cro forum

Breaking Point: Critical Infrastructures Disrupted

November 2023

Table of Contents

Executive Summary **3**

1. Introduction **4**
- 1.1 Definition of scope 4
- 1.2 Review of previous papers 4
- 1.3 Risk interconnectivities 5

2. Threats to critical infrastructure **6**
- 2.1 Climate change 6
- 2.2 Cyber threats 9

3. In-depth examples of critical infrastructures at risk **10**
- 3.1 Electricity 10
- 3.2 Medical supplies 12
- 3.3 Water supply 14
- 3.4 Transport 15

4. Insurance and reinsurance aspects **16**
- 4.1 Coverage in Property and Casualty (P&C) and Life and Health (L&H) 16
- 4.2 Impact on investments and financial markets 19
- 4.3 Impact on reinsurance 19
- 4.4 Managing insurance and financial risk exposure 20

5. Resilience and operational risk management **22**
- 5.1 Operational resilience 22
- 5.2 Managing operational risk exposure 22
- 5.3 Managing operational risks: Example – energy supply / power blackouts 25
- 5.4 EU regulation 25

6. Conclusion **26**

Appendices **27**

References **29**

Executive Summary

The risk of critical infrastructure disruption is constantly present today. In addition to climate change and the threat of cyber attacks, the COVID-19 pandemic and the Russia-Ukraine war are recent examples of how infrastructure that was thought to be safe can be quickly put at risk or suddenly become unavailable.

Most infrastructure systems today are interconnected and the interdependencies are very complex. Severe disruptions within any critical infrastructure system can quickly spread and expand to other (critical) infrastructures through a series of direct and domino effects. As a consequence, these risks can accumulate and are difficult to monitor, quantify, control and properly manage in their entirety.

Businesses and policymakers have recognised these risks and are working on strategies to improve the resilience of critical infrastructures. For the (re)insurance industry, these issues are of particular importance, as it is not only dependent on a functioning infrastructure to maintain its daily processes, but can also be affected by substantial claims if critical infrastructure is disrupted.

This paper presents examples of threats to critical infrastructure and their impact on various areas of life. It then looks at the possible effects of the disruption of critical infrastructure on different insurance sectors and the options available not only for mitigating losses but also for developing the necessary coverage concepts. Finally, possibilities for improving resilience and aspects of optimised operational risk management are described.

The (re)insurance industry is always working on optimal solutions to strengthen resilience and risk prevention. However, the particular challenges related to the high interconnectivity of risks associated with critical infrastructures require further analysis and modelling efforts and improved collaboration between all stakeholders.

1. Introduction

1.1 Definition of scope

This paper deals with the risks and consequences of the disruption of critical infrastructure. As the term 'critical infrastructure' is not clearly defined, and different countries assign different areas to critical infrastructure, the paper uses the EU *'Directive on the Resilience of Critical Entities'*,[1] which entered into force on 16 January 2023, as a reference.

The Directive covers eleven critical infrastructure sectors, some of which are discussed in more detail through the following topics:


Energy


Transport


Banking


Financial market infrastructure


Public health


Drinking water


Wastewater


Digital infrastructure


Public administration


Space


Food production, processing and distribution

Society – including insurance organisations and insured customers – depends on critical infrastructure. A disruption of critical infrastructure can therefore impact:

- the functioning of society as a whole;
- the operation and continuity of insurance organisations and thus their ability to provide products and (operational) processes to their customers;
- insured infrastructure or other insurance products, resulting in claims and therefore financial implications for insurance organisations.

The following sections elaborate on the topic of critical infrastructure disruption, including the wider consequences for society. Further, it discusses the potential impacts of critical infrastructure disruption on the insurance industry and possible approaches to adapting to these risks.

1.2 Review of previous papers

The risks of critical infrastructure disruption have already been addressed in previous publications of the CRO Forum (see Appendix).[2]

Critical infrastructure disruption is also analysed and assessed on an ongoing basis in the Emerging Risks Initiative (ERI) Group's annual *'ERI Risk Radar'.* As shown in Appendix 1 , the risk *'Critical infrastructure and power blackout'* has been classified as 'high' with "significant impacts already seen in insurance claims" since 2019.

In recent years, impacts on the digital infrastructure of society have been highlighted as increasingly important; in particular, natural catastrophes, solar storms or cyber attacks could impact digital infrastructures (including satellites, GPS and communication systems), which are now considered essential to the functioning of society.

However, as highlighted in previous publications of the CRO Forum, the rise of digital technologies, including the growing prevalence of the 'Internet of Things', raises multiple security, strategic and reputational risks, in addition to being an accumulation risk, i.e. capable of generating losses that are not geographically restricted and that have the potential to impact multiple industries and connected digital ecosystems.

1.3 Risk interconnectivities

According to the *'ERI Risk Radar'*,[3] the disruption of critical infrastructure is considered to be one of the key emerging risks that the (re)insurance industry has to contend with. Looking at the other significant emerging risks on this radar, it is striking that there is a high degree of interconnectivity between these risks and the threats to critical infrastructure.

Emerging risks directly related to the disruption of critical infrastructure are:

- Cyber risks
- Climate-related disasters
- Pandemic risks
- Supply chain risks
- Geopolitical conflicts
- Resource management
- Terrorism risks
- Social issues

All of the above risks have a direct impact on critical infrastructure and are currently highlighted as significant threats according to the 'ERI Risk Radar'.

As an example, the almost complete interruption of Russian oil and gas supplies to the EU starting in 2022 was the result of a geopolitical conflict in combination with a lack of supply of the necessary resources. Here, the threat included the loss of energy-intensive industrial production or interruptions in the transport sector.

The high degree of efficiency optimisation of global supply chains – as well as their complexity and interconnectedness – has made them extremely vulnerable to shortages or failures. Knowledge and experience of disruptions is leading to a gradual adjustment of supply chains. Near-shoring, regionalisation and strategic storage are playing key roles in this shift. Nevertheless, dependence on global supply chains remains and will only diminish over time, if at all.

Taken individually, the aforementioned emerging risks can be regarded as accumulation risks or even systemic risks. Systemic risks are difficult to monitor, quantify, control and manage in their entirety as they often show strong interconnectivities by their very nature. In addition, severe disruptions within any critical infrastructure system can quickly spread and expand to other (critical) infrastructures through a series of direct and domino effects. With the ongoing disruption of critical infrastructure, the risk of social unrest is likely to further increase, which could ultimately contribute to other infrastructure disruptions. As a result, critical infrastructure disruptions should be considered as correlated and may ultimately affect many or all lines of (re)insurance business.

In the following, we look at the different threats to critical infrastructure and provide examples of critical infrastructures at risk. Despite the great importance of pandemics and terrorism, these risks are not dealt with in separate chapters here but are included in the in-depth examples in Chapter 3.

2. Threats to critical infrastructure

2.1 Climate change

Climate change presents numerous threats to critical infrastructure, with potentially severe consequences for societies and economies in the case that adaptation measures are not adopted or are inadequate. Threats to critical infrastructure from climate change operate via various routes, some of which are described below. In many cases, climate change-induced impacts could exacerbate the pressures that many critical infrastructures are already under due to a combination of increased usage, their age and, in some cases, lack of investment in their maintenance.

Impacts of physical risks

The increase in the number and severity of natural catastrophe events and weather extremes puts critical infrastructures under increasing pressure. A few examples are discussed below.

Increasing occurrence of temperature extremes

An increase in the number of extreme hot and cold weather events has the potential to create stress on electricity generation capacity, transport and healthcare systems.

Electricity generation: Extremely hot days will increase electricity demand spikes as people become increasingly reliant on air-conditioning units to keep cool, both in their homes and in public buildings / places of work. The same is true for extremely cold days, when more electricity will be required for the heating of buildings. Freezing weather can also cause damage to power transmission and distribution infrastructure due to ice formation. Ice formation stresses power lines and towers, increasing the probability of breakage, which in severe cases can lead to major power outages (e.g. Texas, 2021). Equally, extremely high temperatures impact the efficiency of electricity production and transmission through power lines, and can reduce the lifespan of transformers over time.[4]

Transport: Extremely hot and cold days can damage transport infrastructures. For example, extremely hot weather can result in rail expansion and the buckling of rail tracks, damage to both road and pavement surfaces (asphalt rutting) as well as bridges due to excessive thermal expansion.[5] Extremely cold weather can also cause damage to tarmac surfaces due to freeze-thaw cycles and, in the case of electrified railway tracks, damage to overhead power cables due to ice formation on power lines. Point failures caused by sub-zero temperatures have also been known to occur.

Healthcare: Both extremely hot and cold weather events are known to aggravate acute health conditions among the general population, placing healthcare infrastructure under increasing pressure during these periods. In terms of climate change impacts, extreme heat is likely to be a major driver of negative effects on public health in the future. Extreme heat increases the occurrence of cardiovascular, pulmonary and cerebrovascular events, and can cause premature births. Hot days are also associated with spikes in levels of air pollution, notably through the formation of ground-level ozone and increased particulate air pollution, which can trigger asthma attacks and cardiovascular incidents. Hot days have also been observed to cause a spike in hospital admissions linked to heat stroke / heat exhaustion and dehydration, particularly in countries that are less adapted or accustomed to dealing with periods of extreme heat. In general, vulnerable sections of society are more prone to suffering from health problems during such periods of extreme heat; either those with pre-existing medical conditions or the very old and very young. In addition, people from lower socio-economic groups also tend to be more vulnerable to suffering during extremely hot or cold spells, having less financial flexibility to spend resources on ways to protect themselves, and tending to live in areas/homes that are more exposed to adverse conditions in the first instance (e.g. areas lacking green spaces, near busy roads, poorly insulated houses).

From the perspective of physical healthcare infrastructure, hospital buildings that are older and do not have air conditioning installed throughout will be more uncomfortable and therefore stressful places for both staff and patients during hot periods, potentially impacting on quality of care and patient outcomes. This has been shown to be particularly the case in certain public healthcare settings, which have reported a number of incidents related to episodes of hot weather, including negative impacts on both staff and patients, and failures in the operation of essential equipment.[6]

Drought

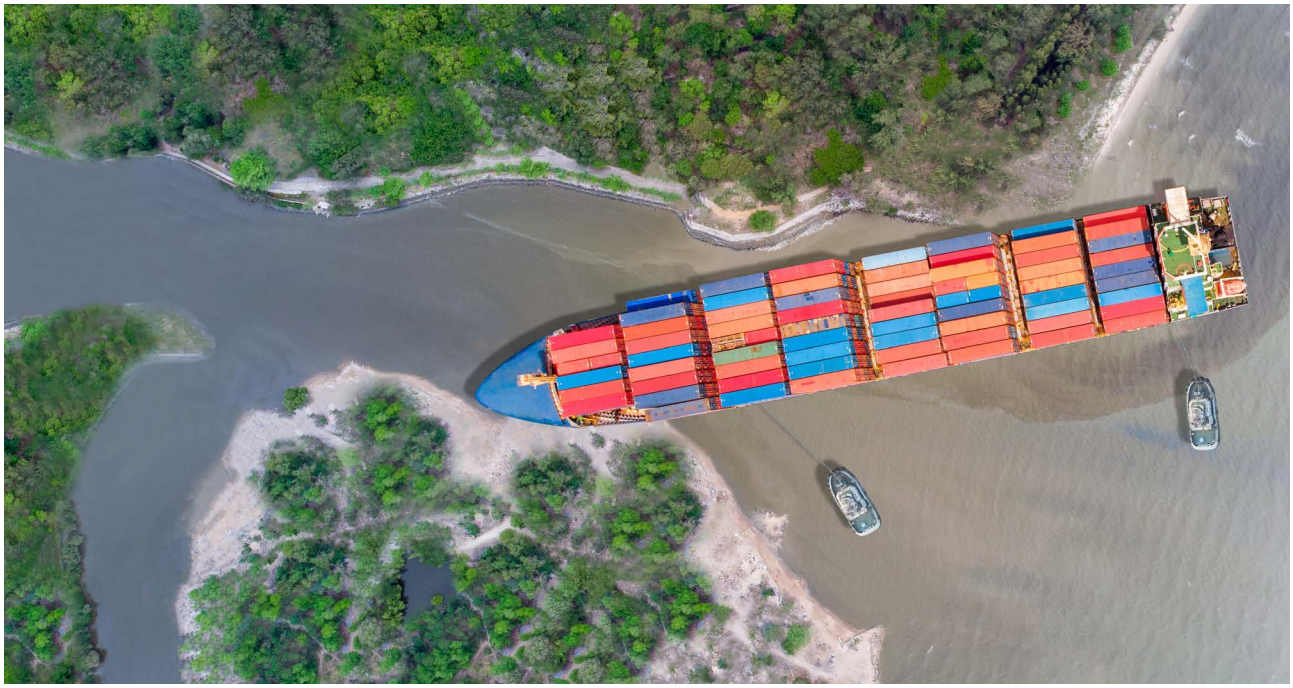
Water shortages, which are likely to become more frequent as the climate warms, could increasingly pose difficulties for different parts of the critical infrastructure network.

Electricity generation: In the case that nuclear reactor plants are located inland, water shortages could impact electricity generation by reducing the availability of reactor coolant water supplies. This was recently observed during the drought that impacted Western Europe in the summer of 2022, when low water levels and higher water temperatures in the Rhône, Garonne and Loire rivers disrupted the operation of several nuclear power plants in France. Electricity generated by pumped storage hydropower plants can equally be impacted in the case of a reduction in the volume of hydropower plant reservoirs. This occurred in Southern Europe during 2022, when a poor year for hydropower generation added to the strains on gas and electricity markets caused by the war in Ukraine.

Transport: Inland waterways play a significant role in the transportation of freight from various sectors within Europe. Drought can have a major impact on river transport when water levels become critically low, reducing the navigability of vessels. In such cases, vessels will either have to reduce their loads or cease transportation altogether until water levels rise. In 2022, the ongoing drought across Western Europe caused significant disruption to shipping operations on major routes on the Danube and Rhine rivers. Several companies across sectors, including chemicals, mineral extraction, steel production and oil refining, had to reduce or halt operations, with downstream impacts (e.g. retail) on the supply chain. Similar situations were experienced in 2018, underlining that unpredictable water fluctuations in Europe's major rivers due to changing weather patterns are an ongoing challenge for shippers and manufacturing in the region.

Food production: Depending on the length, frequency or timing of a given drought and the crop variety, agricultural production may be impacted to a greater or lesser extent. However, as the climate warms and fresh water supplies are placed under increasing pressure, especially crops that require large amounts of water will be increasingly difficult (or justifiable) to grow.

Healthcare: Any drought that has wider repercussions on the provision of a safe and reliable water supply will have a major impact on the health of the population – either from direct causes (in the case of contamination events) or from the mental stress imposed on populations that are forced to



find drinking water from other towns/cities or to buy bottled supplies. People may suffer from the impacts of water-borne diseases in extreme cases, or from dehydration if they do not drink enough water (compounded by heat waves).

Such incidents, when affecting a significant number of people simultaneously, will place additional stress on healthcare services.

Flood

Increasing flood risks caused by extreme rainfall and river flooding, in addition to gradual sea-level rise, could put more critical infrastructure facilities at risk of inundation. Such facilities include power generation plants, wastewater treatment plants, hospitals and transport infrastructure, all of which may be at risk of inundation if appropriate flood defences are not in place or if flood defences fail. The consequences of the tsunami at the Fukushima Daiichi nuclear power facility in Japan in 2011, illustrate the scale of the impact of a sudden inundation event and highlight the risks of building critical infrastructure in hazard zones. In relation to nuclear power plant facilities – which need to be built on either coastal or riverine locations due to the requirement for reactor coolant water – the US Nuclear Regulatory Commission has concluded that the vast majority of its nuclear sites were never designed to withstand the future climate impacts they face.[7] In the case of climate-related impacts, a flood defence breach or hurricane-induced coastal flooding could have consequences similar to a tsunami for vulnerable electricity generation infrastructures.

Transport infrastructures of all kinds (airports, railways, roads, seaports, river transportation) are also vulnerable to damage and/or service interruption in the face of extreme natural catastrophes that include a flooding component. In the EU, for example, several airports are located near the coast and are therefore exposed to the risk of sea level rise and storm surges, with inundation levels of 1-3 metres expected to have adverse impacts on their operations. Additionally, the number of seaports in Europe that face the risk of inundation due to sea level rise is expected to increase by more than 50% between 2020 and 2080, with this trend being more pronounced along the North Sea coast.[8]

Climate change and energy transition

To reduce the impacts of climate change, a transformation of the energy generation sector away from fossil fuels and towards renewable energy generation is underway. This shift to renewable electricity production and the increasingly distributed nature of power generation (for example from buildings equipped with solar panels) necessitates a complete transformation of the electricity grid, which is currently designed for one-way production and distribution of electricity from the point of generation to the point of consumer. As we move towards a more dynamic ‘smart grid’ that allows for multiple feed-in points, there is a potential risk of power outages, either caused by the combination of new technologies with existing infrastructure, or by the increased exposure of the grid to cyber attacks as the electricity generation and distribution system becomes more interconnected. The increasingly interconnected nature of electricity grids, both within and between countries (e.g. across the EU), has the potential to generate large-scale power outages with cascading impacts. Also, increased demand for electricity driven by new technologies that are facilitating the energy transition (e.g. electric cars, installation of heat pumps in residential buildings) will put extra pressure on the grid during the transition phase, compounding the risk of power outage.

2.2 Cyber threats

Today's cyber threats – a threat defined by the Financial Stability Board[9] as *"a circumstance with the potential to exploit one or more vulnerabilities that adversely affects cyber security"* – are increasingly intertwined with other risks. Together, they have the power to severely affect critical infrastructures.

In 2023, this interconnection resonates even more dramatically in light of the ongoing war in Ukraine. Looking at this example, we can identify some of these combinations affecting critical infrastructures:

- usage of cyber attacks alongside more traditional types of warfare, both at the beginning of the war in February 2022 (e.g. disruptive operations against Viasat) and at various points during the conflict (e.g. attacks against multiple critical infrastructures);
- combination of traditional warfare with troop movements on the ground, together with the use of a nuclear power plant (Zaporijia) as a bargaining chip;
- weaponisation of the large Nova Kakhovka barrage to complicate the Ukrainian infantry counter-offensive in June 2023.

We now have a better understanding of how the cyber threat can interact with other types of well-known risks, and how these various threats can be associated. The correlation between physical, cyber and geopolitical risks is becoming more apparent as geopolitical conflicts now routinely use the cyber vector to deliver targeted or massive cyber attacks in addition to more traditional means of warfare.

Cyber risk has specific characteristics. Cyber risk is a man-made risk that is constantly evolving through the development of new techniques, whose features are evolving over time and are therefore difficult to model. The accumulation potential of cyber risk stems from the fact that a large number of cyber incidents may occur simultaneously over a wide geographical area or across different sectors. This could result in significant losses for insurance companies, which can be difficult to manage. The systemic features of cyber risk severely limit insurance capacity. Last but not least, there is still a lack of knowledge about the frequency and severity of potential cyber events, and valuable data is scarce.

In today's world, cyber security is shaped by the ever-changing nature of cyber space, coupled with the digitalisation of our societies, their reliance on more devices and machinery, including the use of artificial intelligence and machine learning capabilities. This provides a larger global attack surface and more opportunities for malevolent attacks. The result is a higher frequency of adverse cyber security events and a greater number of victims. While new technologies can increase the opportunities for cyber attacks, techniques for managing cyber risks are emerging from both traditional infrastructure systems and new technologies themselves. However, the overall impression is that the new technonogies currently enable more attack than defence.

Cyber risk is possibly most visible when applied to critical infrastructure systems – the most telling illustration of the impact of the digital world on the physical. In this area, building resilience to cyber risk relies on 'resilience by design' techniques that integrate the potential for an attack into the operation of a system, providing buffers, flexible sourcing options or temporary built-in disconnection from the network to continue critical production in the event of an attack. As Professor Giovanni Sansavini of ETH Zürich explains:[10] *"Modern society relies on networks. We are interconnected in everything from food supply and water treatment to energy supply. Networks allow us to balance commodities and be more efficient. The electricity network for instance is used to balance excess electricity produced in one place to another place with less supply at that time. However, networks also make us interdependent."*

3. In-depth examples of critical infrastructures at risk

3.1 Electricity

The risk of disruption to a consistent, stable and affordable supply of energy has recently been brought into focus by a combination of the effects of Russia's invasion of Ukraine in 2022 on energy markets, ambitious global targets to reduce carbon emissions, and increased demand from both industry (e.g. energy-consuming data centres) and individual needs (e.g. charging electric vehicles and operating heat pumps). Combined with the threat of attacks on critical infrastructure or natural disasters, the risk of blackout scenarios is increasing.

This risk is illustrated by industry and mainstream media reporting, including the following examples:

- **Demand** – The International Energy Agency (IEA) observed that global electricity demand grew by 5% in 2021[11], and its 'Electricity Market Report 2023' shows 2% growth in 2022, driven by India, the US and China.[12] The report adds that long-term trends indicate continual growth.
- **Supply** – The IEA reported in March 2022 that Russian gas accounted for ~45% of EU gas imports and ~40% of EU gas consumption in 2021,[13] with the EU importing 83% of its natural gas[14] that year. Ambitious EU carbon reduction targets also require increased renewable energy production, but a World Economic Forum report, published in January 2023, noted that projects suffer from "long lead and permitting times", alongside "supply-chain bottlenecks, a growing skills gap, lack of collaboration with local communities, geopolitics, and trade-offs between infrastructure build-out and biodiversity loss".[15]

Major threats to energy supply

The risk of energy infrastructure disruption, with far-reaching effects on the lives of millions of people and all industrial sectors, and consequently the insurance sector, is more likely to arise from natural disasters, terrorist attacks and cyber attacks, all of which are on the increase.[16] The impacts of these man-made and natural disasters on the power infrastructure are briefly discussed below.

Natural disasters: Natural disasters such as hurricanes, tornadoes, earthquakes, wildfires and floods can cause significant damage to the electricity network. High winds can topple power lines and damage transformers, while floods can damage underground cables and substations. For example, Hurricane Katrina (2005) caused widespread power outages in the US, leaving millions of people without electricity for weeks.

Cyber threats: Cyber attacks are increasingly common and pose a significant threat to the electricity network. Hackers can gain access to the control systems of power plants and substations, causing them to malfunction or shut down. This can lead to blackouts and other problems. In 2015, for example, a cyber attack on the Ukrainian power grid caused a blackout that left over two hundred thousand people without electricity.

Physical attacks: Physical attacks on the electricity network can also cause significant disruption. Vandals can damage power lines and transformers, while terrorists can target substations and power plants. Such cases are on the rise in the US, where suspected domestic extremists have been vandalising power infrastructure to cause blackouts and trigger civil unrest. For example, in 2022, shootings at two Duke Energy substations caused a power blackout for forty-five thousand people in North Carolina.[17]

Equipment failures: Equipment failures are a common cause of power outages. Transformers, circuit breakers and other equipment can fail due to age, wear and tear or other factors. Combined with the effects of natural disasters and increased load (due to a growing population and the influx of electric vehicles), aging and worn equipment are like a dormant volcano.

Impact of power outages on society[18]

Power outages can be planned and announced in advance, such as a periodic shutdown with the intention of load shedding (brownouts). On the other hand, blackouts result from an unplanned, complete loss of power in the affected area. Table 1 describes how the impact on society progresses as the duration of a major power outage increases.

Table 1: Immediate impact of an outage[18,19]

Time	Impact
0-2 hours	Traffic lights/traffic management, internet, TV, landline communications, electric vehicles and majority of ATMs stop functioning. Stores close. Chaotic traffic leads to many accidents. Commercial and industrial insurance: damage to goods in production.
2-8 hours	Widespread cell phone interruption. Stranded passengers walking home. Limited quality and quantity of potable water. Cash still available in certain banks. Trading limited but possible for professionals provided communications are secured. Commercial and industrial insurance: fires due to lack of cooling.
8-24 hours	Traffic comes to a standstill. Stores selling remaining stock manually. First violent disputes. No wastewater treatment. Loss of frozen goods.
2nd day	30% of population running out of food. Further reduction in potable water. First looting. First hospitals running out of (backup) power. Animals die in the meat production industry. Commercial and industrial insurance: Widespread loss of frozen goods. Fires, looting, property damage.
3rd day	50% without own food supplies. Increased panic-driven looting. Food security becoming first priority for government.
1 week	95% of population out of own supplies. Widespread outage of emergency power. No cash available. Commercial and industrial insurance: Property damage due to lack of maintenance.

Due to the growing dependence on critical infrastructures, a widespread power blackout would result in the population no longer being supplied with essential goods and services within a short period of time. The associated threat to public safety would probably lead to a situation that would be difficult to control within a few days. It is therefore imperative to take appropriate precautionary measures in all critical infrastructure sectors to prepare for such an eventuality in order to mitigate the cascading damage effects.

IT and telecommunications: Massive negative impact on the structures of the entire communications and information sector, such as: data centres, internet, mobile and fixed telephony, broadcasting and press. A large-scale, long-term power blackout, especially in the information technology and telecommunications sectors, would have dramatic consequences with enormous cascading effects on other sectors. The special significance of an internet outage must be emphasised here. Since a large proportion of data traffic and also trade is now carried out via the internet, the effects on this are already massive immediately after the start of a power blackout.

Transportation and traffic: Within a very short period of time, serious impacts on the central transport modes of road, rail, air and water are to be expected. In particular, the use of and dependence on modern information technologies in the transport/traffic sector would lead to a rapid collapse of transport routes. Petrol stations will be out of service due to dead pumps.

Water supply: Not only the supply of drinking water but also the use of water in economic activities (e.g. in the production of chemical products) would no longer be ensured due to the failure of mostly electrically operated pumps.

Food supply: The agricultural and livestock production sectors, as well as the food retail industry, would be directly affected by a major power outage. In particular, the checkout and refrigeration systems of supermarkets and retailers would be immediately impacted unless supported by emergency generators.

Healthcare: In the healthcare sector, there would be serious repercussions for hospitals, doctors' practices, pharmacies, retirement and nursing homes, and emergency services. Despite emergency power already being established in some sectors, high death and injury rates would quickly occur due to deteriorating availability of treatment and diagnostic systems.

Financial services: Larger banks and insurance companies are already required by law to make provisions to compensate for a power outage for a certain period of time. Nevertheless, severe negative effects would be expected due to interconnectedness and cascading effects. In particular, the possible unavailability of cash at ATMs entails a high potential for escalation in an existing crisis.

Power generation and distribution presents some complexity from an insurance perspective. There is no single point of failure from which the likelihood and impact can be easily assessed for insurance purposes. As the (re)insurance industry learns to navigate the intricacies of assessing power infrastructure, it could be useful to study other countries where unreliable power supply and distribution are almost endemic. Possibly there are lessons to be learned about the steps taken by small and large businesses, as well as citizens, to cope with unpredictable and long-lasting blackouts, and how doing so largely avoids panic and decreased work output.

3.2 Medical supplies

The health sector, as one of the essential elements of critical infrastructure, is particularly vulnerable to disruptions in global supply chains. When medical supplies fail, lives are endangered by lack of pharmaceuticals or surgical procedures that can't be performed without specific medical devices. One of the first substantial problems to emerge during the COVID19 pandemic was a massive shortage of drugs and medical equipment in almost all countries. In particular, protective devices such as gloves, mouth protection, respirator masks, protective clothing and disinfection materials quickly became scarce commodities in the affected areas. However, the pandemic only highlighted a long-standing problem. Global supply chains for drugs and medical devices were already under pressure before the pandemic.

It is well known that the worldwide pharmaceutical market is highly dependent on deliveries from China and India. This affects all areas, including drug raw materials, active pharmaceutical ingredients (APIs), patented medicines, generics and over-the-counter (OTC) medicines. APIs produced and exported by China and India account for about 70-80% of the global supply. In these countries, sometimes only a limited number of production plants supply the

world with the bulk of specific APIs used in drugs. When a surge in demand arises anywhere in the world, it puts a strain on these manufacturers, most of which are already producing at their capacity limits.

If one carries out a cause-and-effect analysis, there are several reasons for supply chain disruptions. It starts with compliance issues (e.g. deviations from good manufacturing practice (GMP) standards). Other factors include production problems due to property damage at the manufacturing site or IT problems. Finally, yet importantly, contamination of APIs has often been a problem leading to product recalls in recent years. The result of any of these issues may be that the factory must temporarily suspend production. Following the outbreak of the COVID-19 pandemic, some governments restricted the export of medical supplies and drugs, resulting in the disruption of established supply channels. Another reason for reduced or interrupted medical supplies is the geopolitical situation between countries due to war or embargo rules, which affect all other countries depending on the supply chain.

In October 2019, a report by the interagency Drug Shortages Task Force[20] led by the FDA in the United States, revealed the economic background to supply chain disruptions in the pharmaceutical market. Increasing demand for drugs and low market prices, in particular for generics, combined with higher production costs in Europe and the US compared to Asia, created unfavourable situations.

The report identifies three root causes of drug shortages:

- Lack of incentives for manufacturers to produce less profitable drugs (i.e. generics).
- The market does not recognise and reward manufacturers for ‘mature quality systems’ that focus on continuous improvement and early detection of supply chain issues.
- Logistical and regulatory challenges make it difficult for the market to recover from a disruption.

The report concludes that drug shortages persist because they do not appear to resolve according to the ‘textbook’ pattern of market response. Unless the overall circumstances change fundamentally, experts conclude that it is very likely that drug shortages will continue to persist.

3.3 Water supply

Water supply networks in many countries, including developed countries such as the US and the UK, are currently suffering the consequences of a lack of essential maintenance for several years due to underinvestment. In the US, for example, a water main break occurs somewhere in the country every two minutes, wasting six million gallons of treated water each day.[21]

In the UK, Thames Water, which supplies drinking water to nine million customers in London and the Thames Valley, has admitted that it loses more than six hundred million litres of water per day. In total, for the principal water companies operating in England and Wales, the daily wastage of water – due to leaks and other losses – amounts to three billion litres, or a fifth of the total supply.[22] The degradation of water supply infrastructure is generally related to the age of many of the components that are essential to the operation of water supply systems such as reservoirs or tanks, pumps, valves, motors and pipes.

In addition to the incremental problems caused by the general ageing of infrastructure, water treatment and supply facilities are currently being placed under greater pressure by a combination of population growth and urbanisation, and the consequences of climate change. Climate change not only has implications for the quantity of water resources available, it can also impact water quality through higher temperatures, which favour the growth of algal and bacterial contaminants, and during catastrophic events such as floods and storms. The additional pressures of climate change and increased demand for water mean that current water supply networks are commonly operating outside the conditions for which they were originally designed.

A further factor is that today's water treatment, storage and distribution systems are increasingly controlled by computer systems, including a specific type of industrial control system known as a Supervisory Control and Data System or SCADA, which is designed to control large-scale processes that span multiple sites and long distances. This means that essential processes that control the supply and safety of public drinking water sources could be additionally vulnerable to cyber attacks.

As well as the broad-scale issues described above, water supply and distribution systems can be vulnerable to both accidental and intentional threats.

Accidental threats

Accidental threats to water supply systems can be caused by natural events (e.g. earthquakes, floods or droughts), or by accidental pollution and equipment failure / use of old piping materials containing lead. Accidents and equipment failures can lead to utility disruptions and loss of customer service, or result in accidental contamination events with potentially serious consequences for public health and ongoing trust in the safety of drinking water. Cases of accidental contamination of water systems are numerous and continue to occur. Past water supply contamination incidents have resulted in many people becoming ill, or even dying, especially in the case of vulnerable people.[23]

Intentional threats

Intentional threats to water supply systems can be caused by physical sabotage, deliberate contamination and cyber attacks (e.g. on information or SCADA systems). Water supply systems are vulnerable to deliberate contamination or sabotage owing to the large size of the system with numerous structural components (e.g. tanks, reservoirs, pumping stations) and open access points for potential contamination entry.

In this respect, post-treatment storage facilities and the distribution system have been identified as particularly vulnerable to deliberate contamination.

Recent examples (e.g. cyber threats / contamination incidents)

Water supply systems around the world have already been the target of several cyber attacks highlighting security weaknesses in systems that control, for example, critical water treatment controls. In August 2022, a Russia-linked ransomware group gained access to the disinfection control interface of a UK water company that supplies drinking water to over one-and-a-half million people. Although the water supply was not compromised in this attack, the incident was described by one cyber security expert as "extremely concerning".[24] In the US, several attempted attacks on critical infrastructures – including the water supply – over the course of 2019-2021 have prompted the federal government to introduce a 'National Cybersecurity Strategy', including new legislation to guarantee that water companies have a minimum level of cyber security systems and controls in place. Attacks on US water infrastructure have included several ransomware attacks on SCADA systems and an incident involving a hacker who attempted to pump a dangerous chemical into Florida's water supply.[25]

3.4 Transport

In a globalised world, reliance on any kind of transport, from the delivery of daily essential goods to the commuting and movement of people, is an essential part of the global economy and our daily lives. However, this sector is facing several threats and vulnerabilities (e.g. the blockade of the Suez Canal in 2021) that could potentially disrupt its operations and cause significant economic damage.

During COVID-19, the world experienced a tremendous shortage of any kind of goods, not only because of delayed production processes or unavailability of personnel, but also because of the unavailability of delivery systems and means of transport due to COVID-19 lockdown restrictions, travel restrictions and border closures. Empty shelves in supermarkets, delayed delivery of online purchases, or entire industries slowing their production lines because of a lack of personnel and/or missing parts, illustrated how fragile the world is without a functioning transportation system. The COVID-19 restrictions equally resulted in significant losses for the airline and shipping industries.

But what are the other current threats for the transport industry?

Climate change and natural disasters: Natural disasters can disrupt navigation and transportation systems, causing delays and damage to infrastructure. For example, flooding in Germany in 2021 caused significant damage to highways, streets and railway systems in the North Rhine-Westphalia and Rhineland regions, disrupting the flow of goods and causing economic losses of about EUR 6 billion.

Shortage of qualified people: One of the primary reasons for the shortage is the ageing workforce. Many experienced workers are retiring and there are not enough young people entering the industry to replace them. Another factor contributing to the shortage is the lack of training and education opportunities.

Many transport companies do not invest enough in training and development programmes, which makes it difficult for employees to acquire the necessary skills and knowledge to advance their careers. The shortage of qualified employees in the transport industry can have severe consequences such as increased costs, reduced productivity and lower quality of service.

Cyber threats: The transport industry is increasingly reliant on technology, making it vulnerable to cyber attacks. Hackers can target transportation systems such as air traffic control, shipping ports and railway networks, causing significant disruptions. In 2017, for example, shipping company Maersk was hit by a cyber attack that caused an estimated EUR 300 million in damage.

Terrorism: The threat of terrorism in the transport industry is a significant concern for governments, transport companies and passengers worldwide. Terrorist attacks on transportation systems can cause significant damage, loss of life and disruption to the economy and society. The transport industry is particularly vulnerable to terrorist attacks due to its open and accessible nature. Airports, railway stations and bus terminals are often crowded and busy, making them attractive targets for terrorists. Additionally, transport systems are critical infrastructure that support the movement of people and goods, making them a prime target for those seeking to disrupt the economy and society.

Geopolitical conflicts or changes: Geopolitical tensions, such as trade disputes and political instability, can affect the transport industry. For example, the ongoing trade dispute between the US and China and the war in Ukraine have disrupted global supply chains, affecting the transportation of goods across the world.

4. Insurance and reinsurance aspects

4.1 Coverage in Property and Casualty (P&C) and Life and Health (L&H)

Coverage issues already start with the definitions of critical infrastructure, which still vary from policy to policy. The disruption of critical infrastructure itself is often not a covered peril, but may indirectly lead to insured losses in P&C policies, depending on the cause and effect. Therefore, the relevant loss scenarios are indirect losses. However, the consequences of critical infrastructure disruption may be covered by several types of insurance policies, such as:

- the spoilage of goods due to the unavailability of cooling devices following a general power blackout;
- freeze damages to water pipelines following a general unavailability of gas for heating systems;
- looting, theft and damage to property in the event of a large-scale power blackout in major cities.

Events such as pandemics or terrorist attacks that disrupt critical infrastructure may also lead to large numbers of fatalities, which could be covered under life and health policies. In addition, there are a number of secondary effects of critical infrastructure disruptions that could trigger payments under L&H policies, such as:

- death or increased morbidity caused by heat waves in combination with insufficient power supply for air conditioning or similar devices;
- death or increased morbidity caused by cold waves in combination with insufficient power or fuel for heating;
- death or increased morbidity caused by insufficient supply of clean water, drugs or medical devices;
- death or increased morbidity caused by a deteriorating health system during a pandemic or large-scale terrorist attack.

Which (re)insurance lines are exposed to critical infrastructure disruptions?

Typically, this would be primarily a property exposure found in (re)insurance portfolios, although the effects could easily spill over into casualty lines of business such as general liability and/or casualty clash portfolios (e.g. liability policies could be affected in the event of a dam collapse).

Contingent Business Interruption (CBI)

Particular attention should be paid to possible repercussion damages (Contingent Business Interruption). However, for this coverage to be triggered, there must be an insured property damage (physical damage trigger) – a 'simple' power failure due to overloading of the power grid or lack of power is generally not covered. For larger commercial policies, the sub-limit for disruption of critical infrastructure is typically very low compared to other policy limits.

The network for intra-European gas transport via various pipelines also represents a relevant critical infrastructure. Although this is in principle very fault-tolerant and the failure of individual pipelines can be absorbed by re-routing, the network could theoretically fail completely – for example in the event of a targeted attack. As a result, power plants and other manufacturing industries would no longer be supplied with gas and production would be impossible.

Any business interruption losses would be covered as Contingent Business Interruption, depending on the design of the original insurance conditions (any exclusions for terrorism, war, etc. must be taken into account). However, the physical damage trigger is important here; accordingly, the cause of the gas supply failure must be due to an insured property damage. Since the failure of the intra-European gas network would affect a large number of companies, there is also an accumulation risk in this case.

A prolonged power outage would also affect oil rigs (Offshore Energy), port facilities and container terminals (Ports & Terminals), etc., which cannot operate without electricity. Since any business interruption losses in such a case would also only

be covered as Contingent Business Interruption, physical damage triggers etc. must be taken into account.

Cyber

As information technology has to be considered as critical infrastructure, some cyber lines and cloud outage products could be exposed, irrespective of the region. Compared to average events with a moderate impact, the 'big event' corresponding to a cyber-related risk is deemed to be very rare, but with extreme consequences. To date, no major event has occurred for which we can calculate the impact. The cost of the 'big one' is therefore subject to interpretation and the estimates made by the adjusters, computer scientists, model builders, etc., who simulate the risks. As a consequence, insurance premiums are an imperfect reflection of the risks covered by insurance. These uncertainties strongly limit the (re)insurance capacity of coverage. Most insurers, notably in Europe, are reluctant to develop this line of business until it is adequately modelled.

Strike, Riots, Civil Commotion (SRCC)

Disruption of critical infrastructure can lead to events covered by SRCC policies. These events may also lead to substantial property damages. Historically, SRCC pricing has been built into the price of general property coverage without any loading. Following several social unrest events (e.g. Chile 2019, South Africa 2021), most (re) insurers have requested that SRCC coverages be priced separately. Multiple restrictions have been implemented to limit loss transfer. More recently, SRCC coverage has been increasingly restricted by reinsurers attempting to strip SRCC out of property treaties.

Professional indemnity

There is potential exposure in professional indemnity where, for example, lawyers miss deadlines due to cyber attacks or power outages, which could result in financial loss to the policyholder's clients.

Directors and Officers (D&O)

D&O policies might be affected. For example, exposure could arise from the failure of management to implement necessary measures/ protection/redundancy, etc.

Contingency

Further exposure exists in contingency business and event cancellation. However, there is often a rolling aggregate limit with a time and area limitation.

Other exposures

Critical infrastructure also includes trade relevant shipping channels, such as the Suez Canal. A prolonged blockade could lead, among other things, to the spoilage of fresh goods, which, depending on the original insurance conditions, would be covered by cargo insurance. An example of a loss event is the stranding of the 'Ever Given' in 2021 and the subsequent six-day blockade of the Suez Canal.

Since many relevant security systems are also likely to fail in the event of a prolonged power failure, possible exposure to Fine Art and Specie insurance must also be taken into account. Museums, as well as banks, jewellers and especially private collectors, will find it difficult to ensure the security of safe-deposit boxes, art and collectors' items, cash, jewellery and other high-value goods during such an event; depending on the cause of the failure of the security systems, such vulnerabilities could be specifically exploited.

Life and Health (L&H)

Infrastructure disruption is likely to have the most serious impact on Life and Health policies due to second-order effects. Such effects include a deterioration in medical care due to a lack of materials, skilled personnel or access to medical facilities, resulting in increased mortality. This scenario would have a negative impact on mortality business and a positive impact on longevity business. Morbidity claims resulting from infrastructure disruptions could also occur, as these are covered by standard insurance policies. Civil unrest or civil war as a consequence of severe infrastructure disruption could have devastating effects on all L&H lines.

Are there specific inclusion or exclusion criteria for critical infrastructure?

The coverage of critical infrastructure risks is often sublimited in individual policies, e.g. coverage for business interruption. Hours clauses and occurrence limits apply for limitation. Furthermore, for Contingent Business Interruption, Tier 1 and named suppliers (e.g. utility companies that supply several customers) are generally sublimited. The ability of insurers to explicitly incorporate exclusions/inclusions in their policies also depends on whether they issue retail or corporate policies.

Some causes of critical infrastructure disruption may be ruled out completely, such as war and terrorism. Cyber risks are typically excluded in property policies. In the case of critical infrastructure disruption caused by war and cyber terrorism, it may be difficult to establish whether the damage was actually caused by such events. As a consequence of loss experience during the COVID-19 pandemic, the (re)insurance industry has developed clearer inclusion and exclusion criteria, in particular for lockdown measures and general large-scale infectious diseases. Some policies also require physical damage as a trigger for claims payments, so that mere loss of power, water or energy would not trigger these payments.

Electrical Power and Energy is an excluded cause in the standard 'Infrastructure failure' exclusion. Such infrastructure exclusions in various versions can be seen as a market standard. When it comes to power outage, policies often exclude transmission and distribution lines. Overhead power transmissions are usually excluded, write backs for the area around the covered structure exist and are common. Payment processors are a future point of discussion as it is unclear whether they can be considered as critical infrastructure. The same is valid for cloud service providers. In property policies, utilities (electricity, water, gas) are usually covered on a strictly sublimited basis. In this case, the policy indemnifies the business interruption loss incurred by a policyholder. These limits are typically in the low single-digit million range.

Critical Infrastructure is a standard exclusion in cyber policies for critical infrastructure that is not under the direct control of the insured. For example, a power plant itself could have a cyber policy that would respond to a cyber event, but all other policyholders affected by a power outage could have a Dependent/Contingent Business Interruption that would not be covered by their cyber policy. Natural perils are excluded in almost all cyber policies. Additionally, infrastructure exclusions with varying definitions are applied to original policies. Exclusions, in particular cyber exclusions, have so far not been stress-tested in court.

There is no critical infrastructure exclusion in Political Violence and SRCC policies, but hours clauses apply. In the case of 'force majeure', liability would depend on the jurisdiction in question.

L&H policies generally have no exclusions for the consequences of critical infrastructure disruptions. Annuity policies would be affected differently than general mortality or health policies.

Are there accumulation risks in the event of severe critical infrastructure disruptions?

Overall, the specific coverage types, inclusions and exclusions reflect an attempt by individual (re) insurance companies to control the potential for accumulative loss payments in a scenario where one or more critical infrastructures fail.

Given the multiple causes of critical infrastructure disruptions and the multiple types of critical infrastructure, it is clear that the accumulation potential cannot be completely avoided and therefore needs to be managed. Since the serious and therefore long-term disruption of critical infrastructure usually means that several policyholders are or could be affected at the same time, there is an accumulation risk in any case. In addition to the possible accumulation of policies in the affected region, there could also be secondary perils that amplify the overall loss. For example, in the event of a prolonged power outage, there could be riots and looting, which would normally be covered by property or political violence (or SRCC) policies.

In the case of communication and IT infrastructure, there might be an accumulation risk if system disruption is covered. As many businesses are

reliant on a small number of cloud providers to run their business, there seems to be a significant concentration risk in this area when it comes to cloud outages.

Overall, there is a need for innovation in non-damage Business Interruption policies. It is to be expected that more (re)insurers will introduce policies against supply chain disturbances to the market. These policies will mostly cover named perils only. At the same time, (re)insurers seek to limit their overall exposure through means of sub-limits and by controlling the accumulation of risks (see Section 4.4). The greatest challenge today remains the control of accumulation and, to the extent that this risk is not explicitly definable, in particular, coverage for supplier disruption remains in the early stages of development. An idea to complement traditional approaches could be the use of parametric triggers.

4.2 Impact on investments and financial markets

Critical infrastructure disruptions can impact investments and financial markets in many ways. Firstly, bonds and shares of those critical infrastructure providers directly impacted by the event are likely to lose value. A long-lasting and/or large-scale event would most likely trigger significant overall volatility and losses in financial markets, potentially on a global scale.

Recent examples include the financial market turbulences in the first half of 2020 following the emergence of the COVID-19 pandemic as well as the significantly elevated market volatility following the Russian invasion of Ukraine. Historical examples include the oil crisis of the mid-1970s. Recovery periods often take several years and are accompanied by disruptive developments, as is the case with the current inflation peaks in many countries.

4.3 Impact on reinsurance

The reinsurance industry is particularly exposed to critical infrastructure disruptions due to the high accumulation potential inherent in these risks and the extreme nature of the potential losses. The effect depends on various factors.

On the 'input' side of reinsurance, it depends on the insurance portfolio that is reinsured. Insurance portfolios may include:

- policies related to critical infrastructure providers, such as the energy or transport sectors, where coverage is activated by the disruption of these critical infrastructures;
- policies indirectly related to the disruption of critical infrastructure, such as disability or life insurance coverage activated in the event of war.

It is important to remember that many policies have their retentions and deductibles and only activate their reinsurance in the event of a peak loss. Policies also have their exclusions, for example for terrorism and acts of war.

On the 'output' side, reinsurers can mitigate their own risk by using adequate risk calculation models, by reinsuring parts of their portfolio (or above a certain limit) to other (groups of) reinsurers, or by hedging the risk.

The following vulnerabilities in this reinsurance process can be identified in the event of a disruption of critical infrastructure:

- The models used to calculate the reinsurance risk are not adapted to the (changed) likelihood or impact of a disrupted critical infrastructure.
- Performance failure of the retrocessionaires to whom (part of) the reinsurance risk is transferred (e.g. due concentration risk and exceptional claim amount at the same time).
- Inadequate operation of immediate hedging capabilities in the event of immediate disruption of critical infrastructure.

4.4 Managing insurance and financial risk exposure

First and foremost, and irrespective of the individual measures taken to deal with underwriting and financial exposure, there is always the imperative of risk prevention and increasing resilience. Here, the transfer of the (re)insurance industry's specific expertise and improved cooperation with all stakeholders is required.

By communicating with clients about possible prevention measures and expected risk management behaviour with respect to anticipated risks, insurers can make it clear that some risks related to critical infrastructure need to be addressed by the insured and cannot benefit from blanket cover. In addition, some insurance clients are themselves actors that are increasingly required to develop resilient operations, for example in the context of certain EU regulations (DORA or NIS) (see Section 5.4) or other regulations on critical operators. This helps to differentiate between the insurer's and the client's responsibilities, by setting standards for what measures clients should have taken in order to mitigate risks to their business continuity.

Business interruption covers are the insurance liabilities most likely to be directly triggered by critical infrastructure disruption. A thorough review of the insurer's policy wording will help to properly identify the actual exposure to such events, thereby helping to assess and mitigate the risk that the portfolio exposure exceeds the risk tolerance level.

Critical infrastructure disruption may result from the realisation of other risks (e.g. water scarcity induced blackouts, or conflict-related disruption of oil and gas availability with knock-on effects on electricity supply), as illustrated in the other sections of this paper. A careful review of exclusions will help to identify potential 'silent covers' currently in the portfolio; these clauses can be reworded to make more explicit the context in which a critical infrastructure disruption may allow insurance pay-outs to be triggered.

Careful matching of reinsurance protection with insurance guarantees is also a way of ensuring that risk transfer strategies remain effective in the context of critical infrastructure disruption.

From a risk management perspective, it is critical to identify risks that are not insurable at a reasonable premium and can only be dealt with by public authorities, and to make sure that they are not included in insurance policies. For example, large-scale cyber attacks by sophisticated, state-sponsored hacker groups targeting critical infrastructure, could be considered acts of war, and should therefore not be covered by insurers.

Cyber-related risks are now inherent in all activities, whether entrepreneurial or individual, and insurers must accompany their clients by providing advice on prevention and protection solutions that meet their needs. The stake for insurers is to be able to serve their clients at all times. In the course of day-to-day activities, insurers protect the data entrusted to them; in the event of a disaster, they assist their clients. In order to develop cyber insurance as a way of protecting economies against a major disruption of critical infrastructures, there is first a need to enhance prevention and protection practices, for example by providing standardised operational cyber security measures to be implemented by SMEs and corporates.[26] Public-Private Partnerships (PPP) should also be explored at national or European level, so that part of the risk is covered by public authorities. By alleviating private (re)insurers of a portion of this risk, this would help to develop the market in the event of a major attack that would endanger the economy and/or sovereignty of a state.

As noted in Section 4.1., accumulation control is crucial for (re)insurers. This is achieved through continuous monitoring of accumulation limits and prospective scenario analysis. These analyses take into account the coincidence of the different events described above in respect of infrastructure disruptions and their impact on insurance covers as well as the capital markets.

Financial risk management in the context of critical infrastructure disruption leverages on traditional risk management techniques:

- identification of potential risk exposure in the portfolio by including critical infrastructure disruption in the risk factors considered when looking at an issuer's risk profile;
- risk mitigation through the use of primary and secondary investment limits to ensure appropriate diversification and avoid concentration of risk in the asset portfolio.

The use of derivatives to address the adverse impacts of critical infrastructure disruption on the investment portfolio is less straightforward, as infrastructure disruption may impact a wide range of assets. In addition, setting up a cost-efficient hedging strategy to match the actual portfolio exposure would be far from straightforward.

Public-Private Partnerships (PPP) – Example: Flood Re (UK)

Critical infrastructure risks may have such a widespread impact that they may no longer be insurable at a reasonable price. In this instance, private insurance cannot be a stand-alone solution. Such questions have already been raised for risks such as flooding, where changing weather patterns could make some geographical regions more vulnerable to flooding or adverse temperatures, which would result in substantial limitations in the supply of insurance. Reinsurers have already begun to assess the level of catastrophe risk attached to such risks.[27] In this case, the option of a PPP has already been explored, for example with the creation of Flood Re in the UK.

Flood Re is a reinsurer set up in the UK for the sole purpose of reinsuring flood risks in areas that might otherwise be unaffordable.[28] It was introduced following the widespread flooding in 2007, when there was a real risk that affordable insurance would not be guaranteed in some areas.[29] The reinsurer is funded by a levy on all insurers. Individual policies are then sold to policyholders as normal, with Flood Re providing reinsurance for the excess flood-related element of the risk in order to reduce the customer's premium to an acceptable level. The scheme has been relatively successful with nearly half a million households benefiting since its inception.[30] An important element of the Flood Re scheme is the cut-off date for properties to enter the scheme, so that properties built after 2009 do not qualify. This recognises that building on flood plains has contributed to the risk in the first place, and so aims to avoid incentivising further building in flood prone areas. The extent to which this has been achieved is debatable, with evidence suggesting that homebuyers remain insufficiently aware of the issue to influence behaviour.[31]

Further, there is evidence that the existence of the insurance leads to increased moral hazard, with households feeling that the insurance coverage means they don't need to do anything to reduce the risk or its effects.[32] To counter part of these risks, Flood Re introduced a 'build back better' element, providing funding to improve flood resilience measures.[33]

This example demonstrates that Public-Private Partnerships can be successful in keeping insurance coverage available to all, however the wider implications of such schemes should also be considered to ensure that they don't risk incentivising counterproductive behaviour and also help to address the underlying risk.

The (re)insurance industry has already developed a sophisticated approach to risk identification and management. However, in order to address the specific challenges linked to the high degree of interconnectivity of risks associated with critical infrastructure, further analytical and modelling efforts are to be pursued. Improved collaboration between all stakeholders – both private and public – will be necessary to develop adequate solutions going forward.

5. Resilience and operational risk management

5.1 Operational resilience

Resilience is defined as the ability to anticipate, prevent, adapt, respond, recover, learn and improve from internal or external disruptions while continuing to provide important business services to customers and clients in a continuously changing environment. This approach minimises the risks associated with various operational disruptions such as climate disasters, sophisticated cyber attacks and global pandemics, to name a few. Despite significant progress in non-financial risk management and business continuity planning, the world today is beset by several crises and changes on a global scale. These events combine together to create a multi-risk scenario. Risk management practices must evolve to adapt to this new multi-risk environment, rather than reacting to each disruption separately. Given this challenging environment, the imperative should be to increase resilience and reduce the risk of direct and indirect impacts. This, combined with an increased regulatory focus on the effects of operational incidents, is broadening the definition of operational resilience beyond business continuity to an end-to-end perspective. The aim is to improve the ability to respond to, recover from and learn from operational disruptions when they occur. Operational resilience is a shift from objectives focused on business continuity to objectives focused on operational resilience, assessing very low probability scenarios that can still have a disruptive impact. Operational resilience must be developed as a key framework that allows not only for the restoration of the status quo following a disruption at a point in time (business continuity), but also for adaptation and improvement over different time frames, including the medium and long terms.

5.2 Managing operational risk exposure

According to research by the European Parliament,[34] a large proportion of critical infrastructure is owned and operated by private-sector companies. As such, the protection of vital assets and systems relies on effective cooperation between state and private actors. Managing operational risk, whether from man-made threats, technological threats or natural disasters, is becoming essential and requires a comprehensive approach. Identifying critical infrastructure understanding interdependencies through risk assessment, monitoring risk exposures, implementing measures to mitigate these risks and responding appropriately to incidents when they occur is key.

The following three aspects play an important role in managing operational risk exposure in critical infrastructure:

1. Business Continuity Planning (BCP) and Resilience Planning

The inherent interdependencies between infrastructure assets and systems increase the complexity of assessing this risk and managing the impact of disruption of services, especially for critical infrastructures supporting cross-border services.

Recently, it was identified that the existing EU framework for protection and resilience of critical infrastructures (see Section 5.4) has not kept pace with the ever increasing interconnectivity of infrastructures, paired with the high dependency of most European Critical Infrastructures (ECIs) on digital infrastructures.[35] In addition, the European Parliament's resolution of 2018 recommended ensuring that the designation of ECIs is carried out on the basis of an analysis of the systems supporting vital and cross-border services, rather than a sector-by-sector approach. The Parliament called for the creation of an obligation for public and private operators of ECIs to report incidents, conduct stress tests, provide appropriate training at designated contact points, and establish quality requirements for business continuity plans, including operational plans.

BCP is the process of creating a plan to ensure the continuation of critical business operations in the event of a disruption or disaster. 'Organisational resilience' is defined as "the ability of an organization to anticipate, prepare for, respond and adapt to incremental change and sudden disruptions in order to survive and prosper".[36]

Figure 1: Business Continuity Planning

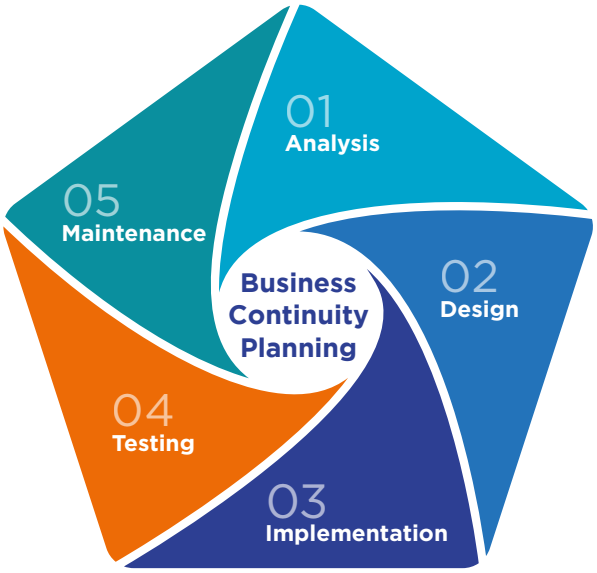


Figure 2: Components of a third-party risk management

To develop and address BCP and Resilience Planning a thorough understanding of critical infrastructure is required, such as the increasing interdependencies and interconnectedness, the fast pace of innovation that is fundamentally transforming infrastructure sectors, as well as the aging infrastructure. To fulfil this task, appropriately sophisticated analysis and simulation tools are a prerequisite. However, the complexity mentioned above poses a challenge that critical infrastructure resilience plans have to cope with.

2. Third-party risk management: Identify exposure of outsourced services and measures put in place by outsourcing service providers

Outsourcing services to third parties is a common practice in the market/industry. However, outsourcing services within critical infrastructure can pose an additional risk, or at least an additional vulnerability, in the communication between organisations and their outsourced service providers. There could be delays in response times, miscommunication and difficulties in coordinating and managing priorities. The outsourcing company has to rely on the reliability and performance of the third-party service provider. It is essential that the outsourcing party carries out due diligence on the outsourcing service provider, monitors their performance, ensures that service providers comply with security and data protection requirements, and establishes clear contractual obligations and service level agreements. Prior to outsourcing, a company should decide which activities can be outsourced and which critical activities should remain with the owner.

3. Identify dependencies stemming from critical infrastructure disruption

The threat to critical infrastructure has changed over the years. Most infrastructure systems today are interconnected in one way or another (see Section 1.3). The dependencies are complex and can be either physical, such as power or water supply or any other natural hazard, or digital, such as data transfer, software integration or a cyber attack. Impairments in one area can affect other locations, industries or sectors and thus have an impact far beyond the original area of risk.

An analysis of the dependencies associated with critical infrastructure should be conducted to identify the areas most vulnerable to operational risk. Once identified, targeted protection measures can be put in place to reduce these dependencies. However, this requires a good understanding of the hazards and risks that can affect infrastructures. For example, during the Omicron wave of the COVID-19 pandemic, the German government provided manuals on operational pandemic planning or guidelines on risk and crisis management. Implementation was the responsibility of the operators of critical infrastructure (such as energy or water suppliers).[37]

Overall, critical infrastructure disruption does not imply a radically new approach to risk management – the essential risk management tools are the same. The difference lies in the depth of vision required to identify the impacts stemming from critical infrastructure disruption and the potential limits to the insurability of some of these risks.

5.3 Managing operational risks: Example – energy supply / power blackouts

With regard to the risk of energy supply failure, the following options for action arise in this context:

Preparation of a hazard overview

In order to be adequately prepared for an area-wide power supply failure, it is necessary to assess and record the potential impact on the energy-sensitive areas of the company. In this context, it is important to determine the dependency of business-critical infrastructure on the various energy sources (electricity, gas, oil). At the same time, a delineation of different main scenarios such as brownouts (pre-announced periodic shutdowns) vs. blackouts (unplanned outages) can help to determine the respective impact on the dependent infrastructure.

Risk rating

Based on the identified scenarios, a risk assessment can be performed for the company's critical infrastructure. This should include an evaluation of the probability of occurrence for each loss scenario and an evaluation of the expected impacts. When assessing potential impacts, it is imperative to apply insights from related disciplines, such as Business Continuity Management (BCM) or IT Service Continuity Management (ITSCM). For example, the impact of a building failure will depend on, among other things, the number of time-critical business processes taking place in the affected buildings. The extent of remote working may also have an influence on the impact of a power failure.

The impact of the disruption of critical IT infrastructure also depends to a large extent on the redundancies already in place. Finally, emergency and crisis management will often already have valuable knowledge of the effects of previous power outages. Depending on the risk appetite of the company and the cost-benefit ratio, the options for dealing with the energy failure can then be determined.

Options for action

Risk treatment usually results in measures to avoid, mitigate or transfer risks and, if necessary, to accept them. Against the background of an imminent power failure, the following practical options for action may arise, the implementation of which must be assessed for appropriateness (that is, cost-benefit):

- conversion of energy supply to alternative energy sources;
- installation of emergency generators;
- stockpiling larger quantities of fuel;
- adjustment of contracts with suppliers;
- split operations between locations / establish back-up locations.

Although dealing with the risks of a power outage can have a safeguarding effect, it can still be assumed that the entire company and its employees will suffer a high level of damage. For this reason, it is additionally necessary to develop rapid response options within the framework of emergency, crisis and business continuity management in order to achieve effective damage limitation in the event of an emergency. In this context, crisis management action plans, internal and external crisis communications and business continuity plans form the backbone of the response capability.

5.4 EU regulation

As mentioned in the introduction, the EU 'Critical Entities Resilience Directive' entered into force in January 2023. The intention of the directive is to provide a framework that supports member states in strengthening the resilience of critical infrastructure against a range of threats and requires the adoption of a national strategy, including regular risk assessments to identify entities considered critical or vital to society and the economy.[38] The EU has been actively addressing the resilience of critical infrastructure through various directives and regulations aimed at protecting against threats and increasing preparedness and collaboration in the event of disruptions to sectors and systems essential to the functioning of society and the economy. Additional legal frameworks to the CER Directive include:

The Network and Information Security (NIS) 2 Directive

In 2023, a revised cyber security framework came into force, effectively accelerating the maturity of organisations' cyber security and resilience to meet the increased levels of exposure to cyber threats. The increased threat was manifested in the largest recorded cyber attack against a European customer in July 2022, alongside supply chain incidents accounting for 17% of breaches in 2021, compared to less than 1% in 2020. The NIS 2 Directive now includes medium and large entities from more sectors including providers of public electronic communications services, digital services, wastewater and waste management, manufacturing of critical products, postal and courier services and public administration at both central and regional levels. The rules effectively expect improved cyber security risk management measures to be taken by more entities. The pre-emptive measures required of entities is reinforced by increased information sharing and cooperation on cyber crisis management at national and EU level.

Digital Operational Resilience Act (DORA)

Here the EU has established a uniform set of requirements for a broad scope of financial services firms in the EU in the areas of cyber and ICT (information and communication technology) risk management. By 2025, critical third parties providing ICT-related services to financial entities must also comply with rules on protection, detection, containment, recovery and repair capabilities against ICT-related incidents. DORA explicitly refers to ICT risks and sets out rules for ICT risk management, incident reporting, operational resilience testing and monitoring of ICT risks by third parties. This regulation acknowledges that ICT incidents and a lack of operational resilience have the possibility to jeopardise the soundness of the entire financial system, even if there is 'adequate' capital for traditional risk categories. The framework reinforces practices for protection, detection, containment, recovery and repair capabilities against ICT-related incidents.

6. Conclusion

The disruption of critical infrastructure is a complex and cross-cutting subject that impacts individuals, governments and the private sector. As critical infrastructures provide the essential services that form the bedrock of a functioning society, current and future ability to effectively maintain these services should be given explicit consideration, especially in the face of modern threats such as cyber terrorism, the consequences of climate change or increasing vulnerability due to growing mutual (inter-) national dependencies.

The (re)insurance industry – with its expertise in risk modelling, risk management and risk transfer solutions – already provides financial support in the case of infrastructure disruption and is therefore optimally positioned to identify further innovative solutions that will help to provide resilience, thus limiting the impact of critical infrastructure disruption in the future. In doing so, challenges relating to the increasing interconnectivity and potential accumulation of risks associated with critical infrastructure disruptions need to be addressed. Such challenges will require further in-depth analysis and modelling efforts, in addition to collaboration with public stakeholders.

Appendix I - Rating of 'Critical Infrastructure Failures' in the annual 'ERI Risk Radar'

ERI Year	Risk category	Time horizon	Description/info
2018	High	First significant impacts expected within 1-5 years	Critical infrastructure & power blackout In many regions of the world, there is a chronic failure to adequately invest in, upgrade and secure infrastructure networks such as electricity provision, water supply or transport infrastructure. The lack of capacity or outages could result in blackouts. This could lead to a higher than expected frequency and severity of large property losses (including BI/CBI). Additionally, the risk of solar storms could impact the electrical grid as well as space-based infrastructure, GPS and communications systems.
2019	High	Significant impacts already seen in insurance claims	Critical infrastructure & power blackout Same as 2018 plus "Also energy transition may impact stability of energy supply".
2020	High	Significant impacts already seen in insurance claims	Same as 2019 and 2018.
2021	High	Significant impacts already seen in insurance claims	Same as above with the addition "A smoothly functioning digital infrastructure is becoming increasingly important, especially in times of remote home office working".
2022	High	Significant impacts already seen in insurance claims	Same as above.
2023	High	Significant impacts already seen in insurance claims	Rephrased: In addition, external factors such as the risk of natural catastrophes, solar storms, cyber attacks or geopolitical conflicts increase the likelihood of disruptions to critical infrastructure. Furthermore, the transition to renewable energy may impact the stability of energy supply.

Appendix II - ERI Publications

The risks of critical infrastructure disruption have already been addressed in previous publications of the CRO Forum. The following papers are particularly worthy of mention:

Terrorism
2007

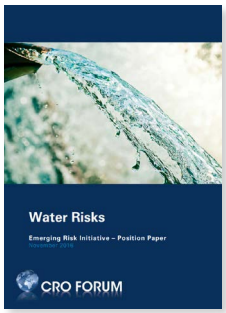
Critical Information Infrastructure
2008

Power Blackout Risks
2011

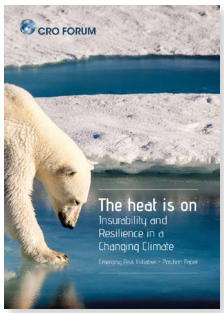
Food and its impact on the risk landscape
2013

Cyber resilience
2014

The Smart Factory
2015

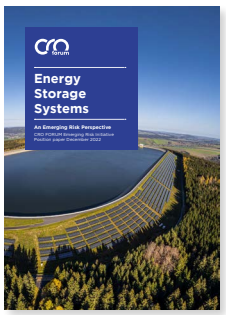


Water Risks
2016



The heat is on – Insurability and Resilience in a Changing Climate
2019

The Internet of Things risk from an insurance perspective
2022



Energy Storage – An Emerging Risk Perspective
2023

References

[1] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC http://data.europa.eu/eli/dir/2022/2557/oj

[2] Publication Archives – The CRO Forum https://www.thecroforum.org/category/publications/

[3] Major Trends and Emerging Risk Radar – Update 2023, CRO Forum – Emerging Risks Initiative Emerging Risk Initiative – Major Trends and Emerging Risk Radar 2023 – The CRO Forum

[4] Climate change impacts and costs to U.S. electricity distribution and transmission infrastructure. C. Fant et al., Energy vol 195. 2020

[5] Impacts of Climate Change on Transport; a focus on road and rail transport infrastructures. JRC Scientific and Policy Reports, 2012; Climate Change Could Wreck a Quarter of Steel Bridges in 21 Years (popularmechanics.com)

[6] Brooks K., Landeg O., Kovats S., et al. Heatwaves, hospitals and health system resilience in England: a qualitative assessment of frontline perspectives from the hot summer of 2019. BMJ Open 2023;13:e068298. doi:10.1136/ bmjopen-2022-068298Brooks K, et al. BMJ Open 2023

[7] Nuclear energy isn't a safe bet in a warming world – here's why (theconversation.com)

[8] Christodoulou A., Demirel H., *Impacts of climate change on transport – A focus on airports, seaports and inland waterways*, EUR 28896 EN, Publications Office of the European Union, Luxembourg, 2018, ISBN 978-92-79-97039-9, doi:10.2760/378464, JRC108865

[9] https://www.fsb.org/wp-content/uploads/P130423-3.pdf

[10] Sansavini, Giovanni (Prof. – ETH Zürich), AXA Research Fund, Building Cyber Resilience, Nov. 2021 (https://www.axa-research.org/en/news/building-cyber-resilience)

[11] Global electricity demand is growing faster than renewables, driving strong increase in generation from fossil fuels – News – IEA

[12] Executive summary – Electricity Market Report 2023 – Analysis – IEA

[13] Europe can cut natural gas imports from Russia significantly within a year – News – IEA

[14] Where does the EU's gas come from? – Consilium (europa.eu)

[15] How to resolve the bottlenecks that slow down the green transition | World Economic Forum (weforum.org)

[16] https://klardenker.kpmg.de/digital-hub/was-fuer-finanzdienstleister-jetzt-zu-tun-ist/

[17] Physical attacks on power grid surge to new peak – POLITICO

[18] Deutscher Bundestag 17/5672 Bericht Technikfolgenabschätzung 2011

[19] https://www.newsd.admin.ch/newsd/message/attachments/40201.pdf

[20] 'Drug Shortages: Root Causes and Potential Solutions', FDA 2019 http://www.fda.gov/media/131130/download

[21] Intense heat and flooding are wreaking havoc on power and water systems as climate change batters America's aging infrastructure (theconversation.com)

[22] The Observer view on the woeful state of England's water industry. The Guardian, August 14, 2022

[23] Chapter 2 – Protecting Water Supply Critical Infrastructure, in 'Securing Water and Wastewater Systems: Global Experiences' edited by Robert M. Clark and Simon Hakim (2014), Springer-Science, 223 Spring Street, New York, NY. 10013

[24] UK Water Supplier Hit by Cyber Attack, Highlighting Critical Infrastructure Vulnerabilities. The Insurer, 18 August 2022

[25] Ransomware hit SCADA systems at three facilities in the U.S. Security Week, 15 October 2021

[26] See FERMA report 'How Europe can lead the way to cyber resilience', June 2023 (https://www.ferma.eu/app/uploads/2023/06/Cyber-Insurance-Dialogue-Report.pdf)

[27] Insuring the Uninsurable: Fighting Systemic Risks with Blended Finance (iceye.com)

[28] Flood Re explained | ABI

[29] Flood Re for household flood insurance (parliament.uk)

[30] Almost half a million households have now benefited from Flood Re. – Flood Re

[31] ABI: 'Extending Flood Re is the wrong answer' | Insurance Business UK (insurancebusinessmag.com)

[32] SMF-Incentivising-household-action-on-flooding_web.pdf (floodre.co.uk)

[33] Building back better to increase flood resilience (jbarisk.com)

[34] European Parliamentary Research Service PE 662.604

[35] (COM(2020) 605) European Parliament

[36] 'Organizational Resilience', BSI (website), accessed on May 10, 2023, Our services – organizational resilience – index report | BSI (bsigroup.com)

[37] Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement Leitfaden für Unternehmen und Behörden www.bmi.bund.de

[38] EU: CER and NIS 2 Directives enter into force | News post | DataGuidance

Disclaimer

Dutch law is applicable to the use of this publication. Any dispute arising out of such use will be brought before the court of Amsterdam, the Netherlands. The material and conclusions contained in this publication are for information purposes only and the editor and author(s) offer(s) no guarantee for the accuracy and completeness of its contents. All liability for the accuracy and completeness or for any damages resulting from the use of the information herein is expressly excluded. Under no circumstances shall the CRO Forum or any of its member organisations be liable for any financial or consequential loss relating to this publication. The contents of this publication are protected by copyright law. The further publication of such contents is only allowed after prior written approval of CRO Forum.

The CRO Forum is supported by a Secretariat
that is run by KPMG Advisory N.V.
Laan van Langerhuize 1, 1186 DS Amstelveen, or
PO Box 74500, 1070 DB Amsterdam
The Netherlands

www.thecroforum.org