LLOYD'S

Shifting powers: physical cyber risk in a changing geopolitical landscape

In association with

Centre for **Risk Studies**

UNIVERSITY OF CAMBRIDGE
Judge Business School

Lloyd's Futureset

Contents

Executive summary 03

Physical cyber risk 04

Cyber deterrence
Understanding cyber physical risk
The threat to businesses
The art of the possible: what cyber physical attacks can and can't do

Cyber physical scenarios 12

A note on tiering cyber powers
Scenario 1 – Asymmetric Attack Exchange: Ransomware on critical infrastructure
Scenario 2 – Offensive Cyber Retaliation: Cyber-physical sabotage of critical infrastructure
Scenario 3 – Symmetric Attack Exchange: Escalation of destructive attacks on critical infrastructure

Insurance solutions 26

Cyber insurance today
Cyber physical insurance
Key considerations for insurers
Product innovation opportunities

Glossary 34

References 36

Executive summary

Cybersecurity is at the top of the agenda for businesses, boards, risk managers and consumers. In recent years, malware and ransomware attacks have been causing severe disruption for global businesses and their supply chains – and increased scrutiny of the mitigation strategies and insurance coverage of those businesses.

Those trends have been underlined by the COVID-19 pandemic and the rise in criminal ransomware activity it triggered; alongside the changing geopolitical landscape in the wake of Russia's invasion of Ukraine. Thankfully, the world is yet to experience a truly catastrophic cyber physical attack. But the potential impacts of such an attack could be significant, crippling entire systems and societies.

For the most part, cyber attacks target the availability, confidentiality or integrity of data – rather than causing operational, environmental or material damage. In some cases, however, the disruption that follows cyber attacks can have a destructive impact on the physical world. This is a growing threat, with attacks targeting critical infrastructure rising from less than 10 in 2013 to almost 400 in 2020.[1] As well as the increase in frequency, the complexity of attacks are evolving, from simply targeting short-term disruption to compromising assets or processes with the intent to cause physical harm or loss of life.

In this context: an effective cybersecurity strategy is paramount. With a risk as complex as cyber – encompassing a huge range of possibilities and uncertainties – one useful tool for risk managers can be scenario planning. This report outlines three hypothetical, but plausible scenarios (summarised below) involving politically motivated cyber attacks intended to cause physical damage. The analysis includes the potential impacts on businesses and the insurance industry.

1. **Asymmetric Attack Exchange:** A rudimentary cyber power sponsors non-state ransomware attacks by cybercriminals targeting another nation's critical infrastructure
2. **Offensive Cyber Retaliation:** Regional tensions over nuclear development programmes spill over into cyber-physical sabotage of critical infrastructure
3. **Symmetric Attack Exchange:** Two sophisticated cyber powers engage in an escalation of destructive cyber attacks on critical infrastructure

While geopolitical interests to date have broadly deterred actors from using their advanced cyber capabilities – as the scenarios developed in this report demonstrate, circumstances can quickly escalate; and the anonymous nature of cyber attacks could allow states and other geopolitical players to deploy espionage, retribution, and attacks with broad plausible deniability. Placed in a climate of increased tension, the risk of a major cyber attack affecting physical systems, national infrastructure and the global economy becomes far more likely.

This report provides a qualitative assessment of the risks to businesses and national economies from 'cyber physical' – virtual attacks triggering material impacts – and highlights the role insurance can play in building resilience against these threats. It highlights how cyber physical represents an under-utilised opportunity for insurers to extend the protection they offer businesses, and thus society, through the products and services they provide. This opportunity is not without its challenges, and more research is needed to understand potential losses and likelihoods; but what the scenarios make clear is that those with effective cyber strategies and scenarios in place will be best equipped to face the unique challenges of this emerging and potentially debilitating risk.

1 Gartner (2022)

Physical cyber risk

Physical cyber risk

In recent years, the worlds of cyber and geopolitics have become increasingly integrated. Concern over the digital interference of state actors with foreign elections has been a visible issue since at least 2015; however digital intrusion, and the projection of unseen influence by state-backed cyber teams, has been around since the turn of the millennium.

Historically, cyberspace has been the domain of non-state actors. Cyber criminals, hacktivists, and other entities have successfully mapped closed networks and exploited secure systems, creating a dark economy of toolkits, services-for-hire, and intelligence that are easy to purchase and develop over time. As a result, the stealing of data, funds, and intelligence in order to project substantial power online is more accessible than ever – to a broader swathe of actors. This includes nation states, non-state threats, insurgents and other unpredictable, maliciously minded groups.

For the most part, state-sponsored cyber operations have been used to gather intelligence and influence real-world politics. However, cyber space offers an opportunity for smaller states to project power beyond traditional military or economic arenas. In these countries, cyber actors are rapidly raising profile. There are also clear signs that a number of states have assembled powerful cyber arsenals, with tools capable of crippling major industries or state projects through economic and physical disruption. Barring a few notable examples, most nations are not known to have carried out attacks using these tools. However, state-sponsored cyber activity is arguably more prevalent – albeit slower moving, largely covert and deployed alongside other foreign policy tools such as sanctions.

Put simply, we don't yet see the damage brought about by sophisticated state-backed cyber attacks – although that doesn't mean they're not happening. As cyber risk and geopolitics have become more closely integrated, cyber attacks affecting physical systems and structures can be both a cause and effect of the changing geopolitical landscape. They may therefore become more obvious and impactful as the geopolitical landscape changes.

Cyber deterrence

In a highly digitised economy, fear of escalating cyber conflict has become a constant for businesses and governments alike. For much of the past decade, a deterrence-based geopolitical climate has largely prevented any public, openly aggressive cyber engagement by states. However in 2018, the publication of the US Cyber Strategy explicitly stated an intention to "defend forward" against cyber adversaries – perhaps heralding a transition from the age of deterrence to one where defence and offence are harder to separate. These new postures directly acknowledge the present threat to vital systems and critical national infrastructure from rival nations and geopolitical entities. At present, however, deterrence appears to be a powerful force in warding off such action. Deliberate 'cyber catastrophes', as a result of cyber operations by major powers, remain unlikely.

At present, states are at a point of equilibrium; powerful cyber teams have proved either unwilling or incapable of causing catastrophic economic impact, yet could plausibly advance the threat suddenly and significantly. However to date, national cyber policies have not differed substantially from foreign policy instruments – including the use of miilitary force and coercive diplomacy. So while cyber is a powerful tool, it is unlikely to be used in a destructive way independent of significant shifts in a nation's foreign policy, as any escalation would quickly prove disastrous.

Physical cyber risk

The involvement of non-state actors, however, increases the risk of cyber catastrophes. As these, often extremist, groups gain traction in cyber operations – intending to cause major shocks to national or international systems, and often with little to lose strategically – the risk of cyber terrorism, cyber protest, and other forms of cyber insurgency increases. Questions remain around precisely how cyber operations can deliver the seismic change many of these groups seek: for example, some radical environmental groups may target the destruction of a major pipeline, but achieving this through cyber means is difficult, expensive, and time-consuming. This means more reliable physical attacks and protests are likely to be relied upon for the foreseeable future.

Profit is also a powerful driver of non-state cyber activity that has the potential – whether deliberate or not – to increase cyber physical threats. Recent incidents, such as the death or further injury of patients in hospitals impacted by ransomware attacks,[2] or the inoperability of multiple systems across the world as seen during 2017's WannaCry, demonstrate that cybercrime can be as harmful as a state-backed cyber attack. This is for the simple reason that these actors are less furtive and may see unintended disruption as a means to gain profile and notoriety.

Recently, there has been an alarming increase in cyber criminals targeting critical national infrastructure systems. By leveraging significant public and political pressure on victims, attackers have been able to extract heavy ransoms. These types of attack can result in system-wide disruption and damage, creating significant national security concerns. States are now addressing this threat by applying dissuasion and suppression to ransomware gangs, reminiscent of the "global war on terror" in their focus on investigations, legal action and strong public rhetoric.

Understanding cyber physical risk

Most cyber attacks on networks are disruptive in nature, affecting the availability, confidentiality or integrity of data, rather than operational safety, environmental safety, or human lives. Put simply, most cyber attacks inflict damage chiefly by shutting down regular business activity. The massive losses seen in the 2017 NotPetya attack, for instance, came from disrupted business, lost sales, reputational damage, and in the repair and replacement of key technology.

In some cases, however, cyber attacks that focus on data can also have a destructive impact on the physical world. A ransomware attack on a hospital's network, for example, may threaten the lives of patients by interrupting the data flow to critical medical tools. This concern has grown throughout the pandemic, even though some ransomware gangs originally issued statements to say that they would not target healthcare networks during the covid outbreak. In 2020, the first death attributed to a ransomware attack was reported in Germany.[3]

Cyber physical attacks trigger physical damage or injury purely by compromising operational technology (OT) and digital control systems or disabling control and safety systems. This includes attacks on Supervisory Control and Data Acquisition (SCADA) systems. Some cyber physical attacks may be targeted (focused on bringing down a particular piece of technology, such as a furnace or fuselage) while others may impact multiple devices across networks, such as batteries or boilers. There is generally a smaller pool of OT or SCADA service providers, compared to enterprise IT for example, which increases the potential risk for businesses.

2 Associated Press. (2020). German hospital hacked; patient taken to another city dies. Available at: https://apnews.com/article/technology-hacking-europe-cf8f8eee1adcec69bcc864f2c4308c94.

3 (O'Neill 2020)

Physical cyber risk

A deliberately physically destructive cyber attack is a difficult thing to accomplish, requiring specialist hackers and detailed strategic planning. The capacity to carry out such attacks currently predominantly sits within nation states and the groups which they support, which means that right now cyber physical risk is closely related to geopolitical risk.

Targeted physical attacks by government-sponsored groups are far more common than systemic ones, partly because smaller attacks create less of an outcry. The diplomatic consequences that follow the discovery of one country's malware in another's power substation are far more manageable than the international reaction and condemnation that would come with the same malware being found across the entire energy network – in essence, governments work in a targeted way to stay under the global diplomatic radar.

However, at any point it is possible that cyber physical hacking capacity could be made available for purchase, meaning that even non-state actors could buy access to powerful tools for carrying out cyber physical attacks provided they had the financial means and strategic interest to do so.

The threat to businesses

Despite the political sponsors who sit behind this threat, the nature of cyber disruption means that it is largely immune to geographical boundaries. Any major change in the cyber threat landscape which increases the sophistication of tools in wide circulation, or lowers the bar for achieving highly impactful attacks, will increase risk to businesses across multiple geographies. Attacks may become more frequent, or more severe in nature, and businesses may be strategically disrupted in order to deal blows to national interests, or suffer from the knock-on consequences of a major cyber attack to critical national infrastructure.

Businesses are also vulnerable to attacks which affect third-party suppliers with less secure networks, or which are located in parts of the world where cyber disruption may increase sharply and suddenly. This has the potential to be disastrous for businesses who are reliant upon them for their supply chains, especially multinational firms with digital supply chains which stretch across multiple complex networks.

The art of the possible: what cyber physical attacks can and can't do

Industrial and highly mechanised environments, including national infrastructure systems, building control managers, energy management systems, traffic grids, and other utilities which aid in business continuity and national safety are all highly vulnerable to cyber attack.

Cyber crime tends to focus on impacting three major components of these types of networks: **controllability, observability** and **operability** (known as the "CO2 framework").

Of the three, operability attacks are the most directly physically damaging. However, compromising any of the CO2 factors may contribute to physical damage, or to a level of disruption that may become damaging if sustained.

Physical cyber risk

Table 1: CO2 framework for industrial compromise[4]		
Controllability	**Observability**	**Operability**
The ability to bring processes into a desired state Failures include: *an inability to control the network, the sequence of control commands is unknown to the operator, system has lost power, etc*	**The ability to measure process state and maintain situational awareness** Failures include: *an inability to monitor sensors, the data is no longer trustworthy, measurements cannot be interpreted, etc*	**The ability of the system to achieve acceptable operations** Failures include: *damage to the physical system, inability to safely shut down, inability to repair the system, etc*

On the plus side, manipulating any of the CO2 factors using cyber means is difficult, and incidents are rare when compared with the high number of data breaches and denial-of-service attacks. This is partly because digital systems are trained for a limited set of outputs and their options are often minimal. For example, a robotic arm on a manufacturing floor can be manipulated into an uncontrolled spin, threatening its surroundings, but it cannot be made to spontaneously explode unless it already contains the code for this.

In order to create physical damage or bodily injury, targeted systems must already feature embedded fuel or energy sources which can be tapped into from digital systems to inflict damage. Examples of energy sources that could be targeted include:

1. **Lithium-ion batteries**

   Batteries in laptop computers, mobile phones, game consoles, power tools, electric vehicles and specific aerospace equipment are a possible power source for attackers. Through 2016 and 2017, Samsung issued a massive recall on the Galaxy Note 7 after a manufacturing defect caused thermal runaway in the devices' lithium batteries, posing a potential fire risk. Attackers might be able to deliberately duplicate similar effects in widely used devices using malicious software updates to exploit battery management systems. Most fire safety and retardation systems are ineffective against lithium fires, meaning blazes could spread and cause significant damage.[5]

2. **Fuel for boilers**

   Combustion fuel for boilers and heating systems stored on-site could be weaponised by attackers exploiting digital building management systems. Attackers may be able create concentrations of fuel in enclosed systems by manipulating these fuel sources. If ignited, this accumulated fuel could rapidly cause a major fire risk with the potential for explosions.

3. **Machinery energy**

   Attacks on industrial machinery, power plants, production lines, furnaces, centrifuges, turbines, generators or transformers could see the internal momentum or heating of a machine compromised in order to cause a fire, explosion, or collision. The pivotal German steel mill attack of 2014 and the Stuxnet worm which affected nuclear processing facilities in Iran in 2010 are alarming examples of industrial machinery systems being accessed via production software or other malware and exploited in order to cause massive damage to the facility.

4 (Krotofil and Larsen 2015; Marie Elisabeth Gaup Moe 2016)

5 (Fernández Lisbona and Snee 2011)

Physical cyber risk

4. **Hazardous materials**

   Many types of stored hazardous materials (including chemicals, methanol, fertiliser, ordnance, petroleum, sewage, pathogens and radioactive material) have potential to be released by cyber actors for destructive ends. Insurers all have long experience of non-cyber-related substance leaks causing contamination and significant business interruption, and are well aware how catastrophically destructive this sort of environmental damage can be, both to people and landscapes.

   One of the first recorded cyber physical attacks took place in Maroochy Shire, Australia, where raw sewage was deliberately released into residential drains.

   Cyber actors could gain remote access to instrumentation and control systems and force leaks and/or build-ups of toxic materials, producing explosion risks within storage spaces. Explosions and fires around hazardous materials create significant physical damage and have a direct impact on the surrounding environment.

5. **Kinetic vehicle**

   Airports, commercial airliners, ports, and major sea vessels have been hijack targets for geopolitical extremists since the mid-20th century. A digital attack on a plane's systems, air traffic control, radars or GPS would require a high level of engineering expertise but may be plausible. Certain factors could not be controlled in a digital plane hijack, such as the impact target. The ultimate level of damage to a vessel in motion would be subject to more factors than a cyber actor is able to control remotely.

6. **Remotely powered vehicles**

   Modern automobiles consist of multiple computer components called Electronic Control Units (ECUs), which might be used for a cyber physical attack scenario. This scenario assumes an attacker gains remote access to an internal automotive network and compromises a safety-critical ECU. Remote exploitation of a vehicle is, however, very complicated and would require significant expertise and range of access.

7. **Pipeline energy sources**

   Geopolitical actors have long shown interest in critical infrastructures as targets for traditional attacks as well as cyber ones. A plausible scenario may involve a threat actor digitally compromising a compressor's station to increase the pressure of natural gas flowing through a pipeline.[6] Such an attack may affect the internal pipeline coating and lead to a rupture, causing physical and environmental damage. A similar attack occurred in 2008 when hackers targeted an oil pipeline in Turkey, causing a significant explosion.

6 (Wadhawan and Neuman 2016)

Physical cyber risk

8. **Explosive material**

   Explosive materials can be combusted via digital means. There is a long history of explosions of natural gas and fissile materials stored at industrial facilities. Hacking into the SCADA systems used to control and monitor flammable gases stored at major sites would give cyber attackers the ability to create such an explosion, and while this type of attack is more likely to occur within the oil and gas and chemical industries, warehouse fissile materials may also be vulnerable.

   Scenarios in which heating, ventilation, or air conditioning (HVAC) systems are compromised, creating conditions in which server farms overheat and start fires, or in which buildings become otherwise hazardous to life, also fall into this category.

9. **Widespread flooding**

   Water is a powerful energy force and deliberate leaks can pose a significant risk to human life, machinery and materials and business continuity. In countries where water is scarce and allocation a political issue, the deliberate leak or contamination of water reserves could also prove a potent attack. By over-riding pumps and flow management systems, actors would also be able to flood vital facilities, rendering them either dangerous or unusable until drained and dried.

10. **Infrastructure outage**

    Depending on the make-up of the local energy grid, some countries may be far more vulnerable to this threat than others. A cyber attack which causes a power outage may not be directly damaging to any critical national infrastructure (although it also may be destructive to these assets) but will cause a level of disruption that will almost certainly be highly economically damaging.

    We must also consider the interruption of energy via digital manipulation as another form of destructive cyber physical attack, simply because continuous electric power is vital to businesses and lives. This forced shutdown of critical national infrastructure also extends to the significant disruption of emergency services, communications, healthcare, or other systems and this may lead to death and injury.

Table 2 below outlines a qualitative assessment of how different business sectors could be exposed to a cyber attack from the factors listed previously. It aims to demonstrate where a targeted or systemic attack could cause physical damage, threaten the environment or put human lives in danger.

Table 2: The exposure of different industry sectors to cyber attacks targeting embedded fuel and/or energy sources

	Industry											
Embedded fuel/energy source targeted	Energy	Materials	Industrials	Consumer discretionary	Consumer staples	Health care	Financials	Information technology	Communication services	Utilities	Real estate	Total
Lithium batteries	1	1	1	1	0	1	1	1	1	1	1	10
Fuel for boilers	1	1	1	1	0	1	1	1	1	1	1	10
Machinery energy	1	1	1	1	0	1	0	0	1	1	0	7
Hazardous materials	1	1	1	0	0	0	0	0	0	1	0	4
Kinetic vehicle	1	1	1	0	0	0	0	1	1	0	1	6
Remotely powered vehicles	0	1	1	1	0	0	0	0	0	1	0	4
Pipeline energy source	1	1	1	1	0	0	0	0	0	1	0	5
Explosive material	1	1	1	0	0	0	0	0	0	1	0	4
Widespread flooding	0	0	0	1	1	1	1	1	1	0	1	7
Infrastructure outage	1	1	1	1	1	1	1	1	1	1	1	11
Total	8	9	9	7	2	5	4	5	6	8	5	

1	Attack mode applies to the industry
0	Attack mode does not apply to the industry

Cyber physical scenarios

Cyber physical scenarios

Developing hypothetical scenarios can be a useful tool for managing uncertainty, especially for risks that are not well understood.

They can help with contingency plan development or the testing of mitigation strategies, for example through wargaming exercises or workshops among senior staff. This understanding can be applied to help with decision making about the future, and facilitate the reporting, management, and mitigation of risks.

The scenarios described here demonstrate plausible circumstances in which deterrents may fail, leading to an escalation of the threat landscape. The circumstances described in each scenario involve major cyber actors but also consider the roles that smaller, developing states or other groups such as activists or terrorists may play in contributing to physical cyber disruption.

A note on tiering cyber powers

For the purposes of these scenarios, the countries are given the names of planets in the solar system. Adopting the International Institute for Strategic Studies (IISS) new methodology for assessing cyber power, we identify three broad categories or 'tiers' of cyber operations through which to discuss geopolitical tensions and escalations.[7]

Countries in these tiers are assessed across in seven categories of cyber capability:

i) Strategy and doctrine,
ii) Governance, command and control,
iii) Core cyber-intelligence capability,
iv) Cyber empowerment and dependence,
v) Cyber security and resilience,
vi) Global leadership in cyberspace affairs,
vii) Offensive cyber capability.

Tiers allow for the anonymous discussion of the impacts of nations or other groups engaging in cyber conflict and other geopolitical statecraft.

– **Tier 1:** are world-leading strengths in all the categories in the methodology
– **Tier 2:** are world-leading strengths in some of the categories
– **Tier 3:** have strengths or potential strengths in some of the categories but significant weaknesses in others

There are weaknesses among Tier 2, and even Tier 1, countries as well, but they are minor when compared with the significant weaknesses of Tier 3 states.

7 International Institute for Strategic Studies. (2021). Cyber Capabilities and National Power: A Net Assessment. Available at: https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power

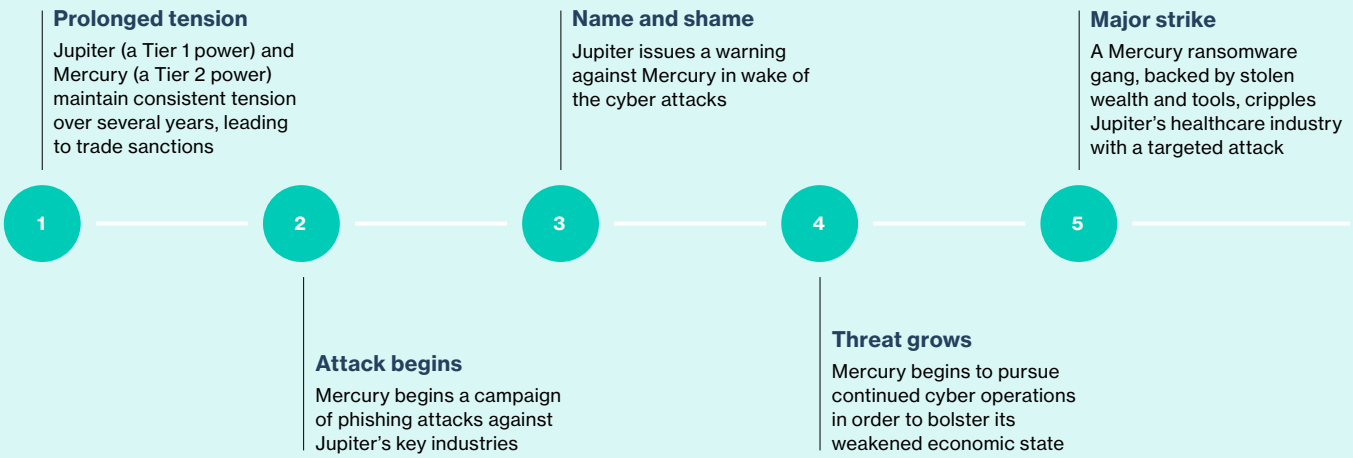
Cyber physical scenarios

Scenario 1 – Asymmetric Attack Exchange: Ransomware on critical infrastructure (Tier 1 vs. Tier 3)

Overview

The target of trade and financial sanctions imposed by Jupiter (a Tier 1 cyber power), Mercury (a Tier 3 cyber power) encourages ransomware operations from criminal actors operating out of its national borders as a means to raise funds while also disrupting its regional rivalry under conditions of plausible deniability. The resulting wave of ransomware attacks strikes Jupiter's healthcare network, causing massive disruption.

Scenario 1



Type of threat	Ransomware on critical infrastructure
Geopolitical framework	Asymmetric geopolitical confrontation
Cyber powers	Tier 1 vs. Tier 3
Trigger	Trade sanctions
Conflict dynamics	Asymmetric warfare strategy through proxies
Threat actor	Cybercriminal group backed by Mercury
Intent	Financial gain / disruption
Target	Healthcare infrastructure
Type of cyber attack	Ransomware
Impact	Operational disruption, ransom payment, health risk
Likelihood	Very likely
Historical precedents	WannaCry (2017); UHS ransomware (2020); HSE ransomware (2021)

Cyber physical scenarios

Scenario narrative

On the back of increasing geopolitical tensions between Jupiter and its regional rival Mercury, the former introduces a series of sanctions against the latter, significantly harming its ability to channel funds for various state-run projects. Shortly after, Jupiter's intelligence agency begins to notice an increase in phishing attacks originating from Mercury and targeting organisations within its borders and in the broader region.

Committed to its well-established name-and-shame policy, Jupiter issues a public announcement accusing Mercury of increased malicious cyber activity along with a warning.

Undeterred, Mercury continues to target its more advanced regional rival through its dedicated cyber teams, which are known to the international intelligence community and classified as advanced persistent threats (APTs). Most importantly, as a way to get around Jupiter's sanctions, Mercury starts relying on cyber attacks to bolster its own economic development by stealing intellectual property and by illicitly collecting money to raise funds and gain access to otherwise unavailable hard currency. It relies on state-sponsored proxies to operate in a regime of plausible deniability and avoid new public accusations. Mercury's government thus turns a blind eye towards cyber attacks carried out by cybercriminals operating out of its domestic borders and actively encourages operations against its rival state.

A fresh wave of ransomware attacks strikes government and private sector's organisations across Jupiter's territory, costing millions in ransom payments and causing widespread disruption to business operations. One of these attacks sees ransomware propagate through the country's hospital network and other key medical infrastructure in the region, causing massive disruption. An attack from a notorious cybercriminal gang operating out of Mercury's borders hits one of the largest providers of hospital and healthcare services in Jupiter and ripples through its 100+ hospitals and clinics, significantly crippling digital services and impacting facilities around the country. In just a matter of days, dozens of health care providers have to reschedule appointments, delay procedures, and even halt operations altogether transferring patients to other facilities.

In its most extreme instances, the network outage leads to a breakdown of emergency care units and major parts of hospitals' infrastructure. Areas of critical patient treatment like operating rooms, emergency departments, intermediate and intensive care areas are down, causing serious risks of harm, or even death, for patients who depend on such medical equipment to be working correctly.

Impacts and insurance lines triggered

As the ransomware quickly slips through hundreds of servers and thousands of devices used to treat hospital patients across Jupiter, the targeted healthcare organisation's IT department responds to the spreading infection by suspending user access to information technology applications needed to operate, and personnel find themselves essentially unable to treat patients and forced to halt operations altogether. All urgent surgical cases and all radiology appointments are cancelled, and several emergency room patients are moved to nearby facilities. On top of this, the healthcare provider is forced to pay the ransom, amounting to several hundred million US dollars in local currency.

Cyber physical scenarios

In this case, certain insurance policy classes see greater exposure than others. Cyber claims are high, but there are also substantial property, casualty and liability losses attributed to the attacks on healthcare and hospital networks. Not only does the disruption lead to delays in medical treatments and an inability to provide care, but networks must be repaired, restored, patched or replaced in the wake of the attack. In the years following the scenario, security and political risks are higher in the area due to ongoing tensions between the two nations.

The table below illustrates the potential claims increase across the insurance industry for major policy classes over the short to mid-term following the scenario narrative.

Policy class	Claims increase from scenario
Commercial	
– Property	**Medium**
– Non-property	**Low**
Marine	**Low**
Energy	**Low**
Aviation	**Low**
Casualty and liability	**Medium**
Cyber	**High**
Surety	**Low**
Security and political risk	**Medium**

Likelihood and historical precedents

This is an extremely likely scenario. Even if actors do not actively intend to target critical infrastructure, the reliance on semi-independent profit-minded criminal groups coupled with the indiscriminate nature of ransomware makes avoiding such targets challenging. When governments use cybercrime as an asymmetrical warfare tool (i.e. as a way to level the playing field against more powerful adversaries while shielding behind difficulties in attributing the attacks) to achieve their strategic goals, critical infrastructure – including hospitals – may easily become collateral damage.

This is coupled by ransomware's increased sophistication and growing effectiveness rate. In fact, ransomware accounted for the vast majority of the successful cyber attacks on health care organisations in the years immediately after the WannaCry incident – even though hospitals were on high alert for ransomware, and many were making changes to strengthen their defences against it. This clearly signals the sector's vulnerability to the threat.[8]

When the WannaCry ransomware hit organisations around the world in May 2017, hospitals and GP surgeries across the UK were particularly badly affected. A significant number of services were disrupted as malware encrypted computers used by NHS trusts, forcing thousands of appointments to be cancelled and patients to be dismissed or transferred.[9]

8 2019 Verizon Breach Report. (2019). Available at: https://www.verizon.com/business/resources/reports/dbir/2019/healthcare/

9 National Audit Office. (2017). Investigation: WannaCry cyber attack and the NHS. Available at: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.

Cyber physical scenarios

Healthcare organisations have remained a cybercriminal favourite ever since, but the trend was further reinforced at the height of the COVID-19 outbreak in 2020, when phishing emails and other cyber attacks on hospitals increased, with cyber criminals seeing the pandemic as an opportunity to exploit and draw profit.[10]

But patient diversions are not the most worrying aspect of this type of attack. In September 2020, a ransomware attack at a Dusseldorf University hospital in Germany resulted in emergency-room diversions to other hospitals which, according to a report by the Ministry of Justice of the State North Rhine-Westphalia, resulted in the death of a patient who had to be taken to a more distant hospital in Wuppertal because of the attack on the clinic's servers.[11]

Due to renewed attention from governments and public authorities, several ransomware gangs eventually pledged not to hit hospitals during the COVID-19 pandemic while others committed not to target critical sectors at all.[12] Nonetheless, incidents of ransomware attacks against critical infrastructure, and in particular hospitals, have still skyrocketed in the past two years.[13]

In 2021, Ireland's public Health Service (HSE) was forced to shut down its IT infrastructure after hackers demanded $20 million to regain access to its network following a major ransomware attack. The resulting disruption meant that hospitals and treatment clinics had extremely limited access to the Irish health system's IT infrastructure for days, forcing staff to resort to handwritten notes as they were unable to access patient records.[14]

10 De Cauwer, H., & Somville, F. (2021). Health Care Organisations: Soft Target during COVID-19 Pandemic. Prehospital and Disaster Medicine, 36(3), 344-347. doi:10.1017/S1049023X2100025X.

11 Associated Press. (2020). German hospital hacked; patient taken to another city dies. Available at: https://apnews.com/article/technology-hacking-europe-cf8f8eee1adcec69bcc864f2c4308c94.

12 Recorded Future. (2021). BlackMatter ransomware targets companies with revenue of $100 million and more. Available at: https://therecord.media/blackmatter-ransomware-targets-companies-with-revenues-of-100-million-and-more/.

13 Health IT Security. (2021). Ransomware Keeps Healthcare in Crosshairs, Triple Extortion Emerges. Available at: https://healthitsecurity.com/news/ransomware-attacks-surge-102-in-2021-as-triple-extortion-emerges.

14 Ireland's public Health Service. (2021). HSE publishes independent report on Conti cyber attack. Available at: https://www.hse.ie/eng/services/news/media/pressrel/hse-publishes-independent-report-on-conti-cyber-attack.html.

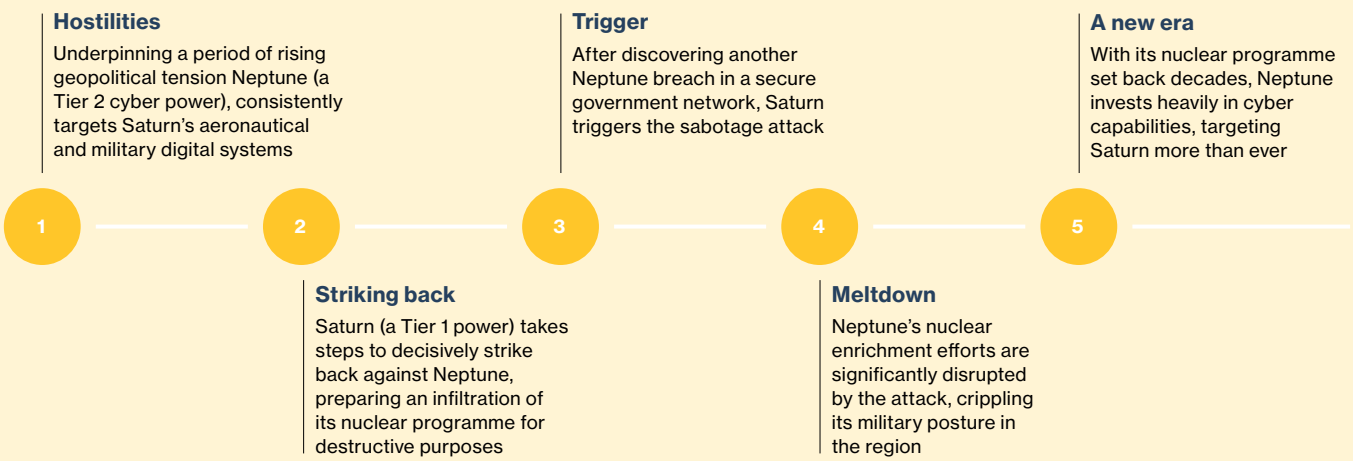
Cyber physical scenarios

Scenario 2 – Offensive Cyber Retaliation: Cyber-physical sabotage of critical infrastructure (Tier 1 vs. Tier 2)

Overview

Saturn (a Tier 1 cyber power) discovers yet another breach in its government networks attributed to its regional rival, Neptune (a Tier 2 cyber power), one that its intelligence traces back to a well-known Neptune-backed APT. Several months later, as part of its new strategic doctrine for cyber operations, Saturn counters by sabotaging a nuclear facility in Neptune's territory. Without any great strategic power to wield in response, Neptune cyber groups prioritise the targeting of Saturn businesses over the next decade.

Scenario 2



Type of threat	Cyber-physical sabotage of critical infrastructure
Geopolitical framework	Regional geopolitical rivalry
Cyber powers	Tier 1 vs. Tier 2
Trigger	Offensive cyber operation
Conflict dynamics	Retaliatory action
Threat actor	Military cyber force
Intent	Sabotage
Target	Nuclear plant
Type of cyber attack	Sophisticated targeted attack on industrial networks
Impacts	Operational shutdowns, damaged equipment, financial loss
Likelihood	Somewhat likely
Historical precedents	Stuxnet (2010); Shamoon (2012); Second Natanz attack (2021)

Cyber physical scenarios

Scenario narrative

Following years of escalating geopolitical tensions with Neptune, and countless cyber espionage attacks, Saturn goes on the offensive and puts into practice a shift in its national cyber security strategy, which allows the use of offensive cyber operations in response to security challenges and concerns in the cyber space. Compared to the previous more passive and reactive responses to Neptune's intrusions, Saturn now decides to counter its adversary's latest campaign with a more coercive response, one that targets the heart of its strategic concerns about Neptune and the main reason for the two countries' hostile relationship – Neptune's nuclear programme.

Several weeks after a defence contractor discovers a breach in its secure data network which is attributed to a notorious Neptune-backed APT (advanced persistent threat), Saturn's newly established offensive hacking unit receives the green light to launch a cyber-sabotage operation against a nuclear enrichment facility in Neptune's territory. Following months of preparation, an insider disguised as a contracting worker hired to carry out routine maintenance work at the plant manages to get physical access to the isolated Industrial Control System (ICS) network. The insider succeeds in manually injecting a customised malware directly into the operational network with a flash drive and getting around the 'air gap'.

The effects of the attack are extremely costly, with the malware – designed to target the plant's specific control systems – leading to a failure of control mechanisms and to the destruction of key physical components. The operation does not cause a catastrophic chain effect but produces a significant disruption in Neptune's enrichment efforts. Officials are forced to investigate the incidents, repair the damage, and make substantial safety adjustments, which considerably slows down the country's nuclear program. Without any great strategic power to wield in response, Neptune's reaction is gradual but determined. The government scales up its investment into building cyber offensive capabilities and its hacking groups prioritise the targeting of Saturn organisations over the next decade.

Impacts and insurance lines triggered

The cyber-sabotage operation is extremely complicated, especially given the hurdles of coordinating action behind enemy lines, but Saturn manages to successfully leverage its very advanced cyber, intelligence, and military capabilities to accomplish the mission. While the attack takes significant time and resources to develop and deploy, however, Neptune's losses are estimated within a few million USD range. The attack does not result in a blast or fire, but several key components at the nuclear plant are severely damaged and all operations are temporarily brought to a standstill. Moreover, the removal of the malware from the plant's system proves a lengthy and challenging process, further delaying the resumption of activities.

On the other hand, given Neptune's limited capabilities, retaliation is gradual and stretches over the following years. Neptune's government scales up its investment into building cyber offensive capabilities and its hacking groups and proxies start prioritising the targeting of Saturn businesses for the next decade. This results in dozens, if not hundreds, of organisations being disrupted by a myriad of attacks and having to invest significant resources into raising their cyber defences.

Cyber physical scenarios

The scenario contributes to added risk and increased claims in a number of major lines of insurance business. Cyber claims are high following the scenario, particularly in light of the new level of risk in the digital landscape between the two countries as well as in allied countries who may engage or influence the state of continued hostilities. Additionally, commercial lines are highly exposed to the increase in cyber attacks which contribute to disruption to intangible assets, necessitate the replacement of networks or technology, and possible physical damage which may result from the scenario. Given the nature of the attack on Neptune's nuclear programme, energy lines, as well as liability and casualty are at high risk of clash in this scenario.

The table below demonstrates the claims increase across major policy classes for the short to mid-term following the scenario narrative.

Policy class	Claims increase from scenario
Commercial	
– Property	Medium
– Non-property	High
Marine	Low
Energy	Medium
Aviation	Low
Casualty and liability	Medium
Cyber	High
Surety	Low
Security and political risk	Low

Likelihood and historical precedents

This is a relatively likely scenario. Nuclear proliferation continues to be one of the main concerns for the international community, and some developing economies pursue nuclear weapons development as a means of increasing their international profile. As this occurs, other states may increase their efforts to prevent them doing so. Cyber offers a very effective tool to pursue this goal, causing as much harm as conventional warfare or sabotage, while offering a veil of anonymity and plausible deniability. In fact, sophisticated cyber-sabotage operations at nuclear facilities are nothing new, the 2010 Stuxnet attack being the prime example.

The Stuxnet attack, also known as Operation Olympic Games, hit the Iranian uranium enrichment facility at Natanz – where the Iranian regime was suspected to be developing nuclear weapons. Stuxnet was a cyber-sabotage operation that ran between 2009 to 2010, which many traced back to the United States and Israel. Stuxnet was a sophisticated computer worm, specifically designed to infiltrate Iranian industrial computers running Siemens Step 7 software via zero-day exploits. When injected into operational networks at Natanz, Stuxnet infected the plant's industrial computers and covertly sabotaged the Supervisory Control and Data Acquisition (SCADA) systems by manipulating the control of the valves that pumped uranium gas into centrifuges in the reactors and causing overheating and serious damage.[15]

15 De Falco, M. (2012). Stuxnet facts report: A technical and strategic analysis. NATO Cooperative Cyber Defense Centre of Excellence.

Cyber physical scenarios

Natanz was again the target of suspected foreign state-sponsored cyber-sabotage in April 2021, when the site experienced a power blackout and, reportedly, an explosion.[16] But Iran's uranium enrichment facility in Natanz is far from being the only target. According to the Nuclear Threat Initiative (NTI), at least 23 publicly disclosed cyber incidents have occurred at nuclear facilities around the world since 1990.[17]

When it comes to potential retaliatory actions, Stuxnet again offers a good case study. Iran's response to the 2010 massive cyber attack on its nuclear facilities was essentially to slowly but steadily ramp up its cyber capabilities and transform itself from a 'Tier 3' country to a vastly more capable cyber actor in the years after. Iranian cyber groups are suspected to have conducted a series of retaliatory attacks against United States and Israeli targets as well as against organisations in neighbouring countries perceived as regional rivals.

16 The New York Times. (2021). Blackout Hits Iran Nuclear Site in What Appears to Be Israeli Sabotage. Available at: https://www.nytimes.com/2021/04/11/world/middleeast/iran-nuclear-natanz.html.

17 Van Dine, A., Assante, M., Stoutland, P., & Nunn, S. (2016). Outpacing cyber threats: Priorities for cybersecurity at nuclear facilities. Nuclear Threat Initiative.

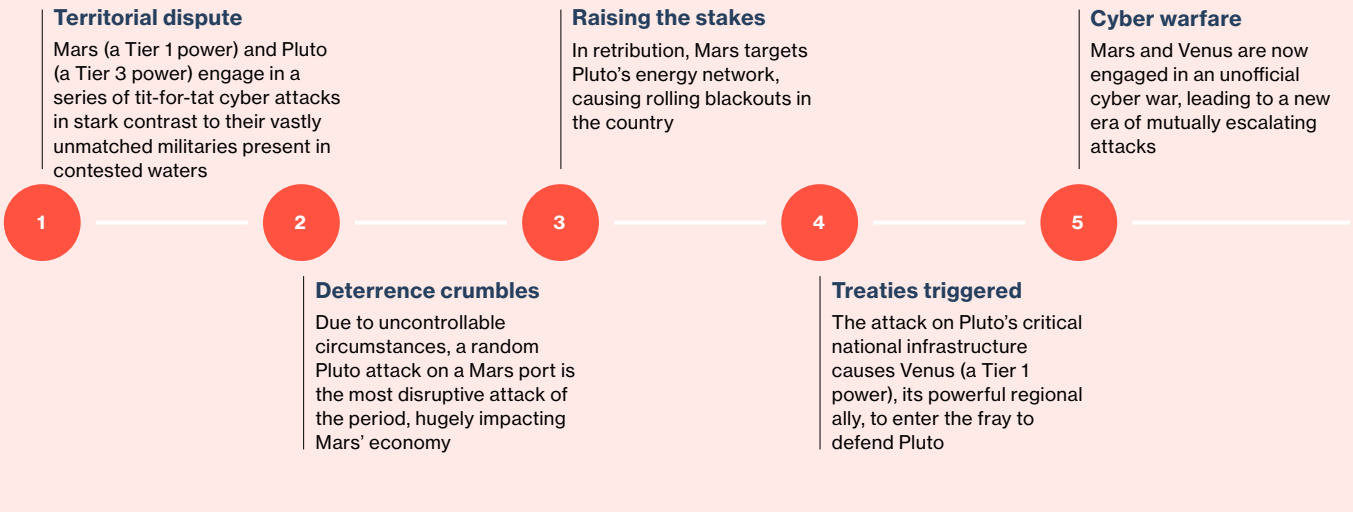
Cyber physical scenarios

Scenario 3 – Symmetric Attack Exchange: Escalation of destructive attacks on critical infrastructure (Tier 1 vs. Tier 1)

Overview

Following a flare up in tensions in the region, hackers backed by Mars (a Tier 1 cyber power) carry out a series of fleeting but disruptive attacks on Tier 3 cyber power Pluto's critical infrastructure, and Pluto retaliates in equal measure. The escalation of attacks triggers the intervention of Venus (another Tier 1 cyber power) in support of its strategic ally, Pluto. A series of tit-for-tat cyber offenses culminates in a destructive attack on Venus's industrial plant network, which causes significant environmental damage.

Scenario 3



Scenario narrative

As geopolitical tensions escalate in contested waters amid competing exclusive economic zone claims between regional rivals, state-sponsor cyber groups backed by emerging regional and global power Mars carry out a series of fleeting but disruptive attacks against the telecommunications infrastructure of aspirational regional middle power Pluto – against which it holds maritime and territorial claims. The attacks, range from disguised ransomware operations, to distributed denial-of-service (DDoS) attacks, to data thefts and leakages, all forcing affected companies to temporarily suspend operations and shut down critical services that consumers and businesses rely on, causing far-reaching disruption.

Once they have established the origin of the attacks, Pluto's modest but rapidly developing cyber collective counters by launching sustained DDoS attacks on a Mars port-management network. Flooding and overwhelming one of the country's busiest shipping terminal port's networks with fake traffic from multiple sources, the attack overloads operational technology (OT) systems and prevents operations from being safely fulfilled. This keeps cargo movement on hold for hours and significantly disrupts operations.

Cyber physical scenarios

Type of threat	Escalation of destructive attacks on critical infrastructure
Geopolitical framework	Great power rivalry
Cyber powers	Tier 1 vs. Tier 1
Trigger	Intervention in support of strategic ally
Conflict dynamics	Escalatory spiral
Threat actor	State-sponsored APTs
Intent	Disruption / destruction
Target	Telecoms, port, energy distribution network, industrial plant
Type of cyber attack	Ransomware, DDoS attacks, disruptive and destructive attacks on ICS
Impacts	Service interruption, operational shutdowns, damaged equipment, business interruption, environmental degradation, health and safety risks
Likelihood	Very unlikely
Historical precedents	Israel vs. Iran cyber conflict (2020 - present)

In retaliation, Mars significantly raises the stakes and targets Pluto's energy distribution network. This causes considerable disturbance in the power grid as well as rolling blackouts. After gaining side-access to a major regional electricity distribution company's network, attackers compromise substations and manipulate the power fed into the grid to cause a system-wide blackout that hits both distribution and transmission. Disruption is massive, with hundreds of thousands of consumers suffering from temporary power outages across parts of the country.

The escalation of attacks against their strategic ally, Pluto combines with Mars's push into disputed maritime territory and forces Venus, another developed regional power, to become invovled in the conflict. A series of tit-for-tat cyber offences from both sides eventually culminates in a destructive attack on Venus's industrial plant network. Although protected by best-practice industrial security, sophisticated attackers manage to compromise the industrial site's network by luring support technicians through targeted phishing emails and infecting their machines with a custom remote access trojan (RAT) malware that gives them remote control of industrial operations while evading anti-virus systems. Using this, the attackers purposedly mis-operate the physical process causing an environmental disaster through a discharge of toxic materials.

Impacts and insurance lines triggered

This scenario sees a succession of different attacks of intensifying scope, sophistication, and impact. The series of disruptive attacks on telecommunications have significant and far-reaching impacts. When companies shut down critical services that consumers and businesses rely on, an attack can quickly affect millions of users, seriously disrupting business and everyday activities. In comparison, the second attack – targeting a port management company network – has far less widespread implications, but carries significantly more serious security risks. As port management becomes an increasingly digitised activity, operations such as autonomous straddle carriers, remote mooring line monitoring and computerised cargo planning cannot be carried out when systems are down. Depending on the size of the port and its daily traffic, the consequences of a DDoS attack may be dire. In 2019, our report *Shen attack: cyber risk in the Asia Pacific ports* highlighted that a single cyber attack on major Asia-Pacific ports could cost about the same as half of global losses from natural catastrophes (about $110 billion).

Cyber physical scenarios

The third attack considered above is by far the most disruptive of all. The consequences of a cyber attack on an active power grid could be disastrous, well beyond just the cost of repairing the immediate damage, because of the disruption to homes, businesses, and services – which all rely on electricity. Finally, the consequences of a cyber-enabled environmental disaster may be incalculable as, besides costly equipment damage and lost production, this would imply public safety risks and possible loss of life.

The scenario's events describe a step-change in the visibility, frequency, and severity of cyber risks to multinationals and critical national infrastructure. This results in a high degree of clash risk, because the increasing level of attacks affects a high number of lines at once, including marine, energy, security, and commercial property and non-property lines.

Policy class	Claims increase from scenario
Commercial	
– Property	**High**
– Non-property	**Medium**
Marine	**Medium**
Energy	**High**
Aviation	**Low**
Casualty and liability	**Medium**
Cyber	**High**
Surety	**Low**
Security and political risk	**High**

Likelihood and historical precedents

An escalatory cyber physical scenario is plausible, although less likely than other types of attack. Sophisticated state-sponsored attacks targeting the industrial control systems (ICS) of adversary nations have occurred occasionally in recent years. These have sometimes resulted in widespread economic and societal disruption but very rarely led to physical damage or destruction. When the stakes are so high, especially within a framework of already escalating geopolitical tensions, these kinds of attack are likely to trigger retaliation and – depending on the capabilities of the actors involved – may lead to similar, if not greater, revenge attacks. This, of course, acts as an important deterrent.

Currently, similar operations require a high level of cyber-sophistication but recent examples show that Tier 2 and Tier 1 cyber powers are capable of attacks targeting Supervisory Control and Data Acquisition (SCADA) systems controlling how power, water, nuclear, manufacturing, and oil and gas are managed and distributed. Attacks on Critical National Infrastructure (CNI) have long been considered cyber worst-case scenarios because of the severity of the disruption that can be caused, which makes CNI a particularly attractive target for everyone from state-backed hackers to terrorists. Meanwhile, the sophistication needed to target ICS is becoming increasingly accessible to less technical actors as the knowledge spreads about how to execute these attacks.

Cyber physical scenarios

In 2021, most attacks on industrial systems were simple ransomware-based extortions, although these were still able to cause widespread disruption and millions worth of economic losses.[18]

In addition to increasingly sophisticated attack capabilities, changing expectations have also increased the risk to critical infrastructure. Organisations increasingly embrace digitisation, including converging IT with Operational Technology (OT) and leveraging cloud and Industrial Internet of Things (IIoT) technologies. This creates an increased number of access paths into a company's operational technology. Meanwhile, the pandemic forced many organisations to quickly enable remote access for their OT personnel, and as a result, operational technology environments also became more exposed to increasingly sophisticated remote cyber threats.

Overall, destructive attacks on critical national infrastructure that could bring about serious physical consequences are more than possible. The controlling element that does most to avert them is actors' awareness of the potential consequences. Such constraint, however, does not seem to apply to hard-to-deter actors (such as terrorist organisations) or in a case of escalatory dynamics spiralling out of control.

18 Forbes. (2021). Turning Up The Heat: A Ransomware Attack On Critical Infrastructure Is A Nightmare Scenario. Available at: https://www.forbes.com/sites/forbestechcouncil/2021/07/20/turning-up-the-heat-a-ransomware-attack-on-critical-infrastructure-is-a-nightmare-scenario/?sh=4911f2981da0.

Insurance solutions

Insurance solutions

Cyber insurance today

Cyber insurance remains a relatively immature although still-growing market in most industrialised countries.

As the cyber threat has grown more tangible and impactful, risk holders have adapted to the circumstances. Demand for cover has grown, as have the number of increasingly specialist policies as the industry has responded. Despite this, insurance penetration remains low even in industrialised countries, with the OECD estimating that the share of global cyber losses that are uninsured is likely above 70% and potentially high as 85% to 90% of all cyber losses incurred.[19]

There are around 20 different types of cover for cyber losses currently available in the global insurance market, amounting to around $6 billion in total affirmative cover. Around 20% of this is insured at Lloyd's. The vast majority of cyber products provide cover for triggers such as data exfiltration, contagious malware, distributed denial of service, and financial thefts, but specifications differ from market to market. Key loss processes may also include the failure of counterparties, or of suppliers who rely on networked systems and are vulnerable to outages and software failures. These account for roughly 90% of all business damage as a result of cyber attack, technological failure, and other malicious digital interference.[20]

Cyber physical insurance

The vast majority of cyber losses, and thus the protection provided by most coverages, concern non-physical damage and disruption. The existing market for cyber physical insurance is small and specialised. Cover for physical asset damage may either be purchased be purchased as part of an inclusive cyber policy or considered as a 'silent' cyber coverage. Lloyd's does not support the provision of silent cyber and cover now needs to be purchased separately in most markets. It is now more likely that customers are not covered unless they have bought affirmative cover.

Most cyber policies specifically exclude cover for physical damage and related business interruption (BI) stemming from digital interference. In recent years, however, some insurers have developed specialty, or 'enhanced' coverage types for physical damage from cyber triggers, which are marketed directly to technology or manufacturing firms. These coverages have strict limits and only apply to first parties, meaning that contingent business interruption (CBI) provisions are not made. Notably, the limits for these policies are much higher than typical cyber policies applied to non-physical impacts, reflecting insurers' understanding that attacks on these systems are far less likely but much more severe.

In the case of a cyber physical attack on a key piece of machinery, like a hydropower turbine or a power grid transformer, there may be no protection for firms indirectly affected by disruption. There are also no specific insurance provisions for bodily injuries or deaths caused by cyber attacks.

19 https://www.oecd.org/daf/fin/insurance/Enhancing-financial-protection-against-catastrophe-risks.pdf

20 Cambridge Centre for Risk Studies 2019

Insurance solutions

Key considerations for insurers

Affirmative and non-affirmative cyber physical cover
Cyber insurance policies are either "affirmative" – meaning they explicitly cover cyber risk and specific losses associated – or "non-affirmative", meaning coverage is non-explicit.

Another term for non-affirmative cover, "silent cyber" refers to the ambiguous coverage for cyber attacks in pre-existing policies and is an issue of unknown exposure for insurers. It is particularly relevant in aviation, aerospace, transport, marine and property lines, where business interruption losses or physical damage resulting from digital interference may be claimed under traditional, all-risk policies. While property and contents damage insurance may not specifically exclude cyber as a trigger, the lack of specificity can leave businesses exposed in scenarios like those described in this report. This "silent" exposure also has the potential to aggregate significantly. Policies with no explicit exclusion, an implicit coverage grant, or where language was ambiguous could be triggered by losses.

Insurers should therefore monitor product coverages carefully across classes for relevance to the cyber-physical peril. This requires an active strategy to consider different potential cyber physical scenarios, and where the losses may fall from these. As part of this, attaining coverage clarity across traditional classes is key.

Lloyd's and global regulators are therefore aligned in their goal to safeguard the sustainability of the insurance market by requiring contract certainty for clients and driving innovation of new cyber products to fill the evolving needs of clients. In 2019, Lloyd's issued requirements for all managing agents to review policy wordings to make clear statements of affirmed or excluded cyber cover by mid-2021. This process has reduced ambiguity over "silent cyber" coverages in the Lloyd's market, limiting industry exposure and clarifying levels of cover to customers. There is therefore now an opportunity to develop bespoke insurance products for the industries and businesses most at risk from cyber physical disruption and destruction.

Cyber terrorism

In 2018, the US Terrorism Reinsurance Act (TRIA) was updated to clarify that standalone cyber insurance policies classed under cyber liability codes would be considered valid "property and casualty insurance" under the stipulations of the act. In the UK, the national terrorism reinsurer, Pool Re, began to extend cover to include physical damage, direct business interruption and non-damage business interruption for policyholders from 2018 onwards – thus providing protection from acts of physically damaging cyber terrorism.

These provisions have triggered a wider conversation in global terrorism pools over how to assess and mitigate the risk from non-state cyber activity, given the scale of potential impacts from a systemic physical cyber event or a targeted attack against critical national infrastructure. The challenge is that the triggering of a relevant clause or wording around, for example, a "cyber-terrorist" event, is highly dependent on the confident attribution of an attack. This can only rarely be determined. In many cases, official attribution may never be made because of the geopolitical repercussions of identifying a specific state or actor as responsible for the damage.

As the cyber class matures, it is likely that the coverage in place on insurance policies will be limited by increasingly sophisticated exclusions of acts of war and systemic risk, with cover bought back separately where there is appetite. This approach is important to ensure that aggregate risks are properly understood, controlled, and priced for, and that customers are clear about what risk they will be protected for and what risk they will retain.

Insurance solutions

Cyber ‘catastrophes’

The insurance industry has yet to encounter a truly catastrophic cyber attack – that is, an event which triggers claims across multiple policies or lines of business. Cyber has a short history, and so far there have been no stand-out loss events stemming from a single trigger. The threat is also fast-evolving, which means that historic trends are sometimes not always useful for predicting the pattern of future shocks.

With all that said, all parties really do need to plan for the realities of a cyber catastrophe before any real world examples occur. This is not just because of the impact on human lives, but also to ensure capital is in place to manage and fund the rebuilding of the infrastructure, companies and national organisations that could be damaged.

Whilst an imminent mass-scale cyberphysical attack may be unlikely, the threat is evolving very rapidly. Precedents strongly point to continual targeting of strategic industrial sectors, as described in this report. Risk managers and insurers should review the ways in which industries and multinationals have been susceptible to strategic disruption or other forms of political reprisal in the past. They can, at least in part, use this to understand their insureds’ vulnerability to sophisticated cyber disruption and damage in future.

Those states which maintain long-running tensions and competition with other states are, for instance, at far higher risk of cyber attacks affecting their critical infrastructure than those which do not. A review of the geopolitical risk landscape will help risk managers to gain clarity on possible sources of the next major cyber event to threaten national economies.

Scenarios like the ones detailed in this report provide a powerful tool for insurers and risk owners looking for data on potential cyber physical attacks and the findings of this report can be used to aid the development of bespoke qualitative and quantitatively imagined hypothetical scenarios to assess potential upper limits for massive loss events stemming from cyber attacks.

The relative increase in claims across the insurance industry by class of business under each of the scenarios described in this report is summarised in the following table. As part of a risk mitigation strategy, insurers also need to monitor the correlation potential, which could be a particular concern for portfolios with concentrations of comparable large industrial risks. Removing ambiguity over silent cyber cover, as required at Lloyd’s, can also help insurers appropriately assess and manage potential losses.

Insurance solutions

Anticipated claims impact of the three cyber physical scenarios described in this report, by class of business

	Scenario 1 Asymmetric Attack Exchange: Ransomware on critical infrastructure (Tier 1 vs. Tier 3)	**Scenario 2** Offensive Cyber Retaliation: Cyber-physical sabotage of critical infrastructure (Tier 1 vs. Tier 2)	**Scenario 3** Symmetric Attack Exchange: Escalation of destructive attacks on critical infrastructure (Tier 1 vs. Tier 1)
Commercial			
– Property	**Medium**	**Medium**	**High**
– Non-property	**Low**	**High**	**Medium**
Marine	**Low**	**Low**	**Medium**
Energy	**Low**	**Medium**	**High**
Aviation	**Low**	**Low**	**Low**
Casualty and liability	**Medium**	**Medium**	**Medium**
Cyber	**High**	**High**	**High**
Surety	**Low**	**Low**	**Low**
Security and political risk	**Medium**	**Low**	**High**

Many scenarios have already been developed to help quantify the likely maximum losses for types of cyber attack. Among these, several focus directly on cyber physical attacks and their direct and indirect economic and insurance impacts. Examples of available cyber physical catastrophe scenarios are listed in the following table.

Insurance solutions

Published PML scenarios and hypothetical stress test scenarios used by the insurance industry to assess impacts and risk appetite adjustment for extreme cyber physical attacks[21]

PML Scenario	Description	Variants	Source
Business Blackout	A malicious attack on transformers causes a major power failure in the US Northeast	3 variants	Lloyd's/CCRS (2015)[22]
UK power distribution failure	An attack on substations creates rolling blackouts in the Southeast UK	3 variants	Lockheed Martin/ CCRS (2016)[23]
Domain Name System (DNS) provider outage	Variable outage lengths affect business continuity in insured companies	SQL programmable script	AIR (2016)
Offshore energy - MODUDP attack	An attack on control systems for multiple offshore drills causes oil spillage and physical damage	Scenario spec for regulatory reporting	Lloyd's (2016)
Aviation - navigation control attack	Malware causes two full passenger jets to crash at different airports	Scenario spec for regulatory reporting	Lloyd's (2016)
Marine - ballast control system attack	Compromise of digital ballast control systems causes large ships to lose control and founder	Scenario spec for regulatory reporting	Lloyd's (2016)
Cyber-induced fires in commercial buildings	A malicious software update allows hackers to start fires by overloaded battery management systems in common laptops	3 variants	CCRS/RMS (2017)
ICS-triggered fires in industrial processing plants	A remote hack of industrial control systems (ICS) causes fires in factories	3 variants	CCRS/RMS (2017)
PCS-triggered explosions on oil rigs	A maliciously motivated insider causes oil rig explosions and leaks after manipulating network operations centres and Platform Control Systems (PCSs)	3 variants	CCRS/RMS (2017)
Cyber-enabled cargo theft from port	Criminals steal cargo from multiple ports by spoofing port management systems	3 variants	CCRS/RMS (2017)

Cyber risk pooling

Since the mid-2010s there has been regular discussion over the necessity of establishing a commercial pool or public-private partnership in order to provide protection from cyber catastrophes that prove too costly for the insurance industry to cover. Pool schemes covering losses from acts of terrorism exist in more than twelve countries.

As the class matures, it is important that insureds, brokers, insurers, governments and regulators work together to define and understand what is covered and not covered by traditional and emerging policies. This can lead to an informed debate about whether governments choose to take proactive or preventative steps to organise a pooling mechanism. Historically however, such a debate has tended to follow a major loss rather than precede one. As cyber remains a relatively immature class with a short history, the development of new solutions is likely to be determined as much by public policy priorities as pure risk based economics.

21 Coburn, Woo, and Leverett 2019, pp. 254-6

22 Available at: https://www.lloyds.com/news-and-insights/risk-reports/library/icsreport

23 Available at: https://www.lloyds.com/businessblackout

Insurance solutions

Product innovation opportunities

At present, the threat of physical damage from cyber risk presents a protection gap for businesses, and an opportunity for insurers to develop their cyber offering. The existing market is small and specialised and it may be that, with an informed understanding and assessment of the risk, more protection can be extended, both to those who would lose the most in the case of an attack and to the participants in the insurance industry who are exposed to accumulation and clash risk resulting from this peril.

This opportunity presents itself in two major avenues for development:

1. **Affirmative physical asset damage offerings**

   Insurers could look to create new affirmative physical asset damage cover, scalable to the size and value of each policyholder and adapted to their operational infrastructure. This kind of cover can sit alongside the provision of expert IT guidance, whilst evidence of consistent cyber security risk management practices could also be used to discount policy premiums. This type of cover is already offered to a limited market, but could be expanded and advertised further.

   When assessing the feasibility of underwriting cyber physical risk in a new sector, insurers will need to consult with industrial engineers and security experts to create a technical risk assessment and suitable exposure estimate. This is necessary in order to reveal all the ways in which a particular type of system may be abused to cause damage, and also protects insurers from claim mismanagement. The exposure estimate should ultimately take into account both the vulnerability and the attractiveness of the industry or network as a target and use this to determine appropriate policy wordings and limits for new cyber policies or add-ons.

   In practice: Cyber marine and affirmative physical asset cyber cover

   Since the NotPetya attack led to more than $200 million in uninsured losses for shipping giant A.P. Moller-Maersk, the Lloyd's market has developed a range of affirmative cyber solutions for the maritime industry worldwide. The new policies address a growing demand from financial indemnity stemming from cyber events, including any potential physical damage to vessels themselves. Protections of this kind can protect global supply chains in times of increased cyber risk, particularly when disruption may contribute to destructive circumstances, such as radar spoofing or ballast manipulation, as well as damage to freight or spoilage. Lloyd's further collaboration with the Cyber Risk Management (CyRiM) project in Singapore, *Shen Attack: Cyber risk in Asia Pacific ports*, also developed extreme scenarios for assessing cyber threats to businesses, including major port systems.

Insurance solutions

2. **Business interruption and contingent business interruption products for losses resulting from cyber physical attacks**

   Clear and simple wording in business interruption (BI) and contingent business interruption (CBI) products is critical to ensuring mutual security in times of increased risk. Wording assessments for any new coverages are essential in the cyber insurance field, and coverage caps will need to be specified.

   In practice: Third party BI and contingent business interruption cover from cyber physical triggers

   A significant opportunity for innovation in cyber physical protections is likely to be the extension of third-party coverage from BI and CBI. As with primary party offerings, BI and CBI policies require either add-on products, or a review and revision of policy wordings to both manage the losses from a major event and provide security to policyholders that the risk is acknowledged and covered.

   Without clear exclusions and affirmative cover, the industry risks silent exposure to cyber physical perils which cause power outages, transport disruption, communication outages, and other damages to business infrastructure. Where there is no specificity regarding the cause of this damage there is a risk that aggregating losses in a destructive cyber catastrophe event could be significant. Risk scenario exercises, such as those outlined in this report, can be helpful in determining the potential size of third-party losses from a major attack on a power grid or transport network.

All policies are subject to their own terms of coverage. Nothing in this report which only provides a high level discussion of the topic, is intended to constitute an opinion on the interpretation of individual policies

Glossary

Glossary

Advanced persistent threat (APT) – a nation state or state-sponsored group with the resources and skills to stage long-term attacks with specific goals to gain unauthorised access to a computer network and remain undetected for an extended period

Air gap – A term used to describe the network security measure of disconnecting a network from other systems, so that it is physically and digitally isolated

Battery management system (BMS) – Technology which monitors, protects, and optimises a battery or battery pack, and reports on battery health and status to external systems

Critical National Infrastructure (CNI) – The facilities, sites, systems, processes and networks which are necessary for a country to function. CNI may refer to both private and public entities, such as healthcare, energy, water and wastewater, communications, transport, emergency services among others

Digital control system – any system which processes sensor-based signals, such as those present in industrial settings to provide real-time network data

Domain Name Service (DNS) – the hierarchical and decentralised naming system for the internet, used to match readable domain names and URLs to machine readable IP addresses

Electrical control unit (ECU) – the embedded technology present in automotive systems that controls electrical systems or subsystems, within a vehicle

Heating, ventilation, and air conditioning (HVAC) – the technologies which control heating, cooling, ventilation, hydration, and air quality, generally within an enclosed space. Many HVAC controls now integrated through a unified building management system

Instrumentation and Control Systems (ICS) – various administrative systems and associated instrumentation such as devices, networks, and more used to operate and automate industrial processes

Information Technology (IT) – hardware and software built to store, retrieve, transmit, and manipulate data or digital information, often via the Internet

Malware – any software that is malicious by design. Malware takes many forms and includes software for establishing command and control, delivering ransomware, etc

Operational technology (OT) – hardware and software built to detect and monitor as well as control and alter physical industrial equipment, assets, processes, and events

Platform Control System (PCS) – systems used in the energy industry to automate or remotely control processes on oil platforms, such as building management and production

Probable Maximum Loss (PML) – the highest loss that an insurer could reasonable expect to ever incur on a policy, essentially a ‘worst case scenario’

Remote access trojan (RAT) – a malware programme that provides an attacker with full administrative control over an infected computer

Supervisory Control and Data Acquisition (SCADA) – the integrated architecture of control systems, software, and hardware which allows industrial supervisors to control processes, gather and monitor data throughout the network. SCADA systems include safety controls and emergency processes for equipment within the network

References

References

2019 Verizon Breach Report. (2019). Available at: https://www.verizon.com/business/resources/reports/dbir/2019/healthcare/.

Associated Press. (2020). German hospital hacked; patient taken to another city dies. Available at: https://apnews.com/article/technology-hacking-europe-cf8f8eee1adcec69bcc864f2c4308c94.

Coburn, Andrew, Gordon Woo, and Eireann Leverett. 2019. Solving Cyber Risk. Wiley.

De Cauwer, H., & Somville, F. (2021). Health Care Organisations: Soft Target during COVID-19 Pandemic. Prehospital and Disaster Medicine, 36(3), 344-347. doi:10.1017/S1049023X2100025X.

De Falco, M. (2012). Stuxnet facts report: A technical and strategic analysis. NATO Cooperative Cyber Defense Centre of Excellence.

Fernández Lisbona, Diego, and Timothy Snee. 2011. A Review of Hazards Associated with Primary Lithium and Lithium-Ion Batteries. Vol. 89. https://doi.org/10.1016/j.psep.2011.06.022.

Forbes. (2021). Turning Up The Heat: A Ransomware Attack On Critical Infrastructure Is A Nightmare Scenario. Available at: https://www.forbes.com/sites/forbestechcouncil/2021/07/20/turning-up-the-heat-a-ransomware-attack-on-critical-infrastructure-is-a-nightmare-scenario/?sh=4911f2981da0.

Gartner (2022). 3 Planning Assumptions for Securing Cyber-Physical Systems of Critical Infrastructure. Available at https://www.gartner.com/en/articles/3-planning-assumptions-for-securing-cyber-physical-systems-of-critical-infrastructure

Health IT Security. (2021). Ransomware Keeps Healthcare in Crosshairs, Triple Extortion Emerges. Available at: https://healthitsecurity.com/news/ransomware-attacks-surge-102-in-2021-as-triple-extortion-emerges.

Ireland Public Health Service. (2021). HSE publishes independent report on Conti cyber attack. Available at: https://www.hse.ie/eng/services/news/media/pressrel/hse-publishes-independent-report-on-conti-cyber-attack.html.

International Institute for Strategic Studies. (2021). Cyber Capabilities and National Power: A Net Assessment. Available at: https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power

Krotofil, Marina, and Jason Larsen. 2015. 'Rocking the Pocket Book: Hacking Chemical Plants for Competition and Extortion'. White Paper. DefCon 23. Hamburg University of Technology. https://infocon.org/cons/DEF%20CON/DEF%20CON%2023/DEF%20CON%2023%20presentations/DEF%20CON%2023%20-%20Marina-Krotofil-Jason-Larsen-Rocking-the-Pocketbook-Hacking-Chemical-Plants-WP-UPDATED.pdf.

Marie Elisabeth Gaup Moe. 2016. 'From Ukraine to Pacemakers!' May 4. https://www.slideshare.net/MarieGMoe/from-ukraine-to-pacemakers.

National Audit Office. (2017). Investigation: WannaCry cyber attack and the NHS. Available at: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.

References

OECD 2021. Enhancing Financial Protection Against Catastrophe Risks: The Role of Catastrophe Risk Insurance Programmes. Available at https://www.oecd.org/daf/fin/insurance/Enhancing-financial-protection-against-catastrophe-risks.pdf.

O'Neill, Patrick Howell. 2020. 'A Patient Has Died after Ransomware Hackers Hit a German Hospital'. MIT Technology Review. 18 September 2020. https://www.technologyreview.com/2020/09/18/1008582/a-patient-has-died-after-ransomware-hackers-hit-a-german-hospital/.

Recorded Future. (2021). BlackMatter ransomware targets companies with revenue of $100 million and more. Available at: https://therecord.media/blackmatter-ransomware-targets-companies-with-revenues-of-100-million-and-more/.

The New York Times. (2021). Blackout Hits Iran Nuclear Site in What Appears to Be Israeli Sabotage. Available at: https://www.nytimes.com/2021/04/11/world/middleeast/iran-nuclear-natanz.html.

Van Dine, A., Assante, M., Stoutland, P., & Nunn, S. (2016). Outpacing cyber threats: Priorities for cybersecurity at nuclear facilities. Nuclear Threat Initiative.

LLOYD'S

Twitter @LloydsofLondon
LinkedIn lloyds.com/linkedin
Facebook lloyds.com/facebook