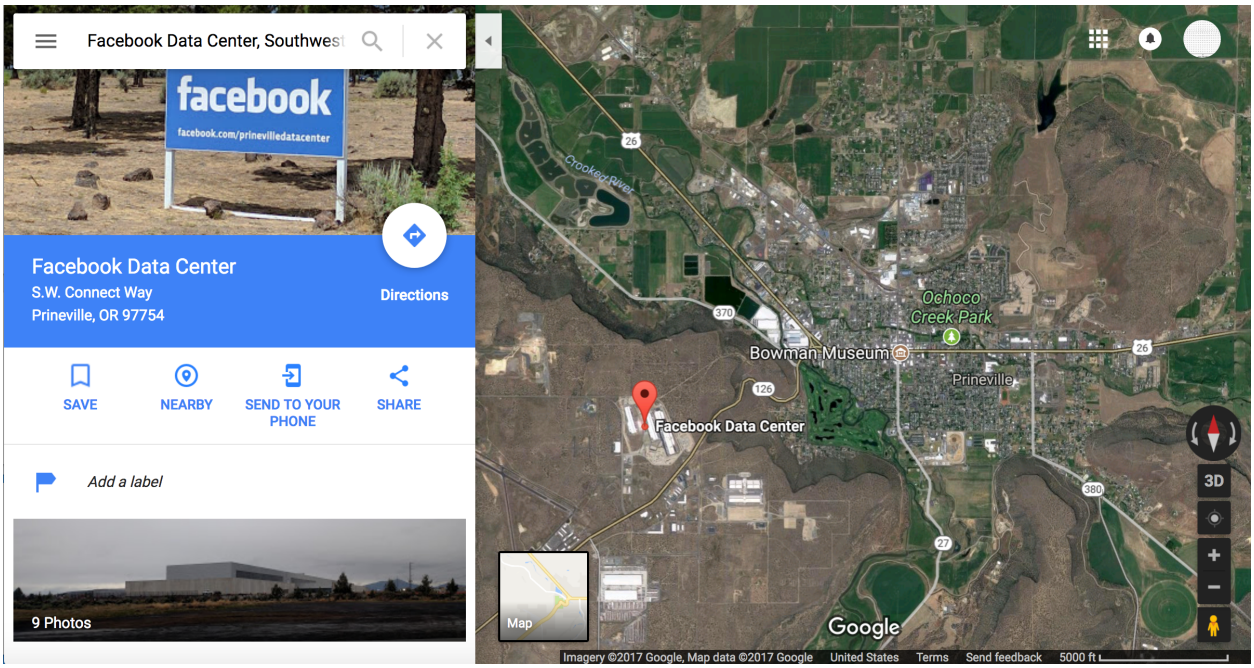
Fundamental to this weather event was this usage of a new type of cooling system (the chiller-less system) which had broken the hermetic seal of the server farm. Suddenly the building was not set apart from the outside environment— instead, it was

breathing, exchanging air with the local climate. The Prineville facility was built complete with intake and outtake vents, which granted it a porosity somewhat unique in 2011. It may not have been the first data center to be tethered to the outside world in such a way (chiller-less cooling was new, but not unheard of) but it was the biggest. It is almost certainly the only one to reproduce a local weather pattern from outside humidity, and perhaps subsequently it is also among the first to be located so severely in its geography.

Of course, no data center is truly absent from its locale; the Prineville facility is also connected to the Prineville electric grid; Prineville locals drive their cars to work and park under the Prineville sky before heading in to monitor the stacks; the data center is visible from Google Maps as distinctly inside of Prineville (at the time of writing, it had a respectable 4.3 star rating on the service). But every data center is also *everywhere,* serving data that escapes its geographic confines at a dizzying speed, populating packets that circle the globe with little care to origin. The information that comprises our websites, email storage, and personal photographs— as well as the computational power that generates our map routes, friend requests, and predictive text— doesn't *feel* like it is coming from Prineville, or Switzerland, or the Faroe Islands. It feels present, palpably *right there*— always.

In *Non-Places: Introduction to an Anthropology of Supermodernity*, Marc Augé describes non-places as a space of hypermodernity, which are predicated on the quality of excess. Non-places do not have history, but are instead places built to be passed through (for example; malls, highways, and airports). They are abstracted places of capital and transit, as well as contract. Although data centers are generally closed to

human traffic, if we consider the information that moves through them as *truly transitory*, a data center may be the ultimate non-place; even the colloquial term 'information super-highway' points at such a system. These places fail to tether themselves to their locations, instead existing as a marker or symbol of everywhere.



The Prineville facility as seen via satellite, 2017.

The problem of the rain cloud (and its element of surprise as it briefly decimated a section of Facebook's equipment racks) is therefore as much a problem of psychology as it is a problem of engineering; like a thunderstorm formed from two opposing weather fronts, the physicality of outside Prineville air met the everywhere-ness of inside space in an impossible, non-Euclidean intersection. Although the rain storm was predictable (climate-control in data centers is a well-studied problem, and Facebook retains engineers who study only this), no one at Facebook saw the cloud coming. I would

argue that this is by design. The rain cloud was a self-inflicted side-effect of a strategy of distance.

Most server farms are rural; Prineville, for example, is a town of roughly 10,000 people in the dead center of Oregon. Other American data centers are even more remote, choosing desert locations in Utah, Idaho, and Nevada. This is due in part to availability of affordable land, energy cost, and the possibility of tax breaks in communities where manufacturing, mining, logging, or other blue-collar jobs have evaporated.

However there is another, subtler reason for the distance; it makes them invisible. Data centers are giant structures, with single buildings sometimes covering as much as 1.1 million square feet. They consume more energy than small cities (Prineville, also home to an Apple facility, cannot support further development on its current power grid). Furthermore, much of this energy consumption is generated by coal — even 'green companies' will often buy carbon offset credits rather than invest in the energy storage required for 24/7 solar or wind power.

The immensity and environmental costliness of server farms are undeniably bad optics, especially for an industry so committed to a vision of self that rests in futurity, promoting a high-tech potential that has nothing to do with the industrial revolution (and all of the pollution and disaffective labor of that era). Instead, the rhetoric of the internet, and especially *storage* on the internet, is that of a light, ephemeral place that requires neither work nor coal nor landscape to hold itself up. It is supposed to be a cloud.

Such a premise allows the internet to exist as an other-space that *while physically extant* is conceptually not beholden to the requisite laws of physics that

demand energy to be consumed, or work to be done, for it to function. It also liberates the idea of 'the network' from a similar history of industry. Because the last— and most important— thing that every server farm needs, even beyond abundant power and space and tax breaks, is connectivity.

There is one other aspect to Prineville that made it an ideal location for Facebook's facility. In 1911, when railroads were connecting the rural towns of central Oregon, Prineville seemed slated to be forgotten. Headed south from The Dalles, the main rail line bypassed the municipality (which was as much a death sentence for a town in 1911 as a new interstate route cutting around an old business district is in 2017). In a 1917 election however, Prineville residents voted 355 to 1 to construct a connection to the main rail line 19 miles away. Run by the city, this railroad has served mostly as a commercial link for the lumber industry. More importantly, however, the publicly-owned rail line means that the City of Prineville retained ownership of the land *under* the rail, a non-interrupted connection to the major industrial lines of the railroad (and later highway) that the Prineville line connects to.

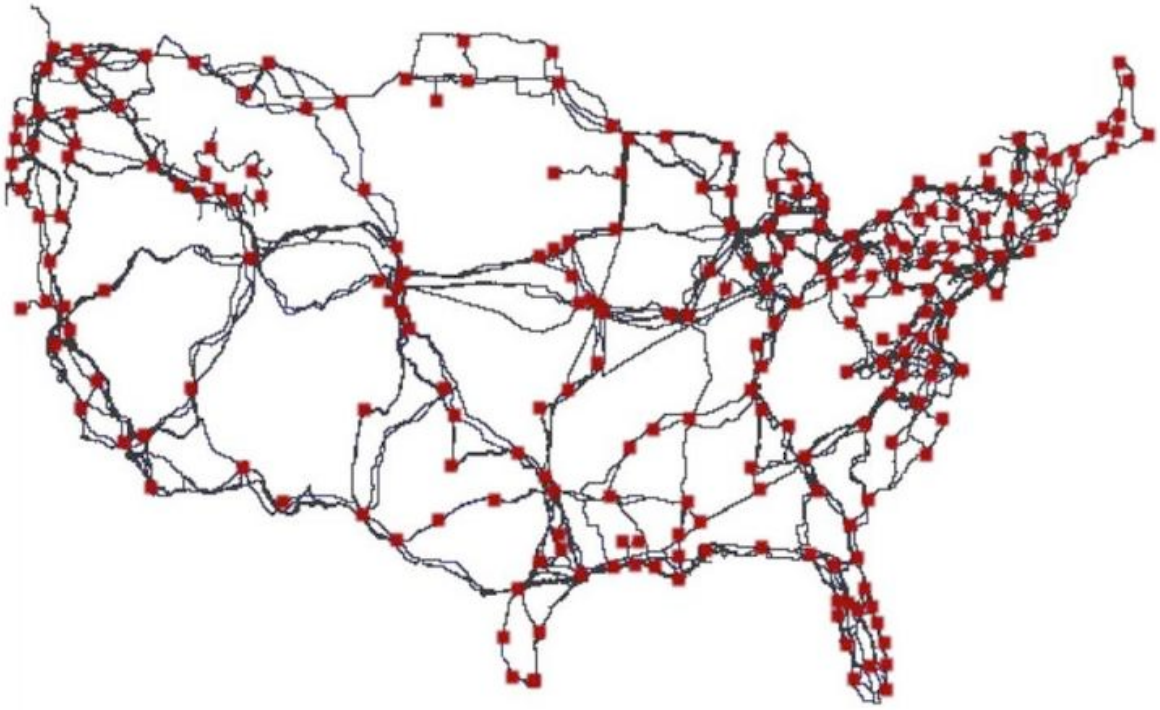
The City of Prineville Railroad spur, in bold

Although the actual paths of fiber-optic cables are considered state and company secrets, it is not unlikely that most or all of the Facebook facility's data runs along this route. In *The Prehistory of the Cloud*, Tung-Hui Hu describes the origin of private data service with telecommunications giant Sprint (Southern Pacific Railroad Internal Network), which sold excess fiber-optic bandwidth along train lines to consumers beginning in 1978. He goes on to state in the same text, that "virtually all traffic on the US Internet runs across the same routes established in the 19th century".

Contemporary fiber-optic retraces the same routes of older infrastructure, buried in or along railroads, highways, telephone lines, utility service byways and subway tunnels. Such a reuse of linear connective tissue is obvious, and almost banal— except when one stops to consider that such information is virtually nonexistent publicly and that any attempt to gain access to American internet infrastructure records is liable to engender a stern rebuff.

A 2015 paper titled *InterTubes: A Study of the US Long-haul Fiber-optic Infrastructure* led by Paul Barford at the University of Wisconson confirms this, stating that *"*despite some 20 years of research efforts that have focused on understanding aspects of the Internet's infrastructure such as its router-level topology… very little is known about today's physical Internet where individual components such as cell towers, routers or switches, and fiber-optic cables are concrete entities with well-defined geographic locations". The 4-year effort used public records from federal, state, and municipal agencies, as well as commercial documentation in the form of advertisement, rights-of-way information, environmental impact studies, and interstate fiber sharing

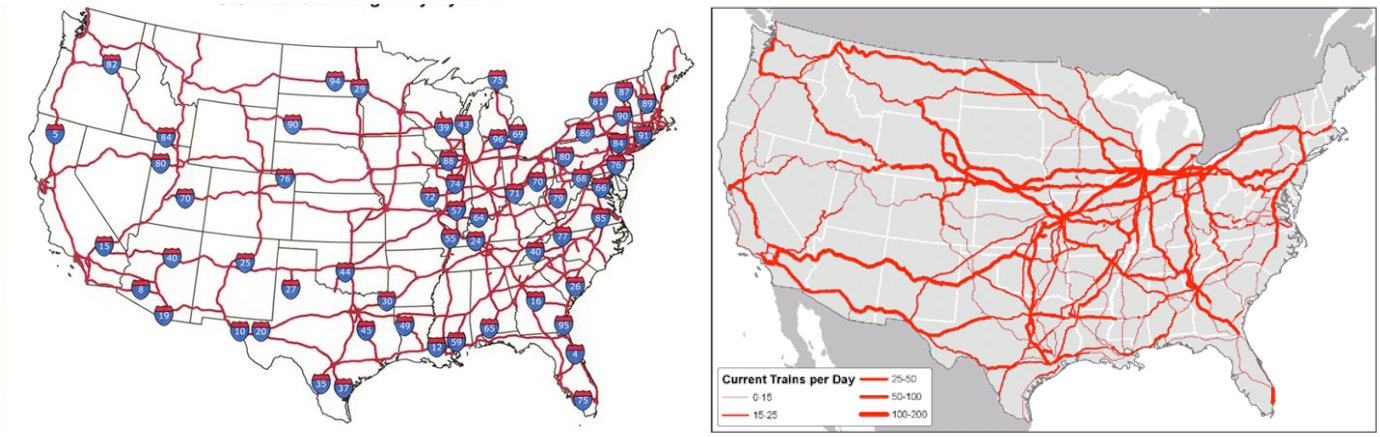
arrangements from various states' transportation departments. The final map (the first of its kind) contains 273 city nodes, 2,411 links, and 542 conduits.



Long-haul fiber-optic cabling. Red squares mark where cables connect in nodes, many in major population centers. University of Wisconsin and ACM SIGCOMM, 2015.

When looking at the map it is easy to see that the Northeast and coastal areas are remarkably dense with nodes, but long-haul cabling thins in the middle of the country in favor of hubs like Denver and Salt Lake City. Furthermore, there are cabling lines that follow almost-identical routes from node-to-node, hinting at corporate competition. Finally, some of the lines do not connect to nodes, but rather end in dead-end spurs; these are particularly prominent in the Northwest, where the Prineville data center (and so many others like it) is located.

Although the overlap is not surprising, it is worth comparing this map of network nodes to both a map of major US freight train lines and the US interstate highway system. Between the two transit maps, one can follow almost every cabling line from node-to-node. The usage of rail and highway network to support contemporary fiber is all but confirmed.



A map of the United States Interstate (left, OnlineAtlas.us) and major freight lines (right, National Surface Transportation Policy) appear remarkably similar to the map of fiber-optic nodes.

Such a discovery would be nothing more than an interesting anecdote outside of commercial repercussions if it were not for the societal complication of historical infrastructure in the United States. Train lines in American society are inextricably linked to ideas of the frontier, the horizon, manifest destiny and potential wealth. The later highway system similarly became synonymous with ideas of freedom, the open road, and the American dream. They have also always been a methodology of conquest, or a fear-response to war. Train lines once cut across indigenous land, carrying supplies, soldiers, and settlers to make this already-lived-in landscape into America. Developed

as part of a nuclear defense network, highway systems were intended to carry civilians out of cities and the military in. (They had the side-effect of catalyzing suburbs while cutting off or running around rural communities.)

The internet and the computer's basis is also in weaponry. If there is any single invention that has had the greatest influence on contemporary computation, it was likely the atomic bomb; and the paranoia-response to this threat tied the network into issues of security (and civilian technological discovery) from the beginning.

* * *

A military-technological apparatus —

50-odd years ago, in a top-secret Cold War think-tank, members of the RAND Corporation were tasked with a problem. The problem was this: In the event of a nuclear war with The Soviet Union (and the possible collapse of the American Government) how were any remaining US authorities to communicate in order to launch counter-attacks?

Nuclear bombs are likely to disrupt relay stations and cabling, no matter how deeply buried or well armored, and command centers are instant targets. The need for a decentralized network without large headquarters seemed obvious, but few communication systems had been built without centers. Designing for this issue, RAND instead proposed a network made of nodes, each with equal authority to send, receive, or originate messages. The messages would be cut up into tiny bits— packets— which would find separate paths through the system of connected parts, haphazardly tossed from node to node until all of the packets arrived at their destination, and the original message could be seen. This was not a particularly efficient system, but was quite rugged— large sections of the networked landscape could be missing, and the packets would eventually find their way.

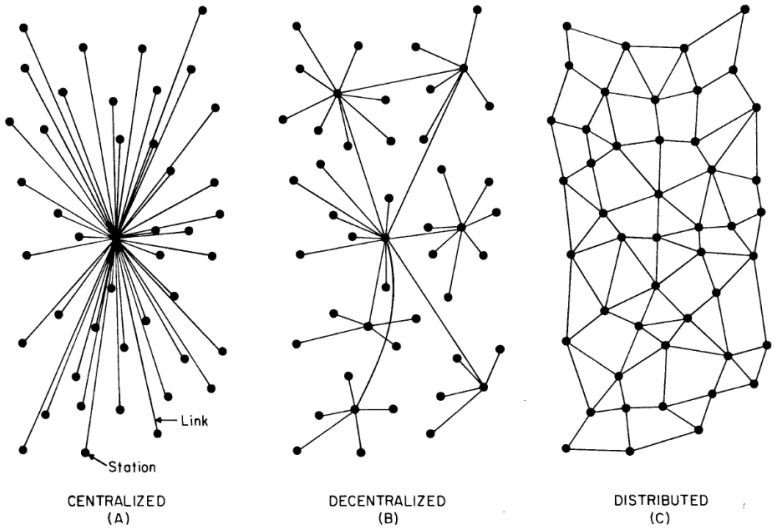


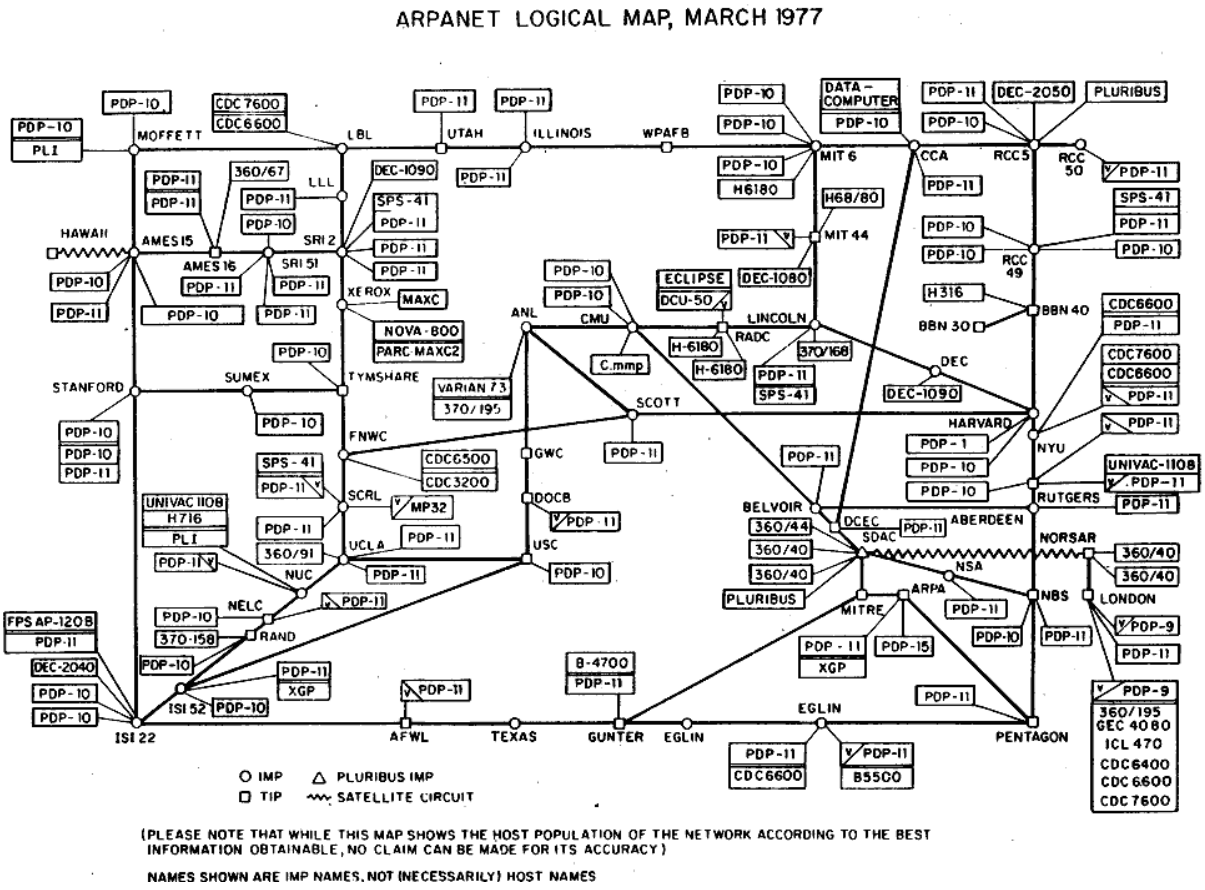
FIG. 1 — Centralized, Decentralized and Distributed Networks

Paul Baran, "On Distributed Communications Networks", RAND Corporation

Although the original distributed node proposal (image C) was not actually enacted (see our examination of cabling running along existing networks, something that looks much more like the decentralized image B), The Pentagon's Advanced Research Projects Agency funded a version of the RAND proposal called ARPANET, which linked University supercomputers in a test-run of the linked, packet-based communication. There seems to some uncertainty about whether ARPANET was actually funded as a nuclear-response system. Stephen J. Lukasik, Director of DARPA from 1967 to 1974, expressly stated that "the goal was to exploit new computer technologies to meet the needs of military command and control against nuclear threats, achieve survivable control of US nuclear forces, and improve military tactical and management decision making," while Charles Herzfeld, ARPA Director from 1965 to 1967, claimed "the ARPANET was not started to create a Command and Control System that would survive a nuclear attack, as many now claim. To build such a system was, clearly, a major military need, but it was not ARPA's mission to do this; in fact, we would have been severely criticized had we tried."

This uncertainty around the use and functionality of the fledgling ARPANET- which served variably as weapon, communication tool, and toy- may have had something to do with its growth. By 1972, there were 37 nodes in the system; by 1983, the year ARPANET adopted TCP/IP protocols, it had 113 nodes. Still, this was fundamentally a military network, despite the prevalence of goofy university email. A 1982 handbook on computing at MIT warned; "It is considered illegal to use the ARPANet for anything which is not in direct support of Government business ... personal messages to other ARPANet subscribers (for example, to arrange a get-together or check and say a

friendly hello) are generally not considered harmful ... Sending electronic mail over the ARPANet for commercial profit or political purposes is both anti-social and illegal. By sending such messages, you can offend many people, and it is possible to get MIT in serious trouble with the Government agencies which manage the ARPANet."



ARPANET logical map, March 1977, The Computer History Museum

Perhaps in response to the prevalence of pot-luck invitations, in 1984 the military moved their own network to a private system (MILNET), with controlled gateways connecting the two networks. ARPANET was suddenly reduced by 68 nodes, but was also unrestricted for public use. Although the military retained operation of ARPANET until its closure in 1990, a number of private companies and internet service providers (and thousands of individuals) entered the field with the establishment of the National

Science Foundation Network (NSFNet) in 1986. In the United States, the internet was fully commercialized in 1995 with the decommission of NSFNet, which removed the last restrictions on the carriage of commercial traffic. Throughout all of this, the fundamental principle of the information-packet, which is routed through a decentralized system of nodes, remained more-or-less unchanged.

Of course, much of the technological development of the last century has been a consequence of war (or war-time anxiety) and the same argument could be made for many advances in seemingly-civilian development like transit, food technologies, and medicine. But the internet— and the computers that provide both portal and support to this network— are inextricably militaristic.

In *Turing's Cathedral*, George Dyson examines the origin of digital spaces by looking at a Princeton super-group led by John von Neumann. Because nuclear weapons cannot be built via trail-and-error, the group was tasked with building a computer that could run simulations of blast waves, detonations, and destructive effects. The first true computer— built on an IAS system— was tested in 1951, "with a thermonuclear calculation that ran for 60 days nonstop." (A small side-note regarding this simulation; much like our data center cloud, the high humidity of a Princeton summer once caused the early computer's air-conditioning units to freeze over, pausing a simulation of atomic heat in deference to the physical problem of de-icing.)

So began the race to build twin technological spires of ever-more-powerful new weapons, and the ever-more-powerful computers necessary to monitor and model their use and effects.

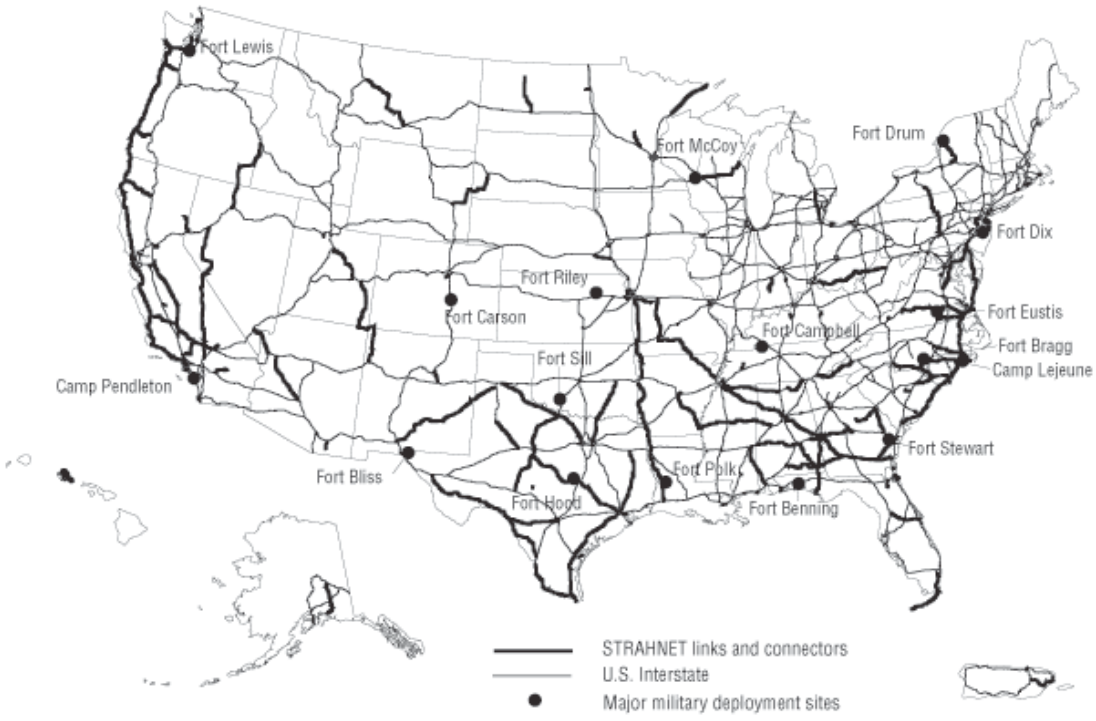
Although the military has been using its own networks for decades now, data centers are still likely to be situated near military installations. This is in part due to similar technical needs— those of electricity, network connectivity, fair climate, and considerable space— but also remind us of the shared desire of both corporate industry and the military for invisibility and secrecy.

A National Guard Armory and testing range that sits next to the Prineville Facebook facility, as seen via satellite, 2017.

* * *

A hollowing out —

In 1956, President Eisenhower established the National System of Interstate and Defense Highways. Formalized into the US Insterstate Highway System and a defense network called STRAHNET (The Strategic Highway Network, named in 1981), these roads serve as a “key deterrent in United States strategic policy”. The Federal Department of Transportation describes STRAHNET as providing “defense access, continuity, and emergency capabilities for movements of personnel and equipment in both peace and war… STRAHNET roadways are those which would be used for the rapid mobilization and deployment of armed forces in the event of war or peacekeeping activity.”

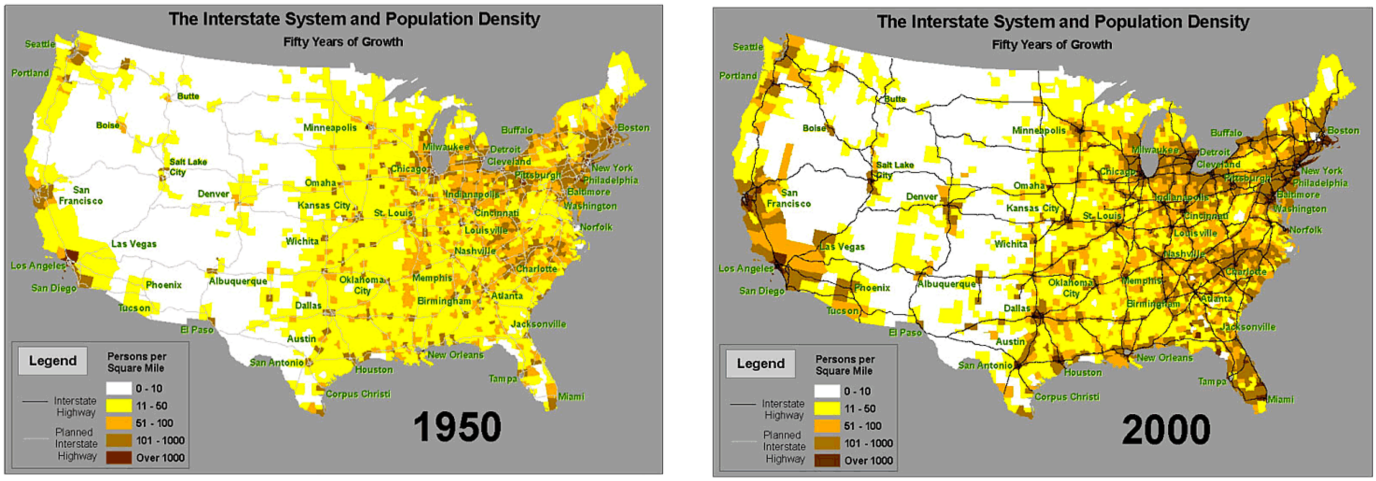


STRAHNET, Wikimedia Commons.

This came at the height of Cold War paranoia, only a few years before the ARPANET proposal that would become our fledgling internet. In many ways, the

actualization of ARPANET was tied to these new highways; they provided federally-controlled byways that cut across what was a formerly state-controlled (and highly variable) system. These roads- which formed governmental linkages between military installations and major population centers- followed exactly the same routes that this initial internet needed to provide connections between university researchers, the military, and the public. It should come as no surprise that our contemporary fiber-optic structure still follows these initial lines.

The establishment of the National System of Interstate and Defense Highways also restructured the placement of the American population, with a shift from a distributed network of small, spatially consistent nodes centered on the North East to a centralized system that prioritized large cities and their resultant sprawl, often in the 'Sunbelt' region of the Mid and South West.



Interstate Density Map from The Federal Highway Administration.

A 1994 West Virginia University study published in *Regional Science and Urban Economics,* Terance Rephann and Andrew Isserman concluded that despite increased connectivity, "the results show that the beneficiaries of the interstate links in terms of

economic growth are interstate counties in close proximity to large cities or having some degree of prior urbanization, such as a city with more than 25,000 residents. Rural interstate and off-interstate counties exhibit few positive effects."

These new highways often cut off communities quite literally, with whole stretches of older state routes suddenly going untrafficked. This can be perfectly visualized along old California Route 66 through the Mohave, which was circumnavigated by the new Interstate I-40. Taking this route, one passes through ghost town after ghost town. With names like Ibis, Bannock, Homer, Goffs, Ludlow, Fenner, Essex, Danby, Chambless, Calico and Summit, each sports a few crumbling road-side structures, a marker on Google Maps, and little more. More commonly, old routes are repurposed as frontage roads or business loops, and town centers are repurposed to serve the needs of the highway— orienting outwards to provide chain gas stations, motels, and fast food to travelers. This kind of commerce- a commerce of anywhere- is a totem of Augé's idea of the non-place. They are the kind of places that are easy to ignore, or to forget.

For our data centers, these places are perfect. Here, cut-out and passed-over, data centers proliferate along utility and fiber-optic routes that bring them power and connectivity while allowing them to be invisible. They sink into a landscape of chain stores and unmarked warehouses, unseen.

* * *

The underground waterfall —

Perhaps the most famous data center is Pionen, located in a nuclear bunker from the Cold War below Stockholm that serves at the headquarters for Bahnhof, which once hosted Wikileaks. Buried under 100 feet of granite and protected by a 40 centimeter-thick steel door that is advertised as 'capable of surviving a hydrogen bomb', Pionen also contains greenhouses, simulated day/night cycles, an aquarium, and a waterfall.

The Pionen data center, as photographed by Bahnhof in 2012.

Pionen, of course, is not hiding in a post-military black-site, but instead the historical bunker is used as both advertisement and distraction. Bahnhof has five other data centers that are far more traditional in their look and scope (as well as their destructibility via nuclear attack). However, it is Pionen that shows up in architectural

magazines and on tech websites, often with titles like “Deep Inside the James Bond Villain Lair That Actually Exists”, and “The world’s most super-designed data center – fit for a James Bond villain”. Pionen is a bait and switch; by designing a plant-filled architectural environment, it promises environmental stewardship; by counting the feet of granite above its head it claims indestructibility; and by treating the *designed* data center as a photo opportunity, it displaces an already fuzzy cultural understanding of what a data center actually *is* into pure fiction.

Returning to *Prehistory of the Cloud*, Hu claims that “the data center remains among the least studied areas of digital culture, with cloud computing producing a layer of abstraction that masks the physical infrastructure of data storage. Paradoxically, then, data centers exist at the border between the dematerialized space of data and the resolutely physical buildings they occupy. Like architecture, data bunkers- and metonymically, the cloud security apparatus of which they are a part— delimit the boundaries between inside and outside.”

Augé, in *Non-Places: Introduction to an Anthropology of Supermodernity,* states*;* “Since non-places are there to be passed through, they are measured in units of time. Itineraries do not work without timetables… They are lived through in the present.” The ‘present’ of a data center is a remarkably small unit of time; with constant information exchange at the literal speed of light, what was physically present only a moment ago is not what is physically present now, or in the very near future. Each packet of traveling information follows a strict contractual obligation, a programmed ruleset that requires it to declare itself upon arrival and departure, much like Augé’s

tourists and travelers. Arrival and departure are nearly simultaneous. Data forms an ultimate now, a now that is beyond the scope of unaided human perception.

This hyper-mobility of data in and out of data centers paired with a strict non-access to the average person (with the notable exceptions of marketing-centers like Pionen) creates a line between a realized outside world and a ephemeral inside. This inside, perfectly illustrated by the Prineville facility before the rain-cloud, is both an everywhere and a nowhere. With the breakage of Augé's time-tables and the push to truly momentary, non-human time, the network becomes omnipresent. It is a non-place in the strictest sense; an everyplace.

Why, though, would Bahnhof seek to adopt a nuclear bunker in the first place? Why would an ISP feel the need to advertise itself as a “Bond Villain Lair”?

Augé states that non-places “… are the particular target of all those whose passion for retaining or conquering territory drives them to terrorism. Airports and aircraft, big stores and railway stations have always been a favoured target for attacks (to say nothing of car bombs); doubtless for reasons of efficiency, if that is the right word. But another reason might be that, in a more or less confused way, those pursuing new socializations and localizations can see non-places as only a negation of their ideal. The non-place is the opposite of utopia; it exists, and it does not contain any organic society.”

Despite the relative physical safety of internet infrastructures (they are several magnitudes more likely to be hit by a denial of service attack than a bomb, for example), we see the repetition of militarized tropes across data structures. Fiber-optic network locations are kept secret; servers are housed in cold-war bunkers; data centers nest

next to military black-sites. All are wrapped in barbed wire, and staffed with armed guards.

But for all the promise of well-guarded blueprints and steel blast-doors, the enemy is already inside. The attack of physical infrastructure via the internet is magnitudes likelier- and easier- than an attack of the internet via physical infrastructure. The call is coming from inside the house.

On December 23rd, 2015, three separate Ukrainian power companies experienced “destructive events” in their regional centers, cutting off electricity for hundreds of thousands of homes. The power wasn't out long- no more than six hours- but inspired a national panic. The attack relied on a fairly common malware called BlackEnergy, which generally is used for corporate espionage but also allows a remote user to control a local computer’s operation. The workers on shift described watching their cursors move of their own accord, unresponsive to the mouse, taking breaker after breaker offline.

The attack could have been significantly more destructive- although the hackers overwrote firmware that required the power plants to transition to manual control, no actual hardware was damaged. In the cold Ukrainian winter, a power outage of even 12 hours could have meant hundreds- if not thousands- of deaths.

But this light touch was not an accident. In *The Darkening Web,* Alexander Klimburg describes the political motivations of this attack, which was almost certainly carried out by a Russian governmental agency or sponsored group. The Ukrainian power stations were a warning, a flex of power; this was not meant to kill but rather to inspire awe and terror, 2 days before Christmas, in the cold.

Technologies are only ever one use-case away from weaponhood (which is so often their origin-state). The car and the train, the drug and the plane; each can be transmuted with ease from an object of civil service to one of danger and terror, a slippage that feels perhaps more threatening because of their prevalence in the everyday. But these examples are individual objects. They may be wielded like a bullet or a bomb- but the car, train, plane, and drug are localized and may only damage what they touch. When the network itself- a network kept intentionally invisible- is at threat of weaponization, we are left with an ambient and ephemeral fear; a paranoia.

* * *

Conclusion—

It was terror that built the network. The need for instant response and communication was based in nuclear readiness, as was the RAND proposal that invented the core functionality of internet connectivity, along with the highway system that later became the pathway for our fiber-optic cabling. The desire for these systems of response and control derived from a constant and ambient fear of total destruction, a Cold War anxiety that permeated daily life.

This terror has coupled with a campaign of distance, a corporate desire for ephemerality that allows the tech industry to side-step environmental and social concerns. This metaphor of the cloud has let data centers (and their parent companies) overtax small-town electric grids, occupy immense physical footprints, use dirty energy sources, and gather massive local tax breaks while employing very few locals— all while remaining invisible. The cloud has successfully occluded the realities of the physical internet, despite its rootedness in space.

The internet has been described as a networks of networks, a system that connects with itself at every possible point. Paranoia is also defined in such a way- a system of over-connections that allows a militarization of thought. Paranoia was certainly at work in the RAND proposal, and in our defense network of interstate highways. Perhaps such a culture of paranoia also explains the existence of data bunkers like Pionen, or the close-guarded secrets of fiber-optic line locations, or even the emergence of our ‘impossible’ rain-cloud.

Each of these situations is a response to omnipresent danger. Pionen promises physical security. The secret fiber-optic lines claim a distributed indestructibility. The

rain-cloud is a side-effect of imagined distance. But each is a trick; despite Pionen's blast-doors and bedrock location, it is porous by design; the unmarked routes of fiber-optic cabling may gesture to the RAND proposal, but they actually follow existent, linear, mapped systems; our rain-cloud is the fallout of a non-place made non-threatening by a corporate campaign of invisibility.

It is exactly when these systems break and rupture that the fog clears, and we can examine how they are situated in space. The systems that hold up this network *are* physically located, despite the best efforts of our cloud-campaign. They are buried along roads and railways, take up hundreds of millions of square-feet of the Southwest desert, are run into reused nuclear shelters, and form the connective tissue that links most American households.

But these component parts of the cloud are also non-places (and therefore every-places). They may be physically extant somewhere, but they are also everywhere- in the same way that a highway, chain store, or airport is everywhere. Trafficked and networked, they reach outward, touching everything else.

As the cloud enters our own towns, devices, homes, and lives, it touches us. This cloud is both present and distant, physical and ephemeral. When the cloud touches us, we also become a part of the network: another node. It is no surprise that we meet such a system with a paranoid response, given the threats inherent in this network. But our paranoia is not a psychosis. Its hyper-connective structure mirrors the structure of the cloud itself; it is the closest thing to a literal examination of this network that is available to us.

Bibliography:

> Auge, Marc. Non-Places: Introduction to an Anthropology of Supermodernity. Verso, 2006.

> Baran, P. "On Distributed Communications Networks." *IEEE Transactions on Communications 12.1 (1964): 1-9.* The United States Air Force RAND. Web.

> “City of Prineville Railroad.” Train Web, www.trainweb.org/highdesertrails/cop.html

> “Congress Approves Federal Highway Act.” History.com, A&E Television Networks, www.history.com/this-day-in-history/congress-approves-federal-highway-act.

> Durairajan, Ramakrishnan, et al. “InterTubes.” Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication - SIGCOMM '15, 2015, doi:10.1145/2785956.2787499

> Dyson, George. Turing's Cathedral: The Origins of the Digital Universe. N.p.: Penguin, 2013. Print.

> Green, Emma. "Mapping the 'Geography' of the Internet." The Atlantic. Atlantic Media Company, 09 Sept. 2013. Web. 06 Apr. 2017.

> Guide to STRAHNET. Department of Defense, www.fdot.gov/planning/statistics/hwydata/strahnetguide.pdf.

> Klimburg, Alexander. The Darkening Web: The War for Cyberspace. N.p.: Penguin, 2017. Print.

> “Highway History.” U.S. Department of Transportation/Federal Highway Administration, 2006, www.fhwa.dot.gov/interstate/densitymap.cfm.

> Hu, Tung-Hui. A Prehistory of the Cloud. Cambridge, MA: MIT, 2015. Print.

> McMillan, Robert. “Deep Inside the James Bond Villain Lair That Actually Exists.” Wired, Conde Nast, 21 Nov. 2012, www.wired.com/2012/11/bahnhof/.

> Rephann, Terance, and Andrew Isserman. “New Highways as Economic Development Tools: An Evaluation Using Quasi-Experimental Matching Methods.” Regional Science and Urban Economics, vol. 24, no. 6, 1994, pp. 723–751.

> Rogoway, Mike. “Prineville Is Running out of Electricity, Jeopardizing New Manufacturing Jobs.” OregonLive.com, Jan. 2017, www.oregonlive.com/silicon-forest/index.ssf/2017/01/prineville_is_running_out_of_e.html

> Sverdlik, Yevgeniy. “Here's How Much Energy All US Data Centers Consume.” Data Center Knowledge, 27 June 2016, www.datacenterknowledge.com/archives/2016/06/27/heres-how-much-energy-all-us-data-centers-consume

> “The World's Most Super-Designed Data Center – Fit for a James Bond Villain.” Pingdom Royal, 22 Aug. 2017, royal.pingdom.com/2008/11/14/the-worlds-most-super-designed-data-center-fit-for-a-james-bond-villain/

> Weiser, Kathy. “Mojave Desert Ghost Towns on Route 66.” Legends Of America, 20 July 2015, www.legendsofamerica.com/ca-mojaveghosttowns.html.