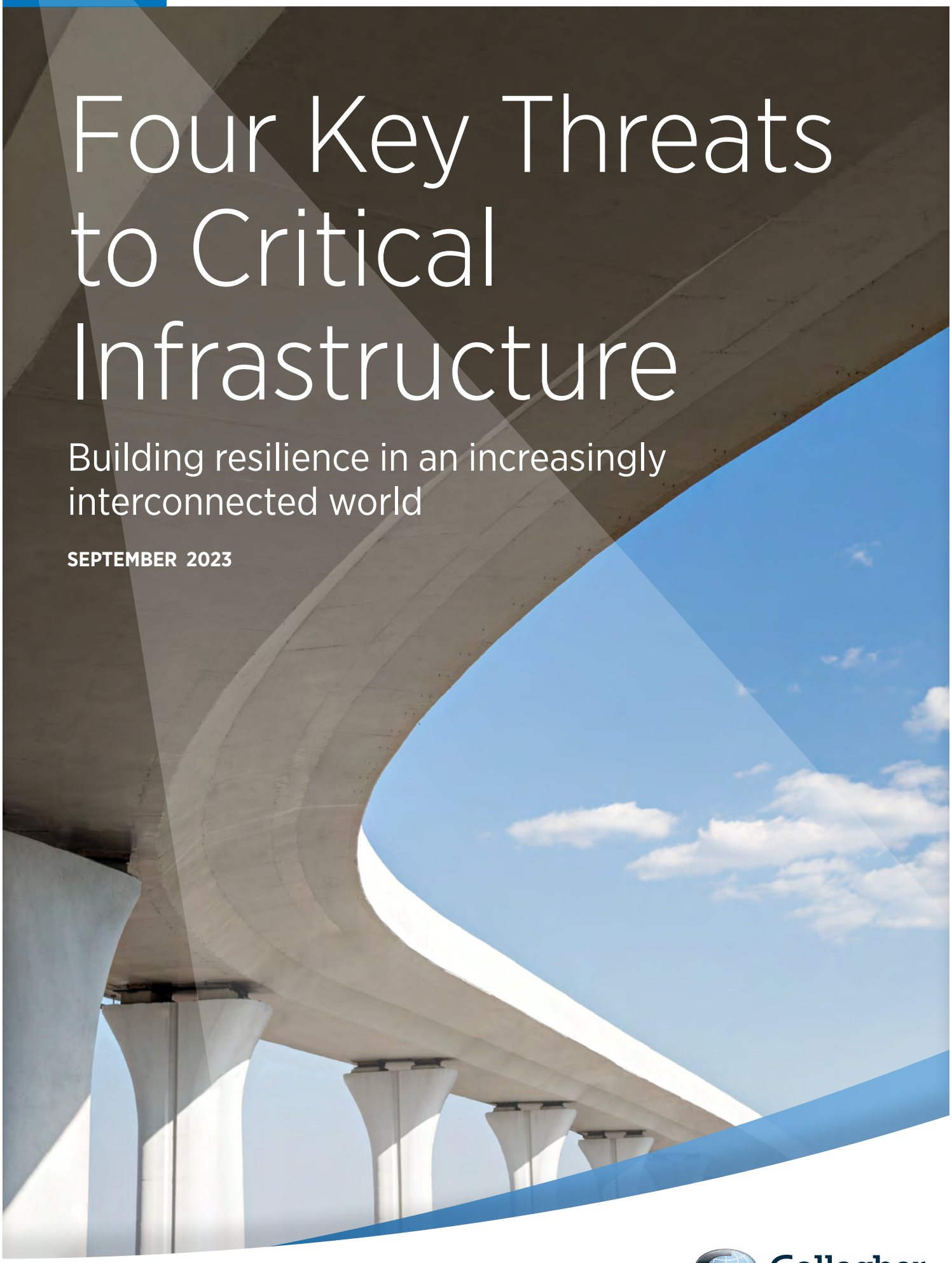
Spotlight

CONFIDENT FUTURES

Four Key Threats to Critical Infrastructure

Building resilience in an increasingly interconnected world

SEPTEMBER 2023



Gallagher

Key findings

1. **Historically, the primary risk exposure for critical infrastructure has been accidents and natural disasters.** Now a new range of exposures are a threat to resilience in an increasingly digital and interconnected world.

2. **Cyber risks and acts of political aggression are taking center stage.** According to Gartner[2], 30% of critical infrastructure organizations will experience a security breach by 2025 that will halt operations. As such, governments are becoming more focused on the protection of critical assets, particularly those that cross country borders.

3. **The number of cyberattacks targeting critical infrastructure has increased over the past five years,** along with flow-on impacts to public safety, economic stability, and national security. Malicious actors are deploying sophisticated techniques to exploit networks, and software, and even wage physical attacks on cyber components.

4. **Climate change and a rising number natural catastrophe events are presenting critical challenges** to infrastructure, with floods, geomagnetic and convective storms, and wildfire damage leading to higher loss severity and supply chain bottlenecks.

5. **Meanwhile, aging and poorly maintained infrastructure is a growing concern.** Particularly in nations where construction is older and budgets are being cut.

Introduction

According to the WEF Global Risks Report 2023[1], the slow decay of public infrastructure and services in both developing and advanced markets may be relatively subtle, but accumulating impacts will be highly corrosive to the strength of human capital and development—a critical mitigant to other global risks faced.

In today's interconnected world, we rely heavily on physical infrastructure systems to sustain our way of life. The intricate networks of energy, transportation, communication, and essential systems ensure the seamless operation of our communities, healthcare systems, economies, and governments.

As our reliance on these systems deepens, so does our vulnerability to the multitude of emerging threats that can compromise their stability, safety, and integrity.

In the past, a power outage would affect the electricity supply to homes and businesses. However, with smart cities shaping the world, power grids have become a core infrastructure component with everyday activities, businesses, and even national security, depending on their smooth operation.

In previous years, the primary threat to critical infrastructure came from accidents and natural disasters. However, the modern landscape has paved the way for a range of new threats. Among these perils, cyber risks and acts of political aggression are taking center stage.

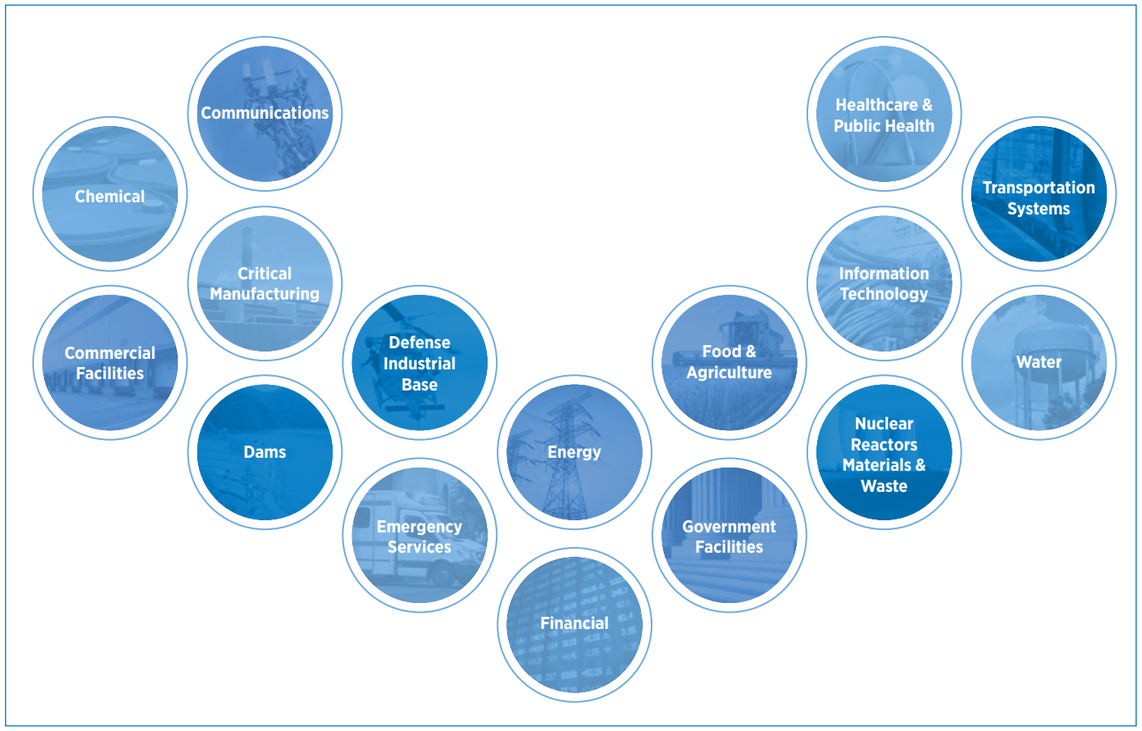
In addition to these evolving threats, other factors contribute to the vulnerability of our critical infrastructure, such as ageing infrastructure and lack of investment. Over time, structures have deteriorated, slowly becoming weakened and susceptible to failure. One example is the crumbling concrete problem currently affecting many public buildings in the UK.

Further, the complexity of the diverse demands of our critical infrastructure systems has the potential to overwhelm legacy IT systems. Threat actors are exploiting these vulnerabilities to compromise essential services.

According to global consulting firm, Gartner, **30% of critical infrastructure organizations will experience a security breach by 2025 that will halt operations** or mission-critical cyber-physical system.[2]

This report focuses on four major threats to critical infrastructure. They are not isolated, working in tandem with other macro-trends, including urbanization, population growth, climate change and digitization, to exacerbate the exposures faced by critical infrastructure.

Critical Infrastructure Sectors



Source: Cyber and Infrastructure Security Agency

1. Geopolitical risk

Geopolitical risk looms large as a pervasive threat, often a product of the interplay between political, economic, and security fractions within and between nations. It encompasses a broad spectrum of factors, from intergovernmental conflicts and trade disputes to territorial disputes and ideological tensions that will adversely affect the critical infrastructure of the involved region.

Threats to critical infrastructure

- **Trade disruptions.** Regional geopolitical tensions can often influence the supply chain through sanctions, embargoes, or trade wars. Dependence on specific regions for essential goods and services can make infrastructure vulnerable to sudden disruptions, leading to delays, shortages, and inevitably higher prices.
- **Physical attacks and terrorism.** Critical infrastructure is often a target for attacks, fuelled by geopolitical and ideological differences. Attacks on power plants, airports, or transportation networks can lead to prolonged economic consequences.
- **New policies.** Tensions between regions can cause alterations in trade agreements, investment policies, or data privacy policies that can impose greater compliance requirements on critical infrastructure operators. Unforeseen regulation changes can affect market prices, disrupt operations, and impede investments.
- **Cybersecurity breaches.** State-sponsored cyberattacks have become a significant arrow in the espionage quiver for countries wanting to disrupt, sabotage, or exert control over vital infrastructure systems.
- **Wartime focus on critical infrastructure.** Targeting critical infrastructure, especially those in the energy sector, is a common practice during times of conflict, as evident from the Russian invasion of Ukraine. The consistent focus of Russian attacks on Ukrainian electricity power grids has resulted in widespread blackouts nationwide. The susceptibility of electrical distribution substations, usually situated in remote areas with limited security, renders them vulnerable to attacks.

The impact of the Kakhovka Dam destruction

The consequences of the destruction of the Kakhovka Dam in southern Ukraine in June 2023, have ranged from significant flood and humanitarian crises to severe environmental and economic impacts.

The dam served a vital role in holding back the Kakhovka Sea, a reservoir that was a significant water source for the communities upstream, which also provided cooling water to the **Zaporizhzhia nuclear power station,** presently under Russian control. The destruction of the reservoir has compromised the availability of irrigation water for these regions.

The floodwaters surging through the dam **carried hundreds of tonnes of industrial lubricant, causing extensive contamination of the river Dnipro.**

The Ukranian Ministry of Agrarian Policy and Food has reported that **31 irrigation supply fields have been disrupted** in Dnipropetrovsk, Kherson, and Zaporizhzhia oblasts. In 2021, these regions were crucial in irrigating half a million hectares, supporting four million tonnes of grain and oilseeds with an **estimated output value of around USD1.5 billion.**[3]

According to experts, **Ukraine may lose 10%-15% of its agricultural potential** due to the indirect or direct influence of the dam breach incident.[4]

Both physical and digital infrastructures bring significant challenges for defence, which are further complicated by the difficulty of attributing cyber attacks to a specific group or state. These intricacies impede effective counteractions and can erode confidence in the country's capacity to neutralise such threats.

In the future, as battle lines are drawn in the fight for precious resources, new geopolitical exposures could arise. Rapid population growth and urbanization amplify the ever-increasing demand for resources such as water, minerals, energy, and arable land. They can cause rising tensions between countries, with critical infrastructure likely to be amongst the collateral damage.

Nord Stream explosions

As tensions with Russia have risen following the invasion of Ukraine, the geopolitical fallout and impact on critical infrastructure has spread across borders to other parts of Europe. The September 26, 2022, explosions that damaged the Nord Stream 1 and Nord Stream 2 gas pipelines underline the fragility of Europe's vital energy and communications infrastructure.

An attack on a pipeline that carries communication, power, or gas can have enormous repercussions on numerous facets of daily life.

Global concerns of the targeting of critical infrastructure have increased over the past year. This is an attractive tactic for both state and non-state actors due to its potential to disrupt supply chains, communication streams, and electricity capabilities. Given that virtually every business relies on critical infrastructure daily, such attacks are guaranteed to have a significant and far-reaching impact.

The most commonly targeted industries are those that are essential to the functioning of society. This includes energy, water, transportation, and healthcare systems, which are all vital to sustaining essential functions and livelihoods.

*— **Laura Hawkes,** Head of Intelligence, Gallagher Specialty's Crisis Consulting practice*

2. Natural catastrophes and extreme climate

Natural disasters and extreme climate are capable of wreaking havoc on essential systems, as recent history has shown. With climate scientists anticipating an increasing frequency and severity of certain natural perils, it is likely this will remain an important exposure, particularly for infrastructure assets in catastrophe-prone regions.[5]

In August 2023, unprecedented floods in Norway and Finland caused the partial collapse of a hydroelectric dam, causing power cuts and evacuations.[6] Meanwhile, record-setting heat in southern Europe sparked a series of devastating wildfires that have torn through communities and destroyed vital infrastructure from Turkey to Spain.[7]

Geomagnetic storms caused by solar flares in the Earth's upper atmosphere have the potential to induce power in long conductors on the Earth's surface, such as power lines, and overload electric grid systems, causing voltage collapse or damage to equipment. While remote, an event of such proportions can have catastrophic and long-term economic consequences in the form of blackouts and high maintenance costs.

Tohoku earthquake and Fukushima meltdowns

The Tohoku earthquake and Fukushima meltdowns are a stark reminder of the vulnerability of critical infrastructure to natural disasters. Following the **Great East Japan Earthquake of 9.0 magnitude**[5] on 11 March 2011, a 15-metre tsunami disabled the power supply and cooling of three Fukushima Daiichi reactors causing a nuclear accident in which all three cores melted in the first three days.

Due to significant radioactive releases during days four to six, which finally totalled over **940 PBq (I-131 eq),** the accident was rated **level 7 on the International Nuclear and Radiological Event Scale.**[8]

In addition to the earthquake and tsunami's **19,500 death toll,** official figures highlight the unfortunate **2,313 disaster-related deaths** among evacuees from Fukushima prefecture.[8]

The tsunami severely crippled the country's infrastructure, destroying homes, businesses, roads, railways, and the three nuclear reactors. Following the level 7 meltdown at Fukushima, there were rolling blackouts across the country, impacting households and business operations.

Quebec geomagnetic storm

One notable geomagnetic storm, known for its impact on the power systems, occurred on 13–14 March 1989, in Quebec. The storm registered strength of **-589 nT on the Dst scale.**[9]

The storm struck the Hydro-Quebec power system around 3 A.M. Eastern Time and caused the grid to collapse in less than two minutes.

The high amount of geomagnetically-induced currents caused the protective systems on the grid to trip and resulted in the **loss of electric power for over six million people** for over nine hours, with an **estimated economic cost of around USD9.6 billion.**[5]

The event was not limited to the province of Quebec. The moment the power grid went down in Quebec, New York Power lost 150 megawatts, and the New England Power Pool lost 1,410 megawatts. The US faced over 200 power grid-related problems within minutes of the start of the storm.[10]

3. Cyber threat

Prior to the advent of digital technology, the internet, and the Internet of Things (IoT), the majority of our essential infrastructure was primarily physical. Now a sizable amount of it has either moved online or is designed to be connected to larger IT systems.

Because of this, critical infrastructure, including power grids, water supplies, and transportation networks, are vulnerable to cyberattacks that attempt to disrupt essential services and cause extensive harm.

The number of cyberattacks targeting critical infrastructure has increased over the past five years, along with their adverse effects on public safety, economic stability, and national security.

Cyberattacks on critical infrastructure consist of various sophisticated techniques engineered to exploit particular vulnerabilities within networks, software, and devices. These include **Distributed Denial of Service (DDoS) attacks, malware and ransomware attacks, insider threats, Advanced Persistent Threats (APTs), and physical attacks on cyber components.**

Identifying high-value or "critical" assets and creating a comprehensive business continuity plan for their prioritized restoration while dealing with cyberattacks is crucial. Additionally, it is essential to establish emergency communication channels between IT, operations, and top executives to react swiftly and effectively to any cyber security compromises.

State-sponsored cyberattacks

The cyber threat landscape includes state-sponsored attacks, with nation states leveraging their hacking capabilities to target the critical infrastructure of other countries to exert political influence, gather intelligence and disrupt operations.

Russia's invasion of Ukraine has created a platform for state-sponsored attacks to thrive

According to Ukrainian government officials and the Slovakian cybersecurity firm ESET, in 2022, Russian hackers targeted the Ukrainian power grid and attempted to cause a blackout that would have hit two million people. According to the state-run Ukrainian Computer Emergency Response Team (CERT), 'at least two successful attack attempts took place,' with one beginning on 19 March, just days after Ukraine joined Europe's power grid in a bid to end its dependence on Russia (see case study box below).

The malware found in the 2022 attacks has been dubbed Industroyer2 due to its similarity to the malware used in the 2016 attack (see case study box below).

Ukraine power grid attacks

A threat actor compromised power distribution companies in western Ukraine in December 2015, causing a **power outage for over 230,000 residents.**[11]

Suspected Russian hackers targeted many control centres, stole operator credentials, and gained access to the Ivano-Frankivsk region's power infrastructure, causing a **power outage of up to six hours** in some areas.

Utilising preinstalled malware, the attackers gained remote control of the human-machine interface (HMI) and switched off most of the switchgears of the grids.

They used **custom-developed malware** to prevent the operator from regaining network control.[12]

The threat actors also continuously **flooded the customer service lines** with calls during downtime to keep customers from reporting the situation.

It was the **first confirmed instance of a successful cyberattack against energy infrastructure.** Another followed in 2016. This time, the incident was an automated attack using malware known as Industroyer.[13]

Spotlight

The 2021 Colonial Pipeline attack

The Colonial Pipeline is one of the largest and most crucial oil pipelines in the US. Comprising more than **5,500 miles of pipeline;** it has been moving oil from the Gulf of Mexico to the states on the East Coast since 1962.

In May 2021, it was shut down for several days following a **ransomware attack** on its digital systems. Cybercrime group **DarkSide** claimed responsibility for the attack but insisted it had not intended to target the operations of country's infrastructure.

The attack was deemed a national security threat and prompted the US to declare a 'state of emergency' due to the disruption in oil flow to industry markets on the East Coast.

The attack occurred in multiple stages:

- On May 6, the attackers first accessed the Colonial Pipeline network and **stole 100 gigabytes of data** within a two-hour window.[14]
- Once the data theft was completed, the attackers **infected the network with ransomware** which compromised many systems, including billing and accounting.
- To prevent the spread of the virus, **Colonial Pipeline had to shut down** pipeline operations while security investigation firm Mandiant took over the investigation.
- On May 12, 2021, Colonial Pipeline paid DarkSide hackers the requested ransom of **75 bitcoin**[14] (USD4.4 million) for the decryption key to regain control of its systems.
- On June 7, 2021, the US Department of Justice recovered **63.7 bitcoin**[14] (approximately USD2.3 million) from the attackers.

The attack highlighted the vulnerability of critical infrastructure to threats such as ransomware-as-a-service. It caused disruption to multiple airports, as a result of limited fuel supplies.

Fear of gas shortages sparked panic-buying across many states, which created real fuel shortages due to the higher-than-usual number of consumers. The incident also brought about a spike in average gas price.[15]

For corporate risk managers [the Colonial Pipeline attack] is an important one because it's all about organisational resilience. It absolutely needs to be on the risk register and embedded into an overall enterprise risk management program. On a broader level, regulation around the protection of critical infrastructure is going to start to become a lot more onerous.

The highest levels of the US government remain laser focused on cyber threats to critical infrastructure. This year, the Biden administration launched their National Cybersecurity Strategy. This outlines a cohesive strategy that imposes responsibilities on both the public and private sectors with a specific goal to improve cyber defenses in critical infrastructure.

*— **John Farley,** Managing Director, Cyber Liability Practice at Gallagher*

Many of the entities responsible for overseeing critical infrastructure have exhibited a gradual pace in embracing enhanced security frameworks. The predicament is further complicated by the challenges in conveying the risks associated with operational technology and IT to board members and top-level executives.

The gap in communication is obstructing well-informed decision-making within the upper echelons of organisations, impeding the prompt execution of vital cybersecurity protocols.

Submarine cables—a growing exposure

The global submarine network, which carries significant transoceanic data, is a critical element of infrastructure that deserves more attention.

750,000 miles of cable which connect the continents act as the core physical infrastructure of the digital age, carrying up to 99% of all transoceanic digital communications (including financial transactions, phone calls, email messages, etc.).

In early April, high-voltage electrical substations in Ukraine were targeted with the Industroyer2 malware[16], with the aim of damaging them by manipulating industrial control systems (ICS).

On April 13, 2022, the Department of Energy (DOE), the Cybersecurity and Infrastructure Security Agency (CISA), NSA, and the FBI issued a warning stating that threat actors had developed customised tools capable of targeting ICS and supervisory control and data acquisition (SCADA) devices.[16]

With countries having the capabilities to tap cables with backside entry during cable construction and while at sea, as demonstrated by the Russian spy ship Yantar[17], submarine cables should now be considered a major battleground, and treated as a critical issue in security studies, geopolitics, and peace and conflict research.

"The big concern is that we're lagging behind in protection of infrastructure between countries, and a lot of that is under the sea," says Jake Hernandez, Chief Executive, AnotherDay, a Gallagher company.

"Europe is going to become increasingly reliant on undersea electricity cables to North Africa, for example, and the Russian capability in this area is significantly ahead of ours. So that's a good example of where we're trying to play catch up."

Spotlight

4. Ageing infrastructure

Risks are evolving as infrastructure is challenged to meet today's resource demands. Continuous maintenance and engineering updates are required to ensure its safety from modern risk factors.

Ageing infrastructure requires frequent maintenance and monitoring as deteriorating structures will inevitably reach a point of failure, potentially resulting in severe injuries, loss of life, and property damage, as well as bringing critical infrastructure operations to a halt.

The scope of such events can be global, with negative knock-on implications for the supply chain, transport, and health.

Britain is currently facing a crisis whereby many of its older public buildings—including hospitals, schools and government offices, have been deemed unsafe following the failure of a school roof in 2018 and, more recently, a beam collapse. The issue relates not just to the age of the buildings but construction material that was in use between the 1950s and mid 1990s. Reinforced autoclaved aerated concrete, or Raac, is a weaker porous material which corrodes at a faster rate than traditional reinforced concrete. Experts say it has a 30-year lifespan before retrofits are necessary.[18]

Italy's Morandi Bridge collapse

On August 14, 2018, a 200–metre section of the Morandi Bridge collapsed in Genoa, Italy, claiming 43 lives and leaving 600 homeless.[19]

In the incident report, experts cite the cause of the collapse of the bridge as **'the corrosion to which the upper part of the southern tie rod on the Genoa side of pylon 9 was subjected.'**[20]

Due to its proximity to the sea, and toxic emissions from nearby industrial activity, the Morandi Bridge was exposed to a high-salinity environment.

The corrosion is thought to have begun in the early stages of the bridge's life, which even Riccardo Morandi, the engineer who designed the bridge, was surprised by. In 1979 he wrote a report detailing a list of maintenance interventions that should be carried out to protect the structure.[21]

However, little was done, and by 1992, the **concrete cables were heavily corroded.** The company managing the bridge then decided to add new cables alongside the existing corroded ones instead of replacing them.

The bridge, which once represented the magnificence of Italian engineering, is now a reminder of the price when infrastructure is not adequately maintained. It has also highlighted the state of Italy's deteriorating transport infrastructure.[21]

Public installations are often financed via taxes, with political preferences playing a crucial role in the timely rollout of funds. As a result, maintenance can take a backseat to projects which have more immediate public appeal.

Lack of investment in physical infrastructure in the current economic climate is a substantial threat, hampering economic progress and recovery, and exposing businesses and communities to significant risks.

> The problem of ageing infrastructure is more pronounced in the West. We saw the power outages during the Texas Freeze of 2021 following Storm Uri, and that was mainly due to the ageing power plants and natural gas infrastructure. We're seeing companies move from China to Mexico because supply chains are diverging from a geopolitical point of view. But then, when they get to Mexico, there's not enough electricity for them to operate because the grids are ageing and there has not been enough investment.
>
> — ***Jake Hernandez,*** *Gallagher Specialty's Crisis Consulting practice*

Closing remarks

In the face of critical infrastructure disruptions, the success, resilience and sustainability of future economies depend on the robust, predictable performance of critical infrastructure, including transportation, energy and power systems, communication networks and healthcare.

Organizations can proactively respond to disruptions and minimize the impact of critical infrastructure failure by analyzing and planning for possible scenarios. This can help risk professionals update their business continuity plans, to ensure day-to-day operations can recover quickly if and when the worst happens.

Contingency planning, crisis management and insurance are essential for responding to incidents that disrupt power supplies and other critical infrastructure. Corporate risk and insurance managers should work with their brokers to stress test how coverage will respond in such instances.

Ensuring our critical infrastructure can cope with today's demands and the constantly evolving needs of society must remain a primary focus. This requires collaboration between public and private sectors, significant investment and innovative risk transfer solutions to cope with emerging threats.

Policymakers must foster collaboration between these sectors to address infrastructure vulnerabilities. Incentivising knowledge sharing, joint planning, and investment in infrastructure is a start. Meanwhile, new rules and regulations will help to shape best practice around the protection of critical infrastructure.

As we develop new, more digitised technologies as part of the green transition and 'smart cities', these must factor in the need for resilience in an increasingly uncertain and interconnected world.

Spotlight

The definition of critical infrastructure is presently undergoing expansion. While satellites have always been considered critical infrastructure, elements such as satellite imagery collection also now fall within this category.

Additionally, the manufacture and design of semiconductors and the machinery involved in their production are now classified as highly critical infrastructure. Artificial intelligence is also poised to become an essential critical infrastructure component. With the broadening scope of critical infrastructure, we will inevitably witness the gradual expansion of regulations. This evolution is likely to encompass multiple areas.

The heightened emphasis that countries place on comprehending interconnections within supply chains is of significant importance. Nations are increasingly explicit about minimizing exposure within their supply chains to countries they deem trade competitors or hostile. This shift could pose challenges for businesses that have operated within the context of a globalized world, especially those with assets in countries embroiled in geopolitical tensions, as such practices could no longer be viable.

— ***Jake Hernandez,*** *Gallagher Specialty's Crisis Consulting practice*

Citations

1 Global Risks Report 2023 | World Economic Forum | World Economic Forum (weforum.org)
2 Gartner Predicts 30% of Critical Infrastructure Organizations Will Experience a Security Breach by 2025
3 Significant damage to the agriculture of Ukraine was caused by the destruction of the Kakhovska hydro electric station by the russians| Ministry of Agrarian Policy and Food of Ukraine (minagro.gov.ua)
4 Ukraine dam breach to have economic, ecological consequences: Expert (business-standard.com)
5 Climate and weather related disasters surge five-fold over 50 years, but early warnings save lives—WMO report | UN News
6 Norwegian River Dam Partly Collapses, Government Expects More Floods (usnews.com)
7 Wildfires in 2023—Wikipedia
8 Fukushima Daiichi Accident—World Nuclear Association (world-nuclear.org)
9 Solar Storm Risk to the North American Electric Grid (lloyds.com)
10 The Day the Sun Brought Darkness | NASA
11 Compromise of a power grid in eastern Ukraine | CFR Interactives
12 Special Section: Ukrainian power grids cyberattack—ISA
13 Russian hackers tried to bring down Ukraine's power grid to help the invasion | MIT Technology Review
14 Office of Public Affairs | Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside | United States Department of Justice
15 Colonial Pipeline hack explained: Everything you need to know (techtarget.com)
16 Economic Warfare: Attacks on Critical Infrastructure Part of Geopolitical Conflict—SecurityWeek
17 What makes Russia's new spy ship Yantar special?—BBC News
18 Britain's crumbling public buildings | Financial Times (ft.com)
19 Genoa bridge disaster: Risk of collapse 'was known for years'—BBC News
20 The corrosion of the Morandi Bridge: the story of a predictable collapse?—IPCM
21 What caused the Genoa bridge collapse—and the end of an Italian national myth? | Cities | The Guardian

AJG.com **The Gallagher Way.** Since 1927.