

Insuring Hostile Cyber Activity: In search of sustainable solutions

Insuring Hostile Cyber Activity: In search of sustainable solutions

Rachel Anne Carter, Managing Director, Carter Insurance Innovations

Darren Pain, Director Cyber and Evolving Liability, The Geneva Association

Julian Enoizi, CEO, Pool Re, and Secretary, International Forum of Terrorism Risk (Re)Insurance Pools

The Geneva Association

The Geneva Association was created in 1973 and is the only global association of insurance companies; our members are insurance and reinsurance Chief Executive Officers (CEOs). Based on rigorous research conducted in collaboration with our members, academic institutions and multilateral organisations, our mission is to identify and investigate key trends that are likely to shape or impact the insurance industry in the future, highlighting what is at stake for the industry; develop recommendations for the industry and for policymakers; provide a platform to our members, policymakers, academics, multilateral and non-governmental organisations to discuss these trends and recommendations; reach out to global opinion leaders and influential organisations to highlight the positive contributions of insurance to better understanding risks and to building resilient and prosperous economies and societies, and thus a more sustainable world.

International Forum of Terrorism Risk (Re)Insurance Pools

The International Forum of Terrorism Risk (Re)Insurance Pools (IFTRIP) is a collaboration between global terrorism (re)insurance pools. It was formally ratified at the National Terrorism Reinsurance Pools Congress organised by the Australian Reinsurance Pool Corporation (ARPC) in Canberra in October 2016. The organisation was founded with the goal of promoting initiatives for closer international collaboration and sharing expertise and experience to combat the threat of potential major economic loss resulting from terrorism. The activities of IFTRIP include facilitating a range of international cross-organisational working groups, collective impact initiatives and international events, including an annual conference where a community of experts from the industry alongside business decision-makers ensure delegates stay up to date with the latest thinking and discussions around the risks posed by extreme events. IFTRIP is governed by the IFTRIP charter and is bound by local and international regulations.

Photo credits:

Cover page— Den Rise / Shutterstock.com

Geneva Association publications:

Pamela Corn, Director Communications

Hannah Dean, Editor and Content Manager

Petr Neugebauer, Digital Media Manager

Suggested citation: The Geneva Association. 2022.

Insuring Hostile Cyber Activity: In search of sustainable solutions.

Authors: Rachel Anne Carter, Darren Pain and Julian Enoizi.

January.

© The Geneva Association, 2022 All rights reserved

www.genevaassociation.org

Contents

Foreword	5
1. Executive summary	6
2. The emerging cyber risk landscape	8
2.1 Evolving threats and vulnerabilities	8
2.2 The cyber insurance market	10
2.3 Hostile cyber activity	12
3. Quantifying HCA risks	16
3.1 Realistic disaster scenarios	16
3.2 Uncertainty around quantification	18
3.3 Obstacles to modelling and quantifying HCA risks	19
4. Assessing the insurability of HCA and alternative risk transfer options	21
4.1 Boundaries between insurable and uninsurable risks	21
4.2 Enlarging market capacity for insurable risks	22
5. Public-sector solutions to catalyse future market development	25
5.1 Designing a government-backed insurance solution for HCA	26
5.2 International operability and potential for cross-jurisdictional PPPs	32
6. Conclusions	33
Appendix	
Characteristics of existing PPPs for selected insurance risks	34
References	40

Acknowledgements

The report's authors wish to extend their gratitude to the following collaborators:

Expert leadership and contributory authors

- Peter Zimmerli, AXIS Capital
- Rory Egan, Munich Re

Advisory team

- Chuck Jainchill, AIG
- Daniel Mesfin, Allianz
- Christian Wells, Pool Re and IFTRIP
- Tony Ellwood, Lloyd's Market Association
- Cyrus Delarami and Franz Gromotka, Munich Re

Cyber terrorism/cyber war experts

- Neil Arklie, Aviva
- Alexandra Maunie, AXA
- Francois Vilnet, GAREAT and IFTRIP
- Dennis Sno, Hannover Re
- Philipp Lienau, HDI Global
- Jeremy Cottle, Lloyd's
- Daniel Largacha Lamela, MAPFRE
- Chris McEvoy, Partner Re
- Sie Liang and Alexander Bosch, SCOR
- Kei Kato, Tokio Marine
- Masashi Yamashita, Sampo

External interlocutors and contributors

- Raveem Ismail, ASR Re
- Jon Bateman, Carnegie Endowment for International Peace
- Rebecca Boyle, CyberCube
- Yakir Golan, Kovrr
- Steve Coates, Pool Re
- Gordon Woo and Matt Harrison, RMS
- Richard Ifft, TRIP and IFTRIP
- Achim Jansen, DKVG, Extremus and IFTRIP
- Joerg Stapf, Extremus and IFTRIP
- Bethany Vohlers and Felipe Gerhard, Verisk

Foreword

The cyber insurance market continues to evolve and adapt to the changing threat landscape, as cybercriminals and nation states exploit security vulnerabilities and societies' reliance on digital technology. A surge in ransomware claims over the past two years, combined with a growing recognition of the threat posed by cyber risks, has caused many insurers to pause and reassess their cyber underwriting strategy. This has resulted in a reduction in policy limits, a rise in premium rates and a tightening of terms and conditions. It has also triggered a renewed focus on cyber exposure management and deeper consideration for potential future loss scenarios.

State-sponsored cyberattacks that stop short of outright military conflict pose a particular challenge for re/insurers. The first two reports in our series on cyber terror and cyber war introduced the term hostile cyber activity (HCA) to cover such events and mapped out an attribution framework to characterise them. It is hard to precisely define and pin down such incidents, let alone quantify their potential impact. Estimates of losses from some disruptive scenarios, which might be associated with HCA, are on a par with those of large natural catastrophes. However, other HCA-related scenarios involving failure of critical infrastructure could generate much larger losses.

Thankfully, we have yet to experience such system-wide disruption. But recent cyberattacks are a warning: their outcomes had the potential to be much worse. A significant protection gap therefore exists for large-scale cyber losses linked to HCA. To close that gap, at least partly, substantial progress to increase the insurability of catastrophic cyber risk is needed; otherwise, the current hard market for cyber insurance will likely persist and the industry will be reluctant to allocate the additional capital needed to meet growing future demand for cyber insurance. Advances in modelling, greater sharing of cyber threat intelligence and mechanisms to protect re/insurers' balance sheets from large accumulated losses are some of the obvious starting points.

It is clear though that the development of a sustainable private cyber re/insurance market to cover the full scope of cyber risks will ultimately be contingent on the development of some form of public-private partnership (PPP) or government backstop. PPP blueprints are already in place in several countries to share exposures to natural catastrophe as well as terrorism risks and nuclear risks. Cyber risk comes with its own set of complexities, yet the constraints on the private re/insurance sector's capacity to absorb losses from an extreme cyber incident are becoming increasingly obvious.

This third and final report in our series on cyber terror and cyber war explores the ability of the insurance industry to underwrite HCA risks and the potential complementary role for PPPs in future insurance solutions. We hope the considerations put forward will help frame the debate between the public and private sectors to formulate well-designed risk-sharing schemes that increase societal resilience to cyber-related perils.



Jad Ariss
Managing Director,
The Geneva Association



Christopher Wallace
President, IFTRIP
CEO, Australian Reinsurance
Pool Corporation (ARPC)



1. Executive summary

The cyber landscape is evolving rapidly, with digitalisation expanding the range of threats and vulnerabilities. This process is amplified by shifts in working and business practices brought on by COVID-19, some of which are likely to persist beyond the pandemic. Ransomware and supply chain attacks in particular have become more prolific since the onset of the pandemic and with them wider recognition of the potential for large-scale economic disruption from malicious cyber incidents.

A dedicated market for cyber insurance has developed, involving a progressive broadening in the class of risks covered, both first- and third-party losses.

A dedicated market for cyber insurance has developed over time involving a progressive broadening in the class of risks covered, both first- and third-party losses. However, the recent increase in loss ratios, especially on standalone cyber insurance – i.e. dedicated affirmative cover – has prompted re/insurers to recalibrate cyber risks. Coupled with initiatives to remove unintentional cyber exposure from conventional property and casualty policies (non-affirmative or 'silent' cyber), market re/insurance capacity has become scarcer. In the face of continuing strong demand, this has triggered a sharp rerating in the cost of cyber insurance and a tightening in terms and conditions.

A particular challenge for cyber insurers relates to state-sponsored cyberattacks that may be part of ongoing support for terrorist or criminal groups and stop short of outright military conflict. Traditional policy exclusions for war or war-like incidents fail to adequately capture situations where nation states are suspected of being behind an attack, or providing a safe harbour for the hackers, especially if the motives for the attack are unclear. Such issues of attribution and characterisation create significant contractual uncertainty for insurers, which has only added to the recent tightening in cyber insurance market conditions.

More granular classifications of cyber incidents – including Hostile Cyber Activity (HCA) terminology, which provides for a lower burden of proof for state involvement than current widely-used definitions – will help provide greater clarity for insurers and increase comfort levels with their exposure. However, tighter policy language over insured cyber incidents takes time to gain market acceptance and even then will likely only go so far. The systemic characteristic of cyber risks, in particular the potential for multiple losses from a single event or a campaign of attacks linked to HCA, mean that the scale of accumulated losses may exceed levels that can safely and sensibly be absorbed by the private re/insurance sector.

Accumulated losses of some cyber risks linked to HCA may not be able to be safely and sensibly absorbed by the private re/insurance sector.

Quantifying cyber risks with any degree of confidence, however, remains a significant challenge for re/insurers. Deterministic scenario analysis suggests some malicious cyber incidents, such as a temporary disruption to cloud services, might trigger economic losses broadly comparable with some historical natural catastrophe events. But more extreme and long-lasting cyberattacks, including a widespread IT or operational infrastructure outage or failure, could generate significantly larger expected losses. Moreover, the uncertainty surrounding such estimates is very large, meaning that total potential losses could be many multiples of these guesstimates, easily exhausting re/insurers' risk-absorbing capacity. This is especially true of HCA incidents where the ambiguity over hackers' motives, tactics and threat vectors as well as the possibility for relatively minor, isolated attacks to escalate towards full-out cyber warfare, only add to the complications in quantifying cyber risks.

The size of potential losses from a major HCA or similar incident, relative to the extent of cover currently provided by re/insurers, highlights a significant protection gap. In order to close at least some of that gap, significant progress is needed in making catastrophic cyber risk more insurable.

This would require further improvements in modelling of possible cyber incidents in order to quantify potential losses; advances in sharing cyber threat intelligence and identifying/pursuing perpetrators to deter criminals, terrorist groups and governments who promote HCA and other malicious cyber activity; and having mechanisms for re/insurers to cap their aggregate downside exposures that otherwise would exceed their balance sheet capacity.

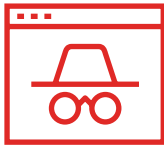
Absent these developments, it is highly likely that cyber re/insurers will continue with their current strategies of ensuring tight wordings and maintaining modest limits on individual affirmative cyber policies and, increasingly, explicit exclusions on non-affirmative contracts to eliminate silent cyber. By the same token, it will be difficult to expand the transfer of such peak cyber exposures to capital market investors until models have advanced sufficiently to promote much more accurate actuarial assessments of the risks.

Building on The Geneva Association/IFTRIP's earlier work on defining HCA and mapping out an attribution framework for such incidents, this paper reviews the current capabilities within private insurance markets to

underwrite HCA risks. A key conclusion is that, ultimately, some form of government backstop or public-private partnership (PPP) to finance extreme cyber risks will be needed in order to foster the development of a sustainable private cyber re/insurance market and thereby boost economy-wide resilience.

Ultimately, some form of government backstop or PPP to finance extreme cyber risks will be needed.

However, designing such government-backed solutions is complex. There will be trade-offs in adopting particular scheme features and difficulties in calibrating how much of the peak losses should be shared among policyholders, private re/insurers and governments. Such design challenges are amplified at the international level. Therefore, while collaborative international solutions would be optimal, priority should be given to developing domestic PPP solutions for large-scale cyber risks.



2. The emerging cyber risk landscape

The ongoing diffusion of new digital technologies into everyday life and business has fundamentally affected the risk landscape facing firms and individuals. Although technological advances create many benefits to improve our lives and lifestyles, they also leave users open to security and associated cyber threats. Many of the developers of new technologies often tend to focus on the technology itself rather than safeguarding the new technology against basic threats. For example, some smart home devices, whilst easing interconnectivity, may not always include basic cybersecurity hygiene features, leaving them prone to failure and/or attack.

More generally, organisations of all sizes, geographies and industries increasingly rely on data analytics and technology, such as cloud computing, the Internet of Things (IoT) and artificial intelligence. In the cyber vernacular, the attack surface/ set of vulnerabilities has grown and the threat vector has expanded, including both accidental, unintentional physical or logical errors¹ and intentional action by malicious attackers. It is the combination of threats and vulnerabilities that gives rise to cyber risks. This heightened risk profile poses a challenge to cyber insurers in terms of sustainably increasing the scope and scale of coverage, especially given the potential for large-scale aggregate losses from a cyber incident.

Technological advances can improve our lives and lifestyles but they also leave users open to security and associated cyber threats.

2.1 Evolving threats and vulnerabilities

With the increasing digitalisation across nearly all industries, businesses depend more and more on externally managed IT service providers, and many new businesses build their entire business model within a cloud environment. Notably, only a handful of large companies provide the vast majority of cloud computing capacity, such as Amazon Web Services, Microsoft Azure or the Google Cloud. Market concentration among a few large cloud providers presents a concerning illustration of a potential 'single point of failure' in the cyber domain,² although thankfully the risk of a massive outage has so far not crystallised.

¹ Logic errors are design flaws which may be found in computer programmes or software code. As these errors were not seen by the developer of the software, they are in some cases exploited by cyber adversaries and used to ease the effort required to carry out a cyber event.

² Hitzel 2020.

The global spread of COVID-19 has accelerated prevailing digital trends and amplified cyber risks.

The response to the global spread of COVID-19 in 2020/2021 has only accelerated prevailing digital trends and amplified cyber risks. Many sectors of the economy saw widespread adoption of internet-based remote working, virtual interactions via video-conferencing and a pronounced expansion of e-commerce. Accompanying this, the frequency of cyberattacks increased. In a survey conducted in the early days of the COVID-19 outbreak by IT security firm Check Point, 71% of all security professionals reported elevated levels of security threats and attacks.³ This looks to be a persistent shift. According to Willis Re's more recent survey of cyber insurance buyers, underwriters, risk managers, claims professionals, actuaries and brokers, 86% think the frequency of cyberattacks will increase as a result of COVID-19.⁴ A 2021 global survey by Ponemon Institute and IBM also found that the shift to remote operations during the pandemic led to more costly data breaches.

Ransomware and supply chain attacks in particular have grown considerably in the recent past.

Ransomware attacks in particular have grown considerably – by almost 500% from Q1 2018 to Q4 2020 – with no sign of any let up in 2021, significantly outpacing the number of incidents involving data breaches.⁵ This increase in the frequency of attacks has been accompanied by increased sophistication and larger extortion demands, in part linked to the development of 'ransomware-as-a-service' (RaaS), whereby specialist malware developers sell software code to other cybercriminals. According to the U.S. authorities, USD 590 million worth of payments relating to ransomware were made in the first six months of 2021, more than the USD 416 million reported for the whole of 2020.⁶ Critical infrastructure and operational technology have been prone to ransomware

attack – especially those involving RaaS schemes – as aptly illustrated by the recent attack on Colonial Pipeline, which temporarily disrupted the U.S. East Coast's fuel supply.⁷

Software supply chain attacks, i.e. malware introduced via software distributions from legitimate third-party actors, have also received renewed attention, due in large part to the SolarWinds cyberattack revealed in December 2020⁸ and the security breach at Microsoft Server Exchange in early 2021.⁹ Likewise, in February 2021, hackers tampered with a water treatment facility in Florida to change the chemical levels of the water supply, underscoring the vulnerability of industrial infrastructure to such malicious intrusions.¹⁰ More recently, hackers stole login credentials and addresses of over 1 million customers of web-hosting firm and domain registrar GoDaddy, putting those accounts at high risk of being targeted in future business email scams and phishing campaigns.

While large-scale, malicious cyberattacks have not yet been observed, criminal gangs are highly active and continuously expanding their cyber capabilities, often under the protection of nation states.

While cyber terrorist or other large-scale, malicious attacks causing systemic cyber losses have not been observed so far, it is well documented that criminal gangs are highly active and continuously expand their cyber capabilities, often under the cloak of protection of nation states. Indeed, nation-state-sponsored hackers are believed to be behind the recent SolarWinds and Microsoft attacks, not least because of the high level of sophistication and long planning horizons involved.¹¹ Cyber warfare is increasingly regarded as part of a nation's arsenal alongside traditional military force, with correspondingly large resources deployed. Yet so far these state-sponsored cyber incidents have been covert, rather than overt operations. As such, they are part of what is currently best described as a 'cold cyber war' rather than necessarily a prelude to a full-scale kinetic war.

3 Check Point 2020.

4 Willis Re 2020.

5 Aon 2021a.

6 U.S. Treasury 2021.

7 Wired 2021.

8 The 2020 SolarWinds cyberattack was one of the largest and most sophisticated to date. SolarWinds is a major U.S. software company providing management tools for network and infrastructure monitoring. Their client base of over 300,000 high profile companies included many Fortune 500 companies, universities and/or government departments such as the U.S. Department of Homeland Security and U.S. Treasury Department. The SolarWinds cyberattack was the work of a highly-skilled actor. The attack itself involved cyber adversaries incorporating malware into a specific layer of the SolarWinds software. This enabled them to have access to some of the SolarWinds customers who were using the software. It appears the event was motivated by espionage. See The Geneva Association 2021a.

9 See FireEye 2020, Microsoft 2021 and Microsoft 2020.

10 Pew Trusts 2021.

11 Bloomberg 2021.

2.2 The cyber insurance market

In tandem with the evolving risk landscape, the market for cyber insurance has advanced, although the anatomy of cover has changed over time.

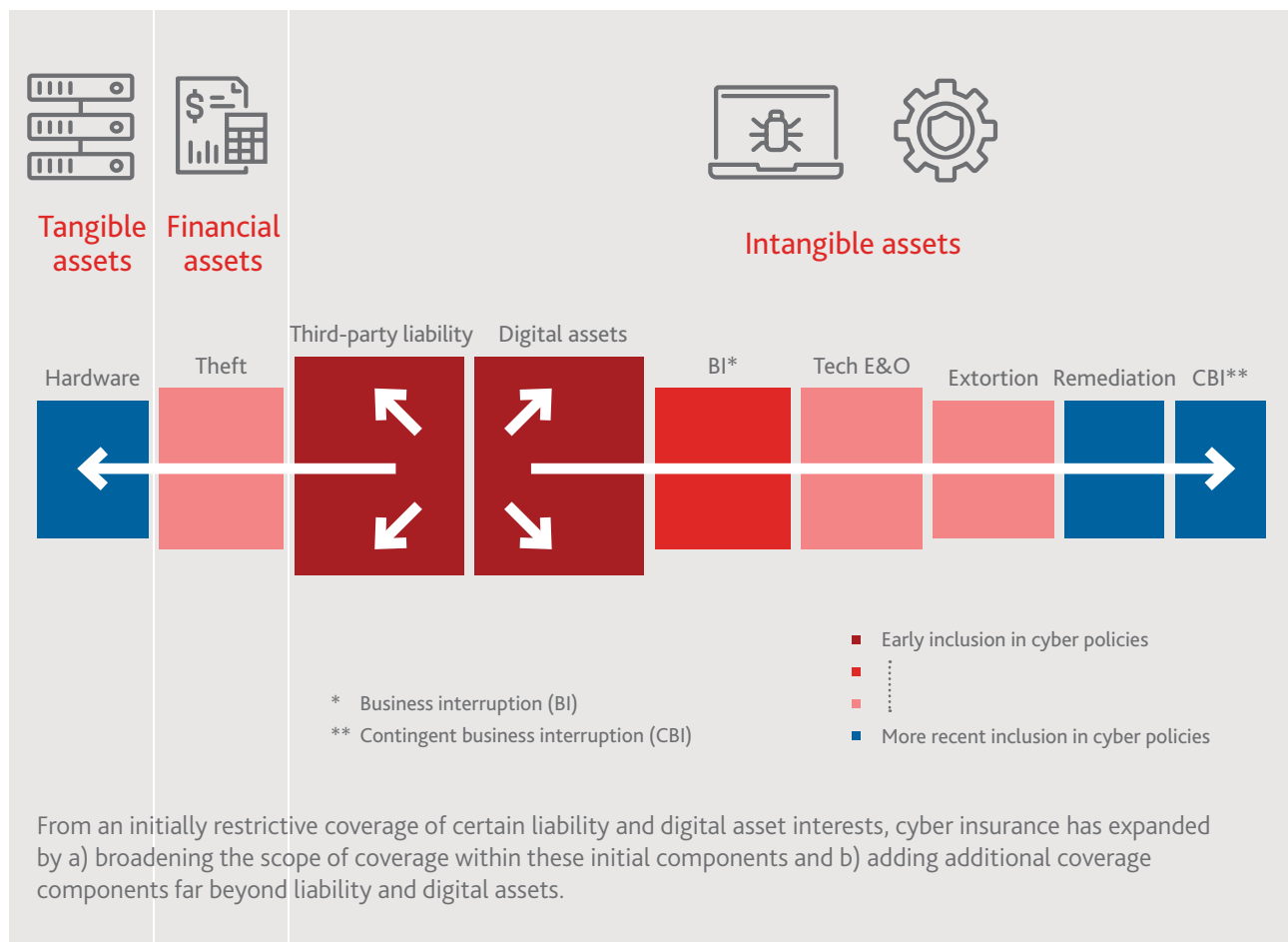
2.2.1 Broadening in standalone coverage

The market for standalone cyber insurance, i.e. dedicated affirmative cover, has grown rapidly over recent years, with premiums more than tripling since 2015 to reach around USD 7.5 billion in 2020.¹² Although that still represents a relatively small share of global expenditure on insurance, over time, the breadth of cover has developed to include a wider set of protected assets, both tangible and intangible (see Figure 1).

Vastly expanded data privacy legislation both in Europe (the EU General Data Protection Regulation, or GDPR) and the U.S. (most notably the California Consumer Privacy Act, or CCPA) have led to further recent expansions in coverage. Nowadays, affirmative cyber insurance typically extends protection to incidents beyond computer security failures and data breaches and combines coverage for a wide range of first-party as well as third-party losses – albeit often with specific and relatively modest policy limits.

The market for standalone cyber insurance, i.e. dedicated affirmative cover, has grown rapidly in recent years.

Figure 1: Historical expansion of coverage offered by affirmative cyber insurance policies



Source: Contributed by Peter Zimmerli (Axis Capital)

12 Global Data 2021.

Affirmative cyber insurance extends protection to a wide range of first-party and third-party losses – albeit often with specific and relatively modest policy limits.

A number of key risks, however, generally remain outside the scope of standalone cyber insurance. Notably these include:

- Bodily injury or physical damage to tangible property due to a cyberattack, with the exception of IT hardware replacement costs.
- Losses caused by the failure of infrastructure that may be vital to IT operations like electricity, gas, water or telecommunication networks.
- Any losses related to fraudulent behaviour or misconduct by the insured.

However, a number of key risks are not covered within affirmative cyber policies, e.g. bodily injury, property damage and losses arising from the failure of critical infrastructure.

2.2.2 Purge in 'silent' cyber

To some extent these types of cyber-related exposures might be captured by other traditional property and liability insurance policies, which may implicitly include or at least do not exclude cyber risk. Unlike standalone cyber insurance, which clearly defines the parameters of cyber cover, many traditional policies do not specifically refer to cyber and might in principle be assumed to pay claims for cyber losses in certain circumstances.

Such non-affirmative or 'silent' exposure came into sharp relief in the wake of the WannaCry and NotPetya attacks in 2017, which, in the case of the latter, ravaged a range of businesses from shipping companies and supermarkets to ad agencies and law firms by irreversibly encrypting data stored in their IT systems. Property Claims Services (PCS) estimates the economic loss from NotPetya at USD 10 billion and the insured loss at more than USD 3 billion. According to PCS, approximately 85% of the

insured loss from NotPetya was from non-affirmative property coverage.¹³

Over the past few years, the insurance industry has strived to minimise exposure to 'silent' cyber given the unintended nature of coverage. In part, this effort is in response to regulatory initiatives¹⁴ that require insurers to explicitly either include or exclude cyber coverage from their regular property and casualty policies. Insurers need to know their exposures and hence be able to calibrate their cyber risk across the full suite of insurance policies and have sufficient solvency capital to guard against possible large loss accumulation events. Equally, the policyholder gains increased contract certainty about cyber risks that are covered and those that are not. Some insurers have clarified coverage by defining cyber risk and then excluding it from non-cyber policies. Some are introducing new policy language and underwriting guidelines. Others, such as Lloyd's of London, require insurers to either expressly exclude or include cyber risk in their traditional lines' policy wordings, from January 2020.¹⁵

2.2.3 Recent withdrawal of risk-absorbing capacity

Amid heightened uncertainty about prospective cyberattacks, especially the potential for ransomware and supply chain incidents to have widespread impacts, re/insurers have recently sought to tighten policy language and withdraw risk-absorbing capacity in order to protect their balance sheets. Measures include coverage exclusions, higher self-insured retentions and more stringent limits/sublimits. This restriction in market capacity, alongside ongoing demand, is showing up in significant increases in the price of affirmative cyber cover as the overall cost of protection has been recalibrated.¹⁶

Re/insurers have recently sought to tighten policy language and withdraw risk-absorbing capacity, prompting a sharp increase in premium rates.

Year-on-year cyber premium rate increases averaged around 15% between January 2020 and June 2021.¹⁷ However, this masks a more significant hardening in the market in late 2020 and the first half of 2021. For cover involving higher policy limits (i.e. excess-of-loss cover) the recent pick-up in rates was even larger, perhaps consistent with increased worries about the frequency and severity of possible large-scale attacks, which could burn through the

¹³ PCS 2019.

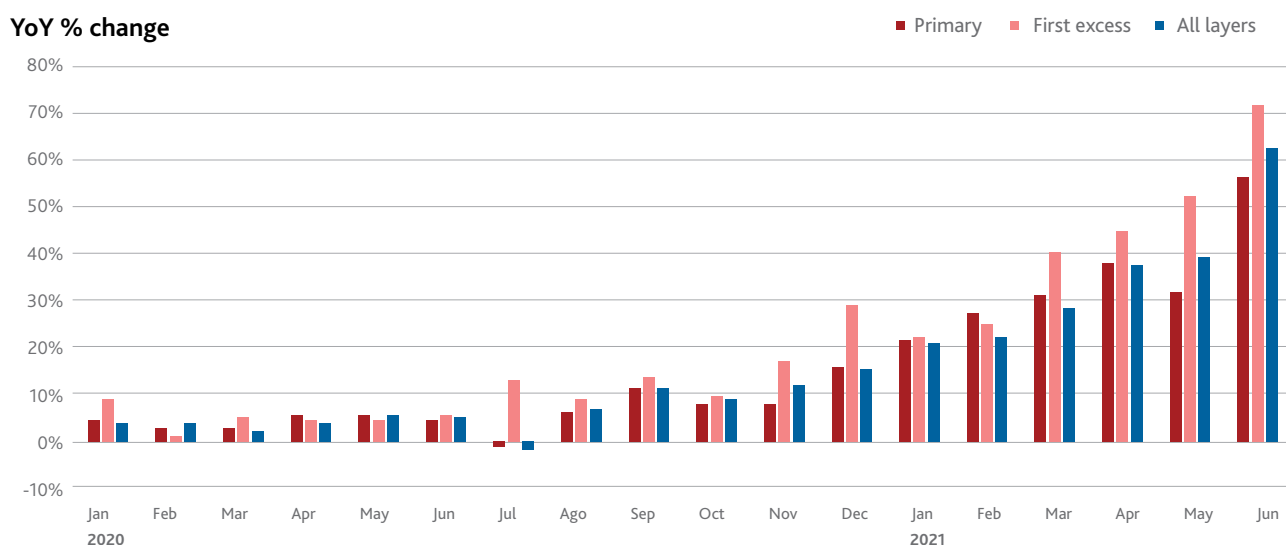
¹⁴ See, for example, Bank of England (Prudential Regulatory Authority) 2019.

¹⁵ Marsh. Undated.

¹⁶ PropertyCasualty360 2021.

¹⁷ Aon 2021b.

Figure 2: Cyber insurance premium rate increases over the course of contract renewals, by layer of cover



In cyber insurance markets such as the U.S., insureds that desire more than USD 10 or USD 15 million in coverage typically layer or stack insurers. The first layer (or primary policy) will set the general terms and conditions for the entire programme. Excess policies provide any needed additional limit. The primary insurer bears 100% of the risk of loss up to its limit. Then, the first excess insurer will bear 100% of its layer on, and so on.

Source: Aon¹⁹

primary layer protection (Figure 2). That upward pricing momentum continued through the remainder of 2021 with rates on affirmative cyber policies increasing in the year to Q3 by 96% in the U.S. and 73% in the U.K., driven by a rise in the frequency and severity of losses.¹⁸

Growth in premium rates has likely not yet arrested the deterioration in underwriting results. According to partial data from the National Association of Insurance Commissioners (NAIC), the aggregate loss ratio on U.S. standalone cyber policies rose to almost 73% in 2020, more than double its level in 2017. The rise appears to be primarily due to an increase in severity with ransomware claims seeing elevated incident response costs as well as extortion demands.²⁰

2.3 Hostile cyber activity

Recent serious supply chain intrusions and ransomware incidents have underscored a long-standing issue for cyber insurers: how much protection can and should insurance provide when the perpetrators of such attacks are linked to nation states? Traditional policy exclusions for war or war-like incidents fail to adequately capture situations where nation states are suspected of being behind an attack or

at least providing a safe harbour for the hackers, especially if the motives for the attack are unclear. Such issues of attribution and characterisation create significant contractual uncertainty for insurers, which has only added recently to the tightening in cyber insurance market conditions.

Traditional war exclusions fail to adequately capture situations where nation states may be behind an attack, creating contractual uncertainty.

Initiatives to tighten cyber policy language and introduce more granular terminology for insured events will no doubt help. For example, The Geneva Association/ IFTRIP proposal to introduce the specific category of HCA provides additional granularity to cover malicious incidents beyond cyber terrorism but not involving cyber warfare. It also assists with the process of attribution and characterisation by lowering the burden associated with having to 'prove' which state was responsible for an event (see Box 1). This will be essential in promoting contract certainty and trust in the value of associated insurance.

¹⁸ Marsh 2021.

¹⁹ Aon 2021b.

²⁰ Ibid.

Box 1: Defining HCA

Typical war exclusions in insurance policies address actions of 'war' as well as 'war-like' and/or 'hostile' operations, conducted by a 'government (de jure or de facto)' or a 'government agent'.²¹ Such clauses often cover an act of war but may not extend to the broader concept of warfare. Nevertheless, cyber exclusion clauses provide few explicit definitions. This has invited considerable legal debate and challenge about what qualifies as an insured event. Most notably, the NotPetya attack in 2017 prompted litigation over whether it was an act of war since the attack was widely believed to be the work of a state-sponsored actor.²²

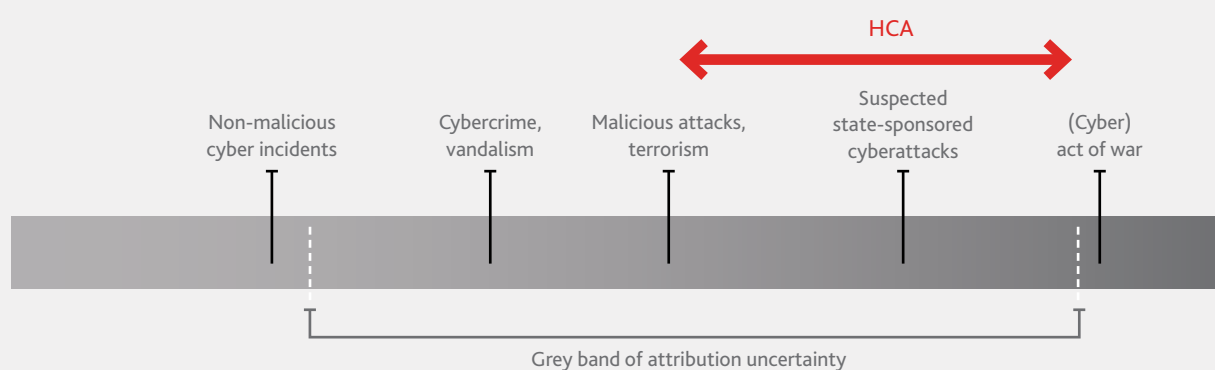
Attribution can quickly become contentious as the differences between state-sponsored attacks and criminal cyber events become harder to establish.

A key difficulty with the existing war exclusions remains that the threshold of legal proof or justification required to show the involvement of a state actor, i.e. determining who is responsible for an incident, is high. The attribution of an attack to a specific group plus the evidence that the group was under the control of a state or acted as a state agent during this attack can prove very difficult.

Even if the perpetrator of a cyber incident is identified and known to be acting under state authority, a supplementary question remains: whether the cyber incident can be characterised as 'hostile or warlike'. The recent SolarWinds event provides a vivid illustration of the conundrum. State actors were reportedly involved but the incident was generally perceived to be linked to espionage rather than an act of aggression, although the data gathered from the attack could ultimately be useful for future openly hostile acts.

In practice, attribution can quickly become contentious as the differences between state-sponsored attacks and criminal cyber events become increasingly difficult to establish. Litigating these issues is time-consuming, expensive, and unpredictable. This creates a 'grey band of uncertainty' surrounding attribution/characterisation that acts as a significant drag on insurers' appetite for cyber risk (Figure 3).²³

Figure 3: Grey band of attribution uncertainty for cyber risk



Source: Adapted from Gallagher Re²⁴

²¹ A detailed discussion of commonly used terms and meanings can be found in Bateman 2020.

²² Most notably, U.S. companies Merck and Mondelez, both hit hard by NotPetya in 2017, sued their respective property insurers who disputed the claims citing war exclusion clauses in the wording of the policies.

²³ Gallagher Re 2020.

²⁴ Ibid.

Tighter and more granular definitions can address some of these issues. In particular, as discussed in The Geneva Association,²⁵ policy language based around HCA – the range of malicious activity located beyond cyber terrorism but short of outright cyber war – will enable insurers to better delineate ‘acts of war’ and state-sponsored attacks from other malicious cyber incidents like cyber terrorism or cybercrime. For instance, clauses referencing HCA might stipulate that it is only necessary to prove a state was involved rather than having to pinpoint which one.²⁶ Moreover, the standard of proof for state involvement in HCA could be based on the balance of probabilities that the event was supported by a nation state. That support may be as simple as a state ignoring activity when they know of its occurrence but decide not to take action.²⁷

New policy language based around HCA will enable insurers to better delineate ‘acts of war’ and state-sponsored attacks from other malicious cyber incidents.

Source: The Geneva Association

In late November 2021, the Lloyd's Market Association issued new cyber war and cyber operation exclusion clauses which seek to articulate the coverage position more clearly in the context of cyber warfare. However, it takes time for such changes in wordings to gain market-wide support let alone be introduced into standard commercial insurance products.

Moreover, the latest incidents also highlight the residual challenges in creating clear-cut, definitive boundaries around what legitimately falls within HCA and what does not. Rather than the pursuit of political aims, which is normally a defining feature of terrorist activity or warfare, many of the recent attacks were carried out by organised criminal gangs principally for financial gain. Nation-state involvement also varied widely, from reported tacit sponsorship, including fostering an environment for developing sophisticated yet easy-to-use malware (e.g. the attack on Colonial Pipeline), to alleged outright supervision and resourcing of hacking campaigns by official arms of a sovereign government (e.g. SolarWinds). In such circumstances, some of the difficulties of direct attribution for HCA resurface, particularly if state actors linked to criminal gangs use false-flag tactics to hide their traces, blame others or otherwise undermine any international consensus about the ultimate source of the attack.

At present, cyber incidents that involve state actors but are akin to a cold-war-type event, are generally covered by the existing re/insurance market, up to certain limits. This should be encouraged if the full benefits of cyber insurance are to be realised. However, insurers have to navigate a tricky path in deciding the extent of cover

they can reasonably offer. On the one hand, excluding coverage for all forms of state-sponsored cyberattacks will undermine some of the value proposition of cyber insurance for improving societal resilience. The reality is that certain governments increasingly deploy illicit cyber intrusion tactics to further their strategic goals that fall short of outright conflict, including political and commercial espionage. Individuals and firms are highly exposed, even those that have invested in robust cybersecurity, and may come to question the benefit of cyber insurance if such largely unavoidable or at least hard to mitigate risks are not covered.²⁸

However, attribution challenges can resurface if state actors linked to criminal gangs use false-flag tactics to hide their traces, blame others or undermine international consensus about the source of the attack.

On the other hand, the systemic characteristic of such cyber risks and in particular the potential for multiple losses from a single incident or a campaign of attacks mean that the scale of accumulated losses may exceed levels that can safely and sensibly be absorbed by the private re/insurance sector. There is often collateral damage surrounding any large-scale malicious cyberattack whereby unintended targets also suffer loss. A number of recent cyberattacks reportedly linked to state actors caused more widespread harm than initially anticipated

25 The Geneva Association 2021b.

26 For HCA risks it will still be necessary to establish that ‘a’ state actor was responsible for the cyber event.

27 The Geneva Association 2021b.

28 A July 2021 survey found that more than one third of organisations worldwide have experienced a ransomware attack or breach that blocked access to systems or data in the previous 12 months (IDC 2021). Another recent survey found that traditional ransomware defenses are failing, with 54% of all victims having anti-phishing training and 49% having perimeter defenses in place at the time of attack (GlobalNewswire 2021).



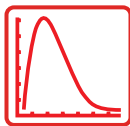
by the perpetrator due to a lack of understanding of how different computer systems were linked.

To some extent too, the latest spate of attacks can be seen as near-misses; if circumstances had transpired differently the scale and breadth of the losses could have been much worse.²⁹ Insurers need to carefully assess such accumulation threats when underwriting cyber risks so that they can safeguard their own balance sheets and thereby remain able to make good on their promises to policyholders.

Ultimately, individual insurers will decide how they balance the commercial attractions of growing their cyber insurance portfolios versus their risk appetite and capacity for absorbing possible peak losses. There is to date, and unlikely to be in the near future, no universal consensus within the re/insurance market regarding how HCA should be included or excluded for various cyber insurance policies. Some carriers may continue to cover HCA but carefully limit their exposure in a bid to prevent potential loss accumulation. Others will shy away from cyber exposure altogether, fearful of the fallout from further escalation in HCA. The cyber insurance market tends to be concentrated, with relatively few insurers targeting this specialty line. A key factor in encouraging both incumbent and prospective insurers to offer increased coverage for HCA and other malicious cyber activity will be advances in modelling and the quantification of cyber risks, as well as reinsurance availability and other mechanisms to share risks.

Individual insurers will decide how they balance the commercial attractions of growing their cyber insurance portfolios versus their risk appetite and capacity for absorbing possible peak losses.

²⁹ A case in point is the recent SolarWinds attack. Of the 33,000 Sunburst software system users, only 18,000 customers were actually affected by the attack. More could have been impacted if the latest software patching updates had been routinely implemented. See SecurityWeek 2020.



3. Quantifying HCA risks

Unlike for natural catastrophe perils such as hurricanes or man-made disasters such as terrorist attacks, cyber as a peril has no geographical borders – the whole world is potentially one cyber catastrophe zone. Beyond issues of attribution and characterisation, assessing the frequency and severity of HCA, especially the potential for large accumulated losses, remains a particularly serious challenge.

3.1 Realistic disaster scenarios

Scenario analysis can help to gauge the potential for losses from HCA, especially complex accumulation. In particular, different configurations of attack (threat source, points of vulnerability, propagation and correlation of attack, etc.) can inform about the scale of potential damages and the economic losses at stake. Catastrophe model vendors and insurers or large re/insurance markets like Lloyd's have articulated cyber catastrophe scenarios (often labelled realistic disaster scenarios) in order to understand the potential financial implications. Typically deterministic, such hypothetical scenarios seek to provide 'what-if' type guesstimates of the impact should downside risks crystallise. By careful selection, construction and analyses of different scenarios, a broad picture of the size of possible losses can be created.³⁰

Scenario analysis can help to gauge the potential for losses from HCA, especially complex accumulation.

There are of course almost unlimited ways in which the major disruption or failure of critical IT or operational technology components could impact economies and thus the insurance industry, as well as society at large. We pick out three examples of already established extreme scenarios that could unfold as part of HCA. These three scenarios are within the realistic disaster scenario catalogue often used by re/insurers to assess cyber accumulation potential. Features of these scenarios also have echoes in some of the recent cyberattacks, which underline the growing dependence on critical service providers and the potential for system-wide, single point of failure losses.

³⁰ Hull 2010.

- **Widespread contagious malware spread:** A 'software supply chain attack' such as seen in the recent SolarWinds or NotPetya attacks, where malware is initially distributed via a software update, that further propagates between private networks to infect other systems and results in deleted, corrupted or encrypted data.
- **Major cloud outage:** A widespread outage or temporary lack of access to one or more cloud service providers, which immediately affects each user of the affected services. Where there is a meaningful business dependency on the availability of this service this leads to interruption of business activity with loss of revenue.³¹
- **Infrastructure disruption or failure (especially power and internet outages):**³² A failure of utilities, in particular telecommunication lines (including the internet), electricity but also transport, gas and water supplies creates a 'blackout' scenario (complete failure of the electricity supply) or a substantial 'brownout' (partial but large failure) of a few hours or even several days, and widespread internet outages.³³ Although such an incident could be linked to non-malicious causes including a natural catastrophe, such infrastructure could also be the target of malicious cyberattacks.

Table 1 below summarises loss estimates from publicly available research documents for each scenario.

Table 1: Existing cyber risk scenario analysis

Scenario	Broad impact	Insurability	Uncertainty of loss estimate	Economic loss estimate (USD billion)	Insured loss estimate (USD billion)
Widespread contagious malware spread ³⁴	Disruptive	Insured / insurable by the cyber market	High	193	27
Major cloud outage ⁽¹⁾	Disruptive	Insured / insurable by the cyber market	High	53	8
Infrastructure disruption or failure (e.g. power outage) ⁽²⁾	Destructive / disruptive	Not insured /insurable for the cyber market, exposure	Very high	1,024	71 (driven by non-affirmative exposure mainly in property)

Notes: (1) Proximate causes for the unavailability are numerous, including technical failures, distributed denial-of-service (DDoS) attacks as well as malware infections. In addition, the scenario also considers the inability of the affected customer to restore the services by themselves.³⁵ (2) Possible triggers causing a blackout include well-known physical perils (such as severe storms or earthquakes), human errors but also malicious acts.³⁶

Source: The Geneva Association and Munich Re³⁷

31 Unless the affected company maintains their own proprietary cloud environment with full system redundancy, the customer of an external cloud provider will need to wait until the cloud service provider resolves the disruption. Insurance coverage is now mostly granted for business interruption caused by the failure of external IT service providers. However, sublimits in coverage might apply.

32 Munich Re 2018.

33 Lloyd's and University of Cambridge 2015.

34 Lloyd's and University of Cambridge 2019.

35 Lloyd's and Cyence 2017.

36 Lloyd's and University of Cambridge 2015.

37 Material put together by Rory Egan, Munich Re.

At face value, projected total economic losses from either a **widespread malware attack** and/or **major cloud outage**, while significant, are not unprecedented. The direct estimated costs are broadly comparable with those previously experienced from a large natural catastrophe – for example, in U.S. communities affected by major hurricanes, the U.S. National Oceanic and Atmospheric Administration's (inflation-adjusted) estimates of economic damage were USD 176 billion for Katrina, USD 77 billion for Sandy, USD 136 billion for Harvey and USD 55 billion for Irma.³⁸

Projected economic losses from a widespread malware attack and/or major cloud outage, while significant, are not unprecedented.

More than for these natural catastrophes, however, the projected share of extreme cyber losses that would be insured – based on current coverages – is relatively small. Assuming that re/insurers can better understand the likelihood of such events, as well as control potential loss accumulation through analysis of the maximum footprint or 'spread' of impacts from such an event, in principle insurance can play a bigger role in closing the protection gap for such risks.

In contrast, the costs of a widespread **infrastructure disruption or failure** are not at all insurable, due to the massive potential spread and inherent difficulty in controlling or measuring the accumulation of losses.³⁹

In contrast, the costs of a widespread infrastructure disruption or failure are not at all insurable.

3.2 Uncertainty surrounding loss quantification

The level of uncertainty surrounding such extreme loss scenario estimates is nevertheless very high. In terms of loss accumulation, it is extremely challenging to identify the full set of dependencies among risks, define scenario footprints and assess the impact of an event on the many companies that could be affected. The frequency and severity of cyber events as well as their co-dependence are not easy to establish, making it difficult to assess potential overall aggregate losses.⁴⁰

The level of uncertainty surrounding such extreme loss scenario estimates is nevertheless very high.

There is a lack of historical data on cyber incidents – including unsuccessful attacks – from which to extrapolate potential losses. Even with detailed information about losses, the past may not be a good guide to the future because threat vectors continuously and rapidly change. The potential for 'unknown-unknown' cyber threats creates significant ambiguity about the underlying sources and size of exposure. Cyber risks are highly interdependent, meaning that losses can often accumulate significantly, especially if any correlating cause takes time to reveal itself.

The potential for 'unknown-unknown' cyber threats creates significant ambiguity about underlying exposures.

Counterfactual simulation analysis (looking at actual events and projecting just how bad they might have been) can help. But determining the potential scale of such an event requires a large element of judgment. Box 2 describes one such analysis in relation to the NotPetya incident.

38 <https://www.ncdc.noaa.gov/billions/events>

39 CNBC 2021.

40 Swiss Re 2017.

Box 2: Counterfactual analysis of NotPetya

Historical data on extreme cyber losses, both economic and insured, remains sparse. This raises doubts over how useful past losses are for gauging the scale of future extreme events, with a return period well in excess of the duration of the internet's existence. One way of expanding the historical set of observed cyber losses is through counterfactual analysis. Every past event is just one realisation of an ensemble of alternatives, which might have happened. For insight into extreme losses, insurers should be especially interested in downward counterfactuals: alternative realisations of historical events where things turn out much worse.⁴¹

A classic demonstration of the value of downward counterfactual analysis is the 2017 cyberattack known as NotPetya. A group of alleged Russian hackers succeeded in adding malware to a tax accounting software update, enabling attackers to remotely access any installation of the software, and instruct it to download and execute malicious code. Once installed on one computer within an organisation, NotPetya spread to other computers on the network.

The cyberattack initially targeted firms in Ukraine with the intention for the malware to spread globally through connected networks. Fortuitously, only a small number of multinational companies downloaded the suspect accounting software update, linked in part to an accidental calendar mismatch with a Ukrainian government deadline for quarterly tax filing. One of these was the global shipping company Maersk, which reported a loss of several hundred million USD. Nevertheless, the loss could well have been an order of magnitude larger if certain knock-on events had transpired. In particular, by another stroke of fortune, the office of Maersk's West African subsidiary was offline due to a power blackout, which meant the shipper's global system could be restored using this office's copy of the shipper's domain controller, reducing the full scale of operational disruption.

By simulating alternative versions of history, a counterfactual catalogue of losses from near-miss events can be constructed. Such counterfactuals can be assessed deterministically, as well as probabilistically, using data on cyber supply chain attacks. Either way, counterfactual thinking provides a systematic way of expanding the horizon on plausible cyber scenarios and helps optimise the existing modelling experience/catalogue.

Source: Gordon Woo, *Catastrophist*, RMS

3.3 Obstacles to modelling and quantifying HCA risks

Scenario-based accumulation risk modelling works well within the normal 'cold war' state of affairs, but it has significant shortcomings at times of heightened potential for rapid intensification of nation-state cyber tactics. As hostile situations escalate from a 'stable' level of isolated, covert offensive HCA to more brazen infiltration campaigns, and even possibly a state of full out 'cyber war', model assumptions around the frequency of a one-off systemic attack may no longer be realistic. For instance, it is imaginable that successive massive retaliatory attacks take place over a short period of time, each of magnitude in line with say a 1-in-100-year event under 'non-war' conditions.

Scenario-based accumulation risk modelling works well within normal 'cold war' conditions but falls short at times of heightened potential for rapid intensification of nation-state cyber tactics.

Continuous tit-for-tat cyber vandalism – attacks without any obvious rational criminal, political or ideological motive – from unidentified state entities, or a government-imposed partial internet shutdown to prevent foreign adversaries spreading misinformation or otherwise interfering in democratic elections, for example, are just two features of HCA scenarios amongst many that have received hardly any attention so far (if

⁴¹ By contrast, an upward counterfactual considers what could have happened if events turned out better. For further discussion of counterfactual analysis see Woo et al. 2017.

any at all). Moreover, it would be naïve to believe that attackers can always precisely predict the penetration success of their campaigns. What might be designed as a relatively localised cyberattack by loosely state-affiliated elements could spread globally and cause unintended but widespread collateral damage. This possibility of truly global loss accumulation severely limits the capability of diversifying cyber tail risks across geographic regions.

The likelihood or severity of losses are unclear if there is an escalation of cyber war-like incidents and the contours of the tail of the aggregate loss probability distribution are highly imprecise.

If insurers cannot rule out the possibility of an ongoing overt conflict, then they need to allow for this in their risk evaluations. However, given the human behavioural aspects involved, it is difficult to assess any retaliatory action and/or the potential for similar or worse attacks to be used as war-like responses to states that are attacked. It is also not known what the potential likelihood or severity would be if there is an escalation of cyber war-like incidents. As a result, the contours of the tail of the aggregate loss probability distribution are highly imprecise.

The obstacles facing insurers in quantifying HCA resemble those for calibrating pandemic risks. Pandemics similar to COVID-19 had for a long time featured on the list of rare events with potentially devastating impacts on society. Yet, nobody could have accurately foreseen the complex interplay of voluntary and government-mandated mechanisms set in motion to counter the spread of the virus or actively fight it, let alone attach precise probabilities to developments. Likewise in the realm of cyber risk, while there is broad agreement on the potential systemic nature of some HCA incidents, quantifying that threat in an actuarial sense – i.e. determining the severity of losses from both direct impacts and cascading effects such as government reactions as well as their associated likelihood – remains an enormous challenge for the re/insurance industry.

The formal assessment of cyber risk in all its features is still in its infancy, and more needs to be done, in particular in the area of systemic risk. While an expansion of insurance offerings for HCA will not only depend on progress in cyber risk quantification, this is nevertheless an important aspect. It remains, for instance, very unclear where and how a line between war and 'non-war' events (such as HCA) is drawn in current approaches to risk assessment. The delineation, particularly for HCA, will need to be clearer in order to assess better the limits of insurability, especially the potential loss accumulation and the effects of governments' responses, both to safeguard against possible attacks and mitigate the fallout from them. This is not an issue that modelling companies can address alone; it will require first and foremost clear guidance from the insurance industry.





4. Assessing the insurability of HCA and alternative risk transfer options

Insurance typically involves a delicate balance between supply and demand. Re/insurers need to set coverage conditions and charge sufficient premiums to cover the costs of providing risk protection, including compensating the providers of their capital for potential unexpected losses. At the same time, there needs to be demand for such cover on those terms. Risks are only insurable in practice if an insurer and an insurance buyer reach an agreement about a specific coverage and its price, including a common understanding of what is insured and what is not. For this reason insurance can only deal with a limited band of the full spectrum of risk.

4.1 Boundaries between insurable and uninsurable risk

In order to understand the potential appetite of the insurance industry to absorb HCA risks, it is worthwhile to briefly review cyber risks against key actuarial criteria for insurability. In particular, the ability to insure cyber risk will often turn on insurers' assessment of how far (a) the probability of loss is random and can be estimated, (b) the presence of insurance influences the probability of loss (i.e. moral hazard), and (c) the loss accumulation potential is economically bearable (see Table 2).

Table 2: Key insurability constraints on expanding cyber policy coverage to HCA

Insurability aspect	Industry concerns
Randomness and risk quantification	• Cyber is a man-made risk in a constantly evolving environment with limited loss experience. • While assessing the risk of medium-to-large losses seems no more inherently difficult than for other classes of insurance (e.g. product liability), ambiguity about the frequency and severity of systemic cyber risk is challenging.
Moral hazard	• Insurers will avoid offering solutions when risks increase due to behavioural changes from stakeholders once insurance acts as a safety net. This could, for example, be the case if state-linked groups act more boldly because insurance would soften the impact of retaliatory attacks.
Loss accumulation	• The capability of the insurance industry to accept risk is defined by the capital it holds to safeguard its solvency even after a major loss event. In particular – albeit not only – state-affiliated actors are seen as capable of attacks that could cause damage that exceed re/insurers' risk-absorbing capacity. • In order to significantly expand offerings for cyber tail risks including those of an HCA nature, insurers will have to find new ways of limiting accumulation risk and/or share risks among themselves and with additional stakeholders like reinsurers, governments or capital markets.

Source: The Geneva Association

The nature of the uncertainty associated with cyberattacks, particularly HCA, is such that it may be impossible to attach reliable probabilities to their timing and impact. While increased knowledge, information and expertise about cyber risks will help to improve modelling capabilities, some HCA-related losses may simply be prone to irreducible or radical uncertainty, which cannot be characterised probabilistically.

Governments could control the frequency of cyberattacks and the presence of insurance might influence their willingness to engage in hostile activities.

Moreover, cyber losses are not the outcomes of a game against nature in the way that, for example, air and ocean surface temperatures create conditions for weather storms. Governments could theoretically control the frequency of attacks at will, and the presence of insurance to cover collateral damage of their own industries might influence their willingness to engage in hostile activities. They could be more likely to launch attacks – or to take other aggressive actions that invite retaliation in cyberspace – if any cyber repercussions are mitigated by insurance payouts.

This potential for government moral hazard contrasts with the situation often facing individuals and firms. There may be limits to what they can do practically to mitigate any losses arising from HCA (as well as for cyber terrorism or cyber war). Insurance plays an important role in incentivising good cyber hygiene behaviours – for example, the requirement for individuals and firms to have minimum and up-to-date security software to prevent obvious intrusions or contagious effects from malware. But these may still be no match for a sustained and sophisticated cyber infiltration campaign. State actor(s) and their affiliates have, in some instances, almost unlimited resources to achieve a certain aim whether that be to infect computer systems with malware, breach data, destroy systems or otherwise infiltrate a system and extract information.

Advances in gathering cyber threat intelligence, including collaboration across firms and governments, will boost risk awareness and preparedness, an important element in building cyber resilience. Such information will enable

insurers to detect vulnerabilities among insureds and make the pricing of cyber insurance more risk-sensitive (i.e. cheaper cover for more resilient firms), thereby encouraging investment in cybersecurity. Likewise, progress by law enforcement agencies in tracing and pursuing the perpetrators of an attack and recovering extorted funds may go some way to deter cybercriminals and increase insurers' comfort levels in offering risk-absorbing capacity.⁴²

However, insurers must not only assess the risk of an individual or company becoming the victim of a cyberattack but also the scope for multiple insureds to be impacted. HCA has the potential to create catastrophic, highly-correlated, unpredictable losses, which insurance contracts were not intended to cover. If the insurance industry were to proactively broaden cover to HCAs, this additional dimension of accumulation risk would seriously need to be addressed.

HCA has the potential to create catastrophic, highly-correlated, unpredictable losses, which insurance contracts were not intended to cover.

4.2 Enlarging market capacity for insurable risks

In some countries, commercial insurance offerings for cyber terrorism may be available under one of the existing terrorism pools, particularly where it results in physical property damage. But policy limits are still, in general, quite low. Most major IFTRIP⁴³ pools, for instance, cover cyber terrorism, with some also including chemical, biological, radiological and nuclear (CBRN) risks, either in a limited way or with government support.⁴⁴ Such developments have raised the prospect of ceding more cyber-related risks, including HCA exposures that currently fall outside traditional terrorism covers, to alternative risk carriers such as captives, re/insurance pools as well as the (broader) capital markets.

42 The seizure by the U.S. Department of Justice of millions of dollars worth of cryptocurrency linked to the ransomware attack on the Colonial Pipeline demonstrated the traceability of cryptocurrencies. Thomson Reuters 2021b.

43 IFTRIP was developed in 2015 to support initiatives for closer international collaboration between sovereign-backed terrorism reinsurance pools. See www.iftrip.org

44 IFTRIP 2018.

4.2.1 Captive insurers

A captive can be a useful way for a company to recognise and gain a better understanding of its cyber exposures. By building up a track record of its losses and expenses as well as its risk mitigation efforts, the captive may be able to secure coverage from the re/insurance market at acceptable terms and pricing. This may particularly be the case when a re/insurer agrees to share certain risks with the captive. For example, a re/insurance carrier may not wish to underwrite the primary layer of losses for certain risks (or industry sectors) but might provide excess-of-loss cover.⁴⁵ There are potentially tax and other benefits in using a captive for risk transfer to cover HCA. It is thus theoretically possible to develop bespoke captive vehicles to facilitate cover for at least some HCA risks.

However, it is most probable that risks arising from HCA are simply assumed by existing captives as part of a portfolio diversification strategy to broaden the scope of retained risks. It is not clear how much this will 'move the needle' in terms of attracting additional investor/reinsurance capital to absorb HCA risks. As a result, while self-insurance based on the build-up of funds by owners of the captive may be used to manage better any losses from HCA, realistically it won't serve as an alternative solution to narrow existing insurance protection gaps for HCA.

4.2.2 Pools

Captives are not alone in preferring discrete risks with clear boundaries. Traditionally, pools have operated for distinct risks within a strictly confined geographical boundary. Most pools are designed to diversify independent risks, or at least shocks that might not hit all of the members of the pool simultaneously. However, such mutualisation of possible losses breaks down when a common event affects all insureds, with the potential for losses to exhaust any buffer funds accumulated by members of the pool. The potential systemic nature of HCA would be difficult for existing terrorism pools to absorb and could only be sanctioned by governments (not the re/insurance market) as they would ultimately be covering the major losses from such incidents.

4.2.3 Insurance-linked securities (ILS)

To date the market for ILS – financial instruments sold to investors and whose value is affected by an insured loss event – has developed substantially within the property catastrophe arena.⁴⁶ This is largely due to the perceived positive risk/reward balance in peak natural catastrophe

perils and the availability of third-party analytic tools. However, natural catastrophe claims over the last three years have seen ILS investors suffer disproportionately large losses from the concentrations in major peak weather catastrophe zones. As a result, some ILS managers and investors are reportedly seeking portfolio diversification by assuming exposure to other insured perils and reducing, in particular, their exposure to U.S. East-Coast wind events.⁴⁷

Some commentators argue that peak cyber risks could be securitised and transferred to capital markets, especially as such instruments would likely attract high yields.

Some commentators argue that peak cyber risks will eventually be securitised and transferred to capital markets, especially as any such instruments would likely attract high yields.⁴⁸ So far, however, such initiatives remain largely theoretical with few, if any, transactions, at least in the public domain. Similar to pandemic risk, the potential for a large-scale cyber incident to simultaneously hit stock and bond market valuations, thereby undermining any diversification benefits, remains a significant hurdle for third-party investors.

Until the correlation between major cyber events and capital market outcomes has been road-tested, ILS for large-scale cyber risks are unlikely to develop significantly.

Enhanced modelling capabilities will no doubt foster risk appetite for cyber exposure, not least because they will enable more accurate actuarial calculations for both re/insurers and investors alike. Nonetheless, until that correlation between major cyber events and capital market outcomes has been thoroughly road-tested, it is unlikely that ILS or other risk transfer instruments involving alternative capital will be developed, at least at scale. Arguably too, if a systemic cyber event were to take place that provides evidence of the empirical correlation, the probable initial outcome could be that there is even

⁴⁵ AIG 2019.

⁴⁶ Although existing ILS tend to focus upon the property catastrophe arena, there are other examples of ILS, e.g. in mortgage and life securitisations as well as more bespoke offerings for particular risks.

⁴⁷ Based on market intelligence from Yakir Golan (Kovrr).

⁴⁸ Artemis 2021.

less appetite to cover cyber risks by the re/insurance markets or alternative capital providers. Box 3 discusses one of the few existing ILS transactions for terrorism and cyber terrorism. Although this does not cover HCA,⁴⁹ it is a good example that illustrates how a potential future ILS transaction for HCA might be structured.

Box 3: A case study of terrorism and cyber terrorism ILS

The Pool Re sponsored ILS issuance for Baltic Re in 2019 was the first standalone terrorism risk catastrophe bond. The transaction provided Pool Re with a three-year source of fully collateralised retrocessional reinsurance, covering it against losses from terror attacks striking the mainland U.K. However, uniquely, the ILS coverage extended to include damage to tangible property caused by cyber terrorism. The GBP 75 million bond was fully subscribed by institutional investors and runs for a three-year term. It is also listed on the Bermuda Stock Exchange. The ILS encompassed conventional terrorism, such as blast damage, as well as non-conventional events such as CBRN and cyber terrorism.

Investors accepted the cyber terrorism risk within a wider terrorism placement. A condition of the ILS was that any cyber coverage was limited to physical damage caused by cyber means and not the traditional subject matter of cyber policies such as data breaches or interference with other information assets.

Although there has been much discussion around the need for additional cyber risk-absorbing capacity from capital markets, this has so far yet to emerge, aside from a few niche propositions. That said, it is possible cyber coverage might have been included within ILS covering other perils. What seems more evident are the reasons why investor interest in ILS for cyber events has thus far been limited. Any ILS issuance relies heavily on modelling to inform both loss evaluation and pricing. With cyber risk models still highly nascent and unproven, it seems likely that investors require the credibility of these models to become firmly established before they are prepared to commit significant capital. Moreover, investors will probably need greater clarity around legal definitions and terminology relevant to cyber, including HCA.

Source: Steve Coates, Pool Re

⁴⁹ Pool Re has no legislative mandate at present to cover HCA, rather only events that are designated terrorist events, including cyber terrorist events that have gone through the designation process.



5. Public-sector solutions to catalyse future market development

As previously highlighted, a key reason why HCA risks are so problematic to insure relates to the potential for large loss aggregations. Typically, prudent insurers underwrite cyber risks using explicit contract wordings and exclusions plus individual policy-level limits/sublimits and look to cede accumulated peak exposures to the reinsurance market. From an insurability perspective, however, insurers (and their reinsurers) are only likely to be able to take on more HCA risk if there is a way of capping overall aggregate losses. The potential scale of accumulated claims from HCA could be too big and too uncertain for the private re/insurance sector to absorb alone.

Re/insurers are only likely to be able to take on more HCA risk if there is a way of capping overall aggregate losses.

Echoing current debates over pandemic-related risks, consideration should thus be given to government-backed solutions to finance these tail cyber risks in order to boost economy-wide resilience. A well-designed PPP could increase risk-absorbing capacity and still encourage cyber market innovations to extend cover further for HCA risks. This is evident in long-standing PPPs for terrorism and other perils.

A well-designed PPP could increase risk-absorbing capacity and still encourage cyber market innovations to further extend cover for HCA risks.

In developing and establishing a PPP in any jurisdiction a key challenge is how to divide the risk between the public and private sectors. To incentivise good cybersecurity, as much risk as possible should remain with firms and individuals and be underwritten by private insurers on commercial terms with public-sector involvement limited to extreme loss outcomes. Any government-backed solutions should not simply be a fiscal solution but also seek with insurers to promote adoption of cybersecurity best practices – including taking out appropriate insurance – in order to reduce the vulnerability of society to such risks.

In the current conjuncture, with fiscal balance sheets under significant strain, political support for countries taking on further contingent liabilities might be constrained. Policymakers' appetite for addressing such issues in the midst of the

ongoing COVID-19 episode may also be limited. Yet with taxpayers in the end likely to be called upon to absorb a significant share of uninsured losses from a cyber catastrophe, it is sensible to look at measures that preempt such an eventuality and put in place appropriate financing arrangements.

5.1 Designing a government-backed insurance solution for HCA

There are many and varied ways in which a government-backed solution for peak cyber risks could be formulated. The main ones are as a direct insurer operated by or alongside the government, a state-run reinsurance facility to protect against large-scale, catastrophic losses or a private-sector pool with a government (retrocession) backstop.⁵⁰

Spain's Consorcio de Compensación de Seguros (CCS) is a government direct insurer that covers risks⁵¹ such as natural catastrophes and terrorism, including cyber terrorism.⁵² In France, the Caisse Centrale de Réassurance (CCR) – a wholly state-owned, full-service reinsurer – provides domestic cedants with reinsurance coverage against natural disasters and certain uninsurable risks such as property damage resulting from terrorist attacks and acts of terrorism. In the U.K., Pool Re is a government-backed mutual terrorism reinsurance facility operated by private insurers. The U.K. government provides an unlimited governmental backstop, which is activated once a designated 'terrorist' event has occurred and Pool Re⁵³ has exhausted its capital (including any retrocession capacity) and is otherwise unable to pay the required compensation for losses arising from the attack.⁵⁴

The criteria for developing a framework upon which a government may either support or be involved in providing insurance solutions revolves around a number of important design questions:

- Should the insurance exist solely for HCA and cyber terrorism perils or as a subset of broader cyber risks? Alternatively, should it be part of a multi-peril solution? Could there be an umbrella pooling scheme in place?
- Should any proposed solution be compulsory or voluntary?
- Should the scheme be pre- or post-funded? What mechanisms may be used to determine factors affecting the capital raising and financial sustainability of the scheme?⁵⁵
- What is the event and claims assessment basis – indemnity or parametric?
- Should any scheme be based on mutuality or solidarity principles?
- Will it be a permanent or temporary scheme?

Taken together, the answers to these questions ought to help shape any government involvement as well as how any PPP could be designed. There are likely trade-offs in adopting particular scheme features and empirical difficulties in calibrating how much of the tail losses should be shared among policyholders, private re/insurers and governments. These trade-offs may vary between jurisdictions and be guided by different commercial realities, economic considerations and political influences. It is unlikely that any single factor will determine the outcome. There may also be scope to continue to adapt and re-optimize the solution, including in response to the evolving nature of the risk and the available capacity of the commercial insurance market to absorb cyber risks.

PPPs come with different features and empirical difficulties in calibrating how much of the tail losses should be shared among policyholders, private re/insurers and governments.

50 Although there are a few examples of the private insurance industry collaborating to create a pool for certain events, the scope of these is limited. For example, in Switzerland, the Swiss natural perils pool (Elementarschaden-Pool, ES pool) is a joint initiative by the 12 private insurers that cover over 90% of the natural perils market. See SVV 2021. However, most pools rely on government support when losses exceed a certain level and thus it is probable that any pool for malicious cyber events will require governmental backing.

51 The CCS extends the covers to most policies underwritten by private insurers, however the policies themselves are underwritten by the private market. Although the CCS covers cyber terrorism, it is implicitly included in the terrorism cover and separately underwritten by the CCS.

52 The Spanish insurance industry work with the CCS to manage the scheme including the collection of the CCS surcharge. In return for collecting the CCS surcharge the insurers will receive 5% of the amount collected. See Consorcio De Compensacion De Seguros 2020.

53 Any primary insurer of commercial property located in Great Britain (i.e. England, Wales and Scotland) is entitled to cede the terrorism component of its portfolio of such risks to Pool Re. To prevent adverse selection, given that Pool Re is obliged to accept such cessions, a member insurer must cede its entire portfolio and policyholders must insure all of their eligible properties with Pool Re members: an 'all or nothing' approach. Further, each carrier ceding to Pool Re will have some 'skin in the game' by bearing a premium-based pro rata share of a market-wide retention.

54 For details of the operation and structure of a cross section of natural catastrophe and terrorism insurance solutions please see a description and comparative table in the Appendix of this report.

55 PEIF 2020a.

5.1.1 Multi-peril or single peril?

As noted previously, it may be possible to extend an existing natural catastrophe or terrorism pool or other PPP to include cyber-related perils. Developing a multi-peril scheme however, raises a number of additional considerations relative to a standalone cyber pool. While a multi-peril scheme may offer some diversification benefits, it also increases the chance of any government backstop being relied upon. Further, from a practical viewpoint, there are additional administrative and cost issues associated with operating a scheme covering multiple perils, particularly if the perils are quite different in nature – for example a NatCat insurance pool also covering cyber.

While a multi-peril scheme may offer some diversification benefits, it also increases the chance of reliance on any government backstop.

There are a number of current examples where either a single peril scheme was expanded into a broader multi-peril pool or a new pool was developed out of necessity to cover several perils. Both types can operate effectively and efficiently. For example, the CCS (Spain) and CCR (France) provide cover both for terrorism and for natural disasters, albeit under different schemes.

Within a PPP insurance arrangement, private insurers often sell and administer policies and offer their knowledge and tools to assess catastrophe damage. Such a division of tasks is, usually, cost-efficient because it makes optimal use of the available expertise of private insurers in providing insurance coverage.⁵⁶

5.1.2 Mandatory or voluntary coverage?

Although a voluntary PPP insurance scheme may be possible, the main challenges will be two-fold. First, there needs to be sufficient capital backing to ensure the scheme is financially sustainable. If the group of policyholders is too small, the pool of collected premiums will likely not be sufficient to cover expected losses from HCA, meaning that the government backstop will invariably be called upon when a serious incident occurs. That in turn will eat into fiscal budgets and could stretch government solvency criteria if it leads to significant additional borrowing.

A second issue for a voluntary scheme is the potential for adverse selection – the tendency for high-risk

policyholders to be included in a PPP while safer risks (who are less susceptible to HCA) are covered by conventional cyber policies provided by the commercial insurance industry. Further, the nature of voluntary PPPs may mean that the take-up rate by the ultimate insureds is lower than a mandatory arrangement.

Mandatory insurance enlarges the potential premium pool but raises the question of how to enforce the scheme and what (if any) sanctions will apply for those not taking out coverage.

Mandatory insurance enlarges the potential premium pool if implemented correctly.⁵⁷ Risk is spread over a larger base and adverse selection is reduced.⁵⁸ But it also raises the question of how to enforce the mandatory aspects of the scheme and what (if any) sanctions will apply for those not taking out coverage. The administration efforts to ensure those required to obtain cover do so and pay the required price may create significant operational costs. One way in which mandatory take-up could be assured is to administer this in conjunction with business taxation or as a requirement for the operation or continued operation of a business.

Some countries, such as Spain and France, have mandatory coverages and pools/schemes (Consortio and GAREAT), which exploit both risk diversification opportunities and administrative efficiency for dealing with major perils. A key practical difficulty in establishing a mandatory scheme is that the relevant jurisdiction will typically require specific statutory legislation. The legislation will need to set out critical features of the scheme such as its operability, structure, funding as well as details on how the take-up of the programme will be monitored and implemented.

5.1.3 Pre- or post-event funded?

The development of a public-private solution will require careful consideration of the type and nature of its funding. One clear benefit of a pre-event funded scheme is that by proactively establishing risk transfer mechanisms it allows purpose built, ex ante incentives to be included in the scheme that promote risk prevention and mitigation. If a scheme is reactive however, the PPP cannot incentivise risk management for the particular event for which it will be called upon to make a pay-out.

⁵⁶ Paudel 2012.

⁵⁷ Ibid.

⁵⁸ Dixon et al. 2004.

A pre-event-funded scheme can build in features to incentivise risk prevention and mitigation.

An additional benefit of a pre-event funded scheme is the ability to have funds and operational facilities readily available for use should an event occur. This provides a signal to the market that as much of the risk as possible is intended to be borne by the industry and only as a last resort will additional government funding be needed.

In contrast, a post-event funded scheme will rely on access to funds after an event and most likely the rapid deployment of infrastructure for the administration and distribution of funds. Almost inevitably this will involve increased government borrowing or other financing arrangements, which ultimately will need to be repaid, perhaps through higher premiums on all future policyholders or general taxation.

Governments tend to favour post-funding arrangements as garnering political support to fund a contingency that may never arise can be challenging.

Governments tend to favour post-funding arrangements. This is not least because garnering political support to fund a contingency that may never arise can often be challenging, especially as it will often squeeze out other priorities. Post-funding may also be attractive because it avoids having to set up a potentially large bureaucracy to collect and invest premiums.⁵⁹ Yet, in the wake of an incident there may not be sufficient time for debate, planning and assessment of the various options to ensure the PPP allocates payouts effectively to legitimate victims. As a result, viable firms may face significant liquidity constraints to finance reparation and recovery from an attack, which may threaten their solvency. Raising new government debt via capital markets can also be expensive after an event, significantly affecting a country's debt service costs.

In looking at existing PPPs, there is no universally preferred funding model. Some operate with a pre-determined mechanism for raising funds or recouping losses after a qualifying incident and others employ a mix of pre- and post-event funding mechanisms. Within the terrorism sphere, most IFTRIP pools, including those in Australia⁶⁰

and the U.K.⁶¹ (Australian Reinsurance Pool Corporation and Pool Re), build up capital ahead of an event. Due to the absence in the past decade of any large-scale, insurable terrorism incident affecting either of these jurisdictions, a sizeable amount of capital and reserves has been accumulated to protect against a future terrorism event.

These pools also have large retrocession programmes in place to maximise coverage within the commercial insurance sphere and ensure government backing is only required in catastrophic events that otherwise exceed the capacity and reserves of the pools. In contrast, the Terrorism Risk Insurance Act (TRIA) in the U.S. adopts a post-event funded approach. Under TRIA, when an event occurs there is a pre-determined mechanism for recovering necessary funds from the industry over a pre-established timeframe.⁶²

5.1.4 Indemnity or parametric trigger?

Although cyber insurance has typically provided indemnity-based coverage, in theory it is possible to develop parametric-based protection products, which pay out should a pre-defined trigger be activated. This could be a physical trigger such as the number of hacked computers or linked to the monetary cost of remedial action or repair. A key advantage of parametric insurance is that it can often provide post-event liquidity much faster and more efficiently than traditional indemnity products, which typically require on-the-ground damage and loss assessments. The main drawback for insureds is that the payout amount may differ significantly from the actual losses incurred – the basis risk – although this may be alleviated somewhat by highly-granular triggers.

Parametric insurance can provide post-event liquidity much faster and more efficiently than traditional indemnity products, but such covers might lead to significant accumulated losses.

To date there has been little commercial appetite to develop parametric insurance for cyber risks. This is most likely due to the potential for parametric triggers to create significant accumulated losses – depending on the scope and breadth of an attack multiple insureds could be impacted, especially if it is part of a sophisticated hacking campaign. However, Box 4 describes the industry's first

59 Dixon et al. 2004.

60 Australian Government Transparency Portal 2020.

61 Pool Re 2020.

62 Congressional Research Service 2019.

dedicated cyber parametric insurance product, including cover for terrorism risks. Although the policy limits are relatively low, this might provide clues as to how future products could be developed for HCA risks to complement and possibly augment traditional insurance, including as part of a broader PPP solution.

5.1.5 *Mutuality or solidarity pricing principles?*

Commercial insurance is based on the premise that risks should be priced in an actuarially fair manner and designed

to incentivise the insured to protect themselves against particular contingencies. If the insurance is set up with mutuality in mind, cover for individual insureds is priced to reflect their contribution to the risk of the overall pool. In contrast, under solidarity principles, there is often a degree of cross-subsidisation whereby some insureds pay higher than actuarially-fair prices in order to subsidise other insureds within the pool. For example, within social insurance schemes some individuals often pay higher premiums in order to make insurance more affordable or more accessible to others.

Box 4: Parametric cyber insurance

It is often thought that parametric insurance only inhabits specialty areas of the reinsurance world, where it is bought by entire countries. Likewise, the product is commonly perceived to require an established reference index. This has certainly been true historically. But the changing cost and availability of data and associated analytics is fostering product innovation beyond natural catastrophes. Any recognisable peril that would cause loss can be incorporated into a parametric insurance solution provided sufficient analytical effort and skill is expended in designing an objective trigger that:

- Protects against fraud.
- Calculates the threshold at which the product pays so that it is sustainable to the insurer and fair to the insured.
- Establishes an insurable interest.
- Minimises as far as possible the basis risk.

In the context of cyber risk, in December 2019, specialty reinsurance group Chaucer partnered with InsurTech Qomplx to launch the first dedicated cyber parametric insurance (WonderCover).⁶³ The policy provides protection against operational losses arising from data breaches, IT interruption and non-property terrorism damage. Specifically, it provides automatic payment of a predetermined amount to the policyholder once any of three triggering event occurs:

- GDPR breach – a digital breach of personal data requiring notification to the U.K.'s Information Commissioner's Office under the EU's GDPR.
- IT outage – an interruption in service.
- Terrorism non-damage business interruption – a terrorist event occurring in the same postcode zone as the insured.

Initially targeted at U.K. small businesses, Wondercover is available for limits between GBP 5,000 and GBP 100,000.

Source: The Geneva Association and Raveem Ismail, ASR Re.

⁶³ Chaucer 2019.

Since HCA could disrupt wide swathes of society, cyber insurance based on solidarity pricing principles could boost take-up, although voluntary schemes would need to deal with free-rider problems.

Given that HCA could disrupt wide swathes of society and many firms and individuals could suffer collateral damage from an attack, arguably solidarity principles for pricing would boost cyber protection among those for whom it might otherwise be impossible to buy insurance. Such ex ante risk sharing may be appealing since governments, and ultimately taxpayers, will likely have to pick up the tab for harm suffered by victims of a large-scale, disruptive cyberattack. Generally, a scheme, which is built on solidarity foundations, would require comprehensiveness and compulsion to spread the risk across enough policyholders and overcome any free-rider problems.

By the same token, the cost of any government guarantee for underwriting extreme cyber risks – which would be incorporated into insurance premiums paid by households and firms – would need to weigh the benefits of making cover for catastrophic cyber incidents widely available at affordable rates against the strain such a potentially unlimited contingent liability could have on fiscal balance sheets. Among existing PPP schemes, the charge for the state guarantee varies widely, with governments in some countries assuming 50% of annual premiums paid into the relevant pool as a fee for providing the unlimited backstop (see Appendix).

5.1.6 Permanent or temporary scheme?

When developing a blueprint for a cyber PPP, its intended duration is a key consideration. Permanent PPP arrangements may offer advantages in terms of developing a long-term strategy for securing funding as well as accumulating capital. This includes mechanisms for the recovery of any shortfall in finances if the governmental guarantee is eventually called upon. But they can face stiff opposition from governments wary of making open-ended commitments that bind future administrations. Policymakers are also cautious of permanent schemes that potentially crowd out private market participants and stifle potential future innovation in insurance, especially if they provide coverage at less than actuarially-fair rates.

Permanent PPPs could help with long-term funding strategy development and capital accumulation, but policymakers are cautious that perpetual schemes could crowd out private market participants.

A number of existing schemes therefore typically build in rolling reviews to assess both their viability and ongoing usefulness. The review period is usually around three years although this varies by jurisdiction. In the case of terrorism risk schemes in Australia (Australian Reinsurance Pool Corporation) and in the U.S. (TRIP), periodic reviews take place to determine the extent to which a protection gap would remain (which cannot or will not be closed by the commercial insurance market) if the pool was disbanded. Such reviews also typically assess any changes to the operability or the functionality of the PPP.

In summary, designing such government-backed solutions for peak cyber risks is complex. There will be pros and cons in adopting particular scheme features and challenges in calibrating how the losses should be shared among policyholders, private re/insurers and governments (Table 3).

Table 3: Summary of the pros/cons of possible features of a PPP scheme

Scheme feature	Possible pros and cons
 Multi-peril (versus single peril)	Pro: Diversification opportunities Con: Higher administration costs
 Mandatory (versus voluntary)	Pro: Enlarges the premium pool and avoids adverse selection Con: Complex to monitor and enforce compliance
 Pre-funded (versus post-funded)	Pro: Incentivises risk prevention and mitigation and funds on-hand for disbursement Con: Political support to fund a contingency can often be challenging
 Parametric (versus indemnity-based)	Pro: Provides post-event liquidity faster and more efficiently Con: Payout may differ from the actual losses incurred
 Solidarity (versus mutuality principles)	Pro: Boosts cyber insurance to those who might otherwise be unable to afford it Con: Often requires comprehensiveness and compulsion
 Permanent (versus temporary)	Pro: Develops a long-term strategy for securing funding as well as accumulating capital Con: Potentially crowds out private market participants and stifles potential future innovation

Source: The Geneva Association

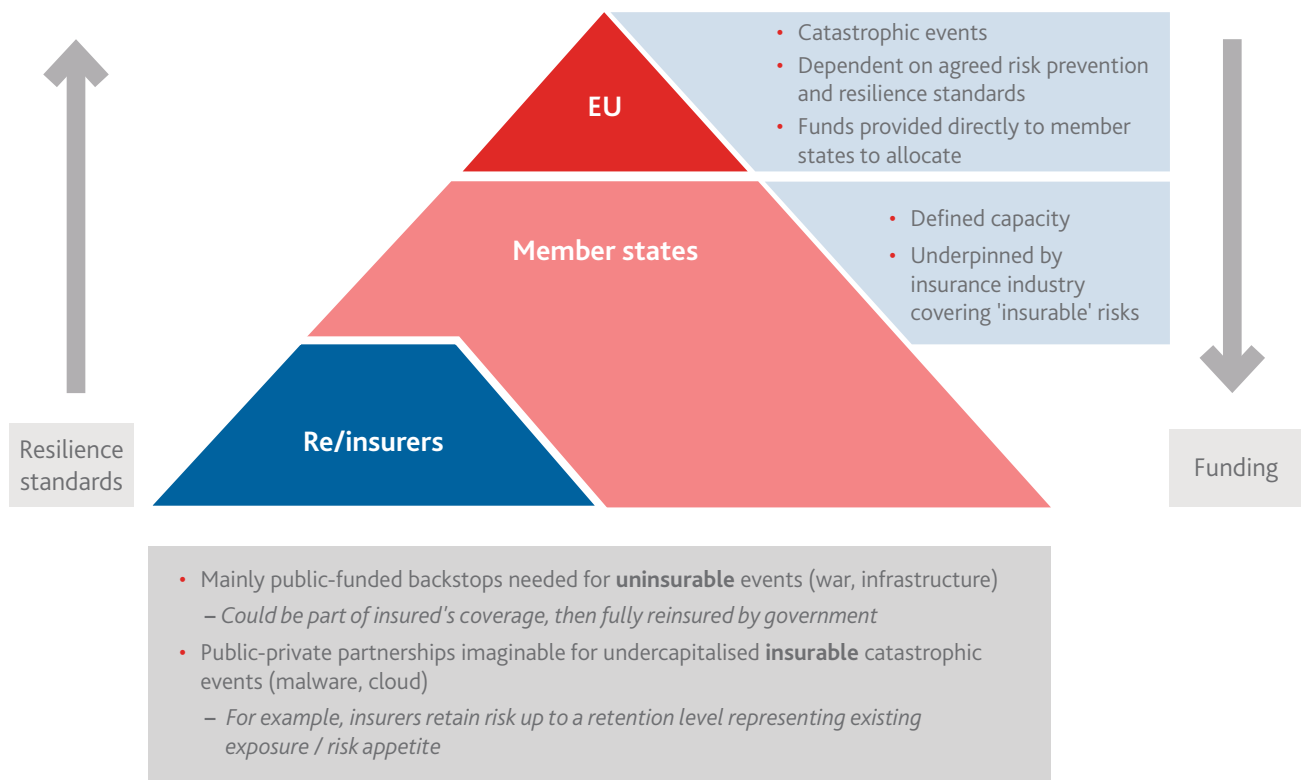
5.2 International operability and potential for cross-jurisdictional PPPs

Ideally, given the interconnected and global nature of cyber risks, co-operative international solutions to cover HCA risks would be an option. However, legal limitations, cultural differences, access to capital and doubts about the willingness of individual governments to share risks across different jurisdictions mean that global solutions remain practically infeasible, at least in the short term. Genuinely international solutions can therefore only be considered as aspirational.

Co-operative international solutions to cover HCA risks are optimal but legal limitations, cultural differences, access to capital and government unwillingness to share risks mean they are currently infeasible.

More realistically, the path towards greater international collaboration may instead begin within regional settings. For example, if a group of EU member states were to begin by sharing information about emerging cyber threats it might over time be possible to harmonise the way that PPPs operate for extreme cyber terrorism and potentially for HCA risks (see Figure 4). Information sharing is likely to promote awareness and preparedness, boosting overall cyber resilience. In turn, this may attract additional private sector re/insurance capacity to underwrite cyber risks, reducing the potential burden on states that provide backstop finance. Once various nation states have the same or comparable systems this could catalyse the search for full region-wide solutions to share risks, exploiting any potential regional diversification benefits against localised cyberattacks, in order to economise on paid-in and/or backstop capital. If successful, this might ultimately pave the way for future pan-regional PPP regimes.

Figure 4: A stylised structure for international cyber risk sharing within the EU



Source: Contributed by Rory Egan, Munich Re



6. Conclusions

This report finalises The Geneva Association's and IFTRIP's research trilogy into cyber terrorism, HCA and cyber warfare risks, which brings together insights into the insurance industry's approach to the insurability of these risks. In particular it builds on the framework developed by The Geneva Association and IFTRIP to define the term HCA.

HCA refers to malicious cyberattacks that extend beyond cyber terrorism but are not cyber war and involve or can be connected in some way to a state actor. It provides terminological clarity over what in many cases would otherwise be a potential grey area in terms of coverage of events. It assists with the process of attribution and characterisation by lowering the burden associated with having to 'prove' which state was responsible for an event.

Such events, which involve state actors but are akin to a cold-war-type event, are at present insured up to certain limits by the private re/insurance sector. Further growth of the commercial cyber insurance market should be encouraged. However, the potential accumulation losses caused by cyber terrorism or HCA events are too big and uncertain for the re/insurance market to absorb alone. As a result, it may ultimately be necessary to develop a PPP solution whereby the public sector absorbs some of the peak cyber risks. Suitably designed, such a PPP could continue to promote expansion and innovation in the private cyber insurance market and ensure fiscal stability to cope with large-scale events.

The structure of any PPP for cyber including HCA or cyber terrorism will differ depending upon the jurisdiction. It may be possible that an existing PPP scheme is extended to include all extreme cyber risks, especially HCA or cyber terrorism. Alternatively, a dedicated pool or other PPP solution for HCA might be developed. Important considerations for any PPP include whether the scheme is mandatory or voluntary, coverage is parametric or indemnity-based or if the scheme is founded upon mutuality or solidarity principles. From a fiscal and feasibility viewpoint, it will also be necessary to ensure that adequate measures are adopted to fund the scheme and to ensure sufficient capital, either on a pre- or post-event basis.

The insurance industry has come a long way in its understanding of cyber terrorism, HCA and cyber war and assessing how to insure such risks. To expand the limits of insurability, insurers need to be proactive in assessing feasible options for sharing cyber risks, including with governments via PPPs. Such collaborative efforts between insurers and governments will enable cyber protection gaps to be narrowed and ensure the full societal benefits of cyberspace can be realised.

Appendix:

Characteristics of existing PPPs for selected insurance risks

1. Terrorism risk

	Germany – EXTREMUS	Belgium – TRIP
Legal format	Private mono-liner acts as primary insurer for the insurance industry	Non-profit organisation, PPP
Distribution and participation	Insurance: Elective. Policies issued by EXTREMUS Reinsurance: Elective	Mandatory insurance policies held by virtually all citizens Membership not compulsory for insurers but high take-up
Risks in scope	Commercial and industrial property, BI and fire. Total sum insured per contract >EUR 25m	Property, casualty, workers comp, life & health lines
Layering concept: liability limits per cedent, market capacity, total pool capacity	Liability limit per cedent/risk EUR 1.5bn Private insurance and reinsurance market EUR 2.52bn State guarantee of EUR 6.48bn Total capacity incl. state guarantee EUR 9bn	Max EUR 75m per policy EUR 300m insurers' retention EUR 696m excess-of-loss EUR 300m reinsurers EUR 300m excess-of-loss EUR 996m Belgian state
State guarantee	Expanded until end-2022 up to EUR 6.48bn	Currently up to EUR 300m
Premium for state backstop	State receives 13.5% of premiums collected	Unknown

Source: PEIF⁶⁴

U.S. – TRIP	France – GAREAT	U.K. – Pool Re
U.S. government reinsurance backstop programme, administered by the U.S. Treasury Department	Non-profit organisation set up as a special vehicle (GIE- economic interest group)	Mutual reinsurer owned by its members/ cedents but underpinned by an unlimited guarantee from HM Treasury (PPP)
All insurers must offer coverage in certain commercial property and casualty lines, but acceptance is elective on the part of the commercial policyholders	Mandatory extension of all property policies without limitations or restrictions Mandatory membership (large risks) for members of the French Federation of Insurance	Policies distributed via member re/insurers Not compulsory. Member insurers must provide cover at the insured's request as a part of commercial policies Mandatory cession to Pool Re
Generally covers property, business interruption, workers compensation and third-party liability losses	All property damage and BI lines with sums insured >EUR 20m at 100%	Commercial property, commercial residential property, construction plants, machinery, NDBI
Once annual aggregate industry losses have exceeded USD 200m, the federal government would cover 80% of each insurer's losses above its deductible until the amount of losses (private and government combined) totals USD 100bn Total limit USD 100bn in aggregate losses	EUR 500m Annual aggregate members' retention EUR 2,280m excess-of-loss EUR 500m open market reinsurance layer Unlimited excess-of-loss EUR 2,780m (CCR layer benefits from unlimited state guarantee)	Members' retention Reinsurance: GBP 2.4bn excess-of-loss GBP 400m Pool Re retained earnings GBP 6.5bn Unlimited state guarantee upon depletion of Pool Re's funds
Yes. Limited to USD 100bn	Unlimited through CCR	Sponsored by HM Treasury; unlimited state guarantee
Insurers do not pay ex-ante contributions, but the U.S. Treasury Secretary will recoup all or part of any government outlays through surcharges on property and casualty insurance policies	State receives fee of 10% of annual premiums collected from large risk insurers At the end of each year, collected premium minus open market reinsurance and CCR reinsurance premium minus retained incurred losses is returned to members.	Pool Re pays 50% of gross written premium (inward) to government for the guarantee (used to be 10%). Any drawdowns under the guarantee would need to be repaid by Pool Re

2. Nuclear risks

Nuclear pool feature	Switzerland – SPN	France – Assuratome
Legal format	Simple company	GIE (Economic Interest Group)
Distribution and participation	Policies issued by a pool member Only the Nuclear Third Party Liability insurance is mandatory	Policies issued by a pool member. Only the Nuclear Third Party Liability insurance is mandatory
Risks in scope	SPN / Assuratome / DKVG provide liability and property insurance / reinsurance capacity for inland nuclear facilities and assume reinsurance shares on nuclear business written by other nuclear pools throughout the world.	
Layering concept: Liability limits per cedent, market capacity, total pool capacity	Nuclear operator liability unlimited Total limit: CHF 1.0bn provided by SPN	Nuclear operator liability limited to EUR 700m provided by Assuratome and private insurers
State involvement / guarantee	State covers insurance exclusions	French/German/U.K. allocation of USD 175m through their participation to the BSC (Brussels Supplementary Convention)
State involvement	Switzerland, France, Germany and the U.K. signed the Revised Paris Convention (due to come into force on 1 January 2022). Once in force, the insurance, or financial guarantee, limits will increase to GBP 1.2bn (min. EUR 700m and in this case, the state will have to cover the gap up to EUR 1.2bn) and an additional layer of EUR 300m will be provided by the States participating to the revised Brussels Supplementary Convention based on a predefined distribution key. Above the total of EUR 1.5bn, operators will stay liable in Switzerland (unlimited liability) and Germany (financial security at 2.5bn).	

Source: PEIF⁶⁵

65 PEIF 2020c.

Germany – DKG	U.K. – NRI	U.S. – ANI
Gesellschaft burgerlichen (Gbr) civil law association	Authorised insurance intermediary that acts as the underwriting agent	Joint underwriting association
Reinsurance policies issued by a DKG on behalf of pool members Only the Nuclear Third Party Liability insurance is mandatory	Policies issued by NRI on behalf of the pool members Only the Nuclear Third Party Liability insurance is mandatory	Policies issued by ANI on behalf of the pool members The Price-Anderson Act requires the nuclear operators to provide financial protection against public liability caused by a nuclear incident
	NRI uses its capacity both to directly write liability and property insurance for nuclear facilities in the U.K. and reciprocally to reinsure other nuclear sites around the world	ANI directly writes nuclear liability insurance for nuclear facilities in the U.S. and assumes reinsurance shares on nuclear business written by other nuclear pools and mutual insurers throughout the world
Nuclear operator liability is unlimited First insurance limit: EUR 256m is covered by the primary insurer and reinsurance by DKG. Second layer up to EUR 2,244bn is covered by the operators	Nuclear operator liability limited to insurance limit: GBP 140m provided by NRI and competitors	Nuclear operator liability limited to approx. USD 12bn (mutual liability for all operators) Insurance limit: USD 450m provided by ANI
		None
		None

3. Natural catastrophe risks

Nat cat pool feature	Switzerland – Elementarschadenspool / IRV (Inter-cantonal Reinsurance Union)	France – CCR
Legal format	ES: Consortium (administered by members) IRV: Reinsurance association of cantonal monopoly insurers	State reinsurer
Distribution and participation	ES: Reinsurance pool of the compulsory insurance in GUSTAVO cantons IRV: IRV manages the pool of the compulsory insurance in cantons with state monopolies. Additional property earthquake benefit in 17 out of 26 cantons (SPE – Schweizer Pool für Erdbeben), mandatory in Zurich (GVZ) Distribution of policies via members in both schemes	Distribution via insurers Natural disaster coverage is compulsory in all property insurance policies CCR unlimited reinsurance is not compulsory. High take-up
Risks in scope	ES: Residential and commercial property IRV: Residential and commercial property Coverage for nine named natural perils	Property, fire, motor, aircraft, vessel hull. Losses resulting from material damage or BI
Layering concept: Liability limits per cedent, market capacity, total pool capacity	ES: Per insured max. indemnity CHF 25m Reinsurance: CHF 1.1bn excess-of-loss up to 500m IRV: Reinsurance CHF 2bn excess-of-loss with annual aggregate deductible of CHF 580m	CCR cover up to an annual EUR 4.5bn event Provides 50% quota share and a non-proportional cover stop-loss to each insurer
State guarantee	No guarantee	Unlimited guarantee
State backstop	None	Through CCR dividend

Source: PEIF⁶⁶

U.K. – Flood Re	U.S. – NFIP	Spain – Consorcio
Limited company owned by U.K. insurers	The NFIP is administered by FEMA, part of the Department of Homeland Security	PPP owned by the government covering losses mainly in Spain
Distribution via U.K. insurers No compulsion for either homeowner to buy nor insurer to offer protection Flood component voluntarily cedent to Flood Re	1. Direct Servicing Agent, which operates on behalf of FEMA for individuals seeking NFIP insurance 2. Write-Your-Own (WYO) where insurance companies are paid to issue and service policies	Extraordinary risks are mandatory, such as natural catastrophes, terror, including political risks, damages of army & security forces (e.g. police) in peace times Motor liability: uninsurable drivers/risks and vehicles of government, uninsured/stolen/unknown vehicles causing third party damage
Flood component of property policy for privately held property build before 2009	Private and small commercial high-risk property exposed to flooding	Nat cat: property (incl. BI), motor own damage and motor damages if only MTPL, accident, life Prerequisite: Additional premium charged and CCS clause attached and premiums paid
Market retention Reinsurance: GBP 2.1bn Above reinsurance layer: Flood Re equity absorbs losses but can levy members for any excess	Reinsurance: total of USD 1.33bn (partial coverage of three layers; 10.25% of USD 4–6bn, 34.7% of USD 6–8bn, 21.8% of USD 8–10bn) Capital markets: USD 1.2bn Total capacity: USD 2.53bn	CSS has to set reserves and act as insurer for those risks (or as insurer of last resort/reinsurer/fall back option) No reinsurance (excess of capital) State guarantee for extraordinary events
No state guarantee	None	None
Insurers	NFIP is self-supporting but can incur debts in extraordinary year	CSS keeps premium to pay covered losses

References

- AIG. 2019. *The Role of Captives in Cyber Risk*. <https://www.aig.com/about-us/knowledge-insights/the-role-of-captives-in-cyber-risk>
- Aon. 2021a. *U.S. Cyber Market Update 2020. US Cyber Insurance Profits and Performance*.
- Aon. 2021b. *Aon's E&O | Cyber Insurance Snapshot. A Focused View of 2021 Risk & Insurance Challenges*.
- Artemis. 2021. *Time Right for ILS to Enter Cyber Reinsurance Market: Chatterjee, Envelop Risk*. <https://www.artemis.bm/news/time-right-for-ils-to-enter-cyber-reinsurance-market-chatterjee-envelop-risk/>
- Australian Government Transparency Portal. 2020. *How ARPCs Terrorism Insurance Scheme Operates*. <https://www.transparency.gov.au/annual-reports/australian-reinsurance-pool-corporation/reporting-year/2019-20-54>
- Bank of England (Prudential Regulatory Authority). 2019. *Letter to Chief Executives of the Specialist General Insurance Firms Regulated by the PRA*. <https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2019/cyber-underwriting-risk-follow-up-survey-results>
- Bateman, J. 2020a. *Alternative Exclusions for Cyber Claims*. Carnegie Endowment for International Peace.
- Bateman, J. 2020b. *War, Terrorism and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions*. Carnegie Endowment for International Peace.
- Bloomberg. 2021. *China's Microsoft Hack, Russia's SolarWinds Attack Threaten to Overwhelm U.S.* <https://www.bloomberg.com/news/articles/2021-03-09/microsoft-solarwinds-breaches-spark-two-front-war-on-hackers?sref=2Cms9tx3>
- Carter. R. 2013. *Cutting Out the Insurance Free Rider When it Comes to Finding Fire Services*. <https://theconversation.com/cutting-out-the-insurance-free-rider-when-it-comes-to-funding-fire-services-15852>
- Centre for Risk Studies. 2016. *Cambridge University: Cyber Terrorism: Assessment of the Threat to Insurance*.
- Chatham House Report. 2010. *On Cyber Warfare*. Author: Paul Cornish. https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf
- Chaucer. 2019. *Chaucer and Qomplx Launch First Ever Parametric Multi-peril Insurance*. <https://www.chaucergroup.com/news/chaucer-and-qomplx-launch-first-ever-parametric-multi-peril-insurance>
- Check Point. 2020. *Increase in Remote Working and Coronavirus Related Threats Creating Perfect Storm of Security Challenges for Organizations, New Survey Finds*. <https://www.checkpoint.com/press/2020/increase-in-remote-working-and-coronavirus-related-threats-creating-perfect-storm-of-security-challenges-for-organizations-new-survey-finds/>
- Coburn, A. et al. 2019. *Solving Cyber Risk: Protecting Your Company and Society*. Wiley.
- Congressional Research Service. 2019. *Protecting America: The Reauthorization of the Terrorism Risk Insurance Program*. <https://www.congress.gov/116/meeting/house/110078/witnesses/HHRG-116-BA04-Wstate-WebelB-20191016.pdf>
- Consorcio De Compensacion De Seguros. 2020. *An Overview*. https://www.consorseguros.es/web/documents/10184/48069/CCS2016_EN.pdf/b7ed4f5e-6400-41f5-a1fb-d98e5f6a3778
- CNBC. 2021. *Cyber Risk Problem Is So Big It Is Not Insurable*. <https://www.cnbc.com/video/2021/05/11/cyber-risk-problem-so-big-its-not-insurable-says-swiss-re-ceo.html>
- CRO Forum. 2016. *Concept Paper on a Proposed Methodology for Cyber-Risk*.
- CrowdStrike. 2020. *Global Threat Report*.
- Dixon, L., J. Arlington, S. Carroll, D. Lakdawalla, R. Reville, and D. Adamson. 2004. *Issues and Options for Government Intervention in the Market for Terrorism Insurance*. RAND Center for Terrorism Risk Management Policy. Occasional Paper.

European Parliament. 2018. *Attribution of the NotPetya Attack*. https://www.europarl.europa.eu/doceo/document/E-8-2018-001005_EN.html

FireEye. 2020. *Sunburst Additional Technical Details*. <https://www.fireeye.com/blog/threat-research/2020/12/sunburst-additional-technical-details.html>

FireEye Report: Reimagined. Various Solution Briefs.

Gallagher Re. 2020. *Cry Cyber and Let Slip the Dogs of War*. <https://www.ajg.com/gallagherre/news-and-insights/2020/aug/whitepaper-cyber-and-acts-of-war/>

Geers, K. et al. *World War C: Understanding Nation-State Motives behind Today's Advanced Cyber Attacks*.

Global Data. 2021. *Cyber Insurance Industry to Exceed \$20bn by 2025*. https://www.globaldata.com/cyber-insurance-industry-exceed-20bn-2025-says-globaldata/?utm_source=dlvr.it&utm_medium=twitter

GlobalNewswire. 2021. *Cloudian Ransomware Survey Finds 65% of Victims Penetrated by Phishing Had Conducted Anti-Phishing Training*. <https://www.globenewswire.com/news-release/2021/07/15/2263492/0/en/Cloudian-Ransomware-Survey-Finds-65-of-Victims-Penetrated-by-Phishing-Had-Conducted-Anti-Phishing-Training.html>

Hitzel, B. 2020. *The Biggest Single Point of Failure in Human History - A Cloud*. <https://www.networkdefenseblog.com/post/biggest-single-point-of-failure>

Hull, T. 2010. A Deterministic Scenario Approach to Risk Management. *2010 Enterprise Risk Management Symposium, Society of Actuaries, 12–15 April 2010*.

IDC. 2021. *IDC Survey Finds More Than One Third of Organizations Worldwide Have Experienced a Ransomware Attack or Breach* <https://www.idc.com/getdoc.jsp?containerId=prUS48159121>

IFTRIP. 2018. *Cyber Terrorism and Pools*.

IFTRIP. 2019. *Cyber Terrorism and Warfare Definitions*.

Lloyd's and University of Cambridge. 2015. *Business Blackout. Insurance Implications of a Cyber-attack on the US Power Grid*. <https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/technology-and-space/lloyds-business-blackout-scenario/>

Lloyd's and Cyence. 2017. *Counting the Cost. Cyber Exposure Decoded*. <https://www.lloyds.com/~media/files/news-and-insight/risk-insight/2017/cyence/emerging-risk-report-2017---counting-the-cost.pdf>

Lloyd's and AIR. 2018. *Cloud Down – Impacts on the U.S. Economy*.

Lloyd's and CyRiM. 2019. *Bashe Attack. Global Infection by Contagious Malware*. <https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/technology-and-space/cyrim-scenario-bashe-attack/>

Marsh (undated). *Silent Cyber: What It is and How You Can Cover Cyber Perils*. <https://www.marsh.com/uk/services/cyber-risk/products/silent-cyber-how-you-can-cover-perils.html>

Marsh. 2021. *Global Insurance Market Index: 2021 Q3*. https://www.marsh.com/dk/en/services/insurance-market-and-placement/insights/global_insurance_market_index.html

Mazarr, M., R. Bauer, A. Casey, S. Heintz, and L. Matthews. 2019. *The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment*. Rand Corporation.

Menapace, M. 2019. *As Cybersecurity Risks Evolve, So Must Our Preparedness*.

Microsoft. 2021. *Deep Dive into the Solorigate Second-stage Activation: From SUNBURST to TEARDROP and Raindrop*. <https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/>

Microsoft. 2020. *Protecting People in Cyberspace: The Vital Role of the United Nations in 2020*. <https://www.un.org/disarmament/wp-content/uploads/2019/12/protecting-people-in-cyberspace-december-2019.pdf>

- Microsoft. 2020. *Using Microsoft 365 Defender to Protect Against Solorigate*. <https://www.microsoft.com/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/>
- Munich Re. 2018. *What if a Major Cyber-attack Strikes Critical Infrastructure?* | *Munich Re Topics Online*. <https://www.munichre.com/topics-online/en/digitalisation/cyber/silent-cyber.html>
- Munich Re. 2020. *Equity Story. Investor Presentation*.
- National Cyber Security Centre (U.K.). 2018. *Russian Military 'Almost Certainly' Responsible for Destructive 2017 Cyber-attack* <https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack>
- Paudel, Y. 2012. A Comparative Study of Public—Private Catastrophe Insurance Systems: Lessons from Current Practices. *The Geneva Papers on Risk and Insurance—Issues and Practice* 37: 257–285.
- PCS. 2019. *Could NotPetya's Tail Be Growing?* <https://www.verisk.com/siteassets/media/pcs/pcs-cyber-catastrophe-notpetyas-tail.pdf>
- PEIF. 2020a. *Cyber Risk Pooling*. Unpublished.
- PEIF. 2020b. *International Comparative of Terror Pools*. As revised by IFTRIP, August 2021. Unpublished.
- PEIF. 2020c. *International Comparison of Nuclear Risk Pools*. Unpublished.
- PEIF. 2020d. *International Comparison of Natural Catastrophe Pools*. Unpublished.
- Pew trusts. 2021. *Florida Hack Exposes Danger to Water Systems*. <https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/03/10/florida-hack-exposes-danger-to-water-systems> March 10, 2021
- Pool Re. 2020. *Guaranteeing Great Britain: Managing Terrorism Risk and Building Resilience – Pool Re's 2020 Review and the Next Five Years*. https://www.poolre.co.uk/wp-content/uploads/2020/09/COH_J012852-PoolRe-White-Paper-web.pdf
- PropertyCasualty360. 2021. *The WFH Impact on the Cyber Insurance Market*. <https://www.propertycasualty360.com/2021/07/22/the-wfh-impact-on-the-cyber-insurance-market/>
- Satter, R., and K. Singh. 2018. *U.K. Government. Foreign Office Minister Condemns Russia for NotPetya Attacks*. <https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks>
- SecurityWeek. 2020. *SolarWinds Says 18,000 Customers May Have Used Compromised Orion Product*. <https://www.securityweek.com/solarwinds-says-18000-customers-may-have-used-compromised-product>
- Sengupta, R., and C. Kousky. 2020. *Parametric Insurance for Disasters*. https://riskcenter.wharton.upenn.edu/wp-content/uploads/2020/09/Parametric-Insurance-for-Disasters_Sep-2020.pdf
- Statement from the U.S. Foreign Policy Press Secretary. 2018. *NotPetya*. <https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/>
- Stoltenberg, J. 2019. *Remarks at the Cyber Defence Pledge Conference, London*. https://www.nato.int/cps/en/natohq/opinions_166039.htm
- SVV. 2021. *Affordable Natural Perils Insurance Thanks to the ES Pool*. <https://www.svv.ch/en/insurance/property-and-casualty-insurance/natural-perils-insurance/affordable-natural-perils>
- Swiss Re. 2017. *Cyber: Getting to Grips with a Complex Risk*. Sigma No.1.
- The Geneva Association. 2018. *Advancing Accumulation Risk Management in Cyber Insurance*. Authors: Daniel Hofmann, Steve Wilson and Rachel Anne Carter. August. <https://www.genevaassociation.org/research-topics/cyber/advancing-accumulation-risk-management-cyber-insurance>
- The Geneva Association. 2020a. *Cyber War and Terrorism: Towards a common language to promote insurability*. Authors: Rachel Anne Carter and Julian Enoizi. July. <https://www.genevaassociation.org/research-topics/cyber/CTCW-common-language>
- The Geneva Association. 2020b. *An Investigation into the Insurability of Pandemic Risk*. Author: Kai Uwe Schanz. October. <https://www.genevaassociation.org/research-topics/socio-economic-resilience/investigation-insurability-pandemic-risk-research-report>
- The Geneva Association. 2021a. *Cyber Expert Forum 2021. Meeting summary*. <https://www.genevaassociation.org/cyber-expert-forum-2021-meeting-summary>
- The Geneva Association. 2021b. *Mapping a Path to Cyber Attribution Consensus*. Authors: Rachel Anne Carter and Julian Enoizi. March. <https://www.genevaassociation.org/research-topics/cyber/cyber-attribution-research-report>

Thomson Reuters. 2021a. *Microsoft Says Group Behind SolarWinds Hack Now Targeting Government Agencies, NGOs*. <https://www.reuters.com/technology/microsoft-says-group-behind-solarwinds-hack-now-targeting-government-agencies-2021-05-28>

Thomson Reuters. 2021b. *Recovery of Colonial Pipeline Ransom Funds Highlights Traceability of Cryptocurrency, Experts Say*. <https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/colonial-pipeline-ransom-funds/>

U.K. Government. *Foreign Secretary Welcomes first EU Sanctions against Malicious Cyber Actors*. 30 July 2020. <https://www.gov.uk/government/news/uk-enforces-new-sanctions-against-russia-for-cyber-attack-on-german-parliament>

United States Cyberspace Solarium Commission, March 2020.

U.S. Government. *Press Briefing on the Attribution of WannaCry Malware Attack to North Korea*. 19 December 2017. <https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/>

U.S. Department of Treasury. *Treasury Sanctions Russian Cyber Actors for Interference with 2016 Elections and Malicious Cyber Attacks*. 15 March 2018. <https://home.treasury.gov/news/press-releases/sm0312>

U.S. Department of Treasury. *Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021*. 15 October 2021. https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf

Voreacos, D. et al. 2019. Merck Cyber Attack's \$1.3 Billion Question: Was It an Act of War? *Bloomberg*. 3 December 2019. <https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war>

Walker, K. 2018. *Blog: An Update on State Sponsored Activity*. <https://blog.google/technology/safety-security/update-state-sponsored-activity>

Willis Re. 2020. *Covid-19 Has Changed How We Think About Cyber Risk*. <https://www.willistowerswatson.com/en-CH/Insights/2020/09/covid-19-has-changed-how-we-think-about-cyber-risk>

Willis Towers Watson. 2019. *The Terrorism Pool Index: Review of Terrorism Insurance Programs in Selected Countries 2019/ 2020*.

Wired. 2018. *The Untold Story of NotPetya: The Most Devastating Cyberattack in History*. <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

Wired. 2019. *US Hackers Strike on Russian Trolls Sends a Message- But What Kind?* <https://www.wired.com/story/cyber-command-ira-strike-sends-signal/>

Wired. 2021. *The Colonial Pipeline Hack Is a New Extreme for Ransomware*. <https://www.wired.com/story/colonial-pipeline-ransomware-attack/>

Woo, G., T. Maynard, and J. Seria. 2017. *Reimagining History: Counterfactual Risk Analysis*.

World Economic Forum. 2020. *Cybersecurity, Emerging Technology and Systemic Risk*.

Wright, J. 2018. *Cyber and International Law in the 21st Century*. Attorney General's Office, United Kingdom.

State-sponsored cyberattacks that stop short of outright military conflict, otherwise known as hostile cyber activity (HCA), pose a threat to insurability due to the scale of potential accumulated losses. This third and final report in our series on cyber terrorism and cyber war examines in detail the ability of the private re/insurance sector to underwrite HCA risks and the role that public-private partnerships can play in fostering effective solutions.

The Geneva Association

International Association for the Study of Insurance Economics

Talstrasse 70, Zurich, Switzerland

Tel: +41 44 200 49 00

www.genevaassociation.org