Special Issue Article

new media & society
2023, Vol. 25(2) 405–430

DOI: 10.1177/14614448221149936
journals.sagepub.com/home/nms
SAGE

Concrete clouds: Bunkers, data, preparedness

ARE Taylor
University of Exeter, UK

Abstract

As visions of the end-times accelerate under neoliberal capitalism, corporations and governments are moving their valuable digital data into that most iconic end-of-the-world architecture: the nuclear bunker. This article traces the rise of the bunker as a prominent architectural form for the industrial storage of data. In doing so, it introduces the concept of 'data preparedness' to explore one way that data centres and cloud back-up providers strategically position themselves and their clients in imaginative relation to threatening futures. Rebranded as an 'ultra-secure' data centre, the bunker is no longer orientated towards the omnipresent threat of nuclear terror that structured everyday life during the Cold War. Rather, the bunkered data centre promises preparedness for an existential threat that lurks behind the screens of daily life in the digital world: the unending prospect of data loss or IT system failure.

Keywords

Anthropology, bunkers, cloud computing, Cold War, data loss, data storage, disaster recovery, preparedness, security

Upon my arrival at DataVault's London office, I am greeted by the company's Marketing Director, David Webster. As Webster shows me around the open plan working space, he talks me through the role that DataVault plays in the IT industry. 'We're a cloud-based data back-up and recovery provider', he explains, 'we help businesses to recover their data or get their IT systems back up and running when disaster strikes'. One of the key selling points of DataVault's disaster recovery service is their 'ultra-secure' data centre that is located inside a nuclear bunker. Formerly owned by the UK Government's Ministry of Defence, the bunker was built in the 1950s and was repurposed as a data centre shortly after the Cold War came to an end. The bunkered data centre is foregrounded on DataVault's

Corresponding author:
ARE Taylor, University of Exeter, Exeter, EX4 4LA, UK.
Email: a.r.e.taylor@exeter.ac.uk

website, where they highlight that the ex-military structure ‘protects data from every potential threat’, ensuring that client data remains ‘ultra-secure and always available’. In Webster’s office, dramatic black-and-white canvas print photos of the bunker are hanging on the wall. He explains that the bunker plays an important role in demonstrating DataVault’s commitment to security. ‘We need to show our clients that we take security seriously’, he informs me, ‘that we are prepared for the worst-case scenario’. With the help of this bunkered data centre, DataVault promise to protect data across multiple scales of disaster, ranging from what Webster terms ‘acts of God’ (extreme weather, earthquakes, and other ‘natural’ disasters) to ‘file corruption or human error’. The threats themselves are less important than their consequences: data loss or IT downtime. ‘If you lose valuable data or if your IT systems go down, even for a second, it could be the end of your business’, Webster warns me. DataVault has a variety of customers from around the world, from local start-ups to large corporates. Their clients include law and financial service firms, logistics companies, charities, transport providers, a fast-food chain, a UK media company, a cultural heritage consultancy, a US-based sportswear brand, a German telecommunications company and a number of UK Government agencies, among others. Webster explains that most of the businesses that DataVault represent are typically less concerned with ensuring their data survives a nuclear winter and more concerned with protecting their digital assets from threats such as distributed denial of service (DDoS) attacks, server theft or hard drive failure. Indeed, he tells me there is little point in ensuring that data survives a catastrophic event if those businesses (or the people running those businessess) have been wiped out in the meantime. Nevertheless, he highlights, ‘knowing that your data is stored in a bunker provides that extra bit of security, because you never know what could happen’. DataVault’s aim, Webster foregrounds during my visit, is not to prevent disaster but to ensure that clients are prepared so that when disaster inevitably strikes, they are ready to respond and recover quickly, with minimal disruption to their business and, hopefully, little to no data loss.

DataVault’s subterranean data shelter is one of a number of bunkers throughout the world that has been reactivated as a ‘disaster-proof’ commercial data centre. In this article, I trace the rise of the bunker as an increasingly normalised architectural form for the storage of digital data. In doing so, I explore how data bunker companies and cloud disaster recovery providers work to position clients in anticipative relation to a future data loss event. In recent years, these bunkered data centres have attracted considerable journalistic and academic attention, capturing the imagination of the popular press and scholars alike (Charles, 2016; Graham, 2013; Hu, 2015; Jakobsson and Stiernstedt, 2012; Jha, 2009; Mingard, 2014). The excessive materiality of the concrete data bunker jars with the images and imaginaries of immateriality typically associated with the digital computing ‘cloud’. As such, a proliferating array of news articles, magazine exposés and video installations have investigated these architectural curiosities, exploring and exposing the striking dissonance between the cloud conceit and the distinctly un-cloudlike infrastructure the bunker presents. Media scholars have explored how the bunker embeds media storage within specific temporal relationships, often focusing on the mountain bunkers that are being utilised for long-term media preservation projects (Mattern, 2017; Murphy, 2014). Beyond serving as marked examples of the materiality of the cloud, bunkered data centres have also proven to be valuable sites for exploring the military histories that

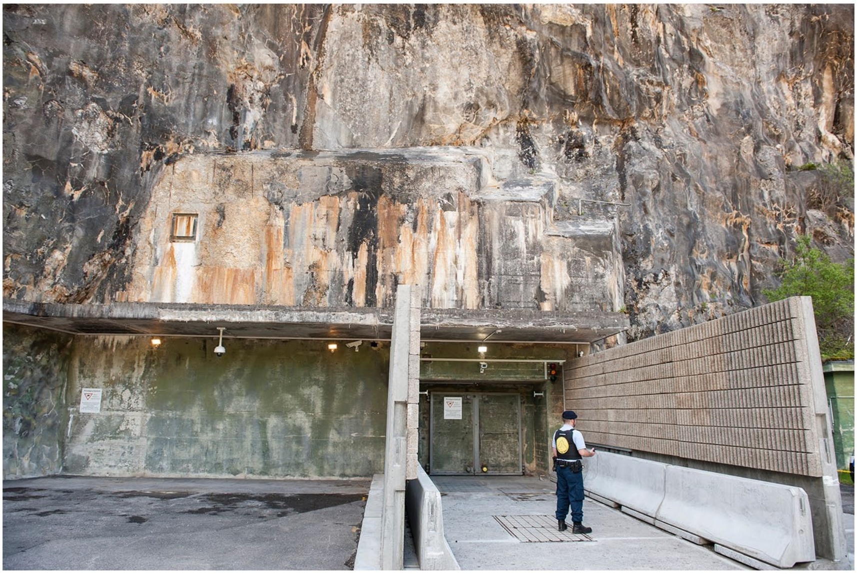

Figure 1. The entrance to one of the two bunkered data centres operated by the cloud back-up provider Mount10 (pronounced ‘Mountain’), both of which are located in former military bunkers in the Swiss Alps. Mount10’s data bunker complex is known as the ‘Swiss Fort Knox’ (image courtesy of Mount10).

haunt networked computing. Scholars have explored how bunkers inscribe virtualised data storage within Cold War politics of sovereignty (Bratton, 2015; Hu, 2015), security (Taylor, 2021a) and shelter (Veel, 2018).

Taking these discussions in a different direction, here I explore how the bunkered data centre extends Cold War logics of preparedness into the domain of digital data storage. Constructed in anticipation of disaster, bunkers have been described as ‘concretised forms of preparedness’ (Deville et al., 2014: 186). After the Cold War, these fortified spaces have been incorporated into new regimes of preparedness, reorientating themselves towards new disasters in order to justify their continued existence (Beck, 2011; Deville et al., 2014; Garrett and Klinke, 2018). In this article, the bunkered data centre provides a material and conceptual entry-point for sketching an analysis of what I term ‘data preparedness’. If, during the Cold War, the bunker both reflected and produced ‘new forms of mental preparedness’ (Lutz, 1997: 246; see also Masco, 2009) for nuclear war, in their repurposed forms as ultra-secure data centres, these sites now participate in the production of ‘backed-up’ subjectivities that are prepared for data loss and IT downtime. As such, I argue, the bunkered data centre directs itself less towards the ambient threat of nuclear war that shaped the second half of the twentieth century, and more towards the ambient threat of data loss that lurks in the background of daily life in an increasingly digitised and datafied world.

Big tech pundits herald data as the ‘new oil’ or the ‘new gold’. Yet, as the purported economic and cultural value of data continues to grow, so too does the impact of data loss.

If digital data should be erased, stolen, damaged or destroyed, the consequences are perceived to be increasingly catastrophic. For individuals, the loss of digital data can be a devastating experience. If a personal device should crash or be hacked or stolen, and no recent back-ups have been made, it can mean the loss of valuable work or cherished memories. Natasha Dow Schüll (2018: 44) has used the language of existential risk to capture the impact of data loss on peoples' personal lives today, describing 'the annihilating sense of loss that strikes when personal information archives crash, inexplicably disappear into the ether of the so-called cloud, or become mysteriously corrupt and inextractable'. With growing numbers of organisations and key sectors of society constructed around a dependence on digital information, data loss has become its own doomsday scenario. For governments, corporations and businesses, a severe data loss event (whether through theft, erasure, bit rot or network failure) could have a significant economic impact or even result in their collapse. As Matt Prigge (2011), a network architect, writes in the technology magazine *InfoWorld*, 'Our enormous appetite for data has bred an equally huge existential dependence on that data being available'. Continuing, Prigge observes:

> It's not just the big names on the Fortune 1000 who can't live without info, either. Businesses as small as florist shops and veterinary clinics can't get by without their delivery schedules and patient records – all of which are stored digitally.

Prigge asks readers to imagine 'what would happen if the lights went out and your data went away?' He proposes a preparedness exercise as the solution, in the form of a 'data-loss fire drill' whereby organisations stage their own table-top 'data outage'. Digital data loss has gradually surfaced as a growing fixture in the collective imagination of catastrophic futures. The plots of films like *Blade Runner 2049* (2017), TV shows like *Mr Robot* (2015–2019) and graphic novels like Enki Bilal's *Bug* (2017) all pivot around large-scale data erasure events that lead to widespread societal collapse. In other equally dystopian data visions, since the mid-1990s, digital archivists have uttered warnings about the prospect of a 'Digital Dark Age'. This is the name given to an imagined epoch in which digitised human knowledge and history are lost due to the rapid speed with which digital storage media become obsolete, rendering their data corrupt or inaccessible.

In keeping with this special issue's exploration of data centre imaginaries and temporalities, bunkered data centres provide a means of exploring the larger cultural imaginaries of data loss and the temporal politics of preparedness that produce and maintain these sites, and that shape, structure and underpin the larger data centre industry. I use the term 'data preparedness' to describe a set of anticipatory practices that are enacted by individuals and organisations to manage the ever-present possibility of data loss – practices that are often encouraged by data back-up companies and cloud computing providers (Taylor, 2021b). Practices of data preparedness can range from everyday acts of backing-up files onto an external hard drive to the more spectacular act of bunkering data in the material ruins of military infrastructure. Preparedness has been widely identified as a characteristic feature of contemporary anticipatory politics (Adams et al., 2009; Anderson, 2010; Duffield, 2013; Huddleston, 2016; Keck, 2016; Lakoff, 2017; Barker, 2020). Based on a distinctly modern vision of the future as a time-space filled with threat (Horn, 2018), preparedness structures the present in relation to an unexpected future event, cultivating a sense of unease and anxiety, in order to mobilise action and produce a state of readiness. These threatening future events are understood to be largely inevitable and unpreventable, but potentially manageable if the right measures are taken to anticipate them. If action is not taken, ‘a threshold will be crossed and a disastrous future will come about’ (Anderson, 2010: 780). Today, as visions of catastrophe proliferate, governments, emergency planners and disaster management providers increasingly warn us that we ‘must be prepared’ (Keck, 2015: 166).

The bunkered data centre offers a generative opening onto the increasing value and relevance that is being attached to digital data, as well as the dystopian fears and imaginaries surrounding the prospect of data loss. In what follows, I conceptualise the bunker as an architecture of data preparedness and examine how these buildings materialise and concretise data loss anxiety. I begin with a brief history of Cold War bunkers as data storage sites. Rather than mark a radical break or rupture in the function of the bunker, today’s bunkered data centres continue a history of subterranean data storage. During the Cold War, the nuclear threat affected governmental and corporate data storage practices (Aronova, 2017). A function of many bunkers was to provide a secure space for the anticipatory storage of analogue and, later, digital records. A focus on the bunker as a data storage site invites us to trace other anxieties that the nuclear threat threw into relief, such as the possibility of a major data loss event. Attentive to the ‘data pasts’ of the bunker, this article thus responds to recent calls to re-read and rethink conceptions of the form and function of these built spaces (Bennett, 2020; Garrett and Klinke, 2018: 16). I then proceed to trace the emergence of the bunkered data centre industry before exploring how data bunkers surface as imaginative sites of data preservation and security today. Finally, I examine how these sites are put to work in the marketing efforts of IT disaster recovery providers, who hope to encourage prospective clients to invest in data preparedness, producing the anticipative subjectivities of back-up culture. Here, I draw from interviews with DataVault employees and from promotional material on their website. The article concludes with a brief discussion of the ‘backed-up’ subjectivity produced through practices of data preparedness.

Data preparedness

Preparedness emerged in the mid-20th century as a technique of anticipatory governance with which Cold War military strategists could grapple with the possibility of a surprise nuclear attack (Collier and Lakoff, 2015; Lakoff, 2008: 406). The uncertainty of nuclear war confounded practices of risk management because this scenario lacked a statistical-archival past from which to calculate its impact. As such, strategists turned to the human imagination. As anthropologist Frédéric Keck (2016) has observed, preparedness is ‘a state of vigilance cultivated through the imagination of disaster’. Under the rubric of preparedness, Cold War strategists developed imaginative new practices with which they could prepare the nation for thermonuclear warfare, such as duck-and-cover drills, scenario planning, disaster simulations, resource stockpiling and, of course, the anticipative construction of bunkers (Bennett, 2011; Masco, 2009).

During the Cold War, bunkers were built in a variety of forms by different actors, from governments to individuals to private corporations, to serve a range of ends. The

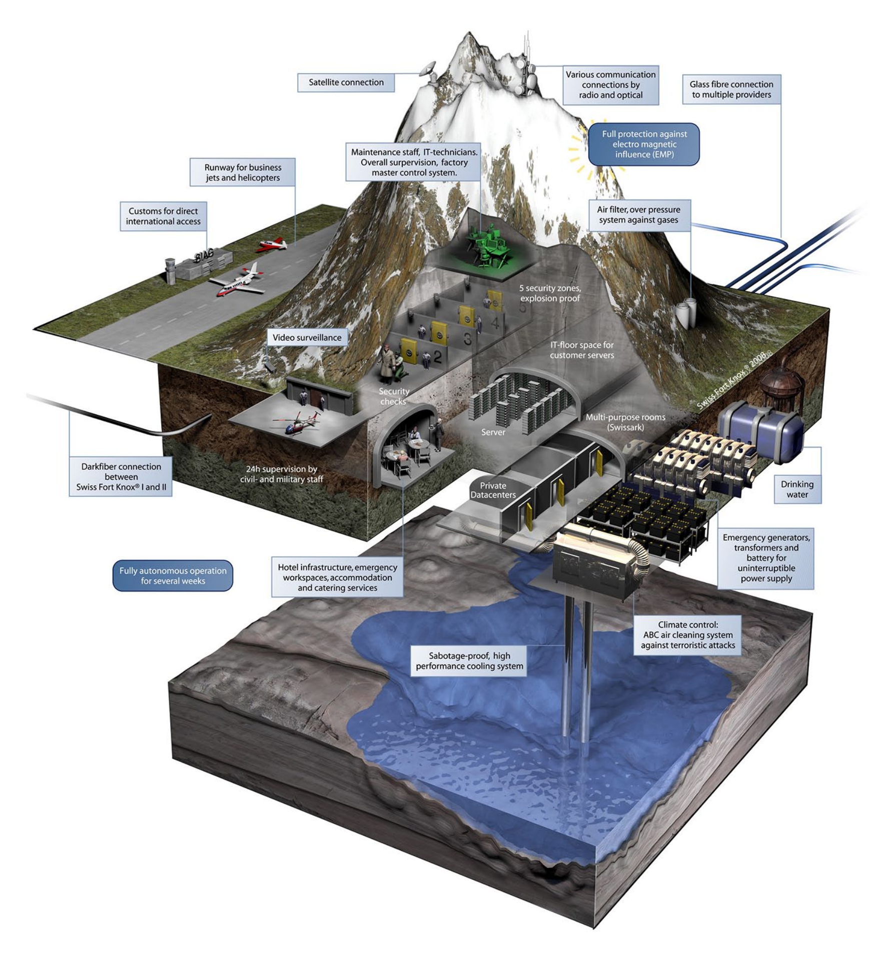
Satellite connection
Various communication connections by radio and optical
Glass fibre connection to multiple providers
Full protection against electro magnetic influence (EMP)
Maintenance staff, IT-technicians. Overall surpervision, factory master control system.
Runway for business jets and helicopters
Customs for direct international access
BIAG
Air filter, over pressure system against gases
5 security zones, explosion proof
2
3
4
5
Video surveillance
IT-floor space for customer servers
Swiss Fort Knox® 2008
Security checks
Server
Multi-purpose rooms (Swissark)
Darkfiber connection between Swiss Fort Knox® I and II
24h supervision by civil- and military staff
Private Datacenters
Drinking water
Emergency generators, transformers and battery for uninterruptible power supply
Fully autonomous operation for several weeks
Hotel infrastructure, emergency workspaces, accommodation and catering services
Climate control: ABC air cleaning system against terroristic attacks
Sabotage-proof, high performance cooling system

Figure 2. A cutaway diagram of one of Mount10's bunker facilities (image courtesy of Mount10).

bunker that DataVault operate had been a node in a hardened government communications infrastructure. It was built in the early 1950s and was continually expanded and reinforced throughout the second half of the 20th century. Outfitted with 10-foot-thick Ferro concrete walls, generators and filtered air conditioning, the hope was that it would survive a near miss by a 20- kT nuclear weapon as well as provide protection from radioactive fallout and biological and chemical agents. For the British government, this facility operated across multiple temporalities of emergency, promising security both before and after an attack. Prior to the imagined attack, the bunker played a key role within the UK Government's national 'early warning' network. Like data centres today, which are connected to a range of telecommunications providers, the bunker was not an isolated facility but a heavily connected site, forming part of a larger preparedness network through hardened telephone lines and microwave and teleprinter links. Connected to radar systems and centres of government via secure communications lines, DataVault's bunker was operated by the Royal Air Force (RAF) as a control and reporting centre. Data and images were transferred from radar stations around the United Kingdom and processed by personnel stationed deep within the bunker. On another temporal scale, in the aftermath of a nuclear strike, political elites hoped that fortified spaces such as DataVault's bunker would have enabled the survival and eventual re-emergence of government in a post-nuclear world. Severed communications would have made centralised governance impossible so state sovereignty would have been divided across regional bunkered spaces. In the United Kingdom, local commissioners would have been empowered to make sovereign decisions from within these autonomous regional centres of subterranean control (Duffield, 2011; Laurie, 1979).

In their genealogy of critical infrastructure protection, Stephen J. Collier and Andrew Lakoff (2008, 2015) have demonstrated that logics of preparedness initiate powerful reconfigurations of value whereby 'vital' assets can come to be prioritised over human life. While nuclear bunkers are often imagined as spaces of human protection, they were also high-tech sites of data protection. Indeed, during the Cold War, data was identified as a vital asset in need of securitisation and, as such, became a target of preparedness efforts. Governments recognised that the survival of data records was essential to the State's ability to continue functioning after a nuclear attack. As Ian Klinke (2018: 86) observes of the West German Government's bunker facility near Bonn, the underground complex sought to protect not only bureaucratic elites and nuclear weapons, but also 'its typewriters and its filing cabinets'. It was hoped that the underground location, in conjunction with the sheer materiality of hardened concrete and 'attack-proof' telecommunications connectivity, would protect the vital assets within the bunker from a nuclear blast and ensure their continued operation and accessibility afterwards.

Throughout the Cold War, DataVault's bunker served as a secure storage site for both analogue and digital data. Computing data was stored on-site in a range of formats, including punched paper tape, large magnetic drums (the size of washing machines), floppy discs and magnetic tape. Important information was often printed out, using teletype or line printers, and stored in blast-proof filing cabinets.[1] In the mid-1960s, the local government proposed that some of the vacant rooms in the DataVault bunker should be converted into document vaults for storing paper records. However, the humidity and moisture levels within the bunker would have required the installation of expensive air conditioning equipment to ensure that the paper would not be damaged by dampness. With civil defence funding cuts in 1968, the idea was abandoned.

Beyond the domain of government, the prospect of nuclear war led to the emergence of new security markets for bunkered data storage, with private companies constructing facilities specifically to preserve and protect vital or valuable materials (such as bank records, federal records, blueprints, patents, formulas, deeds, artworks and media) for corporations, media organisations and governments. A number of commercial records centres were established underground. Library historian Bruce Spencer has traced the emergence of these subterranean storage facilities during the Cold War, arguing that an 'important goal of America's doomsday planning was, in fact, to protect the country's information and cultural heritage' (Spencer, 2014: 145).[2] In 1951, the US-based data

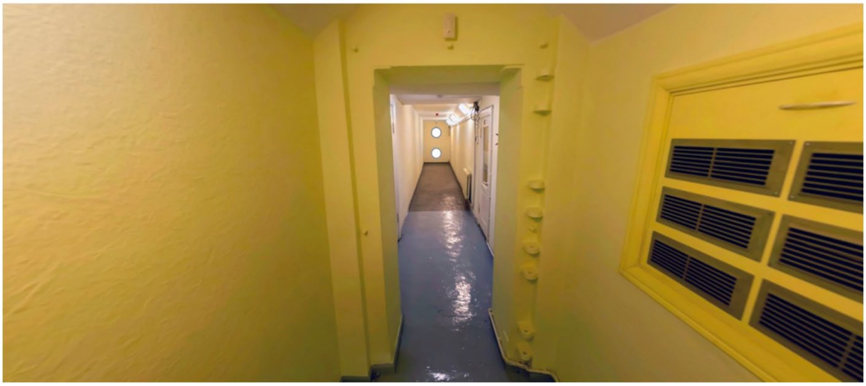

Figure 3. The European cloud provider DEAC has converted a former Soviet army bunker in Riga into a data centre. This screenshot shows the entrance to the facility, which is viewable via an online tour on their website (image reproduced under Fair Use Licence).

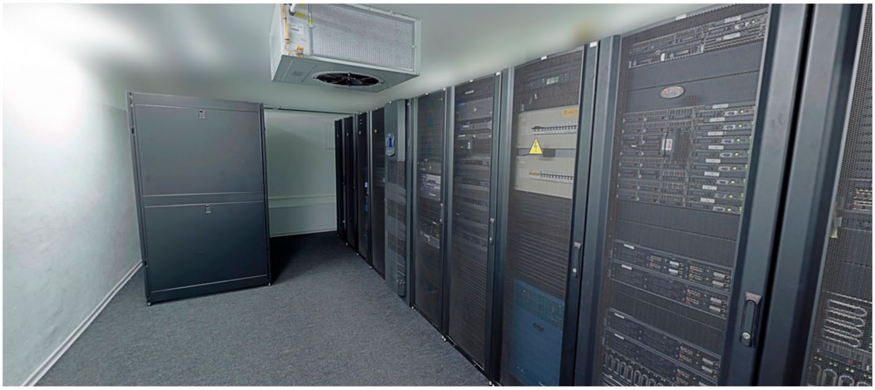

Figure 4. One of the server rooms in DEAC's bunkered data centre, as viewed from the online tour (image reproduced under Fair Use Licence).

management company, Iron Mountain Atomic Storage Corporation (IMASC), began operating secure data storage vaults in a former iron ore mine in upstate New York. Iron Mountain provided a subterranean space for valuable paper, microfilm and magnetic records. Their clients were predominantly New York City banks and insurance companies, who hoped to keep financial data safe and ensure that even a nuclear apocalypse would not wipe credit records. If nothing else, consumer debt would survive the end of the world. Iron Mountain specialised in the provision of business continuity, ensuring that corporate archives, office records and microfilm duplicates were securely protected. As Brian Murphy (2014) writes in his media-archaeological exploration of Iron Mountain:

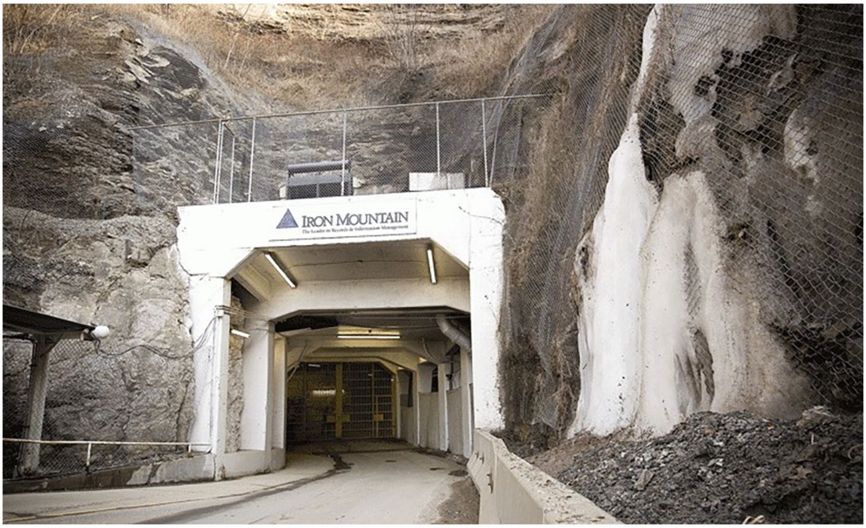

Figure 5. The entrance to one of Iron Mountain's storage vaults (image reproduced under Fair Use Licence).

> 'IMASC met a major need of corporations during the Cold War, the need to preserve their vital records in impervious spaces of preservation to ensure their business continuity – the reconstruction of their business history, the re-building of their facilities and equipment, and the resumption of production as soon as possible after a nuclear attack'.

Many other bunkers were also part of this history of Cold War data preparedness.[3] Towards the end of the Cold War, information management specialist J. Michael Pemberton (1990) highlighted the security affordances of subterranean data storage: 'Underground storage simply provides greater records protection than the above-ground facility can because it is virtually immune to the hazards that can raze even the best built building'.

While preparedness emerged as a mode of governance during the Cold War, it has since become a key feature of social and political life in the 21st century. After the terror attacks of 11 September 2001, preparedness surfaced across a range of sectors and policy domains, from public health to infrastructure security, as a key means of anticipating disaster (Aradau and Van Munster, 2012; Collier and Lakoff, 2015; Lakoff, 2008). Writing in 2006, Lakoff (2006: 265) suggested that preparedness 'is arguably the primary strategic logic through which threats to collective life are now being taken up'. Private sector preparedness consultancies have since proliferated, providing business continuity guidance and resources to organisations. Preparedness has not only provided governments and corporations with a formal framework for anticipating disaster but has taken root among members of the public, giving rise to prepper subcultures (Barker, 2020; Garrett, 2020, 2021; Hu, 2017; Mills, 2018). If prepping was once a fringe practice, represented in the media as a pastime of doomsday fantasists and often subject to media ridicule, cultural commentators have observed that it has now become 'an increasingly mainstream phenomenon' (Campbell et al., 2019: 799). Ethnographic work has suggested that the normalisation of prepping has been propelled by direct experiences of the intensifying conditions of everyday insecurity and permanent crises associated with late neoliberalism. As Bradley Garrett (2021: 403) notes, ‘this infolding of prepping practices into everyday life has also been concurrent with the aging of infrastructural systems, the privatisation of public services, and cuts to social “safety nets” under neoliberal ideologies in much of the western world’.

The material precarity of digital infrastructure and devices has also made preparedness part of the fabric of daily life in digital societies (Taylor, 2021b). Growing reliance on digital data, which is typically stored on fragile and failure-prone computing technologies, is increasingly being positioned as a source of insecurity in an increasingly datafied world. Cloud computing providers and data back-up and recovery companies like DataVault regularly highlight in their marketing communications that computers can crash, hard drives can fail, and smartphones and laptops might be dropped or stolen, encouraging users to invest in IT business continuity plans and cloud subscriptions. As Webster explained to me during my visit to DataVault, ‘digital tech is designed to fail, a disaster is inevitable, the only question is whether or not you’re prepared for it’. Stories and warnings of data loss proliferate in online marketing blogs sponsored by data recovery specialists, where readers are reminded that ‘data loss can occur at any time’ (McMacken, 2012). The regular backing up of devices that users are enjoined to carry out if they want to ensure their data is retrievable in the event of device failure, is one example of preparedness practices being woven into everyday life. Users are increasingly induced to prepare for IT failure through a variety of data preparedness practices, such as backing-up files onto an external hard drive or into the cloud, with the hope that by taking anticipatory action in the present they will avoid losing their valuable data when their digital devices fail in the future. For businesses and organisations, data preparedness takes the form of outsourcing data storage to data centres and investing in disaster recovery services, such as those provided by DataVault. By encouraging individuals and organisations to sequester their data in the cloud in anticipation of disaster, cloud computing companies ask users to internalise a ‘bunker mentality’ (Hu, 2015: 82; see also Bell, 2008). This bunker mentality stretches beyond the cloud, materialising through user practices of copying files across multiple storage media, from USB flash drives to larger back-up hard drives. External hard drives themselves, in their ‘rugged’ and ‘shockproof’ variants, increasingly take the form of portable data ‘bunkers’ (Fig. 6). Lucrative markets for data preparedness have thus emerged under the techno-precarious conditions of digital culture, and the bunker has arisen as both a metaphor for conceptualising back-up practices and as a material data storage site.

From the mushroom cloud to the computing cloud

Since the dissolution of the Soviet Union in 1991, Cold War bunker space has largely been dominated by commercial interests. This is perhaps best captured by the currently fashionable trend of refurbishing bunker complexes into doomsday-ready survival condos for the super-rich to sitout the demise of civilisation (Garrett, 2020, 2021; Graham,

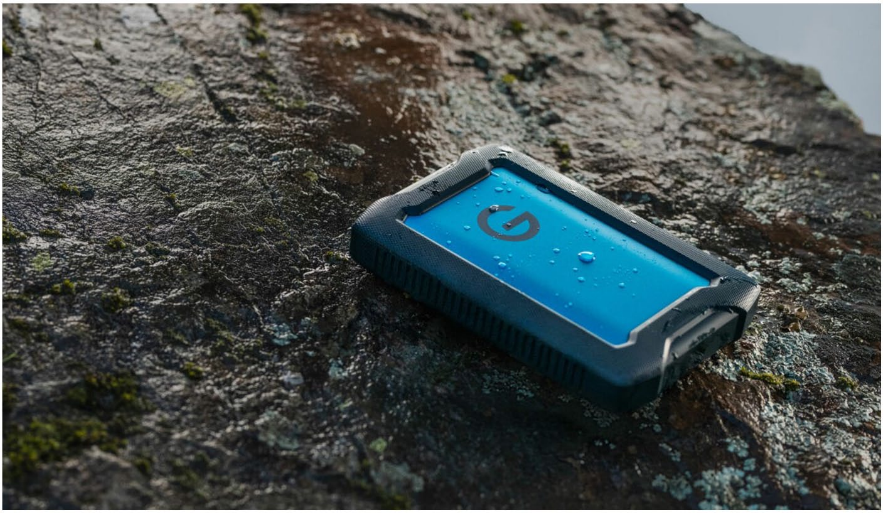

Figure 6. 'Rugged' storage media, like G-Technology's 'ArmorATD', scale down the bunker to the level of the external hard drive. Built into a solid aluminium enclosure, with internal shock mounts and a protective rubber bumper, this armour-plated hard drive promises 'triple- layer shock resistance' and a crush resistance of up to 1000lbs (450 kg). The rain-soaked stone in the backdrop of the advertising shot conjures the material strength, durability and water resistance of the drive (image reproduced under Fair Use Licence).

2016; Preston, 2019). Here, the bunker is no longer branded as a nuclear shelter alone. As Bradley Garrett and Ian Klinke (2018: 13) have observed, the bunkers that are being put to use today are not 'limited to a specific disaster imagination'. Rather, they promise to provide protection from the ever-multiplying disaster scenarios that vie for attention in post-Cold War securityscapes, including terrorism, pandemics and the extreme weather of the Anthropocene.

Among the multitude of uses to which bunkers have been put, they have perhaps found one of their most prolific afterlives as commercial data centres. One of the first businesses to market bunkers as disaster-proof cloud storage sites was the Swiss-based IT security solutions company, Mount10 (pronounced 'Mountain'). Mount10 converted a bunker in the Swiss Alps into a data centre in the early 1990s. Later, a glass fibre connection was installed to link this facility to another bunker located 10 km away. This data bunker complex is still in use today and is known as the 'Swiss Fort Knox'. The play on the name of the famous US bullion depository highlights the security-centric focus of the company while also alluding to the value of data as 'the new gold'. Another early pioneer of the bunkered data centre model was CyberBunker, a Dutch IT company that purchased the shell of an ex-NATO bunker in the Netherlands in the mid-1990s (Caesar, 2020). A couple of years later, in 1999, an abandoned bunker in the south of England was purchased by a London-based web hosting company and the site was marketed as 'The Bunker Secure Hosting Ltd.'

These bunkered data centres embedded data storage within a fittingly millenarian register. By the late 1990s, there was rapidly intensifying corporate and political awareness

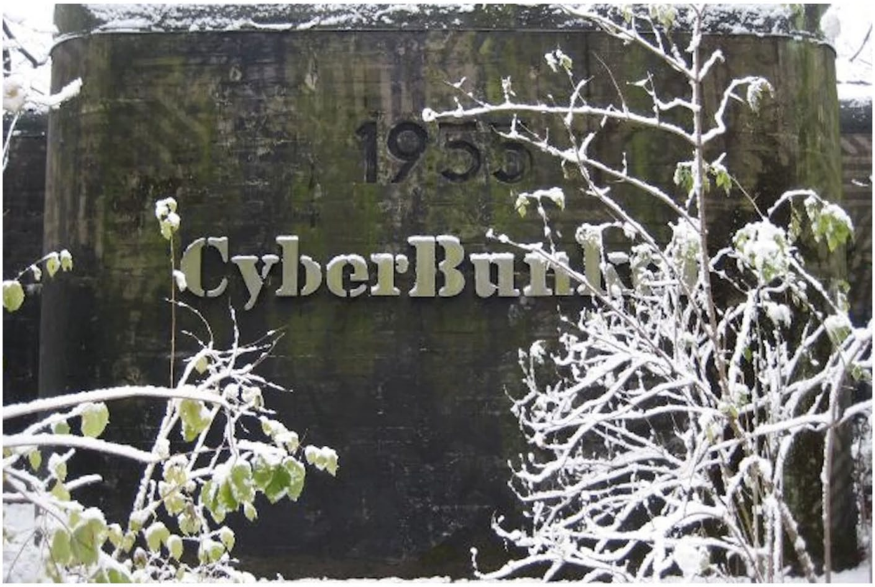

Figure 7. The CyberBunker data centre promised its clients ‘bulletproof web hosting’. It was known for hosting phishing sites and other websites linked to the dark web (Caesar, 2020). Despite its ‘bulletproof’ exterior, in 2002, the servers were removed from the facility after a fire broke out, revealing that the site had also hosted an MDMA manufacturing lab (image reproduced under Fair Use Licence).

of the potential for digital collapse arising from an escalating reliance on vulnerable computer systems. Concerns about the economic and societal impact of cyber attacks were growing (Cavelty, 2008). Anxieties surrounding the apocalyptic scenario of the millennium bug were accelerating, with many organisations concerned that Y2K could potentially ‘reset’ the digital world, leading to extensive data loss (Edwards, 1998; Pärna, 2010). The imagined prospect of the Digital Dark Age was also gaining traction, motivating the development of a number of web archiving projects.

Arising amid these ever-expanding visions of digital threat and collapse, bunkered data centres promised to provide a level of security that their above-ground competitors did not possess. The dot-com bubble (roughly between 1995 - 2002) had seen a boom in data centre construction, as businesses flocked to the internet. Driven by venture capital and speculative investment, the leading priority for data centre developers during this period, was speed of construction, rather than security. This was reflected in the names of data centre developers at the time, such as ‘DataCentersNow’. As *Washington Post* journalist Jackie Spinner (2001) observed of the United States: ‘hundreds of data centres were built around the country and wired for Web servers’. The data centres that were located in bunkers anticipated the prominent role that security would come to play in the making and selling of online data storage over the next two decades. The terror attacks of 11 September 2001 threw into relief the vulnerable materiality of the increasingly virtualised cyber-systems that underpinned digital capitalism. The collapsing Twin Towers destroyed a number of mission-critical data centres in lower Manhattan, leading to IT downtime and data loss for many banks and businesses in the days immediately following the attacks (Miller, 2011). The Internet exchange points, telecommunications carrier hotels and data centres that were not damaged by the falling buildings struggled to operate in a landscape of shattered infrastructure. Dust and other particulate matter from the debris entered the filtration systems of servers and the air conditioning units that kept them cool. This led to equipment overheating and shutting down, leaving those organisations that did not have a back-up data centre somewhere outside of the affected disaster region, offline for extended periods of time.

The post-9/11 securityscape saw growing numbers of data centre providers purchasing nuclear bunkers. In an article discussing his venture into the data bunker business, Larry Hall, the owner of the luxury prepper bunker complex in Kansas known as the Survival Condo, identifies 9/11 as a key security moment, observing that, ‘After 9/11 I thought there would be a need for nuclear-hardened data centres’ (Hall, cited in Moss, 2018a).[4] This ‘bunkering’ of data centres took place amid a wider fortification of the industry. Data centres increasingly promoted their security, with their ‘hardened’ construction becoming a key selling point.[5] While many of these security-centric data centres were not located inside bunkers, they nevertheless expressed the defensive logics of the bunker: they were strategically located in low-risk geographic areas, either on the peripheries of urban centres or in rural settings that were not likely terrorist targets; they were often based in nondescript buildings, designed to disappear into the industrial landscape; they were driven by preparedness, with extensive redundant equipment available and diesel stockpiled to ensure uninterrupted service delivery in the event of a power grid collapse.[6] Commenting in 2002 on the ‘CyberFortress’, a data centre design developed by Fortress Development Co., journalist Tom Vanderbilt (2010 [2002]: 198) identified these new, security-centric data centres as ‘a contemporary incarnation of the Cold War architectural ethos’.[7]

While above-ground data centres became increasingly bunker-like, underground bunker space continued to attract data centre providers.[8] Writing in 2009, the technology journalist Rich Miller (2009) referred to the surging trend of repackaging Cold War bunkers into ultra-secure data storage facilities as ‘the data bunker boomlet’.[9] In the decade following Miller’s article, the trend has further intensified, with journalist Sebastian Moss (2018a) noting in 2018 that, ‘An Apocalyptic legacy is being used to build data centres ready for the next major disaster’.[10] Some providers are even building entirely new bunkers from scratch to house digital data (Moss, 2018a).

Data durabilities

Bunkers have long functioned as complex sites of temporality and apocalyptic imagination. Paul Virilio (1994), W.G. Sebald (1998) and J.G. Ballard (2006) were all drawn to the decaying bunkers of the Second World War and their peculiarly heterochronic temporalities. As 20th century feats of military engineering, they appeared distinctly modern, yet in their dilapidated states they seemed to provide onlookers with an eerie vantage point from which to view artefacts of their own time as ruins of the future. The bunkered data centre conjures apocalyptic visions of the end of the digital world (Taylor, 2021a). The byline of a news article on a data bunker in Paris reads, ‘You may not be there to see the apocalypse,

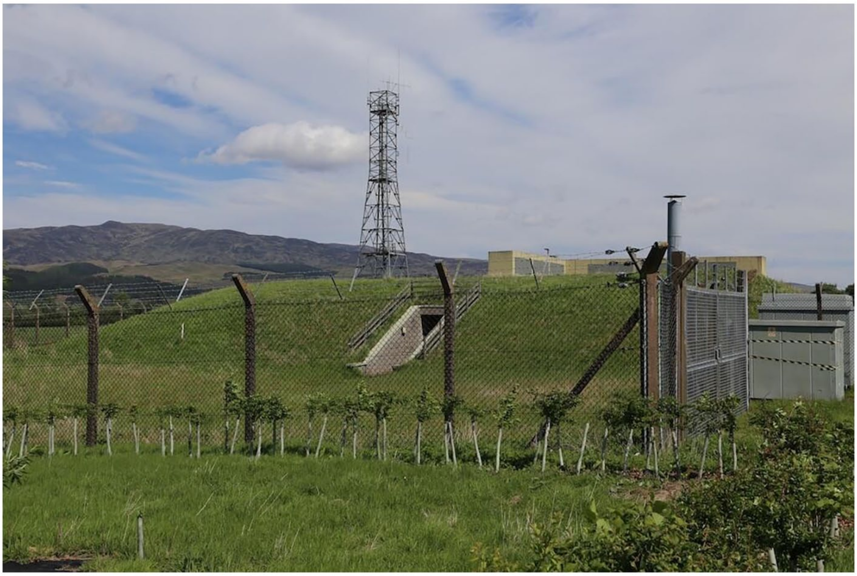

Figure 8. In 2014, the UK-based web service provider Bogons purchased a nuclear bunker near Comrie in Perth and Kinross, Scotland (image reproduced under Fair Use Licence).

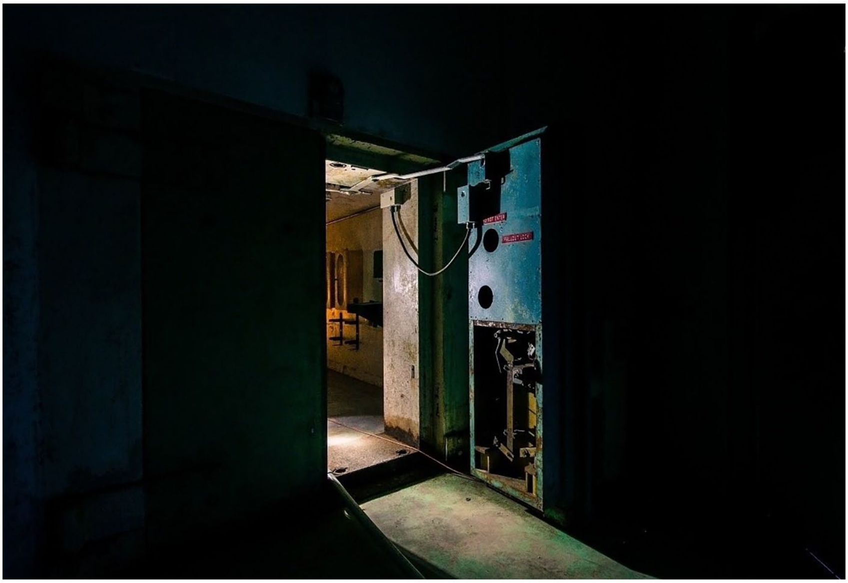

Figure 9. The Florida-based data centre operator Data Shelter uses a former Department of Defence bunker that was built in Fort Pierce during the Cold War by telecommunications company AT&T. Dramatic chiaroscuro photographs of the facility feature on the website (image reproduced under Fair Use Licence).

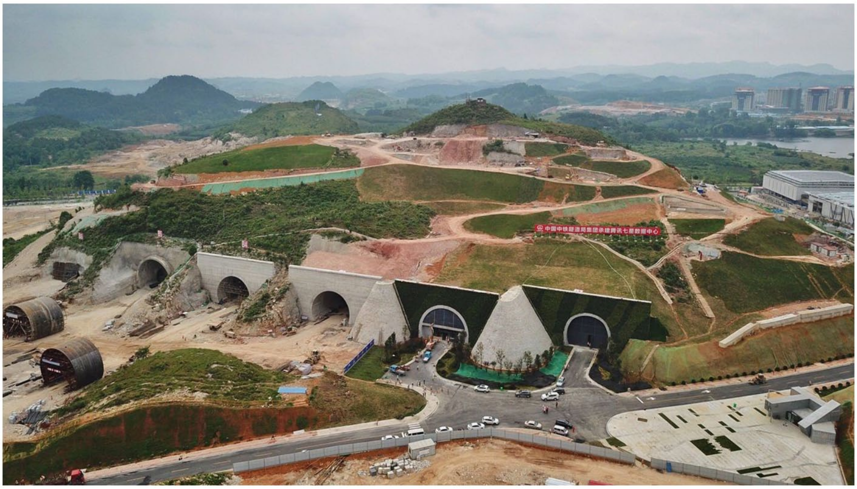

Figure 10. As of 2018, a 51-hectare civil defence shelter complex in the hills of Guizhou, China, is being renovated as a space to store 'the most vital data' (Moss, 2018b) of the Chinese technology company Tencent (image reproduced under Fair Use Licence).

but your selfies will' (Moss, 2016). These sites invite viewers to imagine their subterranean servers as the remnants of digital society after its future collapse. As Paul Scott, a network operations engineer at DataVault's bunker, explained to me during a visit to the site, 'archaeologists of the future will find these hard drives and be fascinated by them'.

The durability of bunkers is a frequent focal point in the promotion and marketing of these sites (Jakobsson and Stiernstedt, 2012). Mark Oxley, the Chief Technology Officer of Florida-based Data Shelter, has argued that bunkers are 'built to last', which makes them superior data security sites: 'A lot of the [security] issues that are occurring are because people are building these warehouse-style facilities that are thrown up very quickly, inexpensively, with very little design thought' (Oxley, cited in Moss 2018). Oxley is keen to foreground the value of data bunkers amidst what he presents as a historical moment of increasing insecurity: 'we're getting into a time in the world where things are becoming less and less secure', he states. The robust materiality of data bunkers is perceived by operators to provide security against threats that range from terror attacks, break-ins, car bombs, electromagnetic pulse (EMP) events, vehicle-ramming attacks and the extreme and unpredictable weather associated with global climate change. As Todd Murren (2018), the General Manager of Bluebird Network, which operates a data centre based in a limestone mine in Missouri, highlights: 'The surrounding rock within a mine creates a natural shield from all weather extremes and events'. Articulating the anytime-anywhere potential for disaster that characterises preparedness, Murren reminds us that severe weather 'exists everywhere' and 'can operationally impact any region or above-ground structure'.

Given the imaginaries of durability and futurity that bunkers conjure, it may come as no surprise that several media preservation providers and archiving projects use bunker-style structures to store their digitised collections. In particular, a number of mountain

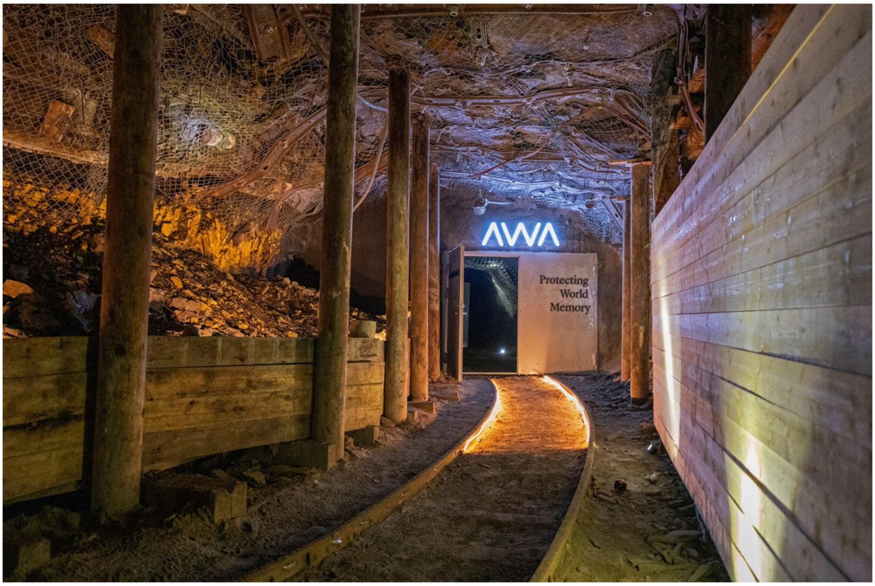

Figure 11. A mineshaft leading into the Arctic World Archive's data preservation site on Svalbard (image courtesy of Piql).

bunkers and former mines have been re-engineered as digital data repositories. Since 2000, the National Library of Norway has stored their digital databanks in mountain vaults near Mo i Rana, just south of the Arctic Circle. In 2004, the Cold War-era information management company Iron Mountain moved into the digital data storage market, establishing its digital assets division 'Iron Mountain Digital'. Secure server rooms are now embedded within a number of their underground complexes, many of which Iron Mountain purchased from their Cold War storage competitors. More recently, in 2017, the data preservation company Piql (pronounced 'pickle') transformed an abandoned coal mine located on the archipelago of Svalbard in Arctic Norway into a data storage site. This subterranean data shelter, known as the Arctic World Archive (AWA), is modelled on the nearby Global Seed Vault. Just as the seeds preserved in the Global Seed Vault promise to help re-build biodiversity in the aftermath of future collapse, the digitised records stored in the AWA promise to help re-boot organisations after their own collapse. The site has been described by some as 'the digital world's "Doomsday Vault" (Carter, 2017). On the AWA website, Piql state that their mission is 'to keep data alive for centuries' and ensure the 'guaranteed future accessibility' of the data that governments, corporations and other economic elites pay to store there. The underground storage facility features prominently on their website, providing viewers with a theatrical glimpse of the secure, solid and durable materiality of the data storage mine.[11]

While digital archiving and media conservation efforts are defined by the long-term temporal horizons of preservation, data centre storage unfolds across a range of temporalities, which are typically described using the metaphor of temperature. 'Hot' and 'cold' data storage services (and variants in between) describe different levels of data access and availability (and different modalities of data preparedness).[12] 'Cold' data refers to data that clients do not need to regularly access. 'Hot' data typically refers to frequently used data and critical files for which clients need 'uninterruptible' access. These different data temporalities often utilise different storage media, with hot data typically using speedy disk-based storage systems like hard disk drives, and cold data often using slower storage media such as magnetic tape, due to its reliability, portability, power efficiency and cheaper cost per gigabyte stored.

One of the key shifts in the transition from the Cold War bunker to the digital data centre, from the perspective of data preparedness, is the expansion of data storage temporalities. If the Cold War bunker primarily locked media in time, with the aim of preserving an organisation's 'least used – but vital – records' (Pemberton, 1990), many of today's bunkered data centres aim to provide continuous, uninterruptable, access to frequently used data. As Wolfgang Ernst has observed, digital media archives represent a shift away from a 'culture concerned primarily with storage, to a new media culture built on permanent transfer' (Ernst, cited in Røssaak, 2010: 19). Data preparedness, for data bunkers and their clients alike, is thus not just about long-term storage, but also about ensuring the constant availability of data on a second-by-second basis.

DataVault offers a range of storage and retrieval services for hot, warm and cold data requirements. However, the majority of their clients are concerned with ensuring uninterruptible access to their hot data. This was highlighted by Paul Scott during my visit to DataVault's bunker. Scott explained that, for many clients, losing access to their data for even a few seconds could have a huge economic impact or put an end to their business. 'It's not the nuclear bomb that we [DataVault], or our customers are really worried about', he explained, 'it's downtime and data loss'. He took the opportunity to emphasise the importance of the bunker for delivering uninterruptible data access and disaster-proof data security. 'Bunkers are not just built to last', he explained, they are 'built to continue operating no matter what'. For Scott, the bunker provided servers with a form of security that surpassed other data centre types. 'Storing data in a bunker may seem a bit like overkill' he conceded, 'but when it comes to server hard drives, which are incredibly fragile, you want them to be stored in a building that wouldn't budge even if there was a nuclear blast'. Describing a downtime or data loss event as 'the nuclear bomb of the digital age', he told me that 'it's no surprise that more and more people are turning to bunkers'.

Data loss dread

A significant part of DataVault's sales and marketing strategy focuses on inviting prospective customers to question the security of their existing data storage provider and promoting the bunker as the most effective, secure solution. Testimonials on their website prompt visitors to imagine a threat to their data and to become prepared. One client testimonial reads: 'We didn't realise how unprepared we were. DataVault have made us more aware of what's at stake if our vital systems go down. Now, we're not just better protected, but we're also better informed. It'd be hard to cope without DataVault in a disaster'. Other testimonials emphasise the bunker, stating that 'DataVault surpassed all our security requirements with their nuclear-proof data centre'. Bunkered data centre marketing teams invest considerable effort in prompting imaginaries of digital disaster in

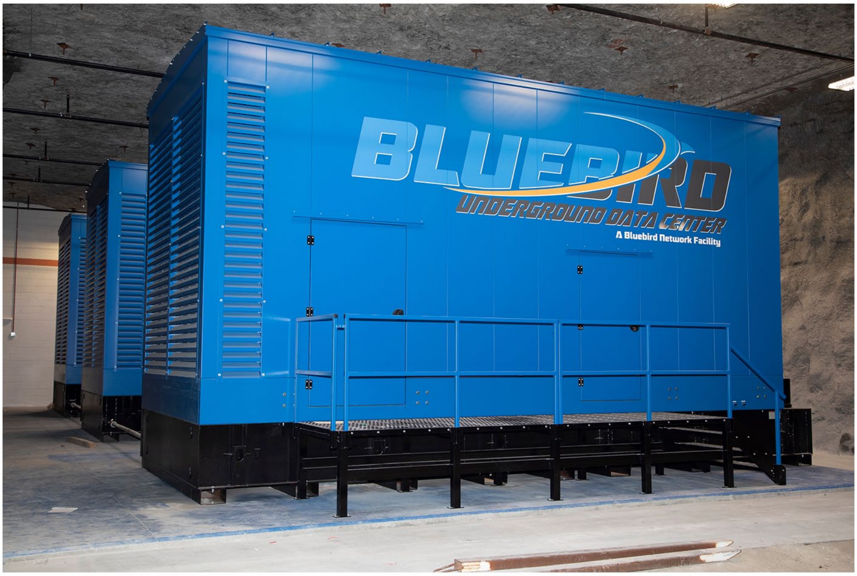

Figure 12. Bluebird Network operates an underground data centre located in a former limestone mine in Missouri. The facility uses 2MW diesel-fuelled generators (pictured above) for its emergency off-grid power supply (image courtesy of Bluebird Network).

order to demonstrate the security affordances and infrastructural endurance of bunkered data storage (Taylor, 2021a). On site tours, the operators of these subterranean data shelters foreground the durability and materiality of their bunkers, hyperbolically promising their clients that their data stands the best chance of remaining online if it is safely entombed underground behind 17-inch-thick blast-proof doors, reinforced concrete walls and razor-wire security fencing. As a security showpiece for disaster recovery providers, bunkers play a leading role in conjuring the prospect of a future 'datapocalypse' so that customers may pre-empt and avoid that dystopian scenario. Indeed, Hu (2015: XXVII) has observed that 'data bunkers [. . .] raise the spectre of attack', prompting potential customers to imagine a threat to their data. While promoting the bunker, then, DataVault are keen to establish the permanent and ever-present possibility of data loss and to promote a sense of dread and anxiety surrounding this prospect.[13] During my visit to DataVault's offices, Webster repeatedly highlighted that, when it comes to IT failure, 'it's not a question of "if" but "when"'. Articulating the temporal logics of emergency and inevitability that drive disaster preparedness, he explained that 'we're all dependent on data today and dependence on anything is always a vulnerability [. . .] the time to prepare was yesterday'. Data preparedness is always an incomplete project, producing an angst-inducing sense that you can never be prepared enough.

At the same time, while bunkered data centres promise preparedness for all manner of threats, they offer little security when it comes to the turbulent market logics of digital capitalism. This is a landscape of mergers and acquisitions, financial speculation,

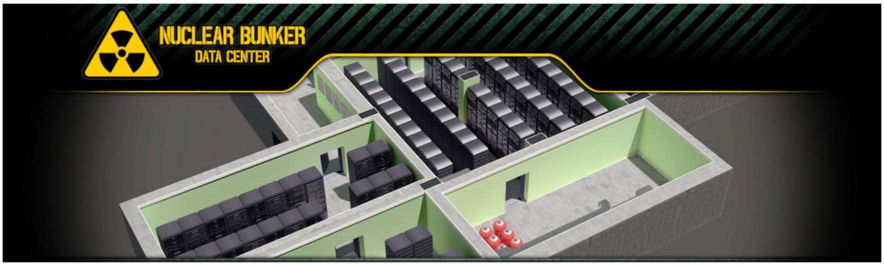

Figure 13. The homepage banner from the website of a Lithuanian data bunker company, The Nuclear Bunker, which was based in a former Soviet bunker in Vilnius but has since closed down. This screenshot was taken in 2018 (image reproduced under Fair Use Licence).

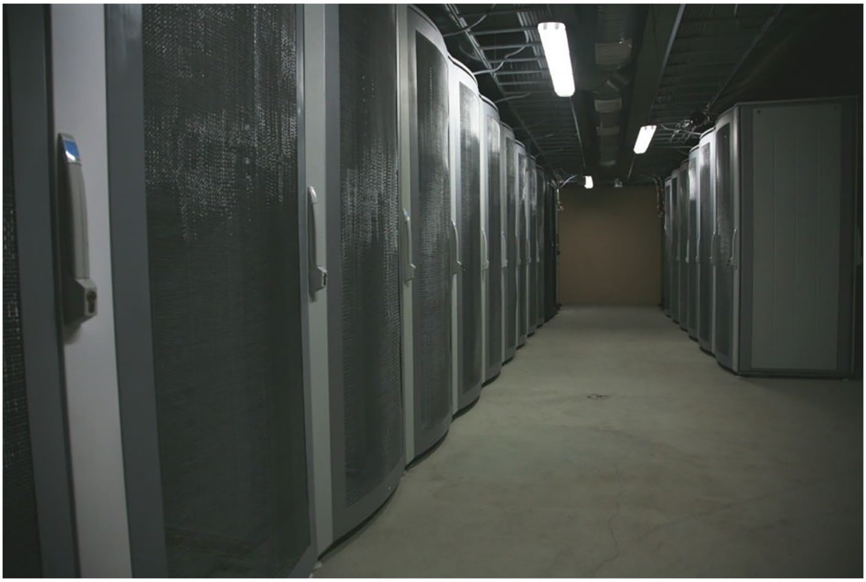

Figure 14. One of the Vilnius Nuclear Bunker's server rooms, prior to closure (image reproduced under Fair Use Licence).

media and marketing performances, shifting corporate strategies and ever-accelerating cycles of technological obsolescence that leaves behind a trail of 'cloud ruins' (Brodie and Velkova, 2021; see also Velkova, 2019). Indeed, the history of the data centre industry is a history of boom and bust which has, over the years, left many data centres vacant, both above-ground and below-ground. After the dot-com bubble burst in the early 2000s, the data centre market was 'saturated with empty buildings [. . .] flooding the commercial real estate market with millions of square feet of space' (Spinner, 2001). In response to the volatile and ever-changing market landscape of the global tech sector, data centre providers are constantly dissolving, rebranding and decomissioning and relocating their facilities. Data centres located in bunkers, mines or other hardened structures may promise 'eternal' or 'ultra-secure' data storage but the durable materiality of the bunkered data centre stands in stark contrast to the fast-paced world of big tech.

Bunkered data centres also face a number of other challenges. It is expensive to maintain these aging structures and it can be costly to retrofit, modify, modernise, reinforce and waterproof them (though often the cheap price of bunker real estate is perceived to balance these costs). Securing permits for underground generators and fuel tanks is also expensive. Data centres need to regularly load and unload large equipment (which is typically refreshed on an annual basis) and this can be a slow and difficult process in the small corridors of a bunker. Irregular surfaces, in the case of mines or caves, can make installing equipment difficult. Bunkers were built in anticipation of disaster, not in anticipation of the accelerated growth of 'Big Data'. As such, they were rarely designed with logics of scalability in mind. It is often a costly enterprise to expand the operational server space of a subterranean facility, though this is not always the case. With the help of tax breaks, Bluebird Network, for example, have twice expanded the size of their bunker-style data centre (Alley, 2019).

Conclusion: the backed-up subject

Cultural geographer Luke Bennett (2011: 157) has suggested that bunkers 'are a material testimony to the anxieties of their creators'. In this article, I have argued that the bunkered data centre provides a valuable entry point for exploring anxieties surfacing around the prospect of data loss. The bunkered data centre does not just respond to the imagined threat of data loss but plays a key role in generating these imaginaries, with commercial data recovery businesses actively working with the bunker to materialise data loss anxiety and enjoin users to become prepared. A significant body of scholarship has highlighted that Cold War bunkers were not simply responses to nuclear threat (Bell, 2008; Duffield, 2011; Lutz, 1997; Masco, 2009). Rather, Civil defence bunker-building projects were a key tool for manufacturing dread and moulding citizens into 'Cold Warrior' subjects who were 'restructured internally for constant readiness and hardened by nuclear fear' (Masco, 2014: 128). Catherine Lutz (1997: 248) has linked the nuclear bunker to a larger 'normalisation of a militarized civilian subjectivity' that took place during the Cold War. If the nuclear bunker produced an anticipative subject that was prepared for the ever-present existential risk posed by atomic weapons, through the bunkered data centre we can trace the production of the 'backed-up' subject of data preparedness. This backed-up subjectivity is not restricted to those who store their data in nuclear bunkers. With data loss and downtime constructed as ambient threats of digital culture, cloud service and back-up providers are engaged in the business of transforming digital citizens into 'data preppers', offering a range of personal cloud subscriptions. For those that are especially concerned about the futurity of their data, the bunker promises shelter from a precarious digital present in which growing dependence on fragile storage media produces the ever-present potential for digital disaster.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

ARE Taylor https://orcid.org/0000-0002-1732-9342

Notes

1. Alex Wallerstein (2011) has described the nuclear explosion tests that were conducted on records storage equipment, such as filing cabinets, to ensure that bureaucratic records would survive a nuclear inferno.
2. Cultural heritage was a key target of Cold War preparedness in the United States. As Shannon Mattern (2017: 55) writes: ‘American government officials and military leaders began working with librarians and archivists to develop strategies for preserving the country’s cultural and scientific resources: devising emergency preparedness plans for safeguarding government and business records; testing the effects of nuclear explosions on different storage media; building vaults in government buildings and establishing “shadow” repositories in off-site subterranean facilities’.
3. See The Centre for Land Use Interpretation’s (CLUI) project on subterranean records storage facilities in the United States (CLUI, 2017a, 2017b).
4. The bunkering of the data centre industry must also be seen as part of a much larger ‘bunkerisation’ of space that intensified after 9/11, with the wealthy increasingly retreating into fortified SUVs, hardened condo complexes, gated communities and other private enclaves (e.g. see Coaffee and Wood, 2006; Graham, 2010; Klauser, 2010; Low, 2003).
5. Luke Munn (2020: 168) has observed, that these data centres promised ‘indestructible operations [. . .] maintained through fortification’.
6. A number of cultural commentators have since compared data centres to bunkers. Adam Fish and Bradley Garrett (2019) have conceptualised the data centre as a continuation and expression of bunker logics, suggesting that data centres might be productively understood as ‘byte bunkers’. In an article exploring the climate-controlled environs of data centres, Jeffrey Moro (2021) has also drawn upon the bunker metaphor, describing data centres as ‘climate bunkers’.
7. Fortress Development Co. was in fact the rebranded name of the dot-com data centre construction company DataCentersNow. Commenting on the name change in the *Washington Post,* Spinner (2001) reflected that this signaled a shift in the business direction of the company and, perhaps, a larger shift in the data centre industry itself, from a focus on speed to a focus on security. Rather than constructing data centres quickly (‘Now’) for the then-booming telecommunications sector, after 9/11 the focus was on building ‘highly secure facilities for corporate or government tenants’ (Spinner, 2001)
8. In 2003, an ex-Ministry of Defence bunker in Lincolnshire (UK) was repurposed as a data centre by Centrinet Limited, a data security company specialising in data network management. That same year, a bomb shelter in Houston, Texas, was repurposed as a data centre that was branded the ‘Houston Bunker’. An Iowa-based date centre operator, Infobunker, purchased a subterranean military bunker in Des Moines (after extensive renovations this facility went live in 2006). In 2004 the UK-based web hosting provider The Bunker Secure Hosting Ltd. purchased a second data bunker at Greenham Common airbase near Newbury. In 2008, the Swedish telecommunications operator Bahnhof opened a data centre inside the former civil defence shelter known as Pionen, located beneath Stockholm. In 2009 a number

of European cloud providers converted derelict Soviet bunkers into data centres in Riga (Latvia), Vilinus (Lithunia), and, in the following year, Kiev (Ukraine).

9. In 2011, the cloud company Deltalis transformed a Swiss Army bunker into a data centre (now defunct). In 2012, a derelict passive defence shelter in Paris, dating back to 1937 (upgraded and expanded during the Cold War) was auctioned off by the state to the cloud operator Online.net, who opened it to clients in 2017. In 2018 renovations began on a fifty-one hectare civil defence shelter complex in the hills of Guizhou, China, converting the site into a data centre for the Chinese technology and entertainment conglomerate Tencent. Also in 2018, a US data centre operator transformed a communications bunker in Fort Pierce, Florida (built during the Cold War by the US Department of Defence and the telecommunications company AT&T) into a data storage site named 'Data Shelter'. Other sites of bunkered data include Nova Scotia (Canada), Comrie (Scotland) and a munitions storage site in the Finger Lakes region of New York.
10. As Hu (2015: 98) observes, 'The establishment of one data bunker produces an imagination of disaster that replicates, endlessly, as more data bunkers'.
11. Peter Jakobsson and Fredrik Stiernstedt (2012) have explored how the materiality of rock and stone is mobilised in the marketing efforts of the Swedish telecommunications operator Bahnhof, who operate an underground data centre located in a former civil defence bunker in Stockholm.
12. Of course, outside the domain of data preservation, the metaphor of temperature has a long history in the field of media and communication studies as a conceptual tool for grappling with the different material properties of media technologies (McLuhan, 1994; Starosielski, 2021).
13. Garrett (2020) has used the felicitous phrase 'dread merchants' to describe the entrepreneurs in the business of selling bunkers to preppers.

References

Adams V, Murphy M and Clarke AE (2009) Anticipation: technoscience, life, affect, temporality. *Subjectivity* 28(1): 246–265.

Alley A (2019) Bluebird Network plans second underground data center expansion. Available at: https://www.datacenterdynamics.com/en/news/bluebird-network-plans-second-underground-data-center-expansion

Anderson B (2010) Preemption, precaution, preparedness: anticipatory action and future geographies. *Progress in Human Geography* 34(6): 777–798.

Aradau C and Van Munster R (2012) The time/space of preparedness: anticipating the 'next terrorist attack'. *Space and Culture* 15(2): 98–109.

Aronova E (2017) Geophysical datascapes of the Cold War: politics and practices of the World Data Centers in the 1950s and 1960s. *OSIRIS* 32: 307–327.

Ballard JG (2006) A handful of dust. Available at: https://www.theguardian.com/artanddesign/2006/mar/20/architecture.communities (accessed 2 August 2021).

Barker K (2020) How to survive the end of the future: preppers, pathology, and the everyday crisis of insecurity. *Transactions of the Institute of British Geographers* 45(2): 483–496.

Beck J (2011) Concrete ambivalence: inside the bunker complex. *Cultural Politics* 7: 79–102.

Bell DF (2008) Bunker busting and bunker mentalities, or is it safe to be underground? *South Atlantic Quarterly* 107(2): 213–229.

Bennett L (2011) The bunker: metaphor, materiality and management. *Culture and Organization* 17(2): 155–173.

Bennett L (2020) The bunker's after-life: cultural production in the ruins of the Cold War. *Journal of War & Culture Studies* 13(1): 1–10.

Bratton BH (2015) *The Stack: On Software and Sovereignty*. Cambridge, MA: MIT Press.

Brodie P and Velkova J (2021) Cloud ruins: Ericsson's Vaudreuil-Dorion data centre and infrastructural abandonment. *Information, Communication & Society* 24(6): 869–885.

Caesar E (2020) The Cold War bunker that became home to a dark-web empire. Available at: https://www.newyorker.com/magazine/2020/08/03/the-cold-war-bunker-that-became-home-to-a-dark-web-empire (accessed 2 August 2021).

Campbell N, Sinclair G and Browne S (2019) Preparing for a world without markets: legitimising strategies of preppers. *Journal of Marketing Management* 35(9–10): 798–817.

Carter J (2017) 10 extreme data centres that look straight out of a sci-fi movie. Available at: https://www.techradar.com/news/10-extreme-datacenters-that-look-straight-out-of-a-sci-fi-movie (accessed 12 July 2021).

Cavelty MD (2008) *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. London: Routledge.

Charles E (2016) White mountain. Available at: http://www.emmacharles.com/white-mountain/ (accessed 12 July 2021).

CLUI (2017a) Hollowed earth: the world of underground business parks. Available at: http://www.clui.org/section/hollowed-earth-world-underground-business-parks (accessed 4 August 2021).

CLUI (2017b) Going deep: an overview of the underground. Available at: http://www.clui.org/newsletter/winter-2017/going-deep (accessed 4 August 2021).

Coaffee J and Wood SM (2006) Security is coming home: rethinking scale and constructing resilience in the global urban response to terrorist risk. *International Relations* 20(4): 503–517.

Collier SJ and Lakoff A (2008) The vulnerability of vital systems: how 'critical infrastructure' became a security problem. In: Cavelty MD and Kristensen KS (eds) *Securing 'The Homeland': Critical Infrastructure, Risk and (In)security*. New York: Routledge, pp. 17–39.

Collier SJ and Lakoff A (2015) Vital systems security: reflexive biopolitics and the government of emergency. *Theory, Culture and Society* 32(2): 19–51.

Deville J, Guggenheim M and Hrdličková Z (2014) Concrete governmentality: shelters and the transformations of preparedness. In: Tironi M, Rodríguez-Giralt I and Guggenheim M (eds) *Disasters and Politics: Materials, Experiments, Preparedness*. Chichester: Wiley Blackwell, pp. 183–210.

Duffield M (2011) Total war as environmental terror: linking liberalism, resilience, and the bunker. *South Atlantic Quarterly* 110: 757–769.

Duffield M (2013) How did we become unprepared? Emergency and resilience in an uncertain world. *British Academy Review* 21: 55–58.

Edwards PN (1998) Y2K: millennial reflections on computers as infrastructure. *History and Technology* 15: 7–29.

Fish A and Garrett BL (2019) Resurrection from bunkers and data centers. *Culture Machine* 18: 1–14.

Garrett B (2020) *Bunker: Building for the End Times*. London: Penguin.

Garrett B (2021) Doomsday preppers and the architecture of dread. *Geoforum* 127: 401–411.

Garrett B and Klinke I (2018) Opening the bunker: function, materiality, temporality. *Environment and Planning C: Politics and Space* 37: 1063–1081.

Graham S (2010) *Cities under Siege: The New Military Urbanism*. London: Verso Books.

Graham S (2013) Stealth architectures and the geographies of back-up. In: Fard A and Meshkani T (eds) *New Geographies 07: Geographies of Information*. Cambridge, MA: Harvard University Press, pp. 29–36.

Graham, S (2016) *Vertical: The City from Satellites to Bunkers*. London and New York: Verso.

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, MA: MIT Press.

Hu T (2017) Black boxes and green lights: media, infrastructure, and the future at any cost. *English Language Notes* 55(1–2): 81–88.

Huddleston C (2016) 'Prepper' as resilient citizen: What preppers can teach us about surviving disaster. In: Companion M and Chaiken MS (eds) *Responses to Disasters and Climate Change: Understanding Vulnerability and Fostering Resilience*. Boca Raton, FL: CRC Press, pp. 239–248.

Jakobsson P and Stiernstedt F (2012) Time, space and clouds of information: data centre discourse and the meaning of durability. In: Bolin G (ed.) *Cultural Technologies: The Shaping of Culture in Media and Society*. New York: Routledge, pp. 103–117.

Jha A (2009) Secrets of the data bunker. Available at: https://www.theguardian.com/technology/2009/nov/11/data-server-farms (accessed 6 August 2021).

Keck F (2015) Sentinel devices: managing uncertainty in species barrier zones. In: Samimian-Darash L and Rabinow P (eds) *Modes of Uncertainty: Anthropological Cases*. Chicago, IL: The University of Chicago Press, pp. 165–181.

Keck F (2016) Preparedness. Available at: https://culanth.org/fieldsights/preparedness (accessed 12 July 2021).

Klauser FR (2010) Splintering spheres of security: Peter Sloterdijk and the contemporary fortress city. *Environment and Planning D: Society and Space* 28(2): 326–340.

Klinke I (2018) *Cryptic Concrete: A Subterranean Journey into Cold War Germany*. Hoboken, NJ: Wiley Blackwell.

Lakoff A (2006) Techniques of preparedness. In: Monahan T (ed.) *Surveillance and Security: Technological Politics and Power in Everyday Life*. New York: Routledge, pp. 265–273.

Lakoff A (2008) The generic biothreat, or, how we became unprepared. *Cultural Anthropology* 23(3): 399–428.

Lakoff A (2017) *Unprepared: Global Health in a Time of Emergency*. Oakland, CA: University of California Press.

Laurie P (1979) *Beneath the City Streets: A Private Enquiry into Government Preparations for National Emergency*. London: Panther.

Low S (2003) *Behind the Gates: Life, Security and the Pursuit of Happiness in Fortress America*. New York and London: Routledge.

Lutz C (1997) Epistemology of the bunker: the brainwashed and other new subjects of permanent war. In: Pfister J and Schnog N (eds) *Inventing the Psychological: Toward a Cultural History of Emotional Life in America*. New Haven, CT; London: Yale University Press, pp. 245–270.

McLuhan M (1994) *Understanding Media: The Extensions of Man*. Cambridge, MA: MIT Press.

McMacken S (2012) Common types of data loss and how to prevent them. Available at: https://www.securedatarecovery.com/blog/common-types-of-data-loss-and-how-to-prevent-them (accessed 12 July 2021).

Masco J (2009) Life underground: building the bunker society. *Anthropology Now* 1: 13–29.

Masco J (2014) *The Theater of Operations: National Security Affect from the Cold War to the War on Terror*. Durham, NC; London: Duke University Press.

Mattern S (2017) Extract and preserve: Underground repositories for a posthuman future? In: Gomez Luque M and Jafari G (eds) *New Geographies 09: Posthuman*. Cambridge, MA: Harvard University Press, pp. 52–58.

Miller R (2009) The data bunker boomlet. Available at: https://www.datacenterknowledge.com/archives/2009/07/14/the-data-bunker-boomlet (accessed 1 August 2021).

Miller R (2011) Sept. 11, 2001: one data centre's story. Available at: https://www.datacenterknowledge.com/archives/2011/09/11/sept-11-2001-one-data-centers-story (accessed 30 July 2021).

Mills MF (2018) Preparing for the unknown unknowns: 'doomsday' prepping and disaster risk anxiety in the United States. *Journal of Risk Research* 22(10): 1267–1279.

Mingard Y (2014) *Deposit*. Göttingen: Steidl.

Moro J (2021) Air-Conditioning the Internet: data center securitization as atmospheric media. Available at: http://mediafieldsjournal.org/air-conditioning-the-internet/ (accessed 12 December 2021).

Moss S (2016) Paris nuclear fallout shelter to become a data center. Available at: https://www.datacenterdynamics.com/en/news/paris-nuclear-fallout-shelter-to-become-a-data-center/ (accessed 1 August 2021).

Moss S (2018a) Children of the Cold War. Available at: https://www.datacenterdynamics.com/analysis/children-of-the-cold-war/ (accessed 1 August 2021).

Moss S (2018b) Tencent plans huge bomb shelter data center in Guizhou. Available at: https://www.datacenterdynamics.com/en/news/tencent-plans-huge-bomb-shelter-data-center-in-guizhou/ (accessed 4 August 2021).

Munn L (2020) Injecting failure: data center infrastructures and the imaginaries of resilience. *The Information Society* 36(3): 167–176.

Murphy B (2014) Bomb-proofing the digital image: an archaeology of media preservation infrastructure. *Media-N* 10(1). Available at: http://median.newmediacaucus.org/art-infrastructures-hardware/bomb-proofing-the-digital-image-an-archaeology-of-media-preservation-infrastructure/ (accessed 1 August 2021).

Murren T (2018) Dig deep for data center assurances. Available at: https://www.datacenterdynamics.com/en/opinions/dig-deep-for-data-center-assurances/ (accessed 23 July 2021).

Pärna K (2010) Digital apocalypse: The implicit religiosity of the Millennium Bug scare. In: Aupers A and Houtman D (eds) *Religions of Modernity: Relocating the Sacred to the Self and the Digital*. Leiden and Boston, MA: Brill, pp. 239–260.

Pemberton JM (1990) Into the depths: a video tour of underground vaults and storage. *Records Management Quarterly* 24(1): 44–46.

Preston J (2019) Billionaire bunkers and disaster capitalism. In: *Grenfell Tower: Preparedness, Race and Disaster Capitalism*. London: Palgrave Macmillan, pp. 55–72.

Prigge M (2011) Why you should stage a data-loss fire drill. Available at: https://www.infoworld.com/article/2623870/why-you-should-stage-a-data-loss-fire-drill.html (accessed 12 July 2021).

Røssaak E (2010) *The Archive in Motion: New Conceptions of the Archive in Contemporary Thought and New Media Practices*. Oslo: Novus Press.

Schüll ND (2018) Digital containment and its discontents. *History and Anthropology* 29(1): 42–48.

Sebald WG (1998) *The Rings of Saturn*. London: Harvill Secker.

Spencer B (2014) Rise of the shadow libraries: America's quest to save its information and culture from nuclear destruction during the Cold War. *Information & Culture* 49(2): 167–168.

Spinner J (2001) Data centers shift focus to security. Available at: https://www.washingtonpost.com/archive/business/2001/12/27/data-centers-shift-focus-to-security/525c2879-14f0-48ea-9a7f-f5fc07bcca11/ (accessed 2 August 2021).

Starosielski N (2021) *Media Hot and Cold*. Durham, NC; London: Duke University Press.

Taylor ARE (2021a) Future-proof: bunkered data centres and the selling of ultra-secure cloud storage. *Journal of the Royal Anthropological Institute* 26: 76–94.

Taylor ARE (2021b) Standing by for data loss: failure, preparedness and the cloud. *Ephemera* 21(1): 59–93.

Vanderbilt T (2010) [2002]) *Survival City: Adventures among the Ruins of Atomic America*. Chicago, IL; London: The University of Chicago Press.

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

Velkova J (2019) Data centers as impermanent infrastructures. *Culture Machine* 19: 1–11.

Virilio P (1994 [1975]) *Bunker Archaeology*. New York: Princeton Architectural Press.

Wallerstein A (2011) The bureaucracy will survive the apocalypse. Available at: http://blog.nuclearsecrecy.com/2011/11/30/weekly-document-4-the-bureaucracy-will-survive-the-apocalypse/ (accessed 8 August 2021).

Author biography

ARE Taylor is a social anthropologist and Lecturer in Communications at the University of Exeter. His research focuses on the material infrastructure of the internet and the space sector. He is a founding member of the Social Studies of Outer Space (SSOS) Network and an Editorial Assistant for the *Journal of Extreme Anthropology*.