

Inside the Nuclear Bunkers, Mines, and Mountains Being Retrofitted as Data Centers

Companies are going to great lengths to protect the infrastructure that provides the backbone of the world's digital services—by burying their data deep underground.



THIS ARTICLE IS *republished from [The Conversation](#) under a [Creative Commons license](#).*

It's a sunny June day in southeast England. I'm driving along a quiet, rural road that stretches through the Kent countryside. The sun flashes through breaks in the hedgerow, offering glimpses of verdant crop fields and old farmhouses.

Thick hawthorn and brambles make it difficult to see the 10-foot-high razor-wire fence that encloses a large grassy mound. You'd never suspect that 100 feet beneath the ground, a high-tech cloud computing facility is whirring away, guarding the most valuable commodity of our age: digital data.

This subterranean data center is located in a former nuclear bunker that was constructed in the early 1950s as a command-and-control center for the Royal Air Force's radar network. You can still see the decaying concrete plinths that the radar dish once sat upon. Personnel stationed in the bunker would have closely watched their screens for signs of nuclear-missile-carrying aircraft.

After the end of the Cold War, the bunker was purchased by a London-based internet security firm for use as an ultra-secure data center. Today, the site is operated by the Cyberfort Group, a cybersecurity services provider.



The Cyberfort bunker is a solid inclined mass of grass-covered concrete that emerges in the center of the compound.
PHOTOGRAPH: CYBERFORT/A.R.E. TAYLOR, CC BY

I'm an anthropologist visiting the Cyberfort bunker as part of my ethnographic research exploring practices of “extreme” data storage. My work focuses on anxieties of data loss and the effort we take—or often forget to take—to back up our data.

As an object of anthropological enquiry, the bunkered data center continues the ancient human practice of storing precious relics in underground sites, like the tumuli and burial mounds of our ancestors, where tools, silver, gold, and other treasures were interred.

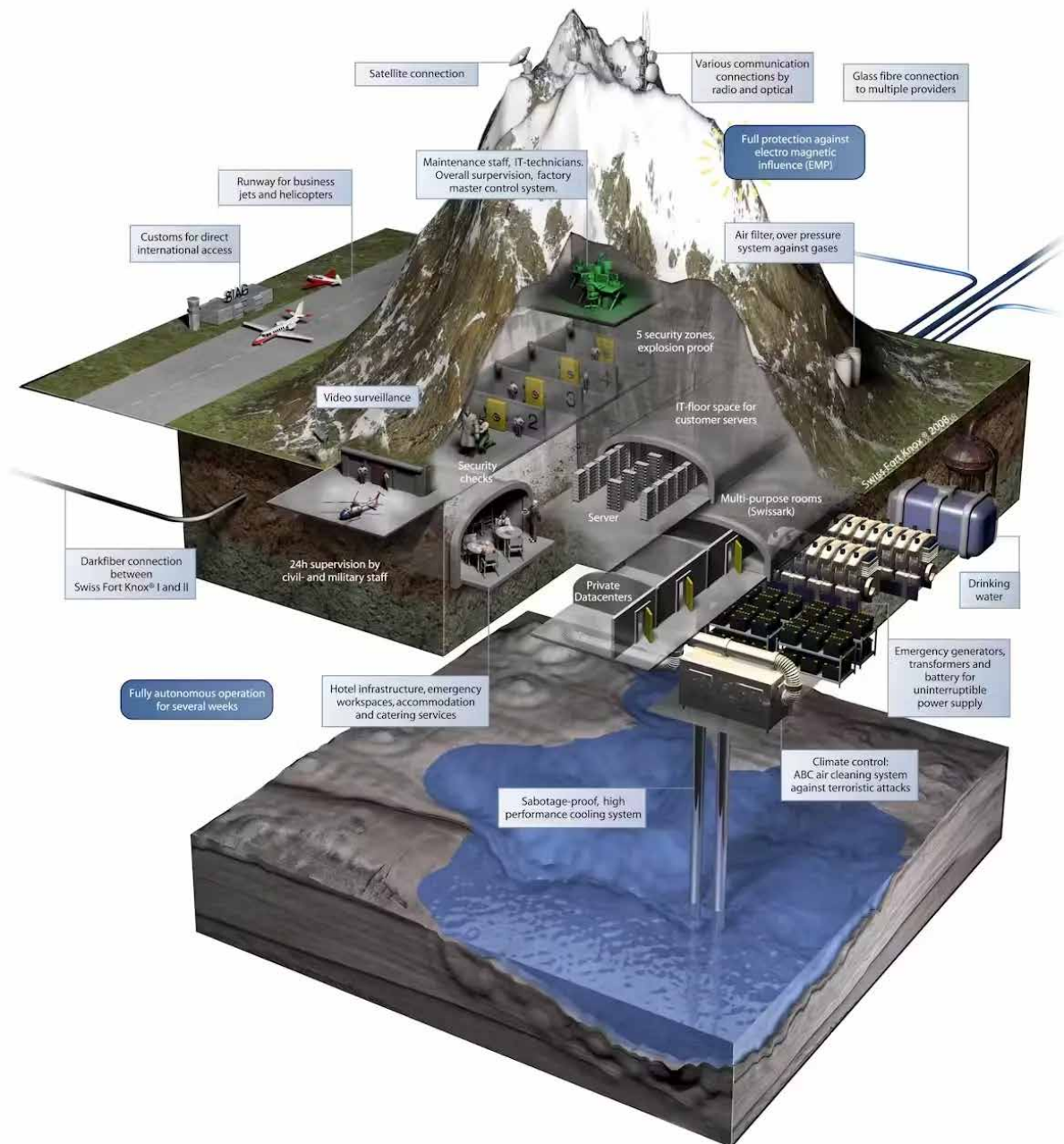
The Cyberfort facility is one of many bunkers around the world that have now been repurposed as cloud storage spaces. Former bomb shelters in China, derelict Soviet command-and-control centers in Kyiv, and abandoned Department of Defense bunkers across the United States have all been repackaged over the last two decades as “future-proof” data storage sites.

I've managed to secure permission to visit some of these high-security sites as part of my fieldwork, including Pionen, a former defense shelter in Stockholm, Sweden, which has attracted considerable media interest over the last two decades because it looks like the high-tech lair of a James Bond villain.

Many abandoned mines and mountain caverns have also been re-engineered as digital data repositories, such as the Mount10 AG complex, which brands itself as the “Swiss Fort Knox” and has buried its operations within the Swiss Alps. Cold War-era information management company Iron Mountain operates an underground data center 10 minutes from downtown Kansas City and another in a former limestone mine in Boyers, Pennsylvania.

The National Library of Norway stores its digital databanks in mountain vaults just south of the Arctic Circle, while a Svalbard coal mine was transformed into a data storage site by the data preservation company Piql. Known as the Arctic World Archive (AWA), this subterranean data preservation facility is modeled on the nearby Global Seed Vault.

Just as the seeds preserved in the Global Seed Vault promise to help rebuild biodiversity in the aftermath of future collapse, the digitized records stored in the AWA promise to help reboot organizations after their collapse.



Bunkers are architectural reflections of cultural anxieties. If nuclear bunkers once mirrored existential fears about atomic warfare, then today's data bunkers speak to the emergence of a new existential threat endemic to digital society: the terrifying prospect of data loss.

Data, the New Gold?

After parking my car, I show my ID to a large and muscular bald-headed guard squeezed into a security booth not much larger than a payphone box. He's wearing a black fleece with "Cyberfort" embroidered on the left side of the chest. He checks my name against today's visitor list, nods, then pushes a button to retract the electric gates.

I follow an open-air corridor constructed from steel grating to the door of the reception building and press a buzzer. The door opens on to the reception area: "Welcome to Cyberfort," receptionist Laura Harper says cheerfully, sitting behind a desk in front of a bulletproof window which faces the car park. I hand her my passport, place my bag in one of the lockers, and take a seat in the waiting area.

Big-tech pundits have heralded data as the "new gold"—a metaphor made all the more vivid when data is stored in abandoned mines. And as the purported economic and cultural value of data continues to grow, so too does the impact of data loss.

For individuals, the loss of digital data can be a devastating experience. If a personal device should crash or be hacked or stolen with no recent back-ups having been made, it can mean the loss of valuable work or cherished memories. Most of us probably have a data-loss horror story we could tell.

For governments, corporations, and businesses, a severe data loss event—whether through theft, erasure, or network failure—can have a significant impact on operations or even result in their collapse. The online services of high-profile companies like Jaguar and Marks & Spencer have recently been impacted by large-

scale cyberattacks that have left them struggling to operate, with systems shutdown and supply chains disrupted. But these companies have been comparatively lucky: a number of organizations had to permanently close down after major data loss events, such as the TravelEx ransomware attack in 2020, and the MediSecure and National Public Data breaches, both in 2024.

With the economic and societal impact of data loss growing, some businesses are turning to bunkers with the hope of avoiding a data loss doomsday scenario.

The Concrete Cloud

One of the first things visitors to the Cyberfort bunker encounter in the waiting area is a 3-foot cylinder of concrete inside a glass display cabinet, showcasing the thickness of the data center's walls. The brute materiality of the bunkered data center stands in stark contrast to the fluffy metaphor of the "cloud," which is often used to discuss online data storage.

Data centers, sometimes known as "server farms," are the buildings where cloud data is stored. When we transfer our data into the cloud, we are transferring it on to servers in a data center (hence the meme "there is no cloud, just someone else's computer"). Data centers typically take the form of windowless, warehouse-scale buildings containing hundreds of servers (pizza-box-shaped computers) stored in cabinets that are arranged in aisles.

Data centers are responsible for running many of the services that underpin the systems we interact with every day. Transportation, logistics, energy, finance, national security, health systems, and other lifeline services all rely on up-to-the-second data stored in and accessed through data centers. Everyday activities such as debit and credit card payments, sending emails, booking tickets, receiving text messages, using social media, search engines, and AI chatbots, streaming TV, making video calls, and storing digital photos all rely on data centers.

These buildings now connect such an incredible range of activities and utilities across government, business, and society that any downtime can have major consequences. The UK government has officially classified data centers as forming part of the country's critical national infrastructure—a move that also conveniently enables the government to justify building many more of these energy-guzzling facilities.

As I sit pondering the concrete reality of the cloud in Cyberfort's waiting area, the company's chief digital officer, Rob Arnold, emerges from a corridor. It was Arnold who arranged my visit, and we head for his office—through a security door with a biometric fingerprint lock—where he talks me through the logic of the bunkered data center.

“The client might not survive the apocalypse, but their data will.”

— ROB ARNOLD, CHIEF DIGITAL OFFICER, CYBERFORT

“The problem with most above-ground data centers is they are often constructed quickly, and not built to withstand physical threats like strong winds, car bombs, or server theft from breaking and entering.” Arnold says that “most people tend to think of the cyber side of data security—hackers, viruses, and cyberattacks—which dangerously overlooks the physical side.”

Amid increasing geopolitical tension, internet infrastructure is now a high-value target as “hybrid” or “cyber-physical” sabotage (when cyberattacks are combined with physical attacks) becomes increasingly common.

The importance of physical internet security has been highlighted by the war in Ukraine, where drone strikes and other attacks on digital infrastructure have led to internet shutdowns. While precise details about the number of data centers destroyed in the conflict remain scant, it has been observed that Russian attacks on local data centers in Ukraine have led many organizations to migrate their data to cloud facilities located outside of the conflict zone.

Bunkers appeal to what Arnold calls “security-conscious” clients. He says: “It’s difficult to find a structure more secure than a bunker”—before adding drily: “The client might not survive the apocalypse, but their data will.”

Cyberfort specializes in serving regulated industries. Its customer base includes companies working in defense, health care, finance, and critical infrastructure. “Our core offering focuses on providing secure, sovereign, and compliant cloud and data-center services,” Arnold explains in a well-rehearsed sales routine. “We do more for our customers than just host systems—we protect their reputations.”



The bunker's external armor-plated door. PHOTOGRAPH: CYBERFORT/A.R.E. TAYLOR, CC BY

Arnold's pitch is disrupted by a knock at the door. The head of security (who I'm calling Richard Thomas here) enters—a 6-foot-tall ex-Royal Marine wearing black cargo trousers, black combat boots, and a black Cyberfort-branded polo shirt. Thomas is going to show me around the facility today.

The entrance to the bunker is located up a short access road. Engineered to withstand the blast and radiation effects of megaton-level thermonuclear detonations, this cloud storage bunker promises its clients that their data will survive any eventuality.

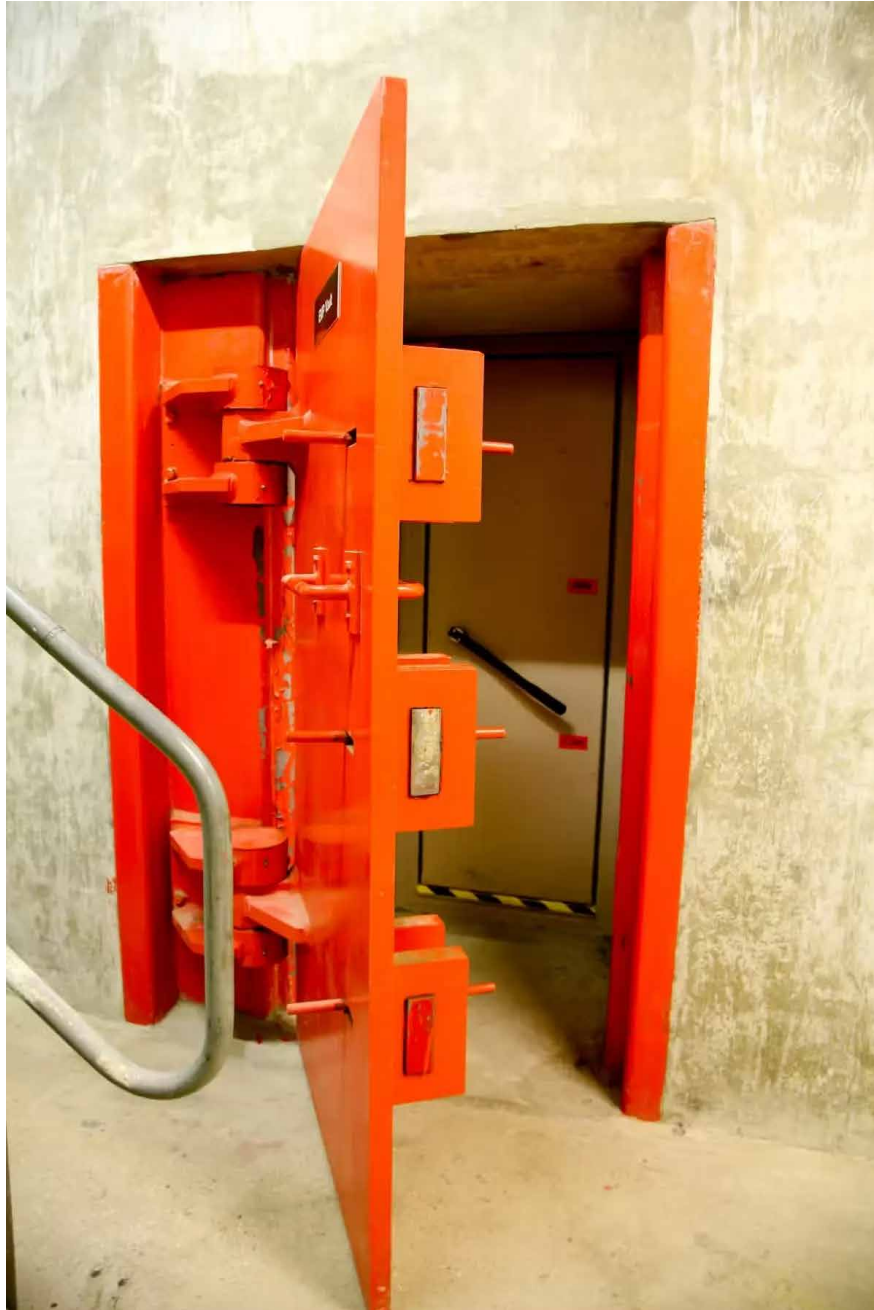
At the armor-plated entrance door, Thomas taps a passcode into the electronic lock and swipes his card through the access control system. Inside, the air is cool and musty. Another security guard sits in a small room behind bulletproof plexiglass. He buzzes us through a metal mantrap and we descend into the depths of the facility via a steel staircase, our footsteps echoing in this cavernous space.

The heavy blast doors and concrete walls of the bunker appear strangely at odds with the virtual “walls” we typically associate with data security: firewalls, anti-virus vaults, and spyware and spam filters. Similarly, the bunker's military logics of enclosure and isolation seem somewhat outdated when faced with the transgressive digital “flows” of networked data.

However, to dismiss the bunkered data center as merely an outmoded piece of security theater is to overlook the importance of physical security—today and in the future.

We often think of the internet as an immaterial or ethereal realm that exists in an electronic non-place. Metaphors like the now retro-sounding cyberspace and, more recently, the cloud perpetuate this way of thinking.

But the cloud is a material infrastructure composed of thousands of miles of cables and rows upon rows of computing equipment. It always “touches the ground” somewhere, making it vulnerable to a range of non-cyber threats—from thieves breaking into data centers and stealing servers, to solar storms disrupting electrical supplies, and even to squirrels chewing through cables.



A blast-proof door in the Cyberfort bunker, behind which lies the server room containing the digital “gold.” PHOTOGRAPH : CYBERFORT/A.R.E. TAYLOR, CC BY

If data center services should go down, even for a few seconds, the economic and societal impact can be calamitous. In recent years we have seen this firsthand.

In July 2020, the 27-minute Cloudflare outage led to a 50 percent collapse in traffic across the globe, disrupting major platforms like Discord, Shopify, Feedly, and Politico. In June 2021, the Fastly outage left some of the world's most visited websites completely inaccessible, including Amazon, PayPal, Reddit, and The New York Times. In October 2021, Meta, which owns Facebook, WhatsApp, and Instagram, experienced an outage for several hours that affected millions of social media users as well as hundreds of businesses.

Perhaps the largest internet outage yet occurred in July 2024 when the CrowdStrike outage left supermarkets, doctors' surgeries, pharmacies, airports, train providers, and banks (among other critical services) unable to operate. This was described by some in the industry as "one of the largest mass outages in IT history."

Internet architecture now relies on such a complex and fragile ecosystem of interdependencies that major outages are getting bigger and occurring more often. Downtime events can have a lasting financial and reputational impact on data center providers. Some attempts to quantify the average cost of an unplanned data center outage range from \$9,000 to \$17,000 per minute.

The geographic location of a data center is also hugely important for data protection regulations, Thomas explains, as we make our way down a brightly lit corridor. "Cyberfort's facilities are all located in the UK, which gives our clients peace of mind, knowing they comply with data sovereignty laws."

Data sovereignty regulations subject data to the legal and privacy standards of the country in which it is stored. This means businesses and organizations must be careful about where in the world their data is being relocated when they move it

into the cloud. For example, if a UK business opts to store their data with a cloud provider that uses data centers based in the US then that data will be subject to US privacy standards, which do not fully comply with UK privacy standards.

In contrast to early perceptions of the internet as transcending space, eradicating national borders and geopolitics, data sovereignty regulations endow locality with renewed significance in the cloud era.

The Survival of Data at All Costs

Towards the end of the corridor, Thomas opens a large red blast-proof door—beyond which is a smaller air-tight door. Thomas waves his card in front of an e-reader, initiating an unlocking process: We're about to enter one of the server rooms.

“Get ready” he says, smiling, “it’s going to be cold and loud!” The door opens, releasing a rush of cold air. The server room is configured and calibrated for the sole purpose of providing optimal conditions for data storage.

Like any computer, servers generate a huge amount of heat when they are running, and must be stored in constantly air-conditioned rooms to ensure they do not overheat. If for any reason a server should crash or fail, it can lead to the loss of a client’s valuable data. Data center technicians work in high-pressure conditions where any unexpected server downtime could mean the end of their job.



The server room at Cyberfort. PHOTOGRAPH: CYBERFORT/A.R.E. TAYLOR, CC BY

To try and make sure the servers run optimally, data centers rely on huge amounts of water and energy, which can significantly limit the availability of these resources for the people who live in the vicinity of the buildings.

An average data center consumes an estimated 200 terawatt-hours of electricity each year. Globally, that adds up to around 1 percent of total electricity demand, which is more than the national energy consumption of some countries. Many of these facilities are powered by nonrenewable energy sources, and the data center industry is expected to emit 2.5 billion tons of carbon dioxide by 2030.

In addition, to meet expectations for “uninterruptible” service levels, data centers rely on an array of fossil-fuel-based backup infrastructure—primarily diesel generators. For this reason, the [Green Web Foundation](#)—a nonprofit organization working to decarbonize the internet—has described the internet as the world’s largest coal-powered machine. Data centers are also noisy and have become sites of protest for local residents upset about noise pollution.

Amid hype and speculation about the rise of AI, which is leading to a boom in the construction of energy-hungry data centers, the carbon footprint of the industry is under increasing scrutiny. Keen to highlight Cyberfort’s efforts to address these issues, Thomas informs me that “environmental impact is a key consideration for Cyberfort, and we take our commitment to these issues very seriously.”

As we walk down a cold aisle of whirring servers, he explains that Cyberfort actively sources electricity from renewable energy supply chains, and uses what he calls a “closed-loop” cooling infrastructure which consumes minimal fresh water.

“Like the Pyramids”

After our walk through the server room, we begin to make our way out of the bunker, heading through another heavy-duty blast door. As we walk down the corridor, Thomas promotes the durability of bunkers as a further security selling point. Patting the cold concrete wall with the palm of his hand, he says: “Bunkers are built to last, like the pyramids.”



Another heavy duty blast door. PHOTOGRAPH: CYBERFORT/A.R.E. TAYLOR, CC BY

Bunker scholars have long noted that these buildings are as much about time as they are about space. Bunkers are designed to preserve and transport their contents through time, from an apocalyptic present into a safe future.

Writers such as Paul Virilio, W.G. Sebald, and J.G. Ballard were drawn to the decaying bunkers of the Second World War and, like Thomas, compared them with enduring megastructures which have outlived the civilizations that built them. In his 1975 book *Bunker Archaeology*, Virilio famously compared the abandoned Nazi bunkers along the coast of France with “the Egyptian *mastabas*, the Etruscan tombs, the Aztec structures.”

Some providers now offer “lifetime” cloud packages with no monthly or yearly payments and no inactivity clause. However, the cloud market is volatile, defined by cycles of boom and bust, with providers and their data centers constantly rebranding, closing, and relocating. In this landscape of mergers and acquisitions, there is no guarantee that lifetime cloud providers will be around long enough to honor these promises.

In addition, the majority of consumer cloud providers currently only offer a maximum of a few terabytes of storage. In the future, most of us will probably need a lot more than this, which could mean a lot more data centers (roughly 100 new data centers are set to be constructed in the UK alone within the next five years). We may also see more bunkers being repurposed as data centers. Some providers, like Florida-based Data Shelter, are even considering building entirely new bunker structures from scratch to house digital data.

Resurfacing

Thomas and I arrive at the steel staircase leading back up to the outside world. The guard buzzes us back through the turnstile, and Thomas unlocks and opens the door. The sunlight stings my eyes.

Back in the reception area, I thank Arnold and Thomas for my surreal trip into the depths of subterranean data storage. The Cyberfort data center is a site of extreme contrasts, where the ethereal promise of the cloud jars with the concrete reality of the bunker.

Sitting in my car, I add to my field notes that the survival of data—whether entombed in bunkers or stored in “lifetime” cloud accounts—is bound to the churn of markets, and depends upon the durability of the infrastructure and organizations behind it.

The bunker's durability invites us to take a long-term view of our own data storage needs, which will only increase over the course of our lives.

For technology behemoths like Apple and Google, cloud storage is a key strategic avenue for long-term revenue growth. While the phones, laptops, and other digital devices they make have limited lifespans, their cloud services offer potentially lifelong data storage. Apple and Google encourage us to perpetually hoard our data rather than delete it, because this locks us into their cloud subscription services, which become increasingly expensive the more storage we need.

Apple's marketing for its cloud storage service, iCloud, encourages users to "take all the photos you want without worrying about space on your devices." Google has made "archive" rather than "delete" the default option on Gmail. While this reduces the likelihood of us accidentally deleting an email, it also means we are steadily consuming more of our Gmail capacity, leading some to purchase more Google Drive storage space.

Cloud Hoarders

It is also increasingly difficult to operate off-cloud. Internal storage space on our digital devices is dwindling as the cloud becomes the default storage option on the majority of digital products being developed. Users must pay a premium if they want more than the basic local storage on their laptop or smartphone. Ports to enable expandable, local storage—such as CD drives or SD card slots—are also being removed by tech manufacturers.

As our personal digital archives expand, our cloud storage needs will continue to grow over our lifetimes, as will the payments for more and more cloud storage space. And while we often imagine we will one day take the time to prune our accumulations of digital photos, files, and emails, that task is often indefinitely postponed. In the meantime, it is quicker and easier to simply purchase more cloud storage.

Permanence, in the digital age, is always provisional. One can't help but imagine future archaeologists discovering this bunker and rummaging through the unreadable remains of our lost digital civilization.

Many consumers simply use whichever cloud storage service is already preinstalled on their devices—often these are neither the cheapest nor most secure option. But once we commit to one provider, it is very difficult to move our data to another if we want a cheaper monthly storage rate, or simply want to switch—this requires investing in enough hard drives on which to download the data from one cloud provider and upload it to another. Not everyone is tech-savvy enough to do that.



Underground: inside the Lefdal Mine Data Centers in Norway. PHOTOGRAPH: BLOOMBERG/GETTY IMAGES

In 2013, bank reforms in the UK introduced a switching service which enabled consumers to easily move their money and payments to different banks, in order to access more favorable rates. Cloud migration services are available for businesses, but until a cloud storage equivalent of the bank switching service is developed for the general public, many of us are essentially locked into whichever cloud provider we have been using. If our data really is the new gold, perhaps we should require cloud providers to offer incentives to deposit it with them.