Partners Universal Journal of Artificial Intelligence Research (PUJAIR)
Volume: 01 Issue: 01 | April-May 2026| www.pujair.com

Data Centers: Critical Infrastructure, Global Risk & Geopolitical Power

Dr.A.Shaji George

Independent Researcher, Chennai, Tamil Nadu, India.

Abstract - For most of the twentieth century, critical infrastructure referred to tangible, visible assets power grids, transportation networks, water systems, and communication towers. These were the pillars on which national security and economic continuity were based. A category of infrastructure that's not as well-known but is ever more central to that discussion has been introduced into the mix. In the 21st century. No longer considered to be niche back-office facilities of information technology departments, data centers are now a cornerstone of the functioning of modern economies, governments, and military systems. This article will explore the history of critical infrastructure thinking, the metamorphosis of data centres as key national assets and the geopolitical, economic and security implications of digital dependency. The article delves into the centralization vs. resilience question in digital infrastructure design, drawing on documented geopolitical events, such as in conflicts in Middle Eastern and Eastern European countries where infrastructure has been targeted. It also offers a structured framework for enterprises considering moving to the cloud and examines new national strategies to build sovereign digital infrastructure and the cross-over of artificial intelligence and compute geopolitics. The article concludes with concrete policy recommendations for governments and organisations wanting to create true digital resilience in an ever-changing world, one in which they are now under more pressure than ever.

Keywords: Data Centers, Critical Infrastructure, Digital Resilience, Cloud Strategy, Geopolitics of Technology, Sovereign Cloud, National Security, AI Infrastructure

1. INTRODUCTION

1.1 The Infrastructure Beneath the Infrastructure

The most essential things go along with an invisibility of their own. Unless the power goes out, people take the electrical grid for granted. Until the water taps run dry, they don't think about water infrastructure. The world economy had enjoyed a similar blithe indifference towards data centres for some 30 years. While they conducted the world's transactions, kept records, handled its communications, and provided its power to its governments these facilities were largely missing from strategic conversations that informed national security policy and corporate risk management.

Those days of complacency are over, and these are the days that should draw the attention of those at all levels of decision making. With the last five years of events unfolding, it's clear that the strategic importance of data centers can no longer be overlooked. Cloud Computing is now bigger than its original architects envisioned. Artificial Intelligence has moved from the research labs to the core of finance, medicine, logistics and defense. COVID-19 brought about a complete or partial reorganization of entire economies and a level of dependence on continuous digital access that is only now becoming apparent. In multiple active conflict zones, adversaries have done the same with the same deliberate strategic intent that they typically use to target power stations, bridges, and command posts data centers.

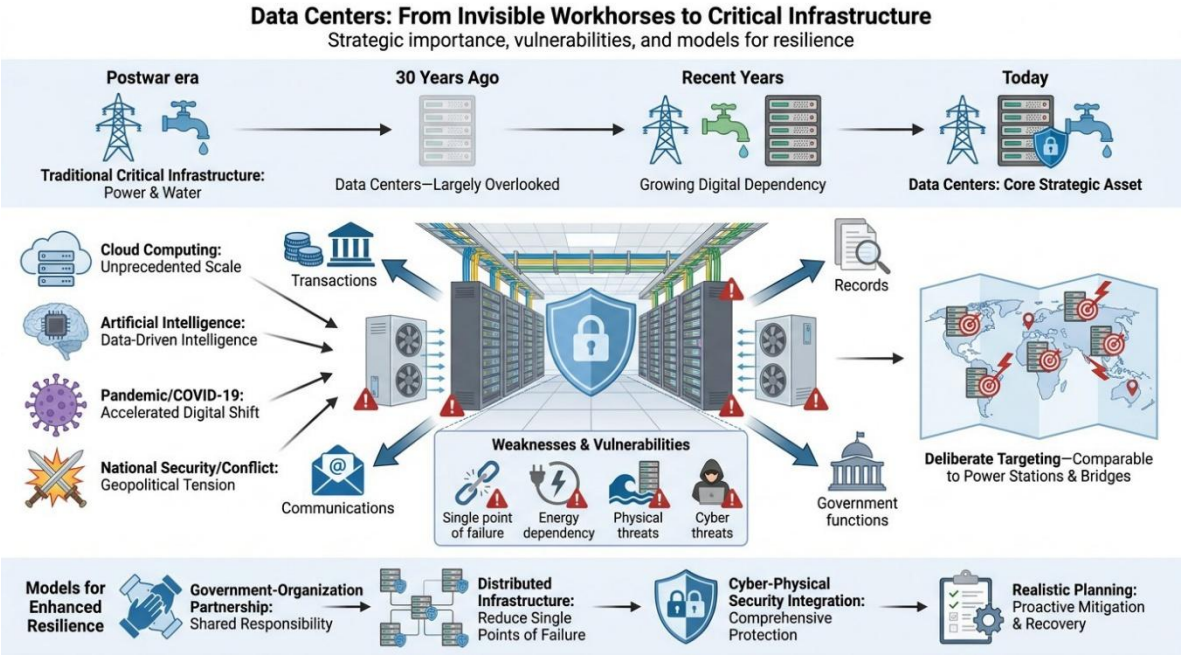

Fig -1: Data Centers From Visible Workhorses to Critical Infrastructure

This article is an effort to think straight on these developments. It reviews the development of critical infrastructure thinking since the postwar era to the present, establishes why data centers are now definitely critical infrastructure, dissects the inherent weaknesses of the current way of delivering digital infrastructure, and provides concrete models for government and organisations that must react to be ready. The analysis is based on reported rather than forecast events, and recommendations are realistic rather than idealistic.

2. OBJECTIVES

This article has the following main objectives. First, the article aims to create a solid analytical basis for the definition of data centres as critical national infrastructure (CNI), based on the economic dependency data, conflict patterns documented and security policy developments. Second, it strives to explore the strategic paradox of centralization of infrastructure and resilience of operation and to consider the implications of this paradox on a national and enterprise context. Third, the article offers a realistic decision-making model for corporate and governmental cloud decision makers considering cloud adoption, data center investments, and the digital resilience strategy. Fourth, it explores the geopolitical relationship between the deployment of artificial intelligence and data centers, claiming that the compute infrastructure is now a part of national power. Fifth and finally, the article points to some possible areas where existing policies and research fall short and suggests areas for future research in digital infrastructure security and governance.

3. HISTORICAL EVOLUTION OF CRITICAL INFRASTRUCTURE THINKING

Understanding why data centers have become strategic assets requires understanding how the broader concept of critical infrastructure developed. The idea did not emerge fully formed from a single policy

document. It evolved through the accumulated lessons of two world wars, a prolonged Cold War confrontation, and several decades of technological transformation.

During World War II, strategic bombing doctrine on both sides of the conflict was shaped by a central insight: disabling the industrial and logistical systems that sustained a military was often more decisive than engaging armies in direct combat. German attacks on British radar stations during the Battle of Britain, Allied bombing of German synthetic fuel plants, and the systematic targeting of railway networks all reflected this logic. The goal was not merely to destroy assets but to sever the connective tissue of an opponent's capacity to function.

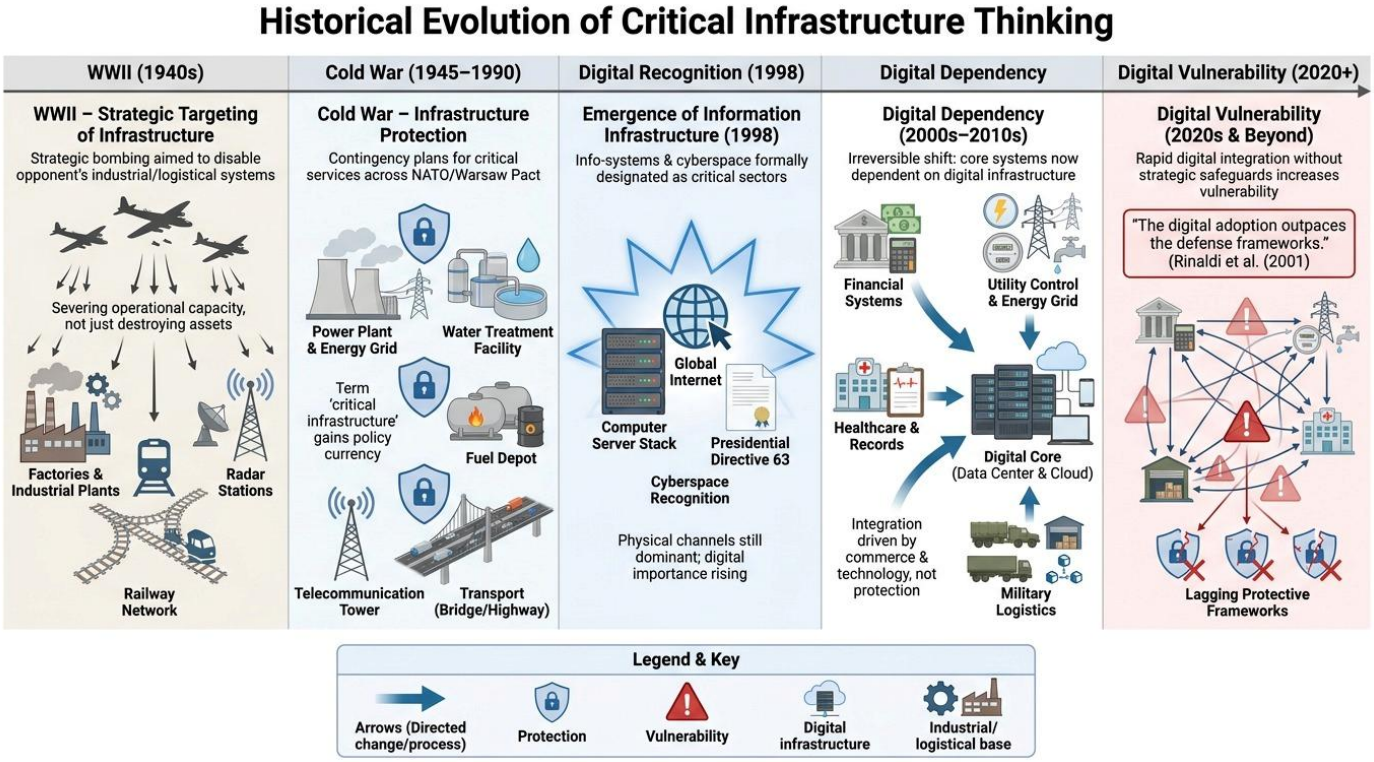

Fig -2: Historical Evolution of Critical Infrastructure Thinking

After 1945, this thinking was institutionalized in Cold War defense planning across NATO and the Warsaw Pact. Western governments developed detailed contingency plans for the protection and continuity of power generation, water treatment, fuel distribution, telecommunications, and transportation. The term "critical infrastructure" gained policy currency as a designation for assets whose disruption would produce cascading effects across national security, public health, and economic stability.

The United States made its first formal policy acknowledgment of information systems within this framework in 1998, when Presidential Decision Directive 63 designated cyberspace and information infrastructure as critical sectors requiring protection. That decision was prescient, though its full significance was not widely appreciated at the time. The internet existed, but electronic commerce, cloud computing, and digital government services were still embryonic. Most critical economic processes still ran through physical channels that could be protected by conventional means.

The following decade changed that equation fundamentally. By the mid-2000s, financial clearing

systems, tax collection, healthcare records, utility management, and military logistics had all become dependent on digital infrastructure in ways that were not merely convenient but structurally irreversible. The digital transformation of the 2010s deepened that dependency further, and by the time the COVID-19 pandemic arrived in 2020, the question was no longer whether economies were dependent on digital infrastructure but how completely and how vulnerable.

Researchers studying infrastructure resilience have noted that the speed of digital adoption consistently outpaced the development of protective frameworks. Systems integration happened through commercial incentive and technological opportunity rather than strategic design, with the result that dependencies accumulated without corresponding attention to the vulnerabilities they created. That observation, made decades ago, describes precisely the situation that governments and organizations are now working urgently to correct.

4. WHAT DATA CENTERS ACTUALLY DO THE OPERATIONAL FOUNDATION OF MODERN ECONOMIES

To appreciate the value of data center assets as strategic assets, it is important to have a grasp of the overall evolution of what critical infrastructure is. This was not a policy document in isolation that led to the idea. It's developed across the learning experiences of two World Wars, one long Cold War rivalry and over several decades of technological change.

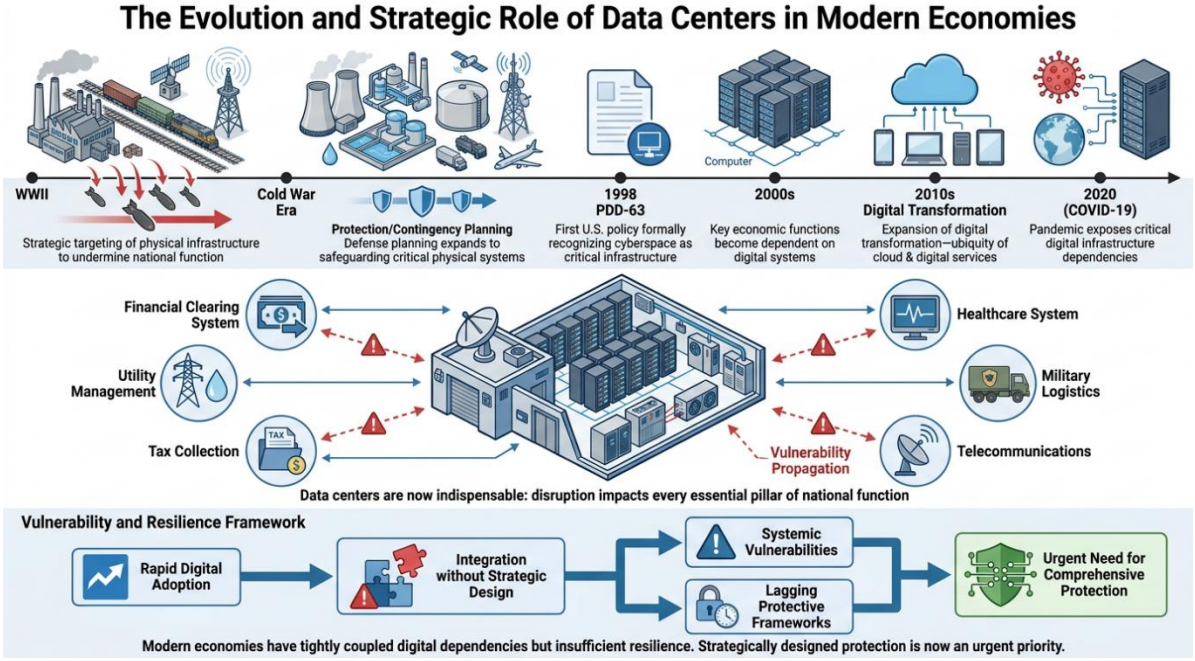

Fig -3: The Evolution and Strategic Role of Data Center in Modern Economies

A key element of strategic bombing doctrine in both belligerents during World War II was to try to make the military system of the other country irrelevant to the conflict, by targeting its industrial and logistical base. This mirrored the fact that German attacks on British radar stations during the Battle of Britain, Allied bombing of German synthetic fuel plants and the systematic attacks on the railway network. Not only were they out to destroy assets, but to cut the glue that held an opponent together.

This thinking was institutionalized in the defense planning of the Warsaw Pact and NATO countries after 1945, in the context of the Cold War. Western governments created comprehensive contingency plans for safeguarding power generation, for water treatment, for fuel distribution and for telecommunications and transportation. "Critical infrastructure" became a policy term to describe systems which, if disrupted, would have an impact on national security, public health, and economic stability.

This was the first formal policy statement by the United States that acknowledged information systems as a policy domain, in 1998 with the Presidential Decision Directive 63 which identified cyberspace and information infrastructure as critical sectors that need protection. That proved to be a good move, but it did not have the full significance recognized at the time. While the internet was there, electronic commerce, cloud computing and digital government services were still in their infancy. Most of the critical economic processes were still physically based and could be secured via the traditional means.

All that changed in the next 10 years. By the mid-2000s, records of financial clearing systems, tax collection, healthcare, utility management, and military logistics were all dependent on digital systems and in ways that were no longer merely convenient, but structurally impossible. That dependence was further exacerbated by the digital transformation of the 2010s, to the point that the arrival of the COVID-19 pandemic in 2020 was no longer a matter of dependence or not, but how much and how exposed are the economies.

The rate of digital adoption has always outpaced the rate of the creation of protecting frameworks, as has been noted by infrastructure resilience researchers. The systems integration was a function of commercial incentive and technological opportunity, and there was no strategic design either and the dependencies built up without there being any consideration of the vulnerabilities that it caused. That's the exact situation that governments and organisations are striving to correct in a hurry today, decades after the observation was made.

5. CURRENT TRENDS IN DATA CENTER DEVELOPMENT

A legitimate case for considering data centers as critical infrastructure needs to be based on understanding their purpose, and why it's important. The word is thrown around freely in the public debate and its widely used nature blurs the magnitude of the issue at stake.

A data center is a brick-and-mortar establishment one with computers, servers, storage systems, networking equipment, power and cooling solutions designed to keep these computing technologies running around the clock. A data center, at the hardware level, is a facility that's filled with hardware. At the functional level, it is the basis for operation of almost all important economic and governmental activities in the modern world.

The best example is the financial system. This equates to around 1.8 trillion transactions in 2023, which is just the numbers for the global card networks. For each transaction, it was necessary to conduct real-time verification, fraud screening, routing, and settlement, which were all done by computing systems situated in data centers. The internal treasury management systems of all large corporations, the central bank payment networks, foreign exchange systems, and derivatives markets are also reliant. If a big financial data center goes down for an extended period, it would not only cause a nuisance to account holders. It would put a stop to the clearing and settlement processes which continue to support international trade.

The situation is no different on the government services side. Today, governments are using data center systems to manage their tax and welfare programs, immigration records, ID verification systems, and military operations. In the UK, the Government Digital Service has been steadily moving and remodeling core public services to be hosted on cloud-based solutions, and thus dependent on availability of data centres in ways that would not have been ten years ago. Such shifts have taken place in most developed economies and are occurring in more developing economies.

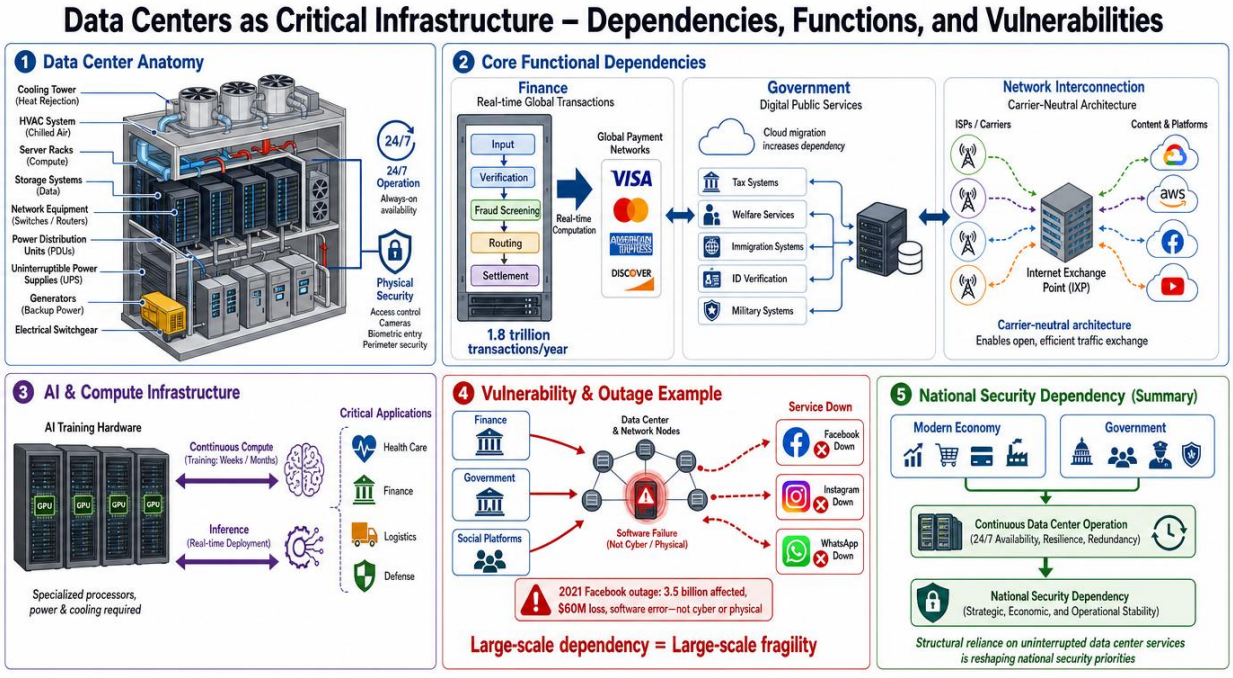

Fig -4: Data Centers as Critical Infrastructure Dependencies, Functions,, and Vulnerabilities

Networks have always relied on a type of data center and internet exchange point (IXP) known by the telecommunications industry as a carrier-neutral facility, where networks intersect to exchange traffic. The 2021 Facebook outage was a prime example of how the failure of a key node in such an architecture can lead to an outage. Facebook, Instagram, and WhatsApp all went down at once for around six hours, due to a configuration error in Facebook's data center network routing infrastructure, leaving 3.5 billion people unable to communicate, and resulting in a loss of direct revenue for Facebook of around 60 million US dollars. The outage was not the result of a cyberattack or physical event instead it happened because of a software error. It showed that a large scale of dependency generates fragility at a large scale.

Now, with the advent of AI as a tool to be used on the operational side of industry and government, there is yet another layer of dependency. To train large scale AI systems, weeks or months of continuous, intensive computation must be performed using thousands of specially designed processors. This calculation takes place in a data center that has certain hardware, power and cooling systems which are not readily available. Compute infrastructure is also important for inference, that is, deploying trained models to real world inputs. The more critical a system becomes to its user, the more critical is the data center that powers the system, especially in health care, finance, logistics, and weaponry systems.

Not that data centers are helpful or that their disruption would be problematic. The bottom-line today's

economies are structurally reconfiguring around a growing reliance on the continuous provision of data center services that are creating real national security dependencies.

6. CONFLICT, DISRUPTION, AND THE WEAPONIZATION OF DIGITAL INFRASTRUCTURE

The best evidence of late for the strategic nature of data centers has not been in policy documents, but in conflicts.

The Russian invasion of Ukraine that started in February 2022 saw one of the first offensive campaigns a massive cyber-attack on the Ukrainian government's systems, financial infrastructure, and communications networks. The attacks were designed to affect Ukrainian state functions and were said to have been launched by Russian state actors, according to several Western intelligence agencies. Ukraine's z answer to the situation the fast migration of government data and services to cloud based platform outside Ukrainian territories was operationally effective and strategic. It has been proven that digital infrastructure distributed and hosted in the cloud can continue to function when a country is under attack.

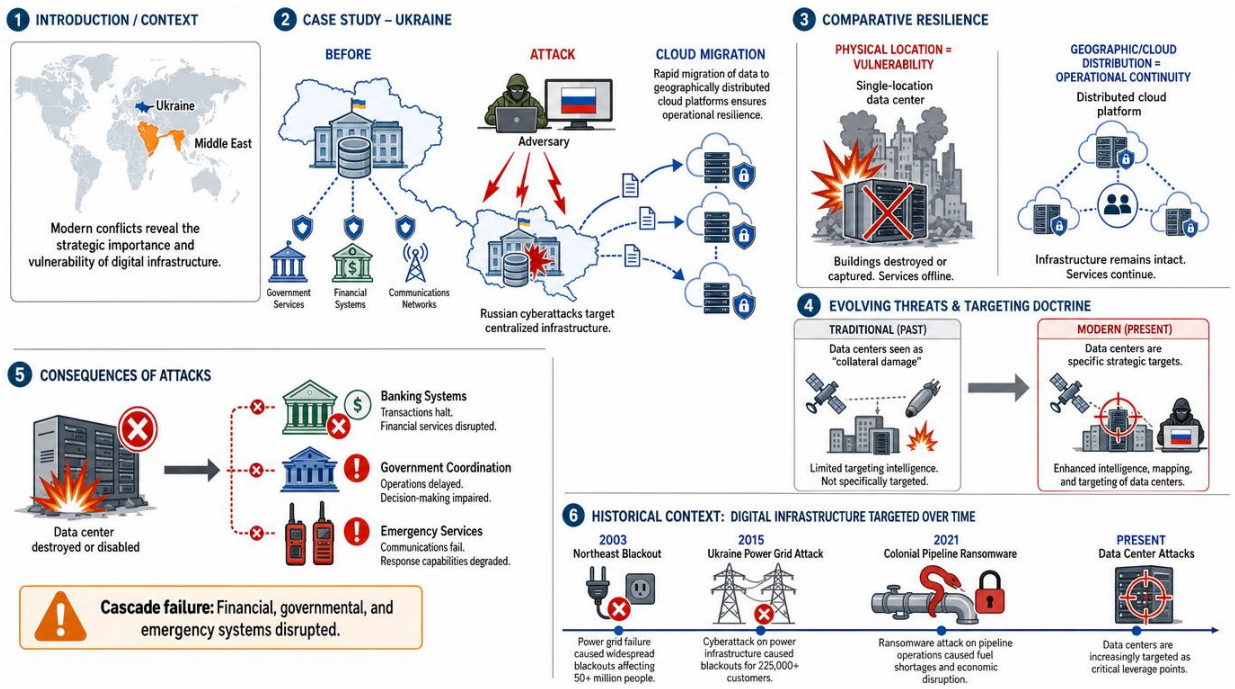

Fig -5: Conflict, Disruption, and the Weaponization of Digital Infrastructure

This is now the Ukrainian experience which defense planners around the world use as a case study. There's a lesson here that's more than just cloud is resilient. The takeaway from the lesson is that the geographic spread of key data and computing power can offer a resiliency that physical infrastructure spread in a single location cannot deliver in a contested physical environment. Housed in buildings on Ukrainian soil, Ukraine's pre-war government data centres would have been destroyed or captured. All data in the cloud was saved.

This trend added to a new layer in the Middle East with conflicts that raged from 2026 onwards. Data centers were now explicitly introduced into military targeting doctrine and destroyed, not as collateral

damage, but on purpose to shut down the economic and command functions of a nation. The consequences of the loss of a data center with a country's banking clearing system, government databases, and telecommunications routing are even more than technical. Financial transactions halt. There is a lack of government coordination. Emergency services are unable to communicate. The consequences of a successful attack on focused digital infrastructure can be as great as if it were against multiple discrete physical targets.

This targeting logic represents real change in the way that adversary targeting analysis and exploitation of infrastructure dependencies is established. Sophisticated state intelligence agencies have mapped the location of key digital services and have included it in their operational planning. The notion that data centers can't be compromised because they're so obscure or that they're so cybersecure is no longer valid. There is physical vulnerability in various senses of the word, and it is authentic.

The overall historic trend accentuates this worry. The 2003 Northeast Blackout in the United States and Canada, the 2015 Ukrainian power grid cyberattack, the 2021 Colonial Pipeline ransomware attack, and a litany of others have proven that focused infrastructure provides leverage points to be exploited by a variety of different adversaries with different levels of sophistication. Data centers are a textbook case of that, and the signs point to the fact that the more sophisticated actors have already realized this, whilst most governments and organizations have yet to adjust their protection strategies.

7. THE CENTRALIZATION PARADOX EFFICIENCY VERSUS RESILIENCE

The first trend over the last decade in data center development has been towards concentration and there is a good efficiency argument for this. The balance between that efficiency and the strategic resilience that it erodes is one of the major issues of digital infrastructure policy.

This is because of the unit economics that are impossible to replicate with distributed architectures hyperscale data centers are more efficient. A 200Mw user can negotiate electricity contracts and engineering solutions that are unattainable by smaller users. The volume of hardware procurements it can do allows pricing that makes it much more cost effective per unit of compute. Its personnel are distributed across a larger space, and can become specialised and have depths of expertise, which smaller teams cannot maintain. The overall effect has been the reduction in the cost-per-unit-of-computation over many decades, which has made possible the explosion of digital services that is the current economy.

But the same focus of resources that yields those economics means there's a vulnerability profile worth looking at. Three cloud providers could be serving the bulk of the digital workloads for a nation, and each of these cloud providers may have a single or two major cloud sites running the regional infrastructure, and that's an awful lot of physical facilities for an adversary to take down to create national level disruption. In this context, two ways of seeing the same architectural decision efficiency, and strategic brittleness.

The example is at a smaller scale in Singapore for 2021. One of the biggest co-location facilities in Singapore suffered a cooling system outage which caused a partial shutdown that affected banking services in the city-state for several hours. Though small, Singapore is one of Asia's most important financial centres, transacting and hosting volumes of financial interactions and data out of proportion to its size. This incident has also led to substantial changes by the Monetary Authority of Singapore (MAS) in its requirements for financial sector data centers' resilience, such as the requirement for critical systems

to be geographically redundant.

What the Singapore incident showed, and what the examples of the larger-scale conflicts showed, is that centralization paradoxes are not something that one can simply let alone, they must be tackled. Centralized infrastructure is efficient and that's a fact. It also leaves them vulnerable and that is a reality. But the right answer is to modestly rethink the concept of efficiency in infrastructure design, so that efficiency improvements do not result in strategic fragility that is no longer acceptable.

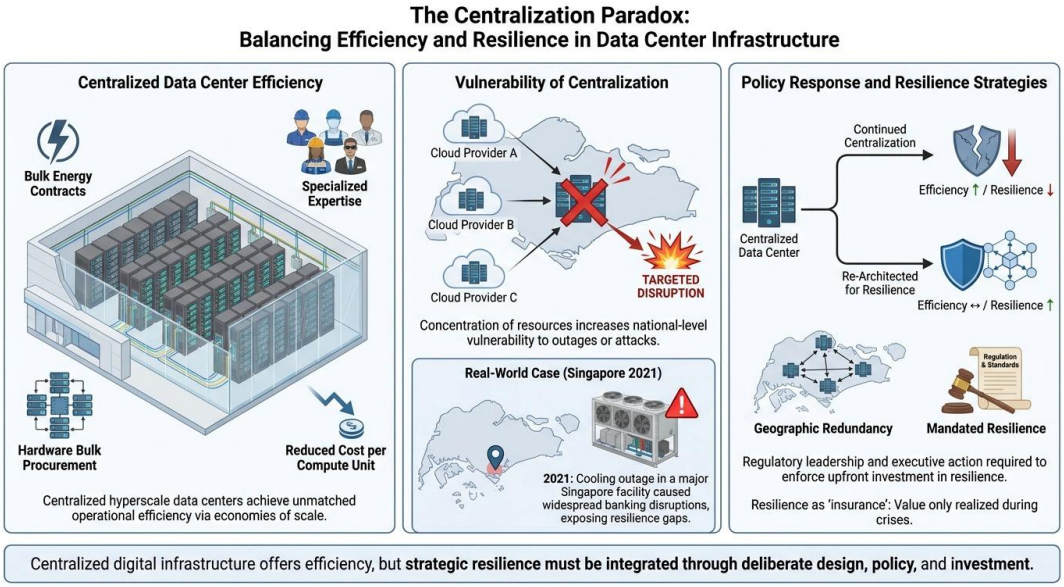

Fig -6: Balancing Efficiency and Resilience in Data Center Infrastructure

The problem for policymakers and enterprise architects is that it involves up-front investment and running costs that won't be reflected on the balance sheet as a return. Resilience is insurance. It has no value when it is going well, and only becomes apparent in the crisis, thus engendering ongoing pressure to under-invest in it. Regulatory mandate and executive leadership is needed to overcome that structural incentive problem, and to take seriously the downside scenarios that resilience is built to avert.

8. GEOGRAPHIC DISTRIBUTION AND SOVEREIGN CLOUD POLICY

The geographic distribution and sovereign cloud is one of the most important new policy positions on digital infrastructure in the last few years, and it has moved beyond an infrastructural preference to a formal policy.

Geographic distribution makes a lot of sense. Computing and data capacity spread across various geographical locations and various jurisdictions can't be destroyed or disabled at the same time. The principle of dispersal in the military that has been used in the development of weapons systems and command structures is also applicable to the development of digital infrastructure. The difficulty lies with its implementation in an environment where commercial considerations are continually pushing for concentration.

GAIA-X is the most ambitious initiative to build a multi-national, distributed cloud infrastructure ecosystem that has explicit sovereignty protection, from the European Union. GAIA-X was initiated in 2019

and is still in the process of development it aims to define technical and governance standards that enable European organisations to deploy workloads in cloud infrastructures which are certified to operate under European legislation and are provided by European or foreign providers that comply with specific data governance requirements. While some issues have arisen in the process of implementing the project, such as the involvement of hyperscale providers that are not European, the general strategic sense and motivation behind the project is correct. A continent whose vital digital services are operated by cloud services that are governed by foreign law and physically outside the continent has little ability to protect the digital services in the event of a crisis.

The SecNumCloud certification scheme in France has taken the lead among the European countries by offering a framework for certifying cloud services as "appropriate" for sensitive government information. The scheme stipulates that certified providers must operate under French jurisdiction, foreign legal jurisdiction (which could require disclosure of data) is excluded and specific physical and organizational security requirements are specified. Similar schemes are in the process of being developed in several other European countries.

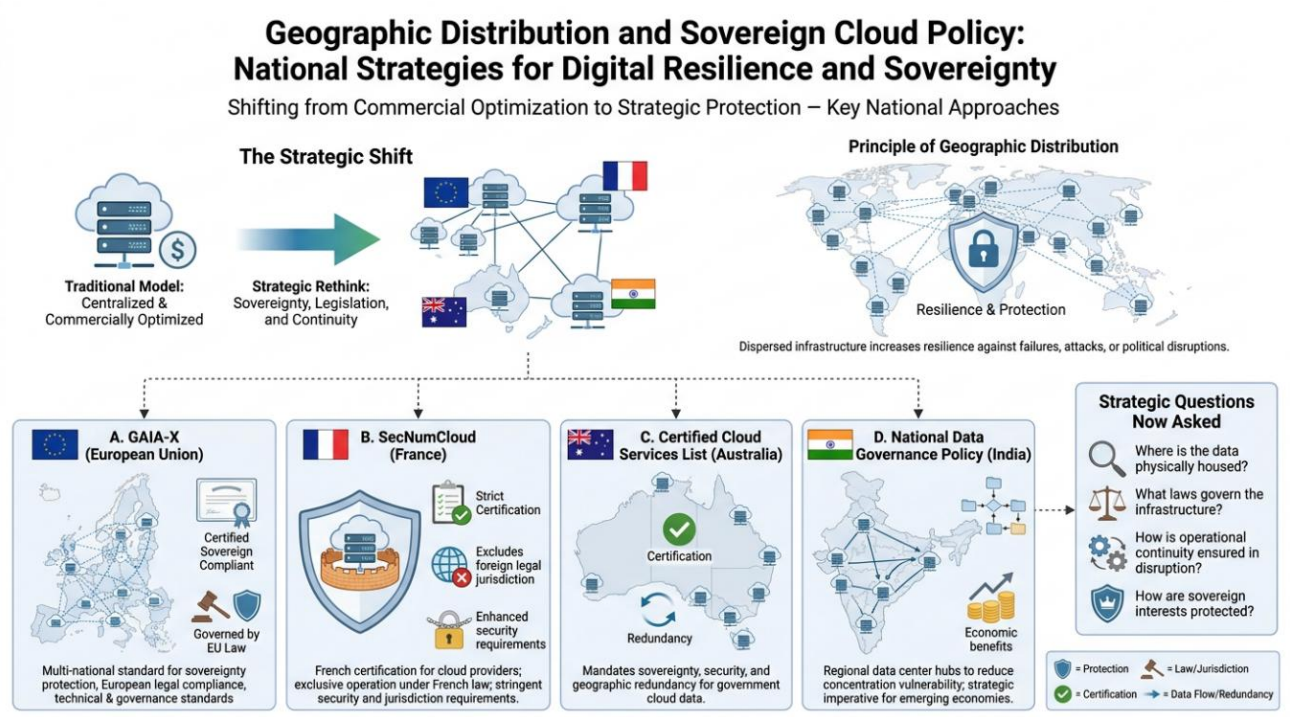

Fig -7: National Strategies for Digital Resilience and Sovereignty

Australia's attitude also now evolved. Cloud service providers who would like to host government cloud data must fulfil certain security, sovereignty and resilience requirements as set out in the Australian government's Certified Cloud Services List. Recent changes have increased geographic redundancy requirements, which require that critical government systems are designed to keep going at geographically diverse locations.

The National Data Governance Policy, which is still in development, demonstrates the rising awareness and consensus that the sovereignty of digital infrastructure is a real strategic imperative for big emerging economies such as India. The regional data center hubs provisions of the policy are a bid to diffuse the

vulnerability of having all the national digital capacity in a single metro region while also sharing the economic advantages.

These national initiatives are all telling signs of a new way of talking about cloud and data center policy. It's no longer just about which provider delivers the best performance at the lowest price. Now the question has become, where is the data physically housed, what laws govern it and what are the options for continuity in case of interruption of infrastructure or the end of the provider relationship. These questions are strategic and strategic answers are being given.

9. ENTERPRISE DECISION-MAKING FRAMEWORK FOR CLOUD STRATEGY THAT REFLECTS REAL RISK

Strategically, data center and cloud questions often become lost in a mix of commercial pressures and enthusiasm for technology. Cloud providers have made significant efforts in selling cloud adoption as the progressive and forward-thinking approach, and on premises/hybrids as legacy roles to be surpassed. This is convenient, but inadequate, framing.

The key honest answers to the enterprise cloud question start with four questions that most organizations have not answered rigorously.

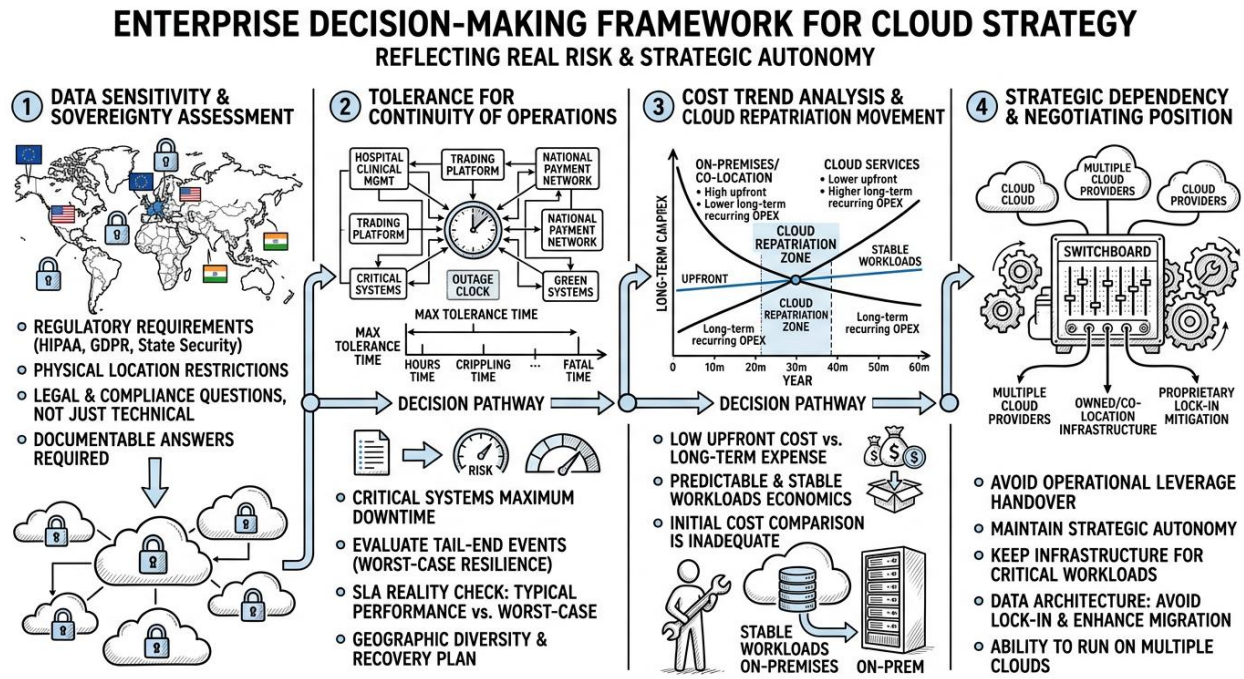

Fig -8: Enterprise Decision Making Framework for Cloud Strategy

The initial question was about data sensitivity and data sovereignty. There are legitimate restrictions on the physical location of data and access to it for organizations that hold data that is subject to specific regulatory requirements, state security classifications, or contractual confidentiality constraints. But it is not only the healthcare providers under HIPAA in the United States, financial institutions under European regulatory frameworks, government contractors with security clearances, and organizations handling personal data under GDPR that must deal with legal requirements; public cloud services may not be able to meet those requirements completely or at all. In these organisations, the question of whether to adopt

the cloud is not just a technical one, but also a legal and regulatory compliance question, which means there need to be specific answers that can be documented.

The second question relates to the tolerance for the continuity of operations. All organizations have a maximum amount of time that outages can last on their most critical systems. A few hours of downtime for a consumer retail system is business crippling, but manageable. A few hours is the death knell for a hospital's clinical management systems, a trading platform or a national payment clearing network. The real question is whether the provider's service levels, the geographical diversity of the provider's infrastructure and the organisation's recovery plan cater for events on the tail of the distribution. Typical commercial cloud SLAs are based on the idea of typical performance, rather than worst-case resilience.

The third question is about the cost trend over the years. Cloud services often have less upfront capital expenditure and lower upfront costs than on-premises, making them an appealing option when scaling up and for workloads that change over time. But the recurring expense of cloud services often surpasses the cost of owned or co-located infrastructure spread out over multiple years in large organisations with predictable and stable workloads. A new trend has been documented in the industry and is known as the "cloud repatriation movement," where organizations are bringing stable workloads back on premises when the cloud economics don't work out on such a large scale. Cloud adoption decisions made from initial cost comparisons, without a view to the future cost trend, may need to be revisited.

The fourth question relates to strategic dependency and negotiating position. By design, when a company's entire digital operation is on one cloud provider it has handed over a substantial amount of operational leverage to that cloud provider. Prices, service alterations, and contractual renegotiations all take place in a situation where the organization has high switching costs. This is accomplished by keeping some owned or co-located infrastructure on hand for critical workloads, by ensuring that the data architecture doesn't create a proprietary lock-in that makes migration too complex, and by keeping the ability to run on multiple clouds. These are not arguments for not going to the cloud. These are arguments for strategic autonomy in adopting the cloud.

10. NATIONAL STRATEGIES PROGRESS, GAPS, AND THE TALENT PROBLEM

In recent years, governments around the world have begun to take data centers much more seriously at the strategic level and formal critical infrastructure designation, sovereign cloud policies and new physical security requirements are real steps forward. The picture is, however, patchy, and there are key areas lacking.

Formal Data center critical infrastructure designation has increased greatly on the positive side. The United States Cybersecurity and Infrastructure Security Agency (CISA) released sector specific guidance for the data center operators, which is part of the larger information and communications technology critical infrastructure sector. Data center security is a key element of the United Kingdom's National Cyber Security Strategy. In 2024, the Critical Infrastructure Protection Plan was updated with specific elements related to digital infrastructure facilities. Germany's Federal Office for Information Security (BSI) has created comprehensive baseline standards for data centers that provide critical services.

The physical security of government class data centers also has been greatly enhanced. Requirements now often include a detailed level of expectation for power redundancy architecture, physical access controls, perimeter security, cooling system resilience, and emergency response planning, far beyond the typical commercial expectation. The improvements are pertinent and needed.

However, in most countries the involvement of the data center operators in the national crisis management is not fully developed. Power utilities have procedures in place to interface with emergency management agencies during emergency situations. There are comparable systems for water utilities. In most jurisdictions, data center operators don't have similar formal ties with national security agencies, emergency management organizations, or military authorities. The consequence is, that if a nation-state level attack or some crisis occurs, where government action is necessary, the process of response is ad hoc.

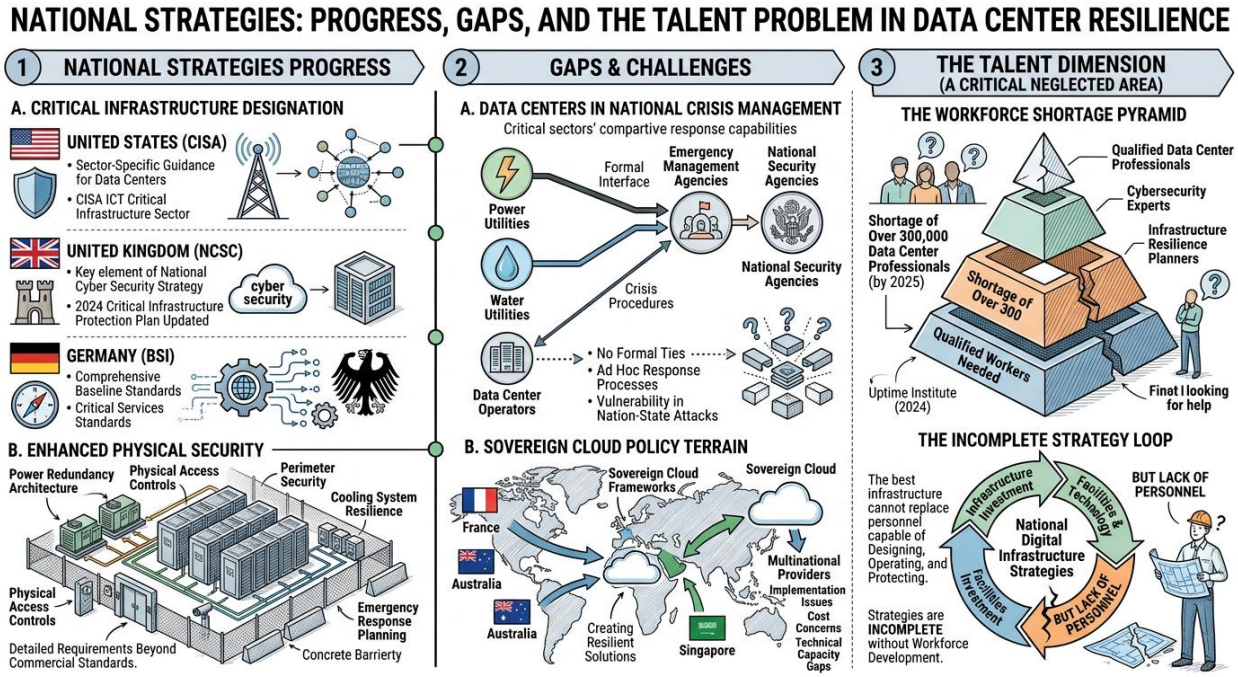

Fig -9: National Strategies Progress, Gaps, and the Talent Problem in Data Center REsilience

The sovereign cloud policy terrain is maturing with a great deal of momentum. Several programs in France, Australia, Saudi Arabia, Singapore, and others are creating solutions and frameworks regarding cloud services that are sovereignly resilient. These programmes are significant developments, but there are significant and ongoing implementation issues about the cost, technical capacity and involvement of multinational providers.

The talent dimension is indeed one of the most chronic and neglected national digital infrastructure strategies. The shortage of qualified data center professionals, cybersecurity experts and data center infrastructure resilience planners is a global trend and well known. In 2024, Uptime Institute found that there would be a shortage of over 300,000 qualified workers in the data center industry across the world by 2025. The best infrastructure investment will not make up for the lack of personnel that can design, operate and protecting the infrastructure. Structurally, national strategies that focus on facilities and technology, but do not allocate the same attention and resources to workforce development, are incomplete.

11. THE AI DIMENSION COMPUTE INFRASTRUCTURE AS GEOPOLITICAL CURRENCY

For this reason, the strategic discussion on data centers has been revolutionized by artificial intelligence and merits its own analysis the AI compute infrastructure question isn't just about performance or cost. It is an open, direct, recorded, and documented power play of the Nation.

These frontier AI systems often demand compute-intensive tasks for long periods of time (weeks or months) across thousands of specialized processors, such as GPUs and dedicated AI accelerators, and are run in a facility that has a significant amount of power and precision cooling. There is not much hardware available that can do this computation. As of early 2025, most world-class AI training infrastructure are in the USA, with a considerable amount in UK, parts of EU, and emerging capacity in the Gulf states. Frontier systems in AI cannot be developed independently by countries that don't have access to this.

This is where the U.S. government interpreted its strategic significance and started taking steps to curb the export of advanced semiconductors to China in 2022, with additional restrictions added in following years. Explicit reasons cited were a strategic competitor's ability to gain access to hardware needed to build AI systems that could be used for military and intelligence purposes. No matter how good or bad, or effective or ineffective, this policy decision is an official recognition that AI compute infrastructure is an area of national power that is subject to the same export control rational that was used when it comes to nuclear technology, advanced weapon systems, and military encryption.

The implications of dependency are high for countries that do not have a compute infrastructure for AI locally. Focusing on foreign hardware, foreign cloud environments, foreign legal jurisdiction, trained and operated AI systems are not AI systems in a meaningful sense of the word. This foreign company will have potential visibility of the data on which the systems are trained and the queries they run. That data could be subject to possible legal requirements for access by the foreign government under the law of which the services are apart. As well as the on-going ability of AI is depending on the on-going capacity of a business and geopolitical partnership that's not totally in the dependent country's control.

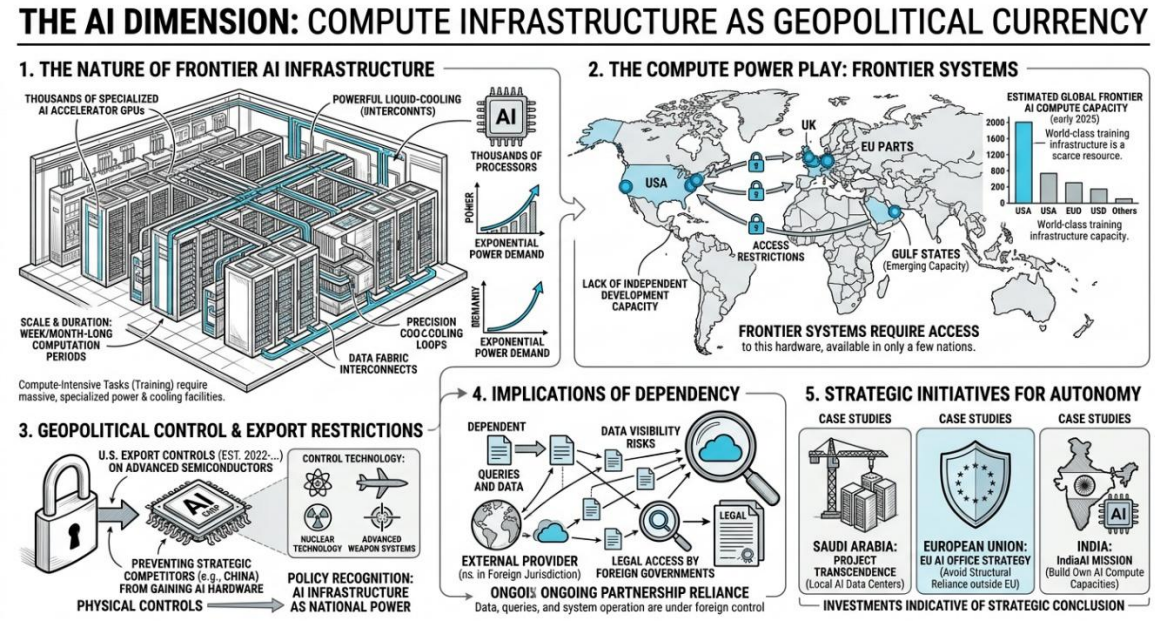

Fig -10: Compute Infrastructure as Geopolitical Currency

This analysis is paving the way for significant investments in the local AI compute infrastructure in various geographies. Another major part of the Saudi Arabia's Project Transcendence, which is announced in 2024, is the construction of local AI data centers. The European AI Office of the European Union is working on strategies to prevent Europe from being structurally reliant on infrastructural support from outside the EU to ensure its AI capability. India AI Mission has a component on India's own AI compute capacities. These investments are indicative of a strategic conclusion coming together in an age where the ability to harness AI is a matter of national competitiveness and security: the infrastructure that powers AI should be regarded as a strategic asset.

12. THE HARDWARE SUPPLY CHAIN

12.1 Semiconductor Dependency, Manufacturing Concentration, and the Hidden Vulnerability in Data Center Infrastructure

All servers in all data centres are silicon based. The computing power in a data center made up of processors, memory chips, network interface cards (NICs) and storage controllers are physical artifacts produced in a particular location, by a particular company, with materials and equipment sourced from a highly concentrated and in certain crucial components extremely fragile, international supply chain.

This supply chain is one of the areas that may be singled out for specific consideration, as it is different structurally from the physically vulnerable and the cyber vulnerabilities discussed elsewhere in the article. Some cyberattacks can be identified and sometimes even are prevented in real-time. A physical strike can be arranged to and for and protected by proper protection measures. However, this vulnerability in the supply chain can take years to become apparent when semiconductors are unavailable, and years longer to correct the vulnerabilities are a result of decades of commercial choices that were individually prudent but collectively dangerous.

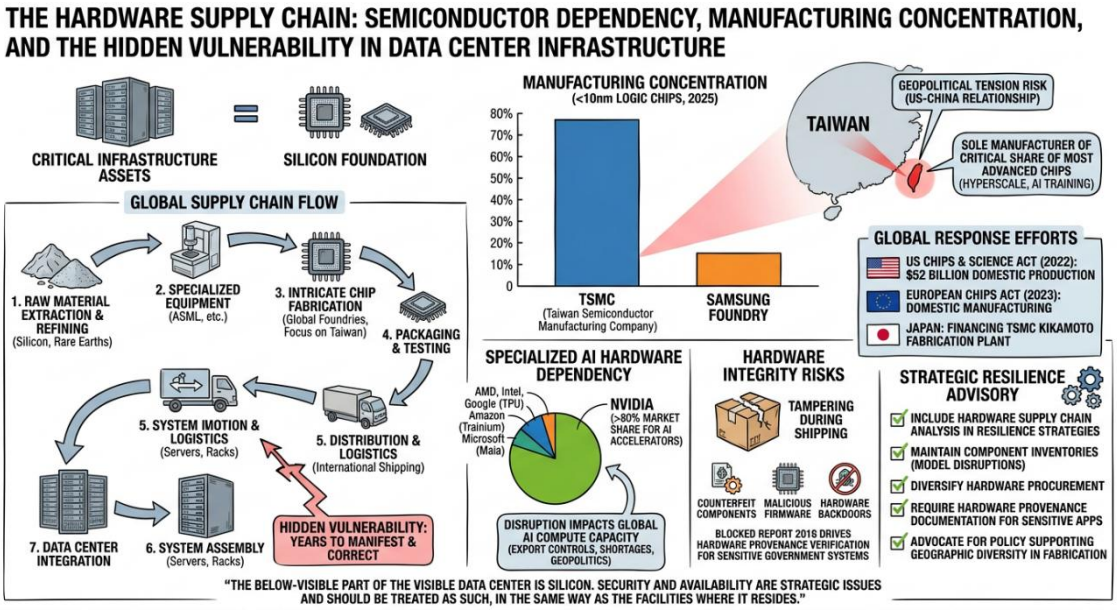

Fig -11: Semiconductor Dependency Manufacturing Concentration and the Hidden Vulnerability in Data Center Infrastructure

The clustering around manufacturing in the production of advanced semiconductors is remarkable. So as of 2025 the production of the most advanced logic chips, less than 10nm, are essentially dominated by two companies, Taiwan Semiconductor Manufacturing Company and Samsung Foundry. Taiwan Semiconductor is the sole manufacturer of a significant share of the world's cutting-edge chips used in hyperscale data centers and AI training facilities, such as processors and AI accelerators. With Taiwan's political stability and physical security being a key concern, the continued stability of the island is essential to hardware supply for the global data center industry, as Taiwan is in an area of demonstrated geopolitical tension between the People's Republic of China and the United States.

The threat of the Taiwan risk is no longer hypothetical. The US Defense Department, European Commission, Japanese, South Korean, and British governments have all reported on the concentration of advanced chip manufacturing there as a vulnerability of the critical supply chain that needs to be mitigated. The CHIPS and Science Act passed in 2022 in the United States allocated $52 billion to domestic semiconductor production, specifically to decrease the dependency. The European Chips Act, which was passed in 2023, was also in this respect an ambitious undertaking in the field of domestic manufacturing in Europe. As at the national level, Japan is willing to pay a significant amount of money to finance a new TSMC fabrication plant in Kumamoto.

In addition to geographic concentration in fabrication, the data center hardware supply chain is subject to two other types of risks, the first is less acknowledged but no less important:

The first one is hardware integrity. The data centre's hardware travels around the globe, through several countries and multiple handling points, creating opportunities for tampering with the hardware, including counterfeit components, malicious changes to firmware, or even hardware backdoors. Although there is some controversy about the Bloomberg report from 2018 regarding supply chain hardware manipulation and the companies are contesting the report, this was a major driver of the increased demand for hardware provenance verification for sensitive government systems worldwide. But that concern was not some ruse, although there were specific details in that report that are disputed. Adopting data centres that process sensitive data requires hardware assurance processes, as well as software running on the hardware.

The second is the expertise of specialized AI hardware. AI training and inference workloads are powered by graphics processing units and AI accelerators from a handful of manufacturers, most notably NVIDIA, and plush contributions from AMD and Intel, and specialized chips from Google (TPUs), Amazon (Trainium) and Microsoft (Maia). It is noteworthy how much it relies on NVIDIA, with estimates indicating NVIDIA has more than 80 percent of the market for AI accelerators in data center training workloads. With a commercial focus, a disruption to NVIDIA's supply chain, whether due to component shortages, export control adjustments or geopolitical events that impact manufacturing in Taiwan, would be a direct hit on the ability to provide AI compute capacity around the world.

The strategic advice is clear-cut. It's important for organizations and governments that rely on data centers for critical operations to include hardware supply chain analysis as part of their resilience strategies, in addition to physical security and cybersecurity. These include the need to maintain inventories of components that can be used to model realistic supply disruption, diversification of hardware procurement where technically possible, requirements for hardware provenance documentation for sensitive applications, and advocacy/support of policy initiatives supporting geographic diversity in advanced semiconductors manufacturing. These are not policy statements. They are business decisions that have tangible resiliency impacts. The below-visible part of the visible data

center is silicon. Security and availability are strategic issues and should be treated as such, in the same way as the facilities where it resides.

13. PRACTICAL FRAMEWORKS FOR BUILDING RESILIENT DIGITAL INFRASTRUCTURE

So, now that the analytical foundation is laid for considering data centres as assets for strategic resilience, it's time to consider the question of what a realistic approach to resilience is for governments and organisations. The first step for national governments is to be able to formally designate data center facilities as critical infrastructure and ensure that they are included in national resilience plans. Designation brings with it a range of regulatory authority, information sharing requirements and security baseline requirements to open the door to a more systematic approach to vulnerability. It also facilitates a requirement for governments to require concentration risk assessment and resilience planning for operators of critical facilities which voluntary frameworks are unable to do.

In addition to designation, governments should mandate periodic systematic risk assessments of national concentration, to explore where critical digital services are concentrated, whether in facilities or providers, and in what situations a relatively small disruption could trigger large-scale national impacts. These audits are likely to turn up uncomfortable concentrations that commercial operators may not have noted for disclosure purposes, as it's not in their commercial interest to do so. The pain serves as feedback and tells you what to do.

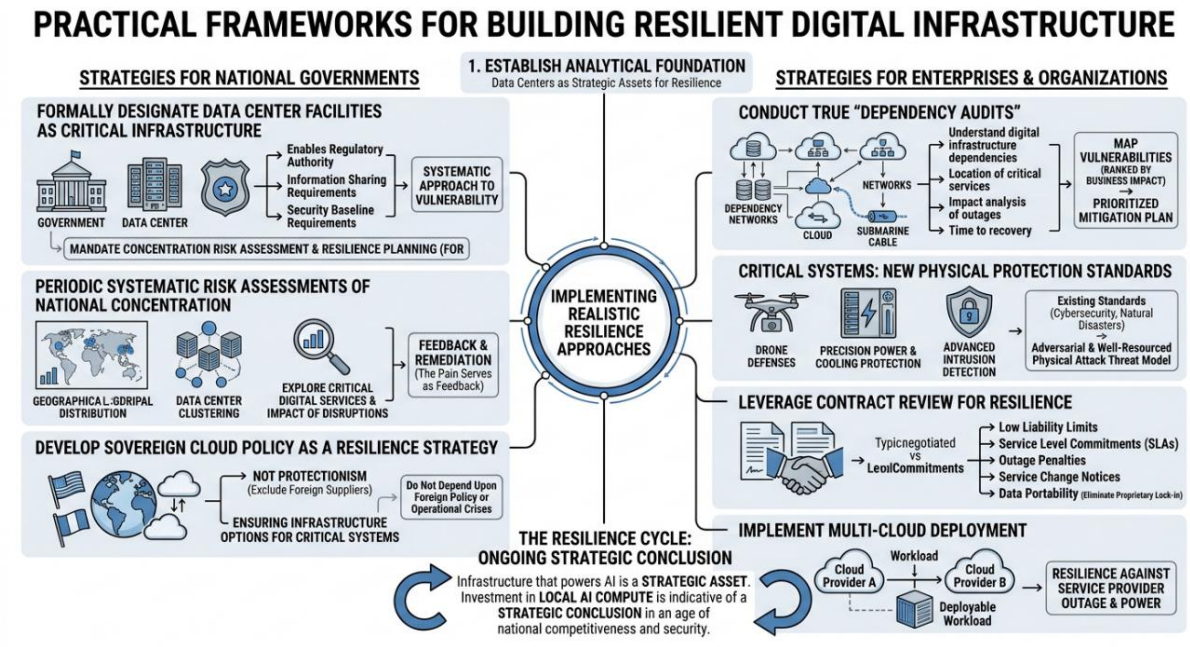

Fig -12: Practical Frameworks for Building Resilient Digital Infrastructure

There is a need to focus on sovereign cloud policy development as a resilience strategy, rather than a protectionist measure, which is important for policy development and for communicating with stakeholders. The idea is not to bar foreign suppliers out of national markets but to make sure that "critical national systems" have infrastructure options that do not depend upon a policy decision or an operational crisis by a foreign government or foreign company. These are goals that can go hand in

hand, and mixing resilience strategy with commercial protectionism is detrimental to both.

Data centers that house critical systems require a new set of physical protection standards, to consider an environment of attacks by drones, precision attacks against power and cooling facilities, and advanced physical intrusion capabilities. Most of the existing standards have been formulated based on a cybersecurity and natural disaster threat model rather than an adversarial and well-resourced physical attack threat model. This gap needs to be dealt with. The next on-the-ground challenge for enterprises is to perform "dependency audit" in true sense of the word. Most large organizations can't see beyond the tip of the iceberg when it comes to understanding their company's digital infrastructure dependencies, such as what cloud services are required for critical operations, where these services are located, what impact an outage of any one service will have, and how long recovery will take. The dependency audit should create a map of vulnerabilities, ranked by the business impact, and the map should lead to a certain mitigation plan with the highest exposures first.

Contract review is a real-life but underutilized aspect of enterprise resilience strategy. Typical commercial cloud contracts have low liability limits for providers and providers can make significant decisions about changing services. If it's a critical workload at stake, then organizations should seek agreements with service level commitments, financial penalties for service outages that impact the business, advance notice of service changes and provisions for data portability to eliminate proprietary lock-in. These terms are negotiable for larger enterprise customers and failure to negotiate them means that you are accepting a one-sided risk in your contract. Unfortunately, multi-cloud is operationally challenging, but it does offer a certain level of resilience if a service provider suffers an outage, as well as lessening the power of any one service provider over an organization. If the cloud investment is warranted, building workloads to be deployable on at least two cloud providers can offer a considerable level of resiliency over a single cloud provider.

14. FUTURE PROSPECTS AND RESEARCH DIRECTIONS

For the future, there are several developments that will influence the future of data centres as critical infrastructure in a way which existing frameworks might not be able to fully anticipate.

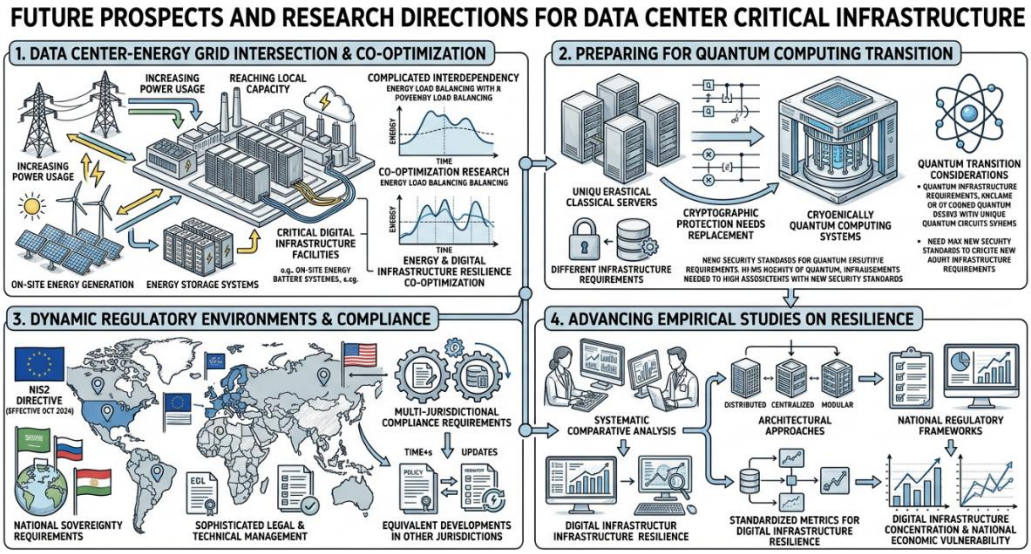

Fig -13: Future Prospects and Research Directions for Data Center Critical Infrastructure

The energy intersection will become increasingly prominent. Power usage in data centers is increasing so quickly that electrical power in high-density areas is starting to stretch thin. The interaction of the data center resilience and energy grid resilience introduces complicated interdependency that needs to be planned across sectors that aren't normally used to planning. An emerging research area is for the co-optimization of energy and digital infrastructure resilience, including the potential of on-site energy generation and energy storage at critical digital infrastructure facilities, such as data centers.

The disruptive factor that exists at a longer horizon is quantum computing. If the quantum systems are to become operational, they will need infrastructure very different from that of current classical computing facilities and cryptographic protection, on which current data security depends, will need to be replaced. Countries, companies, and other entities that are considering quantum transition when investing in digital infrastructure will be more ready than those that have not.

The regulatory environment will remain a very dynamic one. The European Union (EU)'s NIS2 Directive, which takes effect in October 2024, introduces a wide range of new cybersecurity requirements for operators of essential services, which includes specific regulations for digital infrastructure. There are equivalent developments in the regulation of other jurisdictions. An organization that chooses to operate internationally will have ever-growing multi-jurisdictional compliance requirements, with the combination of various national sovereignty requirements for data and computing infrastructure requiring sophisticated legal & technical management.

More empirical studies on the connection between the concentration of the digital infrastructure and national economic vulnerability are needed. While there are case studies of major outages and attacks available, systematic comparative analysis of the resilience outcomes of different architectural approaches and national regulatory frameworks is limited. The creation of such standardized metrics for digital infrastructure resilience, like those used for physical infrastructure resilience, could significantly help to develop policies and enterprise risk management.

15. CONCLUSION

In today's world, data centers are an integral part of the economy and the operation of states. This article has traced their development from specialised technical facilities to becoming strategic national assets and has also analysed how that change in nature has security and geopolitical implications and offered practical government and organizational models for dealing with the implications.

It is important to highlight some of the conclusions. The various "centralization-resilience" trade-offs associated with digital infrastructure are indeed a reality and are not self-evident and self-resolving. It needs to be planned for, and it will cost real money at the policy and architectural level. In the end, sovereign cloud and geographic distribution are not merely technical choices but strategic needs for countries that prioritize their digital sovereignty. The decision to adopt the enterprise cloud should be thought of as one of the biggest strategic moves a company makes, and as such, requires the same intensive risk analysis as other strategic investments such as dependency, regulatory compliance, cost trajectory, and business continuity. AI capability and compute infrastructure combine to usher in a new dimension of country power, redefining the geopolitical stakes of investing in data centers. But the talent piece the human part and resources needed to create, run, and even secure data centers is the most consistently overlooked aspect of the digital resilience strategy. Those organizations and governments that see these findings as operational requirements, and not advice givers, will be better positioned the next time a crisis comes around. This crisis will come in some capacity. The key thing is whether it will be

preceded by preparation.

REFERENCES

[1] Criekemans, D. (2025). Changing technology, shifting geopolitics. The Geopolitics and Geoeconomics of Technology. https://doi.org/10.4324/9781003568810-29
[2] Cârmici, A. A., & Coiciu, I. (2025). Leveraging artificial intelligence for error detection and resolution in data centers as critical infrastructure. International Conference of Management and Industrial Engineering (ICMIE 2025). Agility and Readiness for Sustainable Business Continuity. https://doi.org/10.56177/12icmie2025.205
[3] Cyber.gov.au. (2020). Cloud services | Cyber.gov.au. [online] Available at: https://www.cyber.gov.au/business-government/protecting-devices-systems/assessment-evaluation-programs/irap/cloud-services
[4] Gartner. (2025). Understanding the Landscape of Cloud Repatriation and Geopatriation. [online] Available at: https://www.gartner.com/en/documents/6902466
[5] CISA (2023). Critical Infrastructure Security and Resilience | Cybersecurity and Infrastructure Security Agency CISA. [online] www.cisa.gov. Available at: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience.
[6] World Economic Forum (2024). Global Risks Report 2024. [online] World Economic Forum. Available at: https://www.weforum.org/publications/global-risks-report-2024/.
[7] OECD. (2025). OECD Science, Technology and Industry Policy Papers. [online] Available at: https://www.oecd.org/en/publications/oecd-science-technology-and-industry-policy-papers_23074957.html.
[8] U.S. Congress (2022). H.R.4346 - 117th Congress (2021-2022): Supreme Court Security Funding Act of 2022. [online] www.congress.gov. Available at: https://www.congress.gov/bill/117th-congress/house-bill/4346.
[9] European Commission (2023). European Chips Act | Shaping Europe's digital future. [online] digital-strategy.ec.europa.eu. Available at: https://digital-strategy.ec.europa.eu/en/policies/european-chips-act.
[10] Dowthwaite, J. (2019). Definition and debabelization. Ezra Pound and 20th-Century Theories of Language. https://doi.org/10.4324/9780429292316-5
[11] Meiller, Y. (2025). Digital transformation, covid-19 crisis, digital transformation. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5350898
[12] Power, B., & Weinman, J. (2018). Revenue growth is the primary benefit of the cloud. IEEE Cloud Computing, 5(4), 89-94. https://doi.org/10.1109/mcc.2018.043221018
[13] Setola, R. (2023). Editorial on protection vs resilience by prof. roberto setola. International Journal of Critical Infrastructure Protection, 41, 100608. https://doi.org/10.1016/s1874-5482(23)00021-5
[14] Setola, R. (2025). Protection of critical infrastructures in times of peace and war. International Journal of Critical Infrastructure Protection, 50, 100799. https://doi.org/10.1016/s1874-5482(25)00060-5
[15] Ul Mustafa, A., & Aysan, A. F. (2026). Measuring agentic AI adoption and control frameworks in finance. Modern Finance, 4(1). https://doi.org/10.61351/mf.v4i1.557
[16] (2003). Government data centers. https://doi.org/10.17226/10664
[17] (2012). How we got here: History of data centers and current choices. Business Continuity Planning for Data Centers and Systems, 1-8. https://doi.org/10.1002/9780470428405.ch1
[18] Aven, T., & Kirkeby, S. P. (2018). Reliability targets for oil/gas production systems. Reliability Achievement. https://doi.org/10.1201/9781351076340-4
[19] Billakanti Ravinder, D. (2026). Digital financial systems and global financial inclusion: Opportunities, risks, and the role of digital public infrastructure. International Journal of Research and Analytical Reviews, 13(1). https://doi.org/10.56975/ijrar.v13i1.329442
[20] Lundberg, R. (2026). Critical thinking: Exploring the expansion of critical infrastructure. International Journal of Critical Infrastructure Protection, 52, 100814. https://doi.org/10.1016/j.ijcip.2025.100814
[21] Prior, R. (2022). The weight of the war – the strategic bombing of germany. Conquer We Must. https://doi.org/10.12987/yale/9780300233407.003.0024
[22] George, D. (2026a). Digital dividend data taxation's potential to transform India's economy and redefine fiscal policy in the mobile era. Zenodo (CERN European Organization for Nuclear Research).

https://doi.org/10.5281/zenodo.19021896
[23] Simpson, R. (2021). Digital earth: A world infrastructure for sustaining resilience in complex pandemic scenarios. COVID-19 Pandemic, Geospatial Information, and Community Resilience. https://doi.org/10.1201/9781003181590-36
[24] Smulian, P. R. (2000). The effects of presidential decision directive 63 on the public. https://doi.org/10.21236/ada378309
[25] TELENYK, S. S. (2020). ON THE DEFINITION OF THE CONCEPT OF INFRASTRUCTURE COMPLIANCE OF CRITICAL INFRASTRUCTURE OBJECTS. Law and Society, 2(2), 222-235. https://doi.org/10.32842/2078-3736/2020.2-2.34
[26] George, D. (2025c). The Critical Role of Data Science and Cybersecurity Innovations in Industry 4.0: A Handbook review. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.15199362
[27] Çam, E., Hungerford, Z., Schoch, N., Pinto Miranda, F., Yáñez De León, C. D., & International Energy Agency. (2024). Electricity 2024. In Electricity 2024. https://iea.blob.core.windows.net/assets/18f3ed24-4b26-4c83-a3d2-8a1be51c8cc8/Electricity2024-Analysisandforecastto2026.pdf
[28] George, D. (2025b). The Critical Role of Cybersecurity Insurance in an Era of Exponential Threats: A review of emerging risk realities and policy safeguards for Enterprise resilience. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.15070295
[29] Canadian Centre for Cyber Security. (2022). Cyber threat activity related to the Russian invasion of Ukraine [Report]. https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf
[30] George, D. (2025a). Redefining data centers for the AI revolution. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.14739520
[31] EUROPEAN UNION AGENCY FOR CYBERSECURITY, Ardagna, C., Corbiaux, S., Van Impe, K., & Ostadal, R. (2023). ENISA Threat Landscape 2023 (C. Ciobanu, Ed.).
[32] George, D. (2026b). Healthcare Monopoly and Patient Welfare: Economic analysis of essential dialysis services in underserved markets. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.19165911
[33] Guidelines on Risk Management Practices – Technology risk. (n.d.). https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines
[34] George, D., & George, A. (2025). Anatomy of cybersecurity. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.14738079
[35] Identifying, understanding, and analyzing critical infrastructure interdependencies. (2001, December 1). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/document/969131/
[36] George, D., & George, A. (2023a). The Emergence of Cybersecurity Medicine: Protecting Implanted Devices from Cyber Threats. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.10206563
[37] Janardhan, S., & Changigi. (2021, October 5). Update about the October 4th outage. Engineering at Meta. https://engineering.fb.com/2021/10/04/networking-traffic/outage/
[38] George, D., & George, A. (2023b). Safeguarding the Cyborg: The emerging role of Cybersecurity Doctors in Protecting Human-Implantable Devices. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.10397574
[39] Lee, C.-Y. & Friedrich Naumann Foundation for Freedom Global Innovation Hub. (2023). When globalisation meets geopolitics in the semiconductor supply chain. Friedrich Naumann Foundation for Freedom. https://www.freiheit.org/sites/default/files/2025-01/when-globalisation-meets-geopolitics-in-the-semiconductor-supply-chain_en.pdf
[40] George, D. (2026c). Is India running out of water - An analysis of water bankruptcy, AI data centers, and big finance. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.19259949
[41] Payment, clearing and settlement in various countries. (2014, September 1). https://www.bis.org/cpmi/paysysinfo.htm
[42] George, D. (2025e). Data centers and water crisis in India: Why digital infrastructure could drain our wells dry by 2030. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.17920097
[43] Publication, A. R. R. (2026). Securing Tomorrow: How 6G networks and AI are reshaping the cybersecurity landscape. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.18299699

[44] George, D. (2025d). The Dual Shield: Cybersecurity insurance in an era of evolving digital threats. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.15428076
[45] Uptime Institute Global Data Center Survey 2024, Donnellan, D., Lawrence, A., Bizo, D., Judge, P., O'Brien, J., Davis, J., Smolaks, M., Williams-George, J., & Weinschenk, R. (2024). Uptime Institute Global Data Center Survey 2024. https://datacenter.uptimeinstitute.com/rs/711-RIA-145/images/2024.GlobalDataCenterSurvey.Report.pdf?version=0
[46] (2019). High-altitude daylight precision bombing in world war II. Lectures of the Air Corps Tactical School and American Strategic Bombing in World War II. https://doi.org/10.5810/kentucky/9780813176789.003.0008
[47] (2023). Infrastructure system resilience. American Society of Civil Engineers. https://doi.org/10.1061/9780784485088
[48] Cooper, R. (2004). Treasury systems. Corporate Treasury and Cash Management. https://doi.org/10.1057/9781403946010_18
[49] Franks, P. C. (2015). Government use of cloud-based long term digital preservation as a service: An exploratory study. 2015 Digital Heritage. https://doi.org/10.1109/digitalheritage.2015.7419526
[50] Showstack, R. (2002). Global environmental report card. Eos, Transactions American Geophysical Union, 83(5), 46-46. https://doi.org/10.1029/eo083i005p00046-04
[51] Soualah, O., Fajjari, I., & Aitsaadi, N. (2021). Inter-data center networks: Routing and reliability in virtual network backbone. Management of Data Center Networks, 85-103. https://doi.org/10.1002/9781119647485.ch4
[52] Sprenkamp, K., Dolata, M., Schwabe, G., & Zavolokina, L. (2025). Data-driven intelligence in crisis: The case of ukrainian refugee management. Government Information Quarterly, 42(1), 101978. https://doi.org/10.1016/j.giq.2024.101978
[53] (1984). Large scale scientific computation. https://doi.org/10.1016/c2013-0-11291-3
[54] (2014). Military doctrine and international law. The Concept of Military Objectives in International Law and Targeting Practice. https://doi.org/10.4324/9781315745282-9
[55] (2017). Statement of profit or loss - revenue. Corporate Financial Reporting. https://doi.org/10.5040/9781350394698.ch-007
[56] (2022). Russian invasion raises risk of cascading cyberattack. Emerald Expert Briefings. https://doi.org/10.1108/oxan-es267563
[57] (2022). Cyberattack on ukraine's power grid underlines risk. Emerald Expert Briefings. https://doi.org/10.1108/oxan-es268618
[58] (2024). Chapter 7: Cloud migration and strategies. AWS Cloud Migration. https://doi.org/10.1515/9781501521546-009
[59] Brüning, H., Jossin, J., & Grabow, B. (2025). Transformationsraum n - offene initiative für beschleunigte nachhaltigkeit vor ort. GAIA - Ecological Perspectives for Science and Society, 34(2), 88-93. https://doi.org/10.14512/gaia.34.2.5
[60] Grammatikakis, K. P., & Kolokotronis, N. (2021). Attack graph generation. Cyber-Security Threats, Actors, and Dynamic Mitigation. https://doi.org/10.1201/9781003006145-8
[61] Greenwell, R., Liu, X., Chalmers, K., & Pahl, C. (2016). A task orientated requirements ontology for cloud computing services. Proceedings of the 6th International Conference on Cloud Computing and Services Science. https://doi.org/10.5220/0005752301210128
[62] Mäntysaari, P. (2015). Balancing contracts and balance group contracts. EU Electricity Trade Law. https://doi.org/10.1007/978-3-319-16513-4_9
[63] Schewe, P. F. (2004). The massive northeast blackout. Physics Today, 57(10), 9-9. https://doi.org/10.1063/1.4797191
[64] Souza, P., Marques, W., Reis, R., & Ferreto, T. (2019). IAGREE: Infrastructure-agnostic resilience benchmark tool for cloud native platforms. Proceedings of the 9th International Conference on Cloud Computing and Services Science. https://doi.org/10.5220/0007728503960403
[65] Tomar, N., & Nasreen, R. (2021). Need for national policy on women empowerment. Women and Entrepreneurship in India. https://doi.org/10.4324/9781003160786-16
[66] (1999). Managing the IT procurement process. Handbook of Data Center Management, 1998 edition. https://doi.org/10.1201/9781482287813-47
[67] (2004). Fixed-cost contribution per unit. Dictionary of Marketing Communications. https://doi.org/10.4135/9781452229669.n1310
[68] (2007). Goh chok tong, (born 20 may 1941), senior minister, prime minister's office, singapore, 2004–11, now emeritus; senior adviser, monetary authority of singapore, since 2011 (chairman, 2004–

11). Who's Who. https://doi.org/10.1093/ww/9780199540884.013.u17366
[69](2022). Nation-states, economic protectionism, national security, the solarwinds cyber-attack, and the impact on supply chains from the russian-ukrainian war. International Journal of Social Science and Human Research, 05(07). https://doi.org/10.47191/ijsshr/v5-i7-68
[70](2024). Chapter 7: Cloud migration and strategies. AWS Cloud Migration. https://doi.org/10.1515/9781501521546-009
[71](2025). WHO certification scheme on the quality of pharmaceutical products. World Health Organization. https://doi.org/10.2471/b09336
[72]Akhbar, F., & Ovatman, T. (2015). Quality of service trade-offs between central data centers and nano data centers. Proceedings of the 5th International Conference on Cloud Computing and Services Science. https://doi.org/10.5220/0005439101130118
[73]Hayashi, Y. (2025). Formação de lideranças técnicas e a escassez global de mão de obra. RCMOS - Revista Científica Multidisciplinar O Saber, 1(2). https://doi.org/10.51473/rcmos.v1i2.2025.1297
[74]Hincu, V. (2026). CLOUD REPATRIATION: AN EMPIRICAL ANALYSIS OF WHEN MOVING BACK FROM CLOUD CREATES BUSINESS VALUE. Universum:Technical sciences, 4(145). https://doi.org/10.32743/unitech.2026.145.4.22457
[75]Nutalapati, P. (2022). Compliance and regulatory challenges in public sector cloud adoption. International Journal of Science and Research (IJSR), 11(2), 1362-1366. https://doi.org/10.21275/sr24903075206
[76]Sangam, G. K. (2025). AI and analytics enablement in salesforce hyperforce: Leveraging cloud-native infrastructure for financial insights. The American Journal of Engineering and Technology, 07(12), 40-51. https://doi.org/10.37547/tajet/v7i11-311
[77]Yu, A., & Yu, S. (2026). U.S. semiconductor export structure under innovation and trade policy. Journal of Economics & Management Research. https://doi.org/10.47363/jesmr/2026(7)326
[78](2009). National infrastructure protection plan. Homeland Security and Critical Infrastructure Protection, 35-44. https://doi.org/10.5040/9798216973058.0008
[79](2018). Cloud management baselines, performance, and slas. CompTIA Cloud+ Study Guide Exam CV0-002 2e, 243-263. https://doi.org/10.1002/9781119549543.ch8
[80]Cronin, I. (2026). Scaling training with infrastructure and distributed systems. Building and Training Generative AI Models. https://doi.org/10.1007/979-8-8688-2332-9_6
[81]Hincu, V. (2026). CLOUD REPATRIATION: AN EMPIRICAL ANALYSIS OF WHEN MOVING BACK FROM CLOUD CREATES BUSINESS VALUE. Universum:Technical sciences, 4(145). https://doi.org/10.32743/unitech.2026.145.4.22457
[82]Hunter, R., & Weiss, J. (2021). CYBERSECURITY AND DATA CENTERS. Data Center Handbook, 349-358. https://doi.org/10.1002/9781119597537.ch20
[83]Kohne, A. (2018). Service level agreements. Cloud-Föderationen. https://doi.org/10.1007/978-3-658-20973-5_3
[84]Kolb, A. (1991). Data protection — germany. Computer Law & Security Report, 7(3), 123-126. https://doi.org/10.1016/0267-3649(91)90089-e
[85]Nutalapati, P. (2022). Compliance and regulatory challenges in public sector cloud adoption. International Journal of Science and Research (IJSR), 11(2), 1362-1366. https://doi.org/10.21275/sr24903075206
[86]Seppain, H. (1992). Cocom and US export control policy after 1953. Contrasting US and German Attitudes to Soviet Trade, 1917–91. https://doi.org/10.1007/978-1-349-12602-6_7
[87]Shukla, M., Johnson, S. D., & Jones, P. (2019). Does the NIS implementation strategy effectively address cyber security risks in the UK?. 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). https://doi.org/10.1109/cybersecpods.2019.8884963
[88](2013). Ensuring the disaster recovery planning process delivers business continuity – the experience of a major UK retail bank. IT in Business: A Business Manager's Casebook. https://doi.org/10.4324/9780080496238-21
[89](2021). When is a s&e workforce shortage not a shortage?. AAAS Articles DO Group. https://doi.org/10.1126/article.64408
[90]Daniel, M., & Golemo, K. (2024). Economic and geopolitical challenges in graphics processing unit manufacturing: The case of the taiwan semiconductor manufacturing company market dominance. Azja-Pacyfik, 2024(Tom XXX), 61-88. https://doi.org/10.15804/ap2024.2.03
[91]Hardavellas, N., Ferdman, M., Falsafi, B., & Ailamaki, A. (2011). Toward dark silicon in servers. IEEE Micro, 31(4), 6-15. https://doi.org/10.1109/mm.2011.77

[92] Lee, C. S., & Pecht, M. (2020). Semiconductor market focus. The Taiwan Electronics Industry. https://doi.org/10.1201/9780429332845-6
[93] Miceli, T. (2023). AI/ML efforts at fermilab and plans for future accelerator operations. AI/ML Efforts at Fermilab and Plans for Future Accelerator Operations. https://doi.org/10.2172/1969676
[94] Ramm, P. (2023). Implementation of applied r&d and european activities in the "chips act age". IMAPSource Proceedings, 2023(DPC). https://doi.org/10.4071/001c.90678
[95] Soest, H. V. (2025). Cybersecurity in the european electricity system: The role of the NIS2 directive. European Energy Law Report, 345-362. https://doi.org/10.1017/9781839704635.016
[96] VerWey, J. (2023). Betting the house: Leveraging the CHIPS and science act to increase U.S. microelectronics supply chain resilience. https://doi.org/10.51593/20220054
[97] (2022). Preparing for post-quantum critical infrastructure: Assessments of quantum computing vulnerabilities of national critical functions. https://doi.org/10.7249/rra1367-6
[98] (2023). Challenges to U.S. national security and competitiveness posed by AI. https://doi.org/10.7249/cta2654-1