4 Future-proof: bunkered data centres and the selling of ultra-secure cloud storage

A.R.E. Taylor University of Cambridge

Abandoned after the Cold War, nuclear bunkers around the world have found afterlives as ultra-secure data storage sites for cloud computing providers. The operators of these bunkered data centres capitalize on the spatial, temporal, and material security affordances of their subterranean fortresses, promoting them as ‘future-proof’ cloud storage solutions. Taking the concept of ‘future-proofing’ as its entry-point, this essay explores how data centre professionals work with the imaginative properties of the bunker to configure data as an object to be securitized. The essay takes the form of an ethnographic tour through a UK-based data bunker. During this tour, threatening data futures and fragile data materialities are conjured in order to secure the conditions of possibility for the bunkered data centre’s commercial continuity. Future-proofing, it is argued, provides a conceptual opening onto the entangled imperatives of security and marketing that drive the commercial data storage industry.

Underground clouds
Since the late 1990s, the material remnants of Cold War bunkers around the world have been progressively repurposed as digital data storage facilities for cloud computing companies. Civil defence shelters in Sweden and China, derelict Soviet command and control centres in Latvia and Lithuania, and abandoned Department of Defence bunkers in the United States have all been repackaged as commercial data centres to service the needs of information capitalism. Engineered to withstand the blast and radiation effects of megaton-level thermonuclear detonations, the bunkered data centre promises to provide the data it houses with a level of security unsurpassed by any other built structure. If, as historian Luke Bennett has observed, bunkers ‘are a material testimony to the anxieties of their creators’ (2011: 157), then the bunkered data centre is a site where anxieties surrounding digital data security take architectural form. While anthropologists have begun to explore the role that the accumulation of large volumes of digital data (‘Big Data’) now plays in security regimes, ranging from predictive policing to pandemic preparedness to the climate crisis, anthropological attention has yet fully to turn to the ways in which data itself is arising as an object to be securitized.
Through an ethnographic tour of a bunkered data centre in Northern England, in this essay I trace the ways that data centre professionals work with the material-imaginative affordances of the bunker to market and sell what they call 'future-proof' data security. The term ‘future-proof’ was regularly invoked by employees of the bunkered data centre to describe and promote the security that the site offers. A focus on future-proofing provides an entry-point for exploring the ways that data centre security and marketing discourses, practices, and imaginaries strategically situate digital data storage in time. Such a focus also adds to understandings of the diverse temporal relationships that human beings imaginatively construct with bunkers. These haunting architectural objects have long proven to be complex sites of temporality and security, their concrete materiality generating imaginaries of protection from future threats and durability through time. Nuclear bunkers, in particular, are architectures through which humans have sought to manage time, generating alternative futures in the face of existential risk. As Joseph Masco has observed in his analysis of bunker-building projects during the Cold War: ‘[V]ia the promise of the bunker, the logical outcome of nuclear war – the destruction of the nation state in a radioactive firestorm – was denied and a different future horizon opened’ (2009: 16). Today, with bunkers being rebranded as ‘future-proof’ cloud storage sites, their material, affective, and temporal intensities are being directed towards securing the future of digital data.

The empirical material presented here is drawn from fieldwork that was conducted in a bunkered data centre that is owned and operated by the cloud computing provider Fort Data Centres (hereafter referred to as ‘Fort’).1 The following tour of Fort’s data bunker is divided into four sections. The first section sets the scene for the tour. The second section explores how data centre professionals conjure threatening futures from which the bunker promises protection. The Fort team perform considerable work with the bunker to generate horizons of threat and insecurity that reaffirm the need for bunkered data storage. The third section traces the long-term futures of security that the material and temporal form of the bunker affords. The fourth section examines how the future-orientated durability of the bunker contrasts with the fragile materialities and temporalities of the data storage hardware it contains. Here I trace the ways that the Fort team foreground the vulnerable materiality of server hard drives in order to further certify the utility of the bunker. Through these four sections, I explore how the material properties of bunkered data centres, and the hardware they house, bring with them their own futures, fragilities, and durabilities that call for different modalities of future-proofing. Following Andrew Shryock and Daniel Lord Smail’s observation that, with any storage technology, ‘the relationship between content and container is transformative’ (2018: 49), this essay asks: how might a focus on data transform understandings of the bunker? And how might a focus on bunkers transform understandings of data?

In keeping with the dual mandate of this special issue, the aim of this essay is not only to demonstrate how anthropology, with its attentiveness to the socially generative qualities of materials, can help us better understand the temporal and material dimensions of cloud data storage, but also to expand anthropological explorations of future-orientated security practices and performances (Ghertner, McFann & Goldstein 2020; Holbraad & Pedersen 2013; Low & Maguire 2019; Maguire, Frois & Zurawski 2014). ‘Future-proofing’ adds a rich ethnographic concept to unfolding discussions within the discipline about the ways that futures are being acted upon within the current 'security moment' (Goldstein 2010: 487). The concept of future-proofing is
increasingly finding purchase across a range of sectors and policy domains today, including cultural heritage and conservation, risk and resilience management, urban planning, and infrastructure engineering. Future-proofing typically defines a form of anticipative forward-planning that aims to ensure that the target object or asset – be it infrastructure, cities, businesses, valuable artworks, or digital data – will continue to operate, endure, or accrue value for a significant period of (linear) time ‘into the future’. Future-proofing thus abuts with a number of future-orientated rationalities that have gained political traction over the last two decades, such as ‘resilience’ and ‘preparedness’ (Duffield 2011; 2013; Lakoff 2017). In line with these rationalities, the future is problematized as a timespace of uncertainty that can nevertheless be managed through strategic anticipatory action undertaken in the present (Anderson 2010). In the ethnographic context of the bunkered data centre, future-proofing is characterized by a temporal orientation that aims to protect data assets both for and from the future. Discourses, practices, and imaginaries of future-proof data storage place the emphasis on acting now to ensure the longevity of data whilst simultaneously protecting digital assets from a future that is figured as an unending field of imminent threat.

Beyond its role in data centre security discourses, future-proofing is a marketing term with which data centre professionals promote and position their facilities within a competitive cloud storage marketplace. A focus on future-proofing thus directs attention to the (often contradictory) entanglements of security and marketing in the commercial data centre. In the concluding section of this essay, I therefore reflect on the larger marketing logics of the future-proof data bunker. In doing so, this essay strengthens understandings of the visual politics and security performances of the data centre industry (Holt & Vonderau 2015; Jakobsson & Stiernstedt 2012; Taylor 2019; Veel 2018) and contributes to ongoing explorations of the relationship between digital data and the spaces and places in which it is stored (Johnson & Hogan 2018). Amidst growing interdisciplinary interest in the infrastructures that operate ‘behind the screens’ of cloud computing, data centres have surfaced as valuable infrastructural objects through which the materiality of the cloud, and its associated social and environmental costs, have been unpacked (Hogan 2015; Vonderau 2017). These buildings have provided an entry-point for investigating how cloud infrastructure has been grafted on top of previous industrial, military, colonial, and imperial legacies (Hu 2015; Jacobson & Hogan 2019; Johnson 2019; Pickren 2018; Rossiter 2016). Bunkered data centres have garnered considerable attention, with an array of news articles, magazine exposés, essays, and artworks exploring the striking dissonance between their excessive materiality and the image of immateriality conjured by the cloud metaphor (Charles 2016; Graham 2016; Jha 2009; Mingard 2014). These architectural curiosities have served not only as marked examples of the concrete materiality of cloud computing. With their history as spaces for the preservation and enactment of fractured state sovereignty in the aftermath of nuclear devastation, bunkered data centres have also proven to be valuable sites for thinking through the ways in which sovereign power hauntingly textures the cloud (Bratton 2015; Hu 2015).

While this burgeoning field of data centre studies has demonstrated that space and place continue to matter in globally distributed computing assemblages, considerably less attention has been paid to the security and marketing logics through which cloud providers themselves strive to make space and place matter to their clients. Contrary to the rhetoric that framed early discourses and imaginaries of the internet, which celebrated emancipation from the constraints of space, time, and materiality, the
bunkered data centre presents an opportunity to further explore how these constraints are being rearticulated, reinforced, and attributed with security significance in relation to commercial data storage (DeNicola 2012). The tour that follows thus descends into the depths of subterranean cloud storage in order to examine the role that the bunker plays in the making and marketing of 'future-proof' data security.

**A security safari**

The first sign of Fort’s data bunker, buried 100 feet beneath the countryside of Northern England, emerges in the form of a 11.5-foot-high chain-link fence, topped with barbed coils of razor wire (Fig. 1). The fence cuts through the surrounding farmland, aggressively demarcating the perimeter of the compound. Fort’s main entrance area is complete with an assortment of security technologies: guardhouses, vehicle traps, galvanized steel security gates, rising arm barriers, hydraulic bollards, and CCTV cameras. Visitors are required to show two forms of ID at the security window of the guardhouse. The guard then checks their details against a visitor list and escorts them to the office complex, a flat-roofed, one-storey brick structure built above-ground within the compound. In the reception area, visitors must submit their ID documents to be scanned and logged. They are then issued with a visitor clearance pass.

One of the first things that visitors to the Fort data bunker encounter in the waiting room is a glass display cabinet that stands on the windowsill showcasing a 3-foot cylinder of concrete. The caption beneath reads: ‘Diamond-drilled core showing the construction and depth of concrete between the upper and lower floors of the data centre’. Built from concrete as thick and durable as possible, the bunkered data centre has a ‘brute materiality’ (Dourish 2017: 140) that stands in stark contrast to the soft and fluffy ‘cloud’ conceit. Concrete walls themselves appear strangely at odds with
the virtual ‘walls’ typically associated with data security: firewalls, anti-virus vaults, and spyware and spam filters. Similarly, the bunker’s military logics of enclosure and defence seem somewhat outdated when faced with the transgressive digital ‘flows’ of networked data and the fibre-optic hyperconnectivity required of a data centre. Yet Cold War bunkers have always been paradoxical infrastructures, simultaneously connected and disconnected, open and closed. These sites were designed to ensure continuous communications with branches of government through secure cable corridors whilst also hermetically sealing themselves off from the outside world to function as self-contained ‘security islands’ (Duffield 2011: 766). More than an outmoded piece of security theatre, the reinforced concrete of the bunker is a key component in what Fort call their ‘multi-layered’ approach to security, which combines physical and digital security measures.

The symbolic properties of concrete as a construction material play a strategic role in the security capacities and aesthetics of Fort’s facility, staging the solidity, strength, and durability of the bunker. Images of the concrete walls, along with reinforced steel doors, can be found throughout Fort’s marketing materials, from the promotional leaflets in the waiting room to the image gallery on their website, where they brand their bunker as ‘the UK’s most resilient data centre’. These hardened materials also take centre stage during tours of the facility. Like most commercial data centres, Fort provide prospective clients with opportunities to visit the site. These site visits enable potential customers to experience the security of the data centre first-hand and to meet the data centre employees who will be looking after their precious digital assets. For the facility operators at Fort, these visits are valuable opportunities to showcase the security affordances of the site, promoting the bunker as the future-proof solution to the client’s data storage needs. For this reason, at Fort, these site visits are referred to as ‘security safaris’.

My security safari at the compound was arranged by Jonathan Applegate, Fort’s Managing Director. Applegate met me in the waiting room and led me to his office. Proceeding through a security door with a biometric fingerprint lock, we entered a corridor with long rectangular windows on either side, presenting views onto employees typing at computers and talking on telephones: the service desk operators, systems administrators, and cybersecurity team. A wide range of customers store their data with Fort, including retailers, the NHS, IT disaster recovery vendors, district councils from around the United Kingdom, and some departments of the UK government. The vast majority of Fort’s clients work in the payment card industry and banking. Fort offer a range of IT services, data storage options, and security and recovery solutions, promising to provide their clients with what Applegate called ‘total data assurance’. In his office at the end of the corridor, he took a seat behind his desk in front of a bulletproof window facing the compound’s car park. He talked me through the logic behind the bunkered data centre. In contrast to above-ground data centres, which are often constructed in what he referred to as ‘flimsy-looking warehouses’, he told me that ‘the bunker addresses a need in the data centre marketplace for facilities that provide more robust and resilient physical security’. Applegate explained that data security is persistently dematerialized in popular imaginaries of computing: ‘Most people tend to think of the cyber-side of data security: hackers, viruses, and cyberattacks’, he told me, ‘which dangerously overlooks the physical side’. The principal reasons behind this critical oversight, he suggested, were persistent media attention on
cyberterrorism and the misleading metaphors that are commonly used to apprehend internet infrastructure, such as the ‘cloud’ and ‘cyberspace’.

As many cultural commentators have noted, the metaphorical conceit of the ‘cloud’ presents online data storage as a transcendental, placeless operation, occurring ‘everywhere and nowhere in particular’ (Carruth 2014: 340). Applegate explained that this transcendental imaginary results in a narrow understanding of data security that can lead organizations to unknowingly compromise their ‘digital assets’. He presented a scenario: while data is often duplicated across multiple storage facilities to reduce the likelihood of data loss, an organization’s sensitive digital information could be compromised if an unauthorized actor breached one of those data centres and walked out with a server. ‘It doesn’t matter how backed-up your data is or how great your digital defences are’, he elaborated, ‘if you can’t stop a brute force breach’. Over the last two decades, there have been a number of heists at high-profile data centres, where intruders have gained access and stolen servers containing customer databases, credit card information, and data related to criminal proceedings. Applegate told me that Fort ‘store a lot of sensitive and valuable information’ and their clients need to know that their data isn’t going to be stolen, whether physically or digitally. Fort’s customers also need uninterruptible 24/7/365 access to their data. During our conversation, Applegate thus conjured a multitude of threats that could disrupt the operations of a standard data centre but from which the bunker promises protection, ranging from car bombs to hurricane-force winds to falling trees to microchip-melting electromagnetic pulses (EMPs). ‘Every data centre can deal with cyberattacks’, he told me, ‘but the majority wouldn’t stand a chance if there was a vehicle-ramming attack or a terrorist heist’. The security safari is a key tool through which possible threats to data are further conjured and concretized, providing Fort with an opportunity to foreground the role that materiality and location can play in ‘proofing’ data from these threatening futures.

Conjuring threatening futures

My tour of the Fort data bunker was led by Michael Bates, an ex-Royal Marine and the head of Fort’s team of security guards. Most data centres source their guard labour from military or police backgrounds. At Fort, the uniform of the security team follows a military aesthetic, consisting of black ‘army-tactical’ combat boots, military-grade cargo trousers in black camo, and a black fleece with ‘Fort: Ultra Secure’ embroidered on the left chest. The security guards work in rotating shifts twenty-four hours a day throughout the year. They patrol the perimeter of the compound (often with their Ministry of Defence-trained guard dogs), operate various guard posts, and organize preparedness training exercises for Fort’s staff. Alongside these activities, the security guards also double as ‘tour guides’, escorting clients during their site visits.

The bunker itself is a solid inclined mass of grass-covered concrete that surfaces in the centre of the compound (Fig. 2). As Bates and I left the office complex and made our way up the access road towards the bunker, we passed a derelict brick guardhouse and some large concrete radar plinths; the crumbling remains of the site’s past life as a radar data centre. In their marketing, Fort capitalize on the military heritage of their facility, highlighting that ‘the construction and security standards are what you might expect of such a purpose-built fortress’. A closer look at the site’s past reveals a history of repurposing and technological obsolescence, while also providing a window onto Cold War military ‘data histories’ (Aronova, von Oertzen & Sepkoski 2017). The bunker was built in the early 1950s and formed part of a UK-wide network of radar sites for
making and moving data in anticipation of nuclear warfare. The principal purpose of the bunker was not to protect human beings, but to facilitate data processing. The radars scanned the electromagnetic spectrum, monitoring the movement of potential nuclear missile-carrying aircraft, providing personnel in the bunker below with a view onto an electronic world of data feeds and illuminated blips mediated by console screens. This data was then relayed to sector operations centres via teleprinter networks or in the form of voice communications over dedicated telephone landlines.

Five years after opening, the facility was closed because the radar systems it used were unable to accurately track the faster jet aircraft that had emerged. As David F. Bell has observed, the length of time it took to build such fortifications often meant they were ‘obsolete even before they could actually serve their imagined purpose’ (2008: 216). The bunker remained empty until the mid-1960s, when it was reopened as part of a dual-purpose civil and military radar network. Signal data was stored on large magnetic drums and transferred to command-and-control centres via narrow band data links. In 1974, the site was again closed, only to be reactivated six years later as a reserve Royal Air Force (RAF) reporting centre, with radar data being transferred into the facility from other stations and analysed by operators. The site continued to operate as a data switching point until the dissolution of the Soviet Union in 1991. The bunker was left largely abandoned, with Fort purchasing the freeholds to the site in 1998. The form of the bunker has thus persistently outlasted its function.

As Bates and I neared the entrance to the bunker, he talked me through some of the features that make the facility future-proof. He explained that the bunker’s strategic spatial location outside of high-risk city centre zones reduces its vulnerability to terrorism. He pointed out a number of infrared CCTV cameras that monitor the compound. Fort’s surveillance practices extend beyond the perimeter of the site, with members of the security team patrolling a two-mile radius around the facility, on
foot and in vehicles. He directed my attention to two large EMP-resistant shipping containers above the bunker that contain diesel generators, enabling the facility to operate off-grid for up to two months in the event of an extended power outage.

At the armour-plated entrance door to the bunker (Fig. 3), Bates tapped a passcode into the electronic lock and swiped his card through the access control system. The secure solidity and durability that the hardened materials of the bunker promise are sensorially foregrounded throughout the security safari in a well-rehearsed routine. Bates invited me to try to pull the door open, describing it as ‘weighing several tons’. When I did so, the door moved only with great effort. Inside the facility, another security guard sat in a small room behind some bulletproof plexiglass. He buzzed us through a mantrap (Fig. 4), and we descended into the depths of the facility via a steel staircase, our footsteps echoing in the cavernous space.

The interior of the bunker is divided into three levels that form a nested series of securitized areas within a carapace of concrete, locked behind doors that run along dimly lit corridors. Bates explained that many of the rooms in the bunker remain empty. Empty space is vital to future-proofing Fort as a business. The ability to expand computing capacity in response to demand from future customers is essential to ensuring long-term growth. Unlike many above-ground data centres, which are modular in design, the square footage of the bunker is limited and must therefore be carefully managed. As we made our way through the facility, Bates conjured Cold War threats into the present. ‘The Cold War might be over’, he told me, ‘but the nuclear threat has never gone away’. Patting his hand on the hardened ferrocement wall, he reassured me that, ‘fortunately, this place has been designed to withstand the force of a 22-kiloton nuclear bomb’. Perpetuating the unending possibility of nuclear threat for visiting clients, Bates positioned the Fort bunker in a state of
Figure 4. The author entering the bunkered data centre through a full-height turnstile security gate. (Image provided by Fort Data Centres.)

active waiting for thermonuclear futures. The bunkered data centre stands in stark contrast to the Cold War bunkers that have been converted into heritage or museum sites. John Beck has suggested that musealized bunkers strive to distance visitors from the possibility of nuclear war, functioning as reassuring ‘reminders of how
things are no longer dangerous' (2011: 95). By contrast, the bunkered data centre strives to maintain the bunker’s original threat-related uses and meanings (cf. Bennett 2020: 3). The Fort data bunker thus embeds cloud storage not only within the material remains of a military redoubt but also within its security logics, imaginaries, and futures.

 Conjuring possible future threats against which the solid materiality of the bunker guarantees protection is central to the selling of bunkered data storage. Anna Tsing has used the term ‘conjuring’ to capture the imaginative work that investment companies engage in to entice speculators. ‘In speculative enterprises’, Tsing observes, ‘profit must be imagined before it can be extracted; the possibility of economic performance must be conjured like a spirit to draw an audience of potential investors’ (2001: 159). If financial speculation is based on conjuring utopian futures of profit, the selling of bunkered cloud storage is based on conjuring the spectre of disaster. The bunker plays an active role in the conjuring process, operationalizing certain imaginative horizons while closing down others. Applegate highlighted this during our conversation in his office when he exclaimed: ‘You can’t not think about the end of the world when you see a bunker!’ The bunker is exemplary of the ways that certain infrastructures, landscapes or spaces afford ‘particular imaginary scenarios’ (Nielsen & Pedersen 2015: 250). As a building type born from the anticipation of catastrophe, bunkers are ‘technologies’ (Sneath, Holbraad & Pedersen 2009) through which imaginaries of threatening futures have long been generated.

 At the same time, while the bunker may lend itself to end-of-the-world visions, Bates was careful to remind me that many of Fort’s clients are concerned less with a global technological apocalypse and more with their own ‘personal doomsdays’. He explained that, as organizational reliance on digital information continues to grow, data loss or disruption of service take on an increasingly existential quality, potentially putting an end to their clients’ operations. During the tour, he thus conjured possible threats that could disrupt data centre service delivery, only to rhetorically dispel them with the ‘future-proof’ form of the bunker. ‘Terrorists, nukes, floods: nothing is getting in here’, he told me as he locked a 25-ton blast door behind us (Fig. 5), sealing us inside the ‘closed world’ (Edwards 1996) of Cold War concrete.

 If the Cold War bunker primarily promised sanctuary (however illusory this may have been) from an irradiated nuclear future, in its repurposed form as a data centre, it now peddles protection for the ever-multiplying threats that vie for attention in contemporary securitiescapes. As Bradley Garrett and Ian Klinke have observed, the bunkers that are being put to use today are ‘no longer limited to a specific disaster imagination’ (2018: 1075). Rather, they have been reimagined and rebranded as multi-disaster resistant structures for ‘all-hazards’ preparedness (Deville, Guggenheim & Hrdličková 2014). This is captured by the ‘future-proofing’ concept itself, which is orientated not towards a specific threat but towards an indeterminate future that is filled with catastrophic possibility (Horn 2018). Promising to provide their clients with uninterruptible access to data amidst an ever-expanding spectrum of threat scenarios, on their website Fort brand their bunker as ‘ultra-secure’ and, in reference to the continuous IT uptime it offers, ‘ultra-available’.

Deep-time data storage
The bunker does not only promise to protect data from threatening futures but also strives to ensure that data can survive into the future. As we continued through the bunker, Bates foregrounded the security afforded by the durable form of the built
structure. He invited me to knock on the cold concrete walls to ‘feel how solid they are’, and confidently told me that ‘bunkers are built to last, like the pyramids’. The apparent timelessness of bunkers has previously invited comparisons to the enduring megastructures of ancient civilizations, with Paul Virilio famously comparing them to ‘the Egyptian mastabas, the Etruscan tombs, the Aztec structures’ (2009 [1975]: 11). Conjuring the durable monuments of the ancient Egyptians, Bates worked with the material-imaginative resonances of the bunker to promote the site as a structure that can withstand not only a nuclear blast, but time itself. This material resistance to time is similarly evoked by the metaphor of ‘future-proofing’, which draws its rhetorical efficacy from other ‘proofing’ practices, such as waterproofing and soundproofing, to conjure the future as an almost-material entity against which the present can be shielded through the bunker’s sheer materiality.

The material durability of the bunker has become a central aspect of Fort’s marketing. Emerging regulatory frameworks increasingly require firms to retain and preserve data for decades after its use. Capitalizing on the temporal endurance that the materiality of the bunker affords, bunkered data centres have become key sites in which an emerging market for long-term data storage and preservation has taken root. Fort offer what they call a ‘long-term deep archive solution’ for clients who want to store ‘cold’ data that they don’t need to access often. A number of subterranean data centres have begun to branch out from the provision of business continuity and move into the realm of cultural continuity, positioning themselves as deep-time media infrastructures (Mattern 2015; Zielinski 2006) for the long-term storage and preservation of digital cultural heritage.

Continuing his narrative of eternal data storage, Bates informed me that ‘when we’re wiped out, the data down here will be all that’s left of us’. In this scenario, the digital information stored on the subterranean servers becomes a ‘new type of human remains’.

Figure 5. Steel blast-proof doors with hermetically sealed airlocks promise to ensure that the data stored in the bunker will survive any eventuality. (Image provided by DataGarrison.)
(Lupton 2018: 6) – a future fossil that will most likely be unreadable due to format obsolescence or data decay. Bunkers have long provided an eerie prism through which onlookers have envisioned artefacts of their own time as future ruins. W.G. Sebald famously reimagined the abandoned bunkers at Orford Ness in Suffolk as the 'remains of our own civilisation after its extinction in some future catastrophe' (1998: 237). In Bates's narrative, with the human race annihilated, the bunkered data centre becomes an accidental time capsule: a data tomb.

Scholarship on bunkers has often emphasized their ‘womb- and tomb-like’ properties (Beck 2011: 82; see also Bell 2008: 217; Virilio 2009 [1975]: 46). As Adam Fish and Bradley Garrett (2019) note, the bunker is ‘a socially and culturally constituted womb from which objects, people, and information are meant to be recovered – and a tomb when recovery becomes impossible.’ Fish and Garrett identify ‘recovery’ as a uniting logic of both bunkers and data centres. Recovery services are a key feature of cloud security packages. If a client should experience a disaster, data centres aim to quickly re-boot the IT systems that underpin their businesses. Yet a focus on recovery doesn’t fully capture the everyday operating logic of the bunkered data centre, or the factors that drive clients to store their data with Fort. During my security safari with Bates, he suggested that ‘resilience’, rather than ‘recovery’, is the main selling point of the bunker. ‘Recovery places the emphasis on cleaning up after an event’, he told me, ‘rather than operational continuance during an event’. I encountered a similar logic when I met with James Longley, the Marketing Director of DataGarrison, a London-based business continuity provider that use Fort’s bunker as their primary data storage site. During our conversation, Longley explained that ‘recovery’ is an essential component of business continuity, but ‘with a bunker you increase the likelihood that you won’t get to the recovery stage because they are built to be resilient’. Further reinforcing his point, Longley stated: ‘Why not reduce the need to recover in the first place by storing your data in a resilient infrastructure?’ While definitions of resilience vary, in the domain of disaster management it is often understood as referring to ‘a basic ability to withstand shock and survive disaster … while still retaining essential functionality’ (Duffield 2013: 55). As ‘resilient infrastructures’, bunkers, Longley suggested, are built to withstand disaster and to continue operating through even the most extreme events, meaning there should rarely be a need to ‘recover’ or ‘resurrect’ data. For DataGarrison, the bunker’s promise of future resurrection was secondary to its promise of resilience, endurance, and continuity in the present.

**Fragile data futures**

The durable materiality of the bunker jars with the limited lifespan of the digital hardware it contains, which operates on an altogether different timescale. Fish and Garrett (2019) have suggested that theorization of bunkers must necessarily address the relationship between ‘the materiality of the bunker and temporality of its contents’. Indeed, the security a bunker offers is shaped – and sometimes subverted – by its contents. While the bunker endures, the hard disk drives, servers, and other technical computing components stored within are fragile and prone to failure, decay, and rapid obsolescence. Given the limited lifespan of digital technologies, the servers on which Fort store their clients’ data might typically be conceived as ‘future vulnerable’ rather than ‘future-proof’ (Edwards, Jackson, Bowker & Williams 2009: 371). At Fort, however, the fragile materiality of the computing equipment provides another opportunity to
promote the future-proof data security on offer, as I experienced when Bates and I entered one of the bunker’s data halls.

Mid-way down one of the corridors, Bates waved his card in front of an e-reader next to an armoured door. The unlocking process was initiated with an electronic beeping sound. Releasing a gust of cold air, the door opened onto a room full of server cabinets: the data hall (Fig. 6). Configured and calibrated for the sole purpose of providing optimal conditions for data storage, the data hall is a decidedly nonhuman space. Air conditioners noisily circulate cold air around the rows of servers to prevent them from
overheating. A room temperature of 18–23°C and a humidity level of 45–55 per cent must be maintained to provide ambient cooling and to prevent fires, ensuring that critical server components are not damaged. Whilst walking between the servers, Bates and I met Will Hartley, one of Fort’s technicians. Hartley was wearing a thick North Face parka to avoid the breeze from the air conditioners and was busy installing a new server. He has worked at Fort for the past ten years and spends most of his time in the data hall, fixing and replacing servers. Hartley warned that the hard disk drives (HDDs) inside the servers are particularly fragile and prone to failure. He explained that these devices are therefore routinely replaced every twelve months. Much of Hartley’s work involves what he called ‘pre-emptive upgrading’: the anticipatory retiring of servers, whether they are broken or not. ‘We can’t sit around and wait for a hard drive to fail’, he told me, ‘we have to act before it breaks’. By discarding servers before they have a chance to malfunction, Hartley ‘proofs’ the bunker against future hardware failure, removing hard drives from their trajectories of decay and deterioration. Through this anticipatory maintenance, whereby data is constantly migrated from discarded drives to new drives, data is made to endure across ephemeral hardware (Chun 2011).

Mindful of the excessive waste that pre-emptive upgrading produces, Hartley justified this practice as a standard future-proofing measure throughout the data centre industry and an unavoidable consequence of the fact that businesses, governments, and the lives of individuals are increasingly structured around a dependence on data stored on fragile media. To highlight the fragile materiality of digital storage media, Hartley prised open the casing of a decommissioned server and showed me the delicate mechanical parts of the hard drive housed within. He explained that a variety of contaminants can cause lasting damage to server hard drives. Dust, plant pollens, human hair, smoke fumes, and liquid droplets can all interfere with their fragile mechanisms, causing corrosion, oxide flake-off, or equipment failure. Photoelectric sensors are thus positioned at strategic points within the data hall to detect threatening particulate matter. Here we encounter what Garrett and Klinke have termed the ‘more-than-human bunker’ (2018: 1078).

Reverberations from passing traffic, especially heavy goods vehicles, can also damage hard drive mechanisms. The low traffic levels on the quiet country roads surrounding the Fort facility thus provide an additional layer of security. ‘This is why location is so important when it comes to server storage’, Hartley informed me. Another selling point of the facility in this regard is the ‘vibration-proof’ construction of the walls. One of Fort’s online promotional videos provides viewers with extensive details about the composition of the walls, which are made from ‘three metres of reinforced concrete, followed by one-and-a-half metres of fine-grade flint and tungsten rods, and then a rubber buffer strip’. The rubber buffer strip, we are told, helps absorb the shockwave associated with nuclear blasts and also protects the data centre from earthquakes.

Hartley drew my attention to one corner of the data hall, in which a number of servers were locked inside a Faraday cage: a metal enclosure that was installed during the Cold War to protect the bunker’s computing equipment from EMPs generated by nuclear detonations. Now protecting the servers of clients that want to pay extra to ensure their data will survive an EMP event, the Faraday shielding reinscribes cloud storage within Cold War vectors of threat; a further reminder that, at the Fort data bunker, such threats are not past but actively structure its present technical configurations. ‘Any and every data centre can upgrade hard drives to protect against equipment failure’, Hartley explained, ‘but only the most secure can ensure that hard
drives aren’t damaged if a bomb detonates nearby or an EMP goes off’. Echoing Applegate, Hartley suggested that many organizations put their data at risk when they don’t prioritize the physical security of their cloud provider’s data centres. Despite the promise of placeless, transcendental, or dematerialized data storage, my time in the data hall with Hartley served as a reminder not only that cloud storage is emphatically material, but also that significant stakes are invested in making cloud storage material.

**Conclusion: Re-materializing data storage**

As a security framework, future-proofing constructs the future as a permanent threat-space against which Fort promise to protect clients’ data. The impenetrability of the bunker barricades against external threats like bomb blasts and server heists, while offering a durable architecture to ensure the longevity of the data it contains. Anticipatory practices of pre-emptive upgrading further ‘proof’ data from futures of hardware failure and obsolescence. Future-proofing thus provides the data centre professionals at Fort with an elastic temporal framework with which they can navigate and negotiate shifting scales of security and threat across time. It is also an evocative marketing term that Fort frequently employ in their promotional material.

Back in the main office complex after my security safari with Bates, Applegate further elaborated on the marketing logics of the data bunker. ‘The more we can make people realize that their data, their online services, and all the apps they use are stored in real, fragile buildings somewhere’, he zealously told me, ‘the more they’ll want the best secured data centre to store their stuff’. Applegate presented the selling of future-proof data storage as less about producing (and profiting from) fear, and more about raising awareness of the material vulnerability of cloud storage. He explained that users have a right to what he called ‘robust and resilient’ data security – a right that he felt is obfuscated by the ‘cloud’ conceit.

If, as John Durham Peters has observed, the cloud metaphor evokes ‘ideas of a heavenly record’ (2015: 332), Fort strive to dismantle this vision of data transcendence by rendering cloud storage visible, material, and vulnerable. The security safari is just one tool through which they attempt to do this. Their website, their social media, and their online videos provide other promotional channels, as do the trade fairs and expo events that they attend. Through these different marketing platforms, they strive to render data materially vulnerable, offering the ‘future-proof’ bunker as a secure cloud storage solution. It is thus not only threats to data that are being conjured at Fort but also the threatening material fragility of cloud storage itself. In his forensic history of the hard disk drive, Matthew Kirschenbaum (2008) has traced how, over the course of the twentieth century, digital data storage became increasingly invisible. From punched card and magnetic drums, data storage gradually moved into the computer, becoming locked inside the plastic casing of desktop towers and laptop shells. As new paradigms of distributed computing, such as the cloud, normalize the storing and processing of data at a distance, the materiality of digital storage becomes ‘ever more abstracted and removed from daily awareness’ (Kirschenbaum 2008: 19). At Fort, considerable effort is invested in undoing this process. Online data storage must be made visible and material if it is to be made vulnerable, and it must be made vulnerable if bunkered data storage is to be sold. Through this double conjuring of threat and materiality, the spaces and places of cloud storage are made to matter, producing the conditions of possibility for the bunkered data centre’s commercial continuity.
Fort’s commitment to dispelling the ‘myth of immateriality’ (Appadurai & Alexander 2020: 76) that enshrouds the cloud aligns, if somewhat incongruently, with recent critical efforts to render cloud infrastructure visible. ‘Making the invisible visible’ and ‘grounding the cloud’ have become both mantras and methodologies for directing attention to the infrastructure that is rhetorically erased by the cloud metaphor. By materializing the digital through a variety of visual practices, scholars, journalists, and artists have highlighted the social, material, and environmental impact of cloud computing. The question now is not whether cloud storage is material but how, in what ways, and to what ends is the (im)materiality of online data storage established in different spatiotemporal and geographic settings? The ways that bunkerized data centres themselves work to render cloud storage strategically visible and material invites further reflection on the multiple registers, negotiations, and performances of (in)visibility and (im)materiality involved in the marketing and securitizing of commercial data centres (Amoore 2018; Furlong 2021). While specific types of data centre, such as those operated by intelligence agencies, may strive to remain invisible, for many commercial data centres, which rely on attracting clients through marketing, strategic visibility is often essential. This is especially the case with data centres that have been retrofitted inside nuclear bunkers, where the security promised by the spectacular setting is a unique selling point that must be emphasized as a key factor of product differentiation in the data centre marketplace. As Applegate highlighted: ‘If people think their data’s just stored in some make-believe cloud, this is bad for our business’.

In this sense, the bunkerized data centre departs from the visual logics that guided the Cold War bunker, when these defensive installations were required to remain hidden. As Beck (2011: 83) reminds us, ‘a visible bunker is to a large extent disarmed’. In an attempt to address the vulnerability that accompanies visibility and locatability, Fort have removed their facility from ‘street view’ in Google Maps (but not from the ‘satellite view’). Managing the contradictory imperatives of security and marketing is continuous work. Further vulnerabilities arise from the ageing architecture of the bunker itself, which requires Fort to invest considerable expense in maintaining the property.

The Fort data bunker thus appeals to a particularly security-conscious clientele who are attuned to the role that location, time, and materiality can play in ‘proofing’ digital data from a spectrum of scenarios that unfold across different scales of threat, ranging from server hijackings by hostile actors, to the failure of critical hardware, to regulatory incompliance. With cloud clients increasingly required to meet various security, regulatory, or sustainability mandates, the location and material impact of data centres is taking on heightened significance for both cloud providers and their customers alike. The operators of bunkerized data centres capitalize on the spatial, temporal, and material security value of their subterranean fortresses, promising their clients that their data will survive any eventuality. In the future-proof data bunker, threats to the security and survivability of data are thus simultaneously things against which protection is offered and from which profit can be extracted.

NOTES

I would like to thank the Editors of this special issue, as well as the anonymous reviewers, for their insightful feedback on previous drafts. Funding for the research described in this essay was carried out with the assistance of a Sutasoma Award from the Radcliffe-Brown Trust Fund of the Royal Anthropological Institute.
The material presented in this essay is drawn from ongoing fieldwork and interviews with data centre professionals that began in summer 2015. The names of individuals and companies have been changed to protect the privacy of interlocutors.

Although relatively rare occurrences in comparison to digital breaches, there have been some major server heists: in October 2007, armed intruders broke into CI Host, a Chicago-based colocation data centre and stole twenty servers; in December 2007, five men dressed in police uniforms gained entry to a Verizon data centre in London, stealing £2 million worth of equipment; in July 2008, the Financial Times' web hosting equipment was stolen from a data centre in Watford (UK); in February 2011, thieves stole equipment from a Vodafone data centre in Basingstoke (UK); and in November 2015, five servers were stolen from the data centre of the charity Plan UK, containing the personal details of 90,000 donors.

The data-centre-as-pyramid has recently found architectural expression in the pyramid-shaped facility operated by Switch and located near Grand Rapids, Michigan. Switch, who refer to themselves as 'a globally recognized leader in future-proof data centre design', turn to the pyramid to communicate the future-proof aesthetic.

A similar feature has been highlighted by media theorists Peter Jakobsson and Fredrik Stiernstedt (2012) in their study of Pionen, a data centre located inside a former civil defence bunker built into the bedrock of Stockholm. They examine the role that the geological history of the site plays in staging the facility as a secure storage space 'constructed for eternity' (2012: 112).

The data preservation company Piql (pronounced ‘pickle’) operate the Arctic World Archive from inside an abandoned coal mine on the archipelago of Svalbard, Norway. Modelled on the nearby Global Seed Vault, Piql combine the material endurance of their underground location with a digital data preservation service, whereby they transfer data onto a durable tape-based storage medium – a process they refer to as ‘pickling’ data (hence their name). Known as 'the digital world’s Doomsday Vault', on their website Piql promise 'to keep data alive for centuries'. Elsewhere, the National Library of Norway archive and store their databanks in the mountain facilities at Mo i Rana. The US-based information management services company, Iron Mountain, preserve digital and analogue media in a nuke-proof underground vault in Pennsylvania. The Swiss-based data bunker complex Mount10 (pronounced ‘Mountain’) also specialize in the long-term storage of digital data.

REFERENCES

Amoore, L. 2018. Cloud geographies: computing, data, sovereignty. Progress in Human Geography 42, 4-24.

Anderson, B. 2010. Preemption, precaution, preparedness: anticipatory action and future geographies. Progress in Human Geography 34, 777-98.

Appadurai, A. & N. Alexander 2020. Failure. Cambridge: Polity.

Aravena, E., C. von Oertzen & D. Sepkoski 2017. Introduction: Historicizing big data. Osiris 32, 1-17.

Beck, J. 2011. Concrete ambivalence: inside the bunker complex. Cultural Politics 7, 79-102.

Bell, D.F. 2008. Bunker busting and bunker mentalities, or is it safe to be underground? South Atlantic Quarterly 107, 213-29.

—— 2011. The bunker: metaphor, materiality and management. Culture and Organization 17, 155-73.

Bennett, L. 2020. The bunker’s after-life: cultural production in the ruins of the Cold War. Journal of War & Culture Studies 13, 1-10.

Bratton, B.H. 2015. The stack: on software and sovereignty. Cambridge, Mass.: MIT Press.

Carruth, A. 2014. The digital cloud and the micropolitics of energy. Public Culture 26, 339-64.

Charles, E. 2016. White mountain (available online: http://www.emma-charles.com/white-mountain, accessed 18 January 2021).

Chun, W. 2011. The enduring ephemeral, or the future is a memory. In Media archaeology: approaches, applications and implications (eds) E. Huhtamo & J. Parikka, 184-206. Berkeley: University of California Press.

DeNicola, L. 2012. Geomedia: the reassertion of space within digital culture. In Digital anthropology (eds) H.A. Horst & D. Miller, 80-98. London: Berg.

Deville, J., M. Guggenheim & Z. Hrdličková 2014. Concrete governmentality: shelters and the transformations of preparedness. In Disasters and politics: materials, experiments, preparedness (eds) M. Tironi, I. Rodríguez-Giralt & M. Guggenheim, 183-210. Chichester: Wiley Blackwell, for The Sociological Review.

Dourish, P. 2017. The stuff of bits: an essay on the materialities of information. Cambridge, Mass.: MIT Press.

Duffield, M. 2011. Total war as environmental terror: linking liberalism, resilience, and the bunker. South Atlantic Quarterly 110, 757-69.
Furlong, K. 2021. Geographies of infrastructure II: Concrete, cloud and layered (in)visibilities. Progress in Human Geography 45, 190-8.

Garrett, B. & I. Klinke 2018. Opening the bunker: function, materiality, temporality. Environment and Planning C: Politics and Space 37, 1063-81.

Ghertner, D.A., H. McFann & D.M. Goldstein 2020. Futureproof: security aesthetics and the management of life. Durham, N.C.: Duke University Press.

Goldstein, D. 2010. Toward a critical anthropology of security. Current Anthropology 51, 487-517.

Graham, S. 2016. Vertical: the city from satellites to bunkers. New York: Verso.

Hogan, M. 2015. Data flows and water woes: the Utah Data Center. Big Data & Society 2: 2 (available online: https://journals.sagepub.com/doi/10.1177/2053951715592429, accessed 18 January 2021).

Holbraad, M. & M.A. Pedersen 2013. Times of security: ethnographies of fear, protest and the future. New York: Routledge.

Holt, J. & P. Vonderau 2015. ‘Where the internet lives’: data centers as cloud infrastructure. In Signal traffic: critical studies of media infrastructures (eds) L. Parks & N. Starosielski, 71-93. Urbana: University of Illinois Press.

Horn, E. 2018. The future as catastrophe: imagining disaster in the modern age. New York: Columbia University Press.

Hu, T. 2015. A prehistory of the cloud. Cambridge, Mass.: MIT Press.

Jacobson, K. & M. Hogan 2019. Retrofitted data centers: a new world in the shell of the old. Work Organization, Labor & Globalization 16: 5, 78-94.

Jakobsson, P. & F. Stiernstedt 2012. Time, space and clouds of information: data centre discourse and the meaning of durability. Cultural technologies: the shaping of culture in media and society (ed.) G. Bolin, 103-17. New York: Routledge.

Jha, A. 2009. Secrets of the data bunker. The Guardian, 11 November (available online: https://www.theguardian.com/technology/2009/nov/11/data-server-farms, accessed 18 January 2021).

Johnson, A. 2019. Data centers as infrastructural inbetweens. American Ethnologist 46, 75-88.

—— & M. Hogan 2018. Introducing location and dislocation: global geographies of digital data. Imaginations: Journal of Cross-Cultural Image Studies 8: 2, 4-7.

Kirschbaum, M.G. 2008. Mechanisms: new media and the forensic imagination. Cambridge, Mass.: MIT Press.

Lakoff, A. 2017. Unprepared: global health in a time of emergency. Oakland: University of California Press.

Low, S. & M. Maguire (eds) 2019. Spaces of security: ethnographies of securitiescapes, surveillance and control. New York: University Press.

Lupton, D. 2018. How do data come to matter? Living and becoming with personal data. Big Data & Society 5: 2 (available online: https://journals.sagepub.com/doi/10.1177/2053951717786314, accessed 18 January 2021).

Maguire, M., C. Frois & N. Zurawski 2014. The anthropology of security: perspectives from the frontline of policing, counter-terrorism and border control. London: Pluto.

Masco, J. 2009. Life underground: building the bunker society. Anthropology Now, Special Atomic Issue 1, 13-29.

Mattern, S. 2015. Deep time of media infrastructure. In Signal traffic: critical studies of media infrastructures (eds) L. Parks & N. Starosielski, 94-114. Urbana: University of Illinois Press.

Mingard, Y. 2014. Deposit. Göttingen: Steidl.

Nielsen, M. & M.A. Pedersen 2015. Infrastructural imaginaries: collapsed futures in Mozambique and Mongolia. In Reflections on imagination: human capacity and ethnographic method (eds) M. Harris & N. Rapport, 237-61. London: Routledge.

Peters, J.D. 2015. The marvelous clouds: toward a philosophy of elemental media. Chicago: University Press.
Pickren, G. 2018. The factories of the past are turning into the data centers of the future. *Imaginations: Journal of Cross-Cultural Image Studies* 8: 2, 22-9.

Rossiter, N. 2016. Software, infrastructure, labor: a media theory of logistical nightmares. London: Routledge.

Sebald, W.G. 1998. *The rings of Saturn* (trans. M. Hulse). London: Harvill.

Shryock, A. & D.L. Smail 2018. On containers: a forum. Concluding remarks. *History and Anthropology* 29, 49-51.

Sneath, D., M. Holbraad & M.A. Pedersen 2009. Technologies of the imagination: an introduction. *Ethnos* 74: 5-30.

Taylor, A.R.E. 2019. The data center as technological wilderness. *Culture Machine* 18 (available online: https://culturemachine.net/vol-18-the-nature-of-data-centers/data-center-as-techno-wilderness/, accessed 18 January 2021).

Tsing, A. 2001. Inside the global economy of appearances. In *Globalization* (ed.) A. Appadurai, 155-88. Durham, N.C.: Duke University Press.

Veel, K. 2018. Uncertain architectures: performing shelter and exposure. *Imaginations: Journal of Cross-Cultural Image Studies* 8: 2, 30-41.

Virilio, P. 2009 [1975]. *Bunker archaeology* (trans. G. Collins). New York: Princeton Architectural Press.

Vonderau, A. 2017. Technologies of imagination: locating the cloud in Sweden’s global north. *Imaginations: Journal of Cross-Cultural Image Studies* 8: 2, 8-21.

Zielinski, S. 2006. *Deep time of the media: toward an archaeology of hearing and seeing by technical means*. Cambridge, Mass.: MIT Press.

À l’épreuve du futur : les données bunkérisées ou comment vendre l’ultrasécurisation du nuage

Résumé

Laissés à l’abandon après la Guerre froide, des bunkers antiautomiques du monde entier trouvent une seconde vie en tant que centres de stockage de données ultrasécurisés pour les fournisseurs de services du nuage informatique. Les responsables de ces centres de données misent sur le potentiel spatial, temporel et de sécurité matérielle de leurs forteresses souterraines, en faisant d’elles des solutions de stockage « à l’épreuve du futur ». C’est au prisme de ce concept que l’auteur explore comment les professionnels du stockage de données exploitent l’imaginaire du bunker pour configurer les données comme des objets à protéger. L’article prend la forme d’une visite ethnographique dans un bunker de données britannique. Lors de cette visite, l’on agitera le spectre de matérialités fragiles et de menaces futures sur les données, afin d’assurer la continuité commerciale du bunker. Cette protection contre l’avenir, selon l’auteur, apporte une ouverture conceptuelle sur les impératifs entrelacés de la sécurité et du marketing qui régissent le marché du stockage de données.