HIDDEN RISKS OF DIGITAL WORLD

Angelina Bott [1]

[1] Institute of Radio and Information Systems (IRIS), Vienna, Austria;
iris@media-publisher.eu

Overview of report materials by Technology and Global Affairs Innovation Hub of the Paris School of International Affairs, Sciences Po [11]

DOI: 10.36724/2664-066X-2026-12-2-49-61

Received: 05.05.2026
Accepted: 07.05.2026

Citation: Angelina Bott, "Hidden risks of digital world," *Synchroinfo Journal* **2026**, vol. 12, no. 2, pp. 49-61.

ABSTRACT

As digital systems become ever more central to our lives, the risks that threaten them increasingly transcend sectors, institutions, and borders. Critical digital disruptions, whether driven by natural hazards, infrastructure failure, or systemic interdependencies, can spill over at a speed and scale that existing governance frameworks are not yet designed to manage. This work confronts a growing paradox. While digital infrastructure has brought extraordinary efficiency, connectivity, and resilience to everyday life, it has also created new forms of systemic vulnerability. They unfold quietly, across interdependent systems, until critical functions suddenly stop working, often when they are needed most. Developed through a co-creation process with international experts, this report makes visible the hidden dependencies and knock-on effects that standard risk assessments tend to overlook. Its aim is not prediction, but preparedness: to support a shared understanding of critical digital risks before disruption occurs. This work outlines risk scenarios on Earth, at sea, and in space, analysing the fragility of interconnected digital systems and offering a roadmap for preparedness.

KEYWORDS: *critical digital infrastructure, digital risks, solar storm, space debris, extreme weather*.

Introduction

What if, tomorrow, mobile phones and the internet stopped working, payments failed, hospitals lost patient data, and emergency alerts never arrived? What may sound like science fiction could become reality. A large-scale, escalating failure of critical digital systems, a 'digital pandemic', is a plausible scenario that current management frameworks are not yet designed to address. Modern society runs on critical digital infrastructure: From electricity, finance and transport to healthcare, communication and government services. Everything depends on deeply connected systems that are more fragile than they appear, and whose risks remain largely overlooked.

A solar storm of the magnitude that narrowly missed Earth in 2012 could have knocked out power grids and communications across entire continents. Growing space debris already threatens to push low-Earth orbit toward failure, jeopardizing satellite navigation, financial networks, and weather forecasting all at once. Extreme weather, which is growing more violent with climate change, has already shown its capacity to sever digital infrastructure entirely, turning disasters into humanitarian crises.

Report [11] shows that digital disruptions rarely remain isolated events. They cascade. What begins with a local failure can rapidly spread across sectors and borders. In fact, up to 89% of digital disruptions from natural hazards are caused by secondary spillover effects rather than the initial damage [1]. The number of people ultimately affected can be up to ten times higher than those initially exposed to the initial event [2]. Digital risks often remain invisible until they reach a critical threshold. Systems simply stop working while our physical world is seemingly unaltered. This may delay crisis response when action matters the most.

Meanwhile, our ability to cope without digital systems has eroded. Across sectors, analogue skills and fallback options have disappeared or are no longer tested. When systems fail at scale, manual alternatives often cannot replace them. However, the severity of this challenge varies significantly across contexts: countries with more limited infrastructure redundancy, including small island developing states and least developed countries, face distinct and in some cases more acute vulnerabilities.

Finally, a critical gap persists in how risks are understood. Cyber threats attract significant attention, but non-intentional disruptions of material infrastructure follow different dynamics. The knowledge exists, but we are not paying sufficient attention. And even when we do, we lack the necessary frameworks, standards, and coordination capacities needed to turn that knowledge into preparedness.

Addressing these risks requires action across six priorities, identified through a co-creation process with senior expert practitioners spanning international organizations, national authorities, academic institutions, and the private sector:

1. Building the knowledge base to identify critical risks, model chain reactions, and map cross-sector dependencies;

2. Updating r k management frameworks to recognize non-intentional digital disruptions as a core risk;

3. Strengthening international standards for resilience, encouraging cooperation for analogue fallback capacity, and joint scenario planning;

4. Ramping up proactive coordination on the most acute risk vectors; enhancing societal capacity to absorb and recover from digital disruptions;

5. Building the tr t, shared situational awareness, and

6. Global co aboration needed to translate early warnings into collective action.

Scenarios of critical digital failures

The scenarios that follow translate abstract risk into concrete terms.

Grounded in documented hazards, empirical evidence, and cross-sector expertise spanning telecommunications, digital infrastructure governance, natural hazards, risk management, cybersecurity, and critical systems resilience, the scenarios in this section were developed through a collaborative process. Senior experts from international organizations, national authorities, academic institutions, and the private sector contributed to their design. The scenarios trace plausible chains of events through tightly coupled systems. They are not exercises in forecasting. Instead, they were attempts to make explicit what is usually left implicit: the dependencies that never appear in risk registers, and the moments at which a digital system crosses, without warning, into a large digital disruption. Their purpose is to provide policymakers and practitioners with a shared tool to work from. The severity and nature of impacts will vary substantially across regions, depending on levels of digital integration, infrastructure ownership, and national regulatory capacity.

The data and timelines presented in the three scenarios are illustrative. They are grounded in scientific literature, expert knowledge, and documented past events, but they are not probabilistic predictions: real-world disruptions unfold under conditions of uncertainty and complexity that no model fully captures, and their actual effects may differ significantly from those described here. The scenarios are intended to render visible the structural dynamics of systemic failure and not to prescribe how any specific event will unfold.

Space

In September 1859, a solar storm, an extraordinary burst of energy and charged particles from the sun, struck Earth. Telegraph operators in Europe and North America received electrical shocks. Sparks flew from telegraph equipment, setting some offices alight. Auroras were visible even at tropical latitudes. The event entered history as the Carrington Event, named after the British astronomer who observed it. At the time, the telegraph was the internet. Although the damage was severe, the infrastructure was relatively easy to rebuild, and broader societal functions continued largely unaffected. Probabilistic estimates of a Carrington-class event vary widely across the literature, reflecting different methodological approaches and datasets. Estimates for the next decade range from under 2% to approximately 12%, depending on the statistical model applied [3]. A 2013 Lloyd's of London assessment estimated the North American impact alone at between 0.6 and 2.6 trillion US dollars [4]. Crucially, no event of this magnitude has occurred within the lifetime of any digital system. Yet a near miss in 2012 had a similar strength to the Carrington event. The following scenario illustrates how a similar event would unfold if it were to strike today.

T-18 to T-0 hours: the warning window

Space weather monitoring detects a large coronal mass ejection on an Earth-impact trajectory. The warning window is 16 to 20 hours: sufficient for some protective measures, but insufficient for most. Three power utilities in northern latitudes reduce transformer loads. Airlines begin grounding polar routes, where navigation and communications are most vulnerable to solar interference. A major cloud provider suspends high-latitude operations.

Most organizations do not act. The decision-makers who receive the warning have never experienced anything similar, and the systems they manage have never been tested against it. This is not negligence. It is a structural feature of risk management built on historical data, and the historical record contains only one major entry.

T+2 hours: navigation disappears

Global Navigation Satellite Systems (GNSS) rely on radio-frequency signals from satellites to provide precise position, velocity, and time worldwide. When these signals become globally unreliable, aircraft must revert to fixed flight procedures rather than live radar, slowing traffic to a fraction of normal capacity. Maritime navigation slows. Emergency services lose dispatch routing. Autonomous cars stop. Precision agriculture also halts, affecting food supply. Financial infrastructure does not merely use digital networks for transactions; it uses satellite timing to synchronize them. This timing failure is particularly consequential: When the timestamps become unreliable, clearing systems cannot determine the order of precedence. Transactions are rejected.

T+4 to T+8 hours: The wave of blackouts

Geomagnetically induced currents can cause transformer failures in national grids. The failures do not occur simultaneously: they move with the storm front, creating a travelling wave of outages that exhausts restoration capacity before any grid can fully recover. Initially, blackouts are managed. By hour eight, a number of grids have lost central dispatch capability. Data centres begin exhausting backup power. The disruption accelerates as backup systems reach their limits. Transformer replacement requires twelve to eighteen months per unit under normal manufacturing conditions. There is no strategic reserve, and no established international protocol for the coordination of recovery currently exists.

T+12 to T+72 hours: The failed assumption

Every business continuity plan rests on an assumption that is rarely stated: that manual procedures can substitute for digital systems in case of failure. At scale, under sustained disruption, this assumption is tested, and in even the most advanced economies, it fails. Hospital staff trained exclusively on electronic health record systems cannot locate patient information. Bank branches without cash reserves cannot serve customers. Traffic management in digitized urban centres fails. The skills required for analogue fallback are either absent or have not been rehearsed. Coordination depends on capacities that have been decommissioned or reduced.

The analogue skills problem can be described through the lens of aviation: GNSS navigation has so thoroughly replaced traditional piloting skills that specific training programmes now exist to maintain the capacity to fly without GNSS when disruptions occur. This principle applies across every sector.

Beyond 72 hours: The long silence

The duration of the disruption is determined not by the storm, but by the transformer replacement. When grid restoration requires components manufactured in a few facilities globally, the recovery is measured in months. The scenario does not end with a dramatic event, but with a slow, inequitable process of rebuilding infrastructure whose vulnerability was known and long documented.

What this scenario reveals

Space weather is not integrated into national disaster risk registers in most countries. The Carrington benchmark is scientifically well-established; the probability estimates are credible; the engineering vulnerabilities of high-voltage transformers are well- documented. What is absent is a mechanism that systematically connects this knowledge to coordinated preparedness action across the organizations, jurisdictions, and sectors concerned. The scenario does not require a failure of a warning system or a human error. It requires only not to change our current way of dealing with this risk.

Terrestrial

In 2003, weather forecasts on high temperatures were largely accurate, warnings were issued across Western Europe, and civil protection authorities sent heatwave advisories. The guidance matched the risk, as it was well understood, but the chain of consequences was not. The mechanism to translate a meteorological signal into a public health mobilisation was missing, which resulted in over 70.000 excess deaths across Western Europe. Meanwhile, the heat lowered river levels and raised water temperatures, forcing power plants to cut output just as demand peaked [5]. Although this strained electricity supply, digital infrastructure was not yet deeply embedded in critical systems, so its failure did not cause widespread and systemic disruption. The event would play out differently today.

Days 1-2: Below every threshold, everywhere at once

Several large data centre clusters in the region begin reporting cooling stress on the first morning. Electricity consumption across the grid reaches 97% of capacity by the afternoon. A regional transmission operator, following standard procedure, applies precautionary load-balancing, producing micro-outages of 8 to 12 minutes in suburban and industrial zones. Each of these events falls below the formal alert threshold for its respective system. No emergency is declared. No cross-sector coordination is triggered.

This is how cascading failures begin: not with a dramatic event, but with a convergence of tolerable pressures that no individual operator is positioned to see as a whole.

Day 3: The first cascade

Some data centres switched to a degraded mode, suspending non-critical services in anticipation of backup generator fuel shortages caused by reduced river traffic during the heatwave that noticeably affected the navigability of rivers. Mobile network latency increases by 180%. A major operator's traffic management system, itself hosted in one of the affected centres, begins throttling automatically. Several thousand base stations lose active cooling. A regional cloud provider suspends services and reroutes traffic to northern European nodes, creating congestion on transnational links that have not been designed to absorb the load.

In a meeting room in another country, engineers at a telecommunications company are looking at dashboards that show a problem they had not anticipated: their traffic management decisions were now entangled with the cooling capacity of buildings they did not own, in a city experiencing a weather event they had not included in their resilience planning.

Days 4-5: Health and financial systems learn they are dependent on a server room

An Uninterruptible Power Supply, a form of backup power, continues operating but no longer fully provides backup power or protection at one data centre during a 14-minute grid micro-outage. Recovery takes 31 hours. During this window, the national health authority's patient data exchange system, used for real-time bed availability and ambulance routing, becomes inaccessible. Three hospitals revert to telephone coordination. Emergency response times increase by 34% in the affected area.

The dependency has not appeared in any standard risk register. The health authority had not been consulted when the data exchange platform migrated to cloud infrastructure eighteen months earlier. No one has asked what would happen if the data centre hosting it overheated during a heatwave. The question has not seemed necessary.

A financial clearing system used by regional retailers fails to settle transactions for 19 hours. Smaller merchants suspend electronic payments and close. On the fourth day of a heatwave, in a city where temperatures have reached 42 degrees, many shops are shut not because of the heat but because their card terminals cannot connect to a server that has overheated.

Day 6: The alert that could not be sent

On the final day of the heatwave, a second data centre experiences a cooling failure simultaneously with a peak-load grid event. Mobile connectivity in the core urban area drops to 12% of normal capacity for four independently of data networks, relies on base station transmitters, several hundred of which have been without active cooling since Day 3. The civil protection authority attempts to issue a new emergency public alert, but the primary alert dissemination platform is also down. Radio and analogue systems are activated. Still, a significant proportion of the population does not receive the alert.

What this scenario reveals

The heatwave is forecasted. The data centre stress is measurable. The dependencies, power grid to cooling to cloud to health system to civil alert, have all been documented somewhere, by someone. What does not yet exist is a shared mechanism to view these dependencies together, or any protocol that treats a sustained thermal event as a digital infrastructure emergency. The absence of a visible trigger, no explosion, no cyberattack, no dramatic failure, means that each organization waits for someone else to declare the crisis. By the time anyone does, the alert system that would have reached the public is already offline.

Undersea

On 15 January 2022, the Hunga Tonga-Hunga Ha'apai volcano erupted 40 km north of the Tongan capital. It shredded 80 km of the single submarine cable connecting the archipelago to the rest of the world. The nearest repair ship was stationed in Papua New Guinea, more than 4,200 km away. Tonga went dark for five weeks [6]. The domestic inter-island cable, buried under volcanic debris, took eighteen months more to repair. Tonga carried little global traffic. Had the same cable geography applied to a major routing hub, a choke point where dozens of systems converge, the outage would not have been a footnote of a volcanic eruption. It would have been a financial and logistical crisis measured in continents.

Hour 0-6: The rupture and the governance vacuum it exposes

Several cables are severed immediately. Others sustain damage that instruments will not detect until day eight, when they fail completely, eliminating the residual connectivity. In the first six hours, satellite backup absorbs approximately 8% of normal traffic. Within 90 minutes, even that capacity is overwhelmed.

The affected cables are owned by a consortium of private operators from a number of countries. Repair vessel mobilization requires commercial negotiation and approvals from coastal States, including routing authorisations across three exclusive economic zones. The fastest available cable repair vessel is nine days away. A second is identified but requires 18 days to reach the severed cables. The whole Pacific is covered by a few ships.

Emergency requests to redirect satellite capacity trigger competing national claims on available bandwidth. No agreed protocol for prioritization currently exists, nor a shared definition of what level of connectivity constitutes a humanitarian minimum. This reflects the distributed nature of responsibilities across national authorities, international organizations, and private operators.

Days 2-7: Cascading into economies and bodies

Financial clearing for the region is suspended after 48 hours of degraded connectivity. Businesses can not settle import payments. Port operations slow by 60% as logistics software, dependent on cloud services, becomes inaccessible. A regional central bank declares a connectivity emergency. Health facilities that had migrated patient records to cloud platforms lose access to clinical histories. A doctor treating a patient in a rural clinic has no record of the patient's medications or previous diagnoses. This is the moment when a system that appeared to be about information management reveals itself to be a system of medical safety. The cloud migration has been efficient, but it created a hidden interdependency to be taken into account.

Days 8-21: Three weeks without the internet

The region reverts to operating on high- frequency radio and physical document transport. A generation of administrators, health workers, teachers, and traders who had never worked without digital connectivity discover, under stress, that analogue fallback requires skills that have been lost, equipment that has been decommissioned, and institutional memory that had not survived the transition to digital systems. Misinformation spreads rapidly to fill the information vacuum. With verified information sources unavailable, speculations fill the vacuum. Rumours about the cause of the outage, about when connectivity would return, about which banks had cash reserves and which did not, circulate and are amplified. The information disruption is no longer a secondary effect of the cable rupture; it becomes a crisis of its own.

What this scenario reveals

Submarine cables carry over 99% of international internet traffic. Yet, there are only a few hundred globally. Repair capacity is commercially contracted and geographically limited. While bodies such as the International Cable Protection Committee that include private and public actors, coordinate cable protection and facilitate repair operations, this capacity operates without a strategic reserve requirement or any public international governance framework adequate to a major multi-cable event. In this scenario, every relevant institution, national governments, international organisations, cable operators, satellite providers, and financial regulators have a partial role. However, no actor has the authority required to match its responsibility. The crisis is not only caused by an eruption; it is mainly caused by an architecture in which no single actor holds both the authority and the operational capacity required to match the scale of its responsibilities.

Shared patterns of systemic digital risks

Despite their different triggers, critical digital risk scenarios tend to follow a common set of structural patterns. Notably, different critical digital risk scenarios are equally possible. A prolonged drought could affect the river systems used for data centre cooling. A major volcanic eruption along a submarine cable corridor could replicate and amplify the governance vacuum the undersea cable scenario exposes, while adding atmospheric disruption that degrades satellite backup simultaneously. A major hurricane could level the mobile towers and poles carrying communications fibre of island nations. A progressive collapse of collisions in low Earth orbit makes large numbers of communications satellites inoperable and generates debris fields dense enough to render key orbital shells unusable for decades. Unlike the other scenarios in this report, the scenario, known as the Kessler effect, would leave no immediate recovery path. Read each scenario should therefore be read as a question: not 'could this happen?' but 'what would we do if it did?'

What do those three scenarios share?

These disruptions are preceded by warnings. In each case, the information required to anticipate the disruption existed. The probability of a major solar event was published. The heatwave was forecast. The cable corridor's vulnerability was mapped. What was absent in each case was not knowledge but the architecture to translate knowledge into coordinated action across the organizations, jurisdictions, and sectors that a disruption would cross. Yet this architecture must also extend to risks that have not yet been named: building the capacity to surface unknown unknowns as the vulnerabilities that exist before they appear in any forecast or risk register remains an equally pressing challenge.

They are invisible until they are not. None of these crises announces itself with a single dramatic event. Instead, they accumulate through thresholds that no individual organization is positioned to see in aggregate. By the time the crisis is legible as a crisis, the window for the most effective interventions has already closed.

They expose a specific kind of dependency: the hidden kind. Financial transactions depend on satellite timing. Transport systems depend on real-time data, GNSS navigation, and digital traffic management. Health systems rely on cloud platforms. Emergency alerts depend on the same data centres as everyday services. These dependencies were created through individually rational decisions, by people who were not asked, and had no mechanism to assess what those choices meant for the system as a whole.

Finally, digital risks do not depend simply on how digitalised a country is. The global digital divide, leaving about one quarter of the world offline, creates distinct vulnerabilities: in some Small Island Developing States, connectivity might depend on a single submarine cable, with critical data infrastructure often lying beyond national jurisdiction [7]. The second part of this report examines the analytical foundations that explain why these patterns recur, and what a management response adequate to their scale would require.

Understanding critical digital risks

The scenarios described in the first part of this report are not hypothetical curiosities. They are plausible projections of a risk landscape that has been systematically documented across technical literature, empirical studies of recent infrastructure failures, and the expert co-creation processes on which this report is based. This second part steps back from the narrative level to examine what we actually know about critical digital risks: how they are conceptualized, what structural conditions produce them, where our frameworks remain inadequate, and what forms of management could begin to match the scale of the challenge. Contemporary digital infrastructure is simultaneously more robust and more fragile than ever before. This is not a contradiction but a structural feature of how large-scale networked systems evolve. Decades of investment in redundancy, load balancing, and distributed architecture have made digital systems increasingly resilient to routine and localized failures. A single server outage, a cut fibre link, a software bug: these events can be absorbed by systems designed to handle such failures. Yet this same architecture, tightly coupled, deeply interdependent, optimized for efficiency over slack, creates conditions in which a sufficiently large initial shock can propagate across systems with a speed and scope that no single operator controls or even anticipates.

The literature describes this as the transition from additive to exponential failure dynamics. In traditional risk models, two concurrent hazards produce roughly the sum of their individual impacts. In a tightly coupled digital infrastructure, concurrent stresses interact nonlinearly: the failure of one system removes a redundancy that another depends upon,

which in turn overloads a third, triggering cascading collapse across sectors that were never explicitly connected in any operator's risk register. Empirical evidence confirms that this is not just a theoretical concern. Studies of observed outages show that up to 89 per cent of digital service disruptions caused by natural hazards result not from direct physical damage but from these secondary ripple effects. The number of people ultimately affected is estimated to be up to ten times higher than those exposed to the initial event [8].

This paradox has a second dimension that expert discussions have brought into sharp relief: digital risks are invisible. Unlike floods, earthquakes, or industrial accidents, digital infrastructure failures frequently produce no visible physical signal. Populations and organizations may wake to find nothing altered in their surroundings, yet critical systems have ceased to function. This invisibility delays recognition of severity and postpones activation of response mechanisms precisely when timely action proves most consequential. The 2011 Fukushima nuclear accident illustrates the principle: the multi-sector breakdown from earthquake to tsunami to nuclear crisis created critical information gaps that were themselves a secondary disaster. When the information infrastructure fails, the capacity to assess damage, coordinate response, and communicate guidance is destroyed simultaneously with, or even before, the physical systems it depends on.

Four infrastructure domains and their interdependencies

The core expert group on critical digital risks identified four critical infrastructure domains whose interdependencies constitute the material architecture of digital risks. These are not independent categories but layers of a single ecosystem, each depending on the others in ways that are only partially mapped.

1. Power grids as e foundational layer

Power grids serve as the foundational layer of digital infrastructure. Every other digital system, telecommunications networks, data centres, payment systems, navigation services, and mobile infrastructure, as well as satellite earth stations, depend on a reliable electricity supply. Power grid failures, therefore, ripple immediately across the entire digital ecosystem. The critical implication is that power infrastructure must be assessed in three phases: preventing failure, maintaining degraded operations during disruption, and restoring service within timeframes that prevent dependent.

Historical analysis shows that restoration delays produce sequential failures:

- The 2003 E ropean heatwave triggered power grid stress, which contributed to cascading failures across interdependent systems.
- The 2021 OVHcloud fire in Strasbourg was responsible for the disruption of ~3.6 million websites from a single physical facility failure.
- The Oregon eatwave in 2021 caused data centre outages at multiple cloud providers.
- In 2022, the Oracle and Google Cloud failures in London were linked to cooling capacity during a heat event.
- The 2025 blackout in Spain involved the sudden loss of 15 gigawatts of power, triggering cross-sector failures and knocking out telecommunications across Spain and Portugal. Internet, mobile, and messaging services were widely disrupted, with knock-on effects reaching Morocco and remote villages in Greenland.

2. Submar e cables as the connectivity backbone

Submarine communication cables transmit over 99 per cent of international internet traffic, yet their critical role remains poorly understood in public discourse and risk governance frameworks. Submarine cables are fragile and easily severed by natural hazards or

commercial fishing activities. What makes these events particularly severe is the repair timescale: specialized cable repair vessels exist in limited numbers globally, and restoration can require several months, during which traffic is rerouted through alternative paths, degrading service across the wider network.

The vulnerability of undersea cables to natural hazards is well documented:

- The 2006 Hengchun underwater earthquake severed eight cables simultaneously, degrading connectivity across several Asian countries for weeks.
- The 2022 unga Tonga volcanic eruption isolated an entire island nation from global communications.
- In 2022, a single cable failur on the Shetland Islands isolated communities for several days.
- The 2024 ed Sea cables disruption consisted of multiple cables cut within weeks, with 25% of traffic between Asia and Europe disrupted.
- Multiple precedents of repair ti elines of 3-6 weeks in international waters.

3. Satellite systems an space weather impact

Scientific literature on space weather has extensively documented the power grid vulnerability. Geomagnetically induced currents produced by major solar events can cause half-cycle saturation in high-voltage transformers, leading to permanent damage with replacement timescales measured in months. As the scenario of a Carrington-class event shows, a triggered network-wide effect would potentially destroy transformer infrastructure faster than global manufacturing capacity could replace it. This is not a marginal scenario; it is a credible planning horizon for which current preparedness frameworks are structurally inadequate.

Satellite systems face complementary vulnerabilities from space weather events, with implications for GNSS navigation, financial transactions, transport, and communications. The Kessler syndrome is a chain reaction of space debris collisions that can sustain itself. It is a longer-horizon risk, with some orbits already becoming dangerously crowded. It would unfold across years, creating a sense that it can be managed, while quietly moving past the point of no return.

Despite the singularity of the Carrington event, there are precedents of space weather disruption:

- In 1989, a ge magnetic storm, known as the Quebec blackout, caused a nine-hour total blackout affecting six million people.
- The 2003 alloween storms led to satellite failures, aviation disruption, power grid stress across Northern Europe.

Despite the singularity of the Carrington event, there are precedents of space weather disruption:

- In 1989, a ge magnetic storm, known as the Quebec blackout, caused a nine-hour total blackout affecting six million people.
- The 2003 alloween storms led to satellite failures, aviation disruption, power grid stress across Northern Europe.

4. Data entres as the hidden concentration risk

Despite their centrality to financial services, healthcare, supply chains, and public administration, data centres constitute what the literature identifies as a significant blind spot in critical digital risk scholarship. As of early 2024, the total number of data centre facilities globally, including hyperscale, colocation, and enterprise sites, exceeded 11,800, with the United States alone accounting for around 40% of that total. Growth is accelerating sharply: the sector added 137 new hyperscale facilities in 2024 alone, and AI and cloud computing are projected to drive a 14% compound annual growth rate through 2030 [9]. By 2030, global data centre electricity demand is expected to more than double, from 415 terawatt-hour in 2024 to approximately 945 terawatt-hour, approaching 3% of total global electricity consumption [10].

Geographic concentration amplifies vulnerability. Industry-led standards address some of these risks at the facility level, though they do not cover cross-facility cascade dynamics. Clusters mean that a single extreme weather event affecting a regional hub can simultaneously disrupt cloud computing platforms, content delivery networks, enterprise

systems, and telecommunications infrastructure. The 2021 European floods and multiple hurricane events in the United States of America provide recent empirical examples. Flooding causes immediate and irreversible damage to electrical and cooling systems, while extreme heat events can trigger emergency shutdowns that escalate through interconnected data centre networks as workload redistribution overloads remaining facilities.

Data centre failures, each with the risk of knock-on effects, are not uncommon:

• In 2009, a heavy rainstorm flooded the Vodafone data centre in Istanbul in just eight minutes, destroying equipment and causing a major customer outage.

• The 2012 Hurricane Sandy in New York led to several data centres in lower Manhattan going offline. Operators had to pump out flooded basements and generator rooms and replace damaged switchgear before restoring service.

• The 2015-2016 flooding of the Vodafone facility in Leeds, due to River Aire bursting its banks, caused an outage lasting several days and disrupting mobile services across the region.

• Multiple US hu ricane seasons (notably 2017) during the costliest hurricane season on record led to widespread generator failures, power outages, and data centre shutdowns across the Gulf Coast and East Coast.

Compound risks and the limits of current frameworks

Most risk planning today assumes that one problem happens at a time, lasts for a short period, and can be fixed using well-rehearsed procedures. This is how most emergency plans, risk registers, and business continuity strategies are designed.

But critical digital disruptions rarely work like that.

In reality, several pressures often hit at the same time, interact with each other, and last longer than backup systems were designed to handle. A heatwave may coincide with high electricity demand. A cable cut may occur while networks are already under strain. In such situations, failures do not stay confined to one system or sector. They spread.

Two common patterns explain why impacts quickly become much larger than expected.

• In some cases, one single event affects many systems at once. For example, a major solar storm, an extreme weather event, or damage to a key submarine cable can simultaneously disrupt electricity, communications, data centres, and financial services, even though these systems are often treated as separate.

• In other cases, the timing of events is the problem. One incident stretches backup systems and redundancies; a second, otherwise manageable event, then pushes the system beyond its limits. What would have been recoverable on its own becomes a serious disruption because the safety margin is already gone.

In both situations, systems that usually work reliably become fragile because they rely on each other in ways that are not always visible or fully understood.

These failures are hard to manage not only because they spread, but because they often begin out of sight. This becomes clear when contrasted with cyber threats, where the problem is usually visible, even if its consequences are not.

Cyber incidents usually announce themselves. When systems are hacked or hit by ransomware, it is clear that an attack has taken place, even if the details are not yet known. Non-intentional digital infrastructure failures are different. When they occur, the cause is often invisible to the people experiencing the disruption. Systems simply stop working. Payments fail. Data is unavailable. Alerts do not arrive without any obvious explanation.

For physical digital risks, the problem may lie far away: an overheated data centre, a damaged submarine cable, a power disturbance, or a satellite disruption. But from the user's perspective, there is no clear starting point. The failure looks local, temporary, or technical, even though it is part of a much larger system breakdown. This invisibility is what makes these risks so dangerous. Time is lost searching for the wrong causes, while failures quietly spread across sectors and borders. By the time the real source becomes clear, if it ever does, the disruption has already escalated.

This distinction is analytical, not hierarchical. Cyber and non-intentional risks are increasingly interconnected: a physical disruption can create vulnerabilities that malicious actors exploit, while a cyberattack can trigger cascading physical failures. Both dimensions warrant attention, and their interaction constitutes an additional layer of systemic risk.

Finally, the economic impacts of large digital disruptions are still poorly understood. While available estimates suggest that even a single day of mobile network failure can cause very large economic losses in highly digitalized economies, most analyses focus only on direct effects, such as missed transactions or service outages.

They rarely capture the wider knock-on effects: supply chains that stall, businesses that cannot operate, public services that fail to coordinate, or the longer-term damage to investor confidence and public trust. We still lack economic models that reflect how deeply modern societies depend on digital infrastructure and that could be reliably used for planning at the organisational, national, or international level.

Conclusion and recommendations

Critical digital risks are real, documented, systemic, and largely underestimated. They do not unfold as isolated incidents, but as disruptions across sectors and borders. While many of the risks are already understood in expert communities, they remain insufficiently recognized and acted upon.

Drawing on a co-creation process with senior expert practitioners spanning international organizations, national authorities, academic institutions, and the private sector, this report highlights six priorities for action:

1. Build k wledge:

– Identify critical digital r sks

– Cross-sector dependency mapping adapted to different national contexts, including low- and middle- income countries where infrastructure data availability is more limited and digital integration follows distinct patterns

– Model robabilistic chain reactions

2. Update nagement:

– R cognize non-intentional digital disruptions as a core risk

– Clari y legal definitions

– Re ise disaster risk frameworks

– Establish i centives for preparedness

3. C sider strengthening international standards:

– Ens re analogue fallback capacity

– Conduct joint scenario planning for energy, finance, telecommunications, and emergency management domestically (local + national), regionally and even globally

4. Ramp up proactive coordination on critical risks, especially:

– Space weather

– Submarine cables

– Satellites

– Data centres

5. Strengthen societal resilience:

– Upkeep of analogue skills across professional and public contexts

– Build societal capacity to absorb and recover from digital disruptions

6. Build trust:

– Build capacity for national authorities, local governments, and vulnerable communities

– Convene communities and stakeholders, including private operators across sectors and borders

– Foster shared situational awareness and mutual accountability

Whether these risks remain manageable or escalate into systemic crises will also depend on how these priorities are translated into action.

REFERENCES

[1] E. Koks, et al., “Infrastructure failure cascades quintuple risk of storm and flood-induced service disruptions across the globe,” *One Earth*, 2024, 7(4). https://doi.org/10.1016/j.oneear.2024.XX (available via ScienceDirect).

[2] E. Mühlhofer, D.N. Bresch, E.E. Koks, “Infrastructure failure cascades quintuple risk of storm and flood-induced service disruptions across the globe,” *One Earth*, 2024, 7(4), pp. 714-729. https://doi.org/10.1016/j.oneear.2024.03.010 (available via ScienceDirect).

[3] E.J. Oughton, M. Hapgood, G.S. Richardson, C.D. Beggan, A.W.P. Thomson, M. Gibbs, D. Burnett, C.T. Gaunt, M. Trichas, R., Dada, R.B. Horne, “A risk assessment framework for the socioeconomic impacts of electricity transmission infrastructure failure due to space weather: an application to the United Kingdom,” *Risk Analysis*, 2019, 39(5), pp. 1022-1043. doi:10.1111/risa.13229.

[4] Lloyd's of London and Atmospheric and Environmental Research (2013) Solar storm risk to the North American electric grid. London: Lloyd's of London.

[5] A. De Bono, G. Giuliani, S. Kluser, P. Peduzzi, “Impacts of Summer 2003 Heat Wave in Europe,” *Environment Alert Bulletin* No. 2. 2004, Nairobi: UNEP/GRID-Europe. Available at: https://www.unisdr.org/files/1145_ewheatwave.en.pdf (Accessed: 20 April 2026).

[6] M.A. Clare, et al. “Fast and destructive density currents created by ocean-entering volcanic eruptions,” *Science*, 2023, 381(6662). Available at: https://www.science.org/doi/10.1126/science.adi3038 (Accessed: 20 April 2026).

[7] ITU (International Telecommunication Union). 2025. Facts and Figures 2025: Internet Use. Geneva: ITU. https://www.itu.int/itu-d/reports/statistics/2025/10/15/ff25-internet-use/

[8] E. Mühlhofer, E. E. Koks, C. M. Kropf, G. Sansavini, D. N. Bresch, “A generalized natural hazard risk modelling framework for infrastructure failure cascades,” *Reliability Engineering and System Safety*, 2023, 234, p. 109194. doi:10.1016/j.ress.2023.109194.2024.

[9] International Energy Agency. Electricity 2024: analysis and forecast to 2026. Paris: IEA. Available at: https://www.iea.org/reports/electricity-2024 (Accessed: 14 April 2026).

[10] Synergy Research Group. Hyperscale data center count hits 1,136; average size increases; US accounts for 54% of total capacity [Press release]. 19 March. 2025. Available at: https://www.srgresearch.com/articles/hyperscale-data-center-ount-hits-1136-average-size-increases-us-accounts-for-54-of-total-capacity (Accessed: 14 April 2026).

[11] International Telecommunication Union, United Nations Office for Disaster Risk Reduction, Sciences Po et al. When Digital Systems Fail – An Expert Report on the Hidden Risks of Our Digital World, Paris: Sciences Po. 2026.