Insurance Coverage for Cyber Terrorism in Australia
Insurance Coverage for Cyber Terrorism in Australia
Foreword

The increasing integration of digital technologies into business and infrastructure management and operations has greatly enhanced efficiency but has also led to new vulnerabilities that can be exploited by terrorists and other politically motivated actors to cause harm and economic disruption. In particular, the increasing digitalisation of operational technologies, such as building management systems and industrial control systems, the proliferation of connected devices (“Internet of Things”) and the automation of transport systems will greatly expand the potential for cyber-attacks to lead to serious damage to property, bodily injury and disruptions to critical infrastructure services.

A number of real-life examples of cyber-attacks on operational technologies have led to property damage and/or serious economic disruption, including attacks that resulted in blackouts in the Ukraine and a fire at an industrial facility in Germany. There is also increasing evidence of efforts to access the networks of commercial, industrial and infrastructure facilities in countries around the world. While most of these attacks and intrusions have been attributed to sophisticated nation-state actors, it may only be a matter of time before terrorist organisations gain access to the capabilities and tools necessary to execute destructive attacks.

In response to these developments, several terrorism (re)insurance programmes established to ensure sufficient insurance coverage against losses from conventional (physical) terrorist attacks have been examining the risk of cyber-terrorism and how their programmes might respond. The Australian Reinsurance Pool Corporation (ARPC) initiated a research study on the threat of cyber-terrorism in Australia, including the nature and cost of physical damage to commercial property (including business interruption) which may be caused by acts of cyber terrorism. The ARPC invited the OECD and the University of Cambridge Centre for Risk Studies (CCRS) to:

- develop cyber-terrorism scenarios and estimates of economic impact, including potential systemic risks (CCRS); and
- analyse the available insurance coverage for cyber-terrorism losses, both internationally and in Australia (including from terrorism (re)insurance pools) and assess possible options for extending ARPC coverage to cyber-terrorism (OECD).

This report provides the OECD’s analysis and assessment of insurance coverage and options for extending ARPC coverage. It has been developed based on a review of available policy wordings across four main lines of insurance business (industrial special risk/commercial property, cyber insurance, public/general liability and terrorism insurance) and benefitted from consultations with industrial special risk/commercial property, cyber insurance and public liability underwriters in Australia as well as the administrators of terrorism (re)insurance programmes from around the world.
## Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>3</td>
</tr>
<tr>
<td>Glossary and abbreviations</td>
<td>7</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>9</td>
</tr>
<tr>
<td>1. Private insurance coverage for cyber-terrorism risks</td>
<td>11</td>
</tr>
<tr>
<td>2. ARPC coverage for cyber-terrorism risk</td>
<td>23</td>
</tr>
<tr>
<td>3. Assessment of coverage gaps</td>
<td>27</td>
</tr>
<tr>
<td>4. Providing coverage to cyber-terrorism: options and considerations</td>
<td>34</td>
</tr>
<tr>
<td>Annex A. International approaches to ensuring the availability of coverage for cyber terrorism</td>
<td>47</td>
</tr>
<tr>
<td>References</td>
<td>60</td>
</tr>
<tr>
<td>Notes</td>
<td>70</td>
</tr>
</tbody>
</table>

### Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 3.1.</td>
<td>Laptop Battery Fires attack losses</td>
<td>27</td>
</tr>
<tr>
<td>Table 3.2.</td>
<td>Building Management Systems attack losses</td>
<td>28</td>
</tr>
<tr>
<td>Table 3.3.</td>
<td>ISR coverage of scenario losses</td>
<td>29</td>
</tr>
<tr>
<td>Table 3.4.</td>
<td>Cyber insurance coverage of scenario losses</td>
<td>30</td>
</tr>
<tr>
<td>Table 3.5.</td>
<td>Cyber insurance coverage of scenario losses</td>
<td>31</td>
</tr>
<tr>
<td>Table 3.6.</td>
<td>Stand-alone terrorism insurance coverage of scenario losses</td>
<td>31</td>
</tr>
<tr>
<td>Table 3.7.</td>
<td>Overall insurance coverage for scenario losses</td>
<td>32</td>
</tr>
<tr>
<td>Table A A.1.</td>
<td>Overview of terrorism (re)insurance programmes</td>
<td>48</td>
</tr>
<tr>
<td>Table A A.2.</td>
<td>Definitions of terrorism applied by terrorism (re)insurance programmes</td>
<td>49</td>
</tr>
</tbody>
</table>

### Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1.1.</td>
<td>Types of losses covered in stand-alone cyber insurance policies</td>
<td>12</td>
</tr>
</tbody>
</table>

INSURANCE COVERAGE FOR CYBER TERRORISM IN AUSTRALIA © OECD 2020
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2</td>
<td>The size of the cyber, property and liability insurance markets</td>
<td>13</td>
</tr>
<tr>
<td>2.1</td>
<td>Funding of losses under the ARPC scheme</td>
<td>24</td>
</tr>
<tr>
<td>A A.1</td>
<td>Primary coverage for physical damage and consequential business interruption by terrorism (re)insurance programmes</td>
<td>51</td>
</tr>
<tr>
<td>A A.2</td>
<td>Co-insurance/reinsurance coverage for physical damage and consequential business interruption by terrorism (re)insurance programmes: <em>property policies</em></td>
<td>54</td>
</tr>
<tr>
<td>A A.3</td>
<td>Co-insurance/reinsurance coverage for physical damage and consequential business interruption by terrorism (re)insurance programmes: <em>cyber policies</em></td>
<td>56</td>
</tr>
<tr>
<td>A A.4</td>
<td>Coverage for business interruption without material damage by terrorism (re)insurance programmes</td>
<td>58</td>
</tr>
<tr>
<td>A A.5</td>
<td>Co-insurance/reinsurance coverage for liability by terrorism (re)insurance programmes</td>
<td>59</td>
</tr>
</tbody>
</table>

**Boxes**

<table>
<thead>
<tr>
<th>Box</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Cyber exclusions that may be applied in commercial property policies</td>
<td>16</td>
</tr>
<tr>
<td>1.2</td>
<td>Coverage for losses without physical damage</td>
<td>21</td>
</tr>
<tr>
<td>3.1</td>
<td>Scenario losses – the insurance response in other countries</td>
<td>33</td>
</tr>
<tr>
<td>4.1</td>
<td>Pool Re coverage for cyber-terrorism</td>
<td>38</td>
</tr>
<tr>
<td>4.2</td>
<td>Challenges in assessing exposure to cyber risk</td>
<td>39</td>
</tr>
<tr>
<td>4.3</td>
<td>Litigation on the applicability of war exclusions to cyber-attacks</td>
<td>43</td>
</tr>
<tr>
<td>4.4</td>
<td>Mitigating cyber accumulation risk</td>
<td>45</td>
</tr>
<tr>
<td>4.5</td>
<td>Overspill reinsurance example</td>
<td>46</td>
</tr>
</tbody>
</table>
# Glossary and abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARPC</td>
<td>Australian Reinsurance Pool Corporation (terrorism (re)insurance programme in Australia)</td>
</tr>
<tr>
<td>CCRS</td>
<td>University of Cambridge Centre for Risk Studies</td>
</tr>
<tr>
<td>CCS</td>
<td>Consorcio de Compensación de Seguros (terrorism (re)insurance programme in Spain)</td>
</tr>
<tr>
<td>GAREAT</td>
<td>Gestion de l'Assurance et de la Réassurance des risques Attentats et actes de Terrorisme (terrorism (re)insurance programme in France)</td>
</tr>
<tr>
<td>IFTRIP</td>
<td>International Forum for Terrorism Risk (Re) Insurance Pools (association)</td>
</tr>
<tr>
<td>IMTRIP</td>
<td>Indian Market Terrorism Risk Insurance Pool (terrorism (re)insurance programme in India)</td>
</tr>
<tr>
<td>NBCR</td>
<td>Nuclear, Biological, Chemical and Radiological</td>
</tr>
<tr>
<td>NHT</td>
<td>Nederlandse Hervorzekeringsmaatschappij voor Terrorismschaden (terrorism (re)insurance programme in the Netherlands)</td>
</tr>
<tr>
<td>OVDT</td>
<td>Österreichischer Versicherungspool zur Deckung von Terrorisken (terrorism (re)insurance programme in the Austria)</td>
</tr>
<tr>
<td>RATIP</td>
<td>Russian Anti-Terrorism Insurance Pool (terrorism (re)insurance programme in Russia)</td>
</tr>
<tr>
<td>SRCC</td>
<td>Strikes, Riots and Civil Commotion</td>
</tr>
<tr>
<td>TRIA</td>
<td>Terrorism Risk Insurance Act (the legislation underlying the Terrorism Risk Insurance Program in the United States)</td>
</tr>
<tr>
<td>TRIP</td>
<td>Terrorism Reinsurance and Insurance Pool (terrorism (re)insurance programme in Belgium)</td>
</tr>
</tbody>
</table>

## Glossary of terms

**Declared Terrorist Incident (DTI):** defined under the Terrorism Insurance Act 2003 as an incident that meets the criteria for the Act to apply.

**Deductible/Retention:** The level of losses which either the policyholder (for insurance) or cedant (for reinsurance) must absorb before the (re)insurance coverage is triggered. For business interruption losses, the deductible may be expressed as a time-deductible (number of hours or days of disruption before the insurance coverage is triggered).

**Difference-in-Conditions/Difference-in-Limits:** A type of insurance policy that provides insurance for any gaps in insurance coverage in another policy (for example, the DIC/DIL policy might provide a higher insured limit or a broader scope of coverage).

**Eligible insurance contract:** defined under the Terrorism Insurance Act 2003 as the types of insurance coverages subject to the Act and eligible for ARPC reinsurance coverage.

**Government guarantee/backstop:** in this context, refers to the funding that would be made available by the government for any losses incurred that are beyond the financial capacity of the terrorism (re)insurance programme, which may be limited or unlimited.

**Sub-limit:** a limit on insurance coverage that is lower than the insured limit and may be applied for specific types of losses (such as contingent business interruption losses).
Executive Summary

The increasing digitalisation of operational technologies used in commercial, industrial and infrastructure facilities, the proliferation of connected devices (Internet of Things) and the growing automation of transportation systems has created new vulnerabilities that can be exploited by terrorists and other politically-motivated actors to cause harm and economic disruption. Cyber-attacks on the electricity grid in the Ukraine and an industrial facility in Germany have demonstrated the ability to exploit these vulnerabilities while attempts to access critical infrastructure networks around the world portend to the possibility of destructive attacks in the future. In response, the insurance market – and the terrorism (re)insurance programmes that enable private coverage for terrorism losses – are developing new forms of coverage to address these emerging risks.

Insurance coverage for cyber risks is emerging...

Property insurance companies are expanding the insurance coverage they provide to include cyber incidents as a peril and data and software as covered losses. A cyber insurance market has emerged to provide coverage for the first party costs and third party liability claims that may arise as a result of malicious and accidental cyber incidents – often in response to gaps that have developed in traditional property and liability insurance coverage. While insured limits offered and take-up rates remain low relative to other commercial insurance markets, growing risk awareness and the proliferation of privacy protection legislation are reducing this gap.

...although there is a gap in coverage for politically-motivated, destructive cyber-attacks

In many countries, commercial property policies may apply exclusions for losses resulting from cyber-attacks, even where the attack results in property damage. Where coverage is offered, terrorism and war exclusions will normally apply leaving policyholders uninsured. The cyber insurance market is unlikely to address this gap in coverage, particularly in Australia where the widespread use of Industrial Special Risk (ISR) Mark IV policy wordings has resulted in broad coverage for property damage resulting from cyber-attacks – and little need for the inclusion of such coverage in cyber insurance policies offered in Australia.

Changes to ARPC’s mandate could address the gap in coverage...

Under the Terrorism Insurance Act 2003 and the Terrorism Insurance Regulations 2003, the Australian Reinsurance Pool Corporation (ARPC) offers reinsurance coverage for losses resulting from declared terrorist incidents (DTI) - and almost all commercial property in Australia is reinsured by ARPC. In the event of a DTI, the terrorism exclusions applied to commercial property policies are annulled and insurers are
required to pay claims as they would for any other incurred damages and losses, with the backing of ARPC’s reinsurance. However, insurance coverage provided for cyber-attacks is not currently subject to the Act and is not eligible for ARPC reinsurance. As a result, the losses incurred as a result of a cyber-terrorism incident are likely to be largely uninsured, requiring policyholders to absorb the vast majority of the resulting losses. Based on two cyber-terrorism scenarios developed by the University of Cambridge Centre for Risk Studies (CCRS), these losses could reach AUD 42 billion to AUD 83 billion. Should these risks materialise, it could place a significant burden on commercial property owners and lead to substantial reputational impacts for insurance companies, ARPC and the government. ARPC is relatively unique (if not alone) among terrorism (re)insurance programme in not providing any coverage for cyber-terrorism as a result of a legislative or regulatory restriction.

This report assesses a number of options for addressing the gap in insurance coverage for cyber-terrorism losses, including an extension of the scope of the Act to invalidate the application of exclusions of cyber-terrorism losses as well as options involving an expansion of the coverage provided by ARPC to include cyber-terrorism or potentially a broader set of politically-motivated malicious cyber-attacks. Consultations with market participants suggested that a private market coverage for losses resulting from politically-motivated malicious cyber-attacks is unlikely to emerge in the near-term without the support of ARPC reinsurance coverage. The approach in Australia to insuring property on an all-risk (including cyber) basis combined with the annulment of exclusions provided for in the Act would allow ARPC to provide an effective coverage for cyber-terrorism.

...although would create a number of implementation challenges that would need to be addressed.

An expansion of ARPC coverage would involve a number of implementation challenges related to the pricing of the expanded coverage and the ability of ARPC to secure retrocession coverage. It would also require that difficulties related to the attribution of cyber-attacks be overcome, although this issue would need to be resolved even if no changes were made to the scope of ARPC’s operations. The report provides an initial assessment of these issues as well as some options on possible approaches to limit the potential for accumulated losses and reduce the frequency of claims for ARPC (and the government).
1. Private insurance coverage for cyber-terrorism risks

The growing reliance on digital technologies in commercial activities has led to a need for insurance coverage that provides financial protection against property damage, business interruption, contingent business interruption and financial and liability losses that may be incurred as a result of cyber incidents. Coverage for these losses may be found in traditional commercial property/industrial special risk (ISR) policies and general/public liability policies (whether as a standard coverage or endorsement) as well as in the stand-alone cyber insurance policies that have been developed to address gaps in the coverage for cyber risks provided in traditional policies.

This chapter provides an overview of the coverage that is normally provided for losses resulting from cyber-attacks in stand-alone cyber insurance, commercial property/ISR, general/public liability as well as specialised stand-alone terrorism insurance policies. The overview is focused on the types of losses that may be reinsured by the ARPC in the event of a declared terrorism incident (i.e. property damage, business interruption, contingent business interruption and liability) as well as the treatment of terrorism as a peril in each type of policy.

1.1. Stand-alone cyber insurance

Stand-alone cyber insurance coverage first emerged in the United States in response to gaps in the coverage provided by traditional commercial property and liability policies (sometimes as a result of new exclusions – see Box 1.1.) and was driven by legislation in various US states imposing notification requirements and penalties for privacy breaches. Over the years, the product expanded to become a one-stop-shop for covering most first party and third party losses related to cyber incidents, including (most commonly):

- Coverage for defence costs, fines and penalties and compensation/redress (third party claims) resulting from:
  - Privacy liability: failure to prevent access to – or disclosure of – personal information or confidential commercial information;
  - Network security liability: damages to third parties transmitted through an information technology network (e.g. virus transmission or use of network assets in a denial of service attack); and
  - Media liability: misuse of communication media that results in defamation, libel, slander or patent/copyright infringement.
- Coverage for first party costs resulting from:
  - The need to respond to a cyber incident (including notification costs, public relations, etc.);
  - Damage to - or loss of - data and software;
o Business interruption (and, often, contingent business interruption) losses that are incurred due to a network disruption (often including a disruption at an information technology service provider such as a cloud service); and

o Financial losses resulting from fraud, theft or extortion perpetrated by digital means (such as ransomware or social engineering attacks that lead to fraudulent financial transfers).

Figure 1.1 provides an overview of the types of losses covered in stand-alone cyber insurance policies in different markets around the world, based on a review of the stand-alone cyber insurance policies of the largest cyber insurers (where available) as well as specialty cyber insurers operating on the Australian market.

**Figure 1.1. Types of losses covered in stand-alone cyber insurance policies**

![Figure 1.1. Types of losses covered in stand-alone cyber insurance policies](image)

*Note: Includes all available coverage (including endorsements) provided in stand-alone cyber insurance policies offered by AIG (Australia, UK, US); Allianz Global Corporate & Specialty (Global); Allied World (US); AXA XL (Australia, US); Beazley (UK, US); CFC Underwriting (Global); Chubb (Australia, UK, US); DUAL (Australia); Emergence Insurance (Australia); Hiscox (UK, US); Liberty International Underwriters (Australia); Munich Re Corporate Insurance Partner (Global); QBE (Australia, Europe, US); Swiss Re Corporate Solutions (Global); Tokio Marine HCC (Europe); Zurich Insurance (Australia, Netherlands, US).*

The stand-alone cyber insurance market has grown rapidly in recent years and is expected to continue to grow at a fast-pace as take-up increases in markets outside the United States and as privacy and cyber security requirements are implemented in countries around the world. Most estimates of the size of the market suggest written premiums of approximately USD 4-5 billion globally with expectations that the market will double or triple over the next five years (Deloitte Center for Financial Services, 2018[1]), (Orbis Research, 2018[2]), (OECD, 2017[3]), (Faulkner, 2019[4]). Similar to other countries, the stand-alone cyber insurance market is growing quickly in Australia (partly driven by the introduction of mandatory data breach notification requirements in 2018) with estimates of written premium of around AUD 100 million (Aon, 2019[5]) Despite recent and projected growth, the market remains small relative to the much larger property and liability insurance markets (see Figure 1.2).
Relative to the commercial property and liability insurance markets, take-up rates for cyber insurance remain relatively low. While estimates vary, one recent survey (Hiscox, 2018[7]) found that 33% of surveyed companies in Germany, the Netherlands, Spain, the United Kingdom and the United States had cyber insurance1 although with significant variation between large (250 or more employees) and small companies (57% of large companies had cyber insurance vs. 23% of small companies). In Australia, some estimates have suggested take-up rates to be as high as 48% (Aon, 2017[8]) although market participants consulted for the purposes of this study suggested overall take-up rates closer to 20% of all companies (and 35% of larger companies). By comparison, take-up rates for commercial property coverage in most developed markets approach 100%.

In Australia, insurers’ advertised limits range from AUD 5 million to AUD 20 million for a single policyholder although some insurers are able to offer larger amounts (approximately AUD 100 million) through global programmes. According to one recent report, the Australian market may be able to provide AUD 150 million or more in limits (Aon, 2017[8]) which would be consistent with limits offered by the largest cyber insurers internationally (OECD, 2017[3]). In some cases, coverage towers for cyber risks have also been developed offering reported aggregate limits of USD 600 million in some markets (Willis Towers Watson, 2018[9]). By comparison, AIG offers commercial property limits of up to AUD 1.5 billion in Australia (AIG, n.d.[10]).
1.1.1. Coverage for property damage and business interruption in cyber insurance policies

Only two of the companies whose policies were reviewed offer coverage for property damage resulting from a cyber incident (one in the United States and one offered globally). The policies that offer specific coverage for property damage offer that coverage on a case-by-case basis (Munich Re and Beazley, 2017) or as a tailored policy endorsement (AIG, 2016). There was no coverage for property damage (other than some coverage for computer equipment) in any of the eight reviewed policies offered in the Australian market. Insurance companies providing stand-alone cyber insurance in Australia confirmed that this loss was not covered by cyber insurance in Australia and indicated no plans to begin offering that coverage under cyber insurance policies.

Coverage for business interruption due to a network disruption is provided in most stand-alone cyber insurance policies (27 of 29 policies reviewed) and often (17 of 29 policies reviewed) extends to a disruption at information technology service providers (i.e., a form of contingent business interruption). Some insurers are also extending coverage to network disruptions at other types of (named) suppliers (Insurance Journal, 2019) although disruptions at utility providers (internet service, telecommunications, power) are usually specifically excluded. All of the Australian market policies reviewed included coverage for business interruption with some (at least three policies) extending that coverage to include some types of contingent business interruption but not disruptions to utility providers.

In addition, a few insurance companies are offering coverage for property damage, business interruption (and other types of losses) through difference-in-conditions (DIC) policies. These policies are designed to complement existing property insurance (or other) coverage by insuring property damage not otherwise covered by existing policies (i.e., they are designed to specifically address the gaps in existing coverage) (Carter, 2016). A search for providers of this coverage found only three policies that offer this coverage (sometimes as an endorsement), with marketing focused on US clients (although with a possibility that the coverage may be available in other markets).

At least one insurance company is offering a stand-alone coverage for cyber-attacks, designed to cover first-party damages and losses including property damage, consequential business interruption and crisis management costs. The coverage advertises limits of up to USD 50 million per risk although with a focus on Europe and North America (XL Catlin, n.d.).

1.1.2. Treatment of terrorism as a peril in cyber insurance policies

Stand-alone cyber insurance policies often provide coverage for cyber-terrorism. Among the stand-alone cyber insurance policies reviewed, thirteen provided sufficient detail (e.g., policy wordings) to allow for an assessment of whether cyber-terrorism (or terrorism more generally) was excluded from the policy. In almost all cases, there was no exclusion for cyber-terrorism, as: (i) the policies contained no exclusion for terrorism at all (three cases); (ii) the policies provided affirmative coverage for “cyber-terrorism”, as defined in the policy (two cases); or (iii) a general terrorism exclusion is specifically not applied to cyber-related incidents (six cases). Only one of the thirteen policies contained a general exclusion for terrorism that appeared to also apply to cyber-terrorism.

For the Australian market, five of the eight insurance offerings reviewed provided information on the treatment of cyber-terrorism. Four of the five policies contained general terrorism exclusions although with an exception of the application of these exclusions for “cyber-terrorism” (the fifth policy did not contain any form of terrorism exclusion). In two cases, the terrorism exclusion would not apply to “cyber-terrorism” with a definition of cyber terrorism provided – as “...the use of information technology to execute attacks or threats against the company’s network security...” (Zurich (Australia), 2018) and “...premeditated use
of disruptive activities against any Company's Computer System, OSP's [Outsource Service Provider] Computer System or network, or the explicit threat to use such activities...” (AIG Australia Limited, n.d.[17]). In the other two policy wordings, there is an exception to the general terrorism exclusion for “...any data breach or any actual, alleged or threatened attack against the computer system...” (AXA XL Insurance (Australia), 2019[18]) and “...the following cyber events: crimeware, cyber espionage, cyber extortion, denial of service, distributed denial of service hacking, payment card skimming, point of sale intrusion, web app attacks...” (Emergence, 2018[19]).

As outlined in the Annex, stand-alone cyber insurance policies are usually not eligible for the co-insurance or reinsurance coverage provided by the terrorism (re)insurance programmes (with a few exceptions).

1.2. Commercial property/ISR insurance policies

Commercial property insurance (known as Industrial Special Risks (ISR) insurance in Australia) provides insurance coverage for property damage, business interruption that results from covered property damage and, in many cases, contingent business interruption based on a disruption affecting the insured’s suppliers (potentially including utility service providers) and/or customers.

Commercial property policies in most countries generally take one of two forms, either: (i) named peril; or (ii) all-risk. Named peril policies provide protection against loss or damage to buildings, machinery and equipment (and other physical or “tangible” assets) resulting from one of the perils listed in the policy. All-risk policies provide similar protection for loss and damage from all perils unless specifically excluded. In Australia, ISR policies provide coverage on an all-risk basis subject to specific exclusions (as outlined below).

The coverage for business interruption (i.e. loss of revenue and extra expense) in commercial property policies is (only) triggered when there is property damage resulting from a peril covered under the policy (“consequential business interruption”). Coverage is usually subject to a waiting period, in terms of hours of disruption, before the coverage is activated (“time deductible”). For policies written on a named perils basis, business interruption coverage is only available if the property damage results from a named peril. For all-risk policies, business interruption coverage applies to all perils unless specifically excluded. In Australia, the business interruption coverage provided in ISR policies is available for all risks subject to any exclusions.

Coverage for contingent business interruption (i.e. loss of revenue and extra expense that results from a disruption at the premises of a supplier, customer or other business in proximity or upon which the insured is dependent) is usually provided as an endorsement to commercial property policies with some conditions and often with sub limits (e.g. a percentage, such as 10%, of the total policy limit/insured value of the property). The coverage may only apply to disruptions at a pre-defined list of suppliers and/or customers or may apply more broadly, including to utility service providers such as electricity, water and telecommunications providers. It may also be limited to property damage that would have been covered under the policy of the insured (i.e. any peril exclusions to the insured’s coverage would also be applicable to the insured’s contingent business interruption coverage) (Torpey, 2019[20]). Similar to business interruption, a time deductible is usually applied.

Commercial property insurance take-up in most developed insurance markets approaches 100% and policies provide large limits (normally sufficient to address a full loss of a building). According to APRA data, insurers wrote just under AUD 4.5 billion in premiums for the Fire and ISR class of business in 2018 (APRA, 2019[21]). Large insurers in Australia advertise capacities ranging from USD 120 million to USD 1.5 billion per risk ( (LIU, 2018[22]), (Allied World Insurance, n.d.[23]), (AIG, n.d.[19]). Business interruption is a standard inclusion in commercial property insurance policies (i.e. property policies always include coverage for business interruption). In most countries, the take-up of contingent business interruption has
increased significantly in recent years as supply chains have become more complex. In Australia, coverage for contingent business interruption due to a utility services disruption is usually included as standard coverage in ISR policies. Contingent business interruption coverage for disruptions to a supplier is usually provided as an endorsement, either on a named supplier or open basis, and widely acquired by all types and sizes of business. Contingent business interruption coverage is not normally limited to perils that would otherwise be covered by the policy in the Australian market.

1.2.1. Coverage for cyber risk in commercial property policies

Cyber-related property damages and business interruption losses may be excluded from coverage in commercial property insurance policies for a number of reasons: (i) there may be a general exclusion of any damages or losses as a result of cyber incidents (or certain types of cyber incidents); (ii) where the coverage is provided on a named-peril basis, there may be no named coverage for cyber incidents; (iii) contingent business interruption and/or business interruption coverage may not be triggered if there is no damage to tangible property (data and many types of software are usually not considered to be tangible property); or (iv) contingent business interruption may not be triggered if coverage is only available for perils that are otherwise covered by the policy.

In general, an all-risk policy without a specific exclusion applied to cyber incidents would likely cover property damage and consequential business interruption (and contingent business interruption where included) resulting from a cyber-attack. Standard exclusion wordings for cyber risks exist (see Box 1.1) although the extent to which these are applied in commercial property policies in most countries is unclear (most analyses suggest that the use of exclusions is not widespread). Named peril commercial property policies would normally include fire and explosion among covered (named perils) although “cyber” is not normally (if ever) included in commercial property policies as a named peril.

Box 1.1. Cyber exclusions that may be applied in commercial property policies

In commercial property insurance and reinsurance markets, there are at least three standard exclusions that may be applied to broadly exclude all losses and damages resulting from cyber incidents:

- **Institute Cyber Attack Exclusion (CL 380):** This standard exclusion, originally developed for the marine insurance market and in use for a number of years, excludes “loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system”.

- **IMIA Cyber Exclusion 2018:** A more recent exclusion, developed by the International Association of Engineering Insurers for use in engineering insurance markets, excludes “any loss, damage, liability, costs or expenses directly or indirectly caused by or contributed to or resulting from the cyber incidents as set forth in the following provisions a) to g) are not covered by this Policy, regardless of any other cause or event contributing concurrently or in any other sequence to the loss, damage, liability, costs or expenses: a) Damage to or Loss of Data occurring on the Insured’s Computer Systems, or b) a Computer Malicious Act on the Insured’s Computer Systems, or c) Computer Malware on the Insured’s Computer Systems, or d) a Human Error affecting...
the Insured’s Computer Systems, or e) a System Failure occurring on the Insured’s Computer Systems, or f) a Defect of the Insured’s Computer Systems, or g) a Cyber Extortion” (International Association of Engineering Insurers, 2018[24]).

- **Cyber Loss Exclusion (Property Treaty Reinsurance) LMA 5240**: This exclusion, developed by the Lloyd’s Market Association and used in the property treaty reinsurance market, excludes “Cyber Loss” which is defined as “any loss, damage, liability, claim, cost or expense directly or indirectly caused by, contributed to by, resulting from, arising out of or in connection with any Cyber Act” (defined as “an unauthorised or malicious act or series of related unauthorised or malicious acts, regardless of time and place, or the threat or hoax thereof involving access to, processing of, use of or operation of any Computer System or any data by any person or group(s) of persons” (Lloyd’s Market Association, 2015[25]).

In addition, there is a commonly-used standard exclusion wording that confirms² the exclusion of data and software:

- **Electronic Data Endorsement C (NMA 2914) and Electronic Data Endorsement D (NMA 2915)**: These exclusions, also developed by the Lloyd’s Market Association and used in commercial property insurance (among other classes of insurance), exclude coverage for “loss, damage, destruction, distortion, erasure, corruption or alteration of ELECTRONIC DATA from any cause whatsoever (including but not limited to COMPUTER VIRUS) or loss of use, reduction in functionality, cost, expense of whatsoever nature resulting therefrom, regardless of any other cause or event contributing concurrently or in any other sequence to the loss” (Lloyd’s Market Association, 2015[26], Lloyd’s Market Association, 2015[27]).

1 In May 2019, the International Underwriting Association released wordings for a Cyber Loss Absolute Exclusion Clause and Cyber Loss Limited Exclusion Clause which, once applied, would exclude “any loss, damage, liability, expense, fines or penalties or any other amount” caused directly (limited exclusion) or directly or indirectly (absolute exclusion) from the use or operation of a computer system and the processing and transmission of data (including the inability to make use of computer systems or data) (IUA, 2019[28], IUA, 2019[29]). The clauses are meant for application in multiple classes of business and could potentially be applied in commercial property insurance policies in the future (either as exclusions or endorsements of coverage for cyber risks).

2 In most commercial property policies, data and software is not considered “tangible” property which, if lost or damaged, would be covered by a property policy. As a result, NMA 2914 and 2915 provide a confirmation that these losses are excluded.

As noted above, ISR policies provide coverage on an all-risk basis meaning that property damage, consequential business interruption and contingent business interruption (where included or endorsed) is covered for all perils, unless specifically excluded. The ISR Mark IV wording, which is used almost universally for commercial property coverage in Australia excludes:

“7. physical loss, destruction or damage occasioned by or happening through:

(a) (i) Fraudulent or dishonest acts, fraudulent misappropriation, embezzlement, forgery, counterfeiting data corruption, unauthorized amendment of data and erasure by electronic or non-electronic means involving the Property Insured by the Insured or any employee(s) of the Insured acting alone or in collusion with any other persons(s);

(ii) access by any person(s) other than the Insured or the Insured’s employee(s) to the Insured’s computer system via data communication media that terminate in the Insured’s computer system.”
However, the wording also includes a write-back of coverage for “subsequent loss, destruction or damage to the property insured” by “a peril (not otherwise excluded).” This means that if a cyber-attack causes a fire or explosion or any other peril not excluded from the policy, coverage for property damage, consequential business interruption and contingent business interruption would be provided. This understanding was confirmed by Australian insurance companies. All of the companies consulted for the purposes of this study indicated that their ISR policies would provide coverage for losses due to a fire, explosion or other covered peril resulting from a cyber-attack.

1.2.2. Treatment of terrorism as a peril in commercial property insurance policies

The extent to which an exclusion is applied for damages and losses arising from terrorism attacks in different countries usually depends on whether there is a terrorism (re)insurance programme or pool in that country and the approach of the programme to providing insurance, co-insurance or reinsurance coverage. For example:

- In France and Spain, coverage for losses from terrorist attacks is universally included in commercial property policies as the purchase of such coverage is compulsory. The terrorism risk is transferred in full or in part to the terrorism (re)insurance programmes operating in those countries (as reinsurance in France through GAREAT and as primary insurance for extraordinary risks in Spain through CCS).

- In Belgium, coverage for terrorism losses is not compulsory in commercial property policies although is normally included with an optional reinsurance coverage available through TRIP.

- In the Netherlands, the inclusion of terrorism risk in commercial property policies is not compulsory although insurers that wish to provide the coverage offered through the terrorism (re)insurance programme (NHT) must include a clause indicating that the reimbursement of terrorism losses may be limited by the amount paid to the insurer by the terrorism (re)insurance programme (which is subject to a ceiling on aggregate liability) (IFTRIP, 2017).

- In the United States, insurance companies are required to make coverage for terrorism available in commercial property insurance policies in a way “that does not differ materially from the terms, amounts, and other coverage limitations applicable to losses arising from events other than acts of terrorism” (IFTRIP, 2017). To implement this requirement, insurers must make a specific disclosure to policyholders regarding the option of purchasing coverage for terrorism risk, the involvement of the Terrorism Risk Insurance Program (TRIA) in reimbursing losses and the overall limit of liability related to certified acts of terrorism (National Association of Insurance Commissioners, 2015).

In countries without a terrorism (re)insurance programme, such as Canada and Italy, standard commercial property policies often exclude terrorism (at least for larger insured risks) with coverage only available via endorsement or through the stand-alone terrorism insurance market (Willis Property Investors Division, 2011), (Nienhuis, n.d.).

In Australia, ISR policies almost always apply an exclusion for damages and losses resulting from terrorism attacks (as outlined in chapter 3, these exclusions are made ineffective in the event of a Declared Terrorist Incident (DTI)). The Australian Reinsurance Pool Corporation (ARPC) has developed guidance on the form that terrorism exclusions should take to be effective (ARPC, n.d.) although there are various approaches applied in the market. As outlined in chapter 4, most wordings would likely exclude any loss or damage from a cyber-terrorism incident although some of the approaches that are inconsistent with the ARPC guidance (likely a small minority) may not provide an effective exclusion in the event of a cyber-terrorism attack.
1.3. Commercial/public liability insurance

Another source of potential coverage for damages and losses from cyber-attacks is the public (or general) liability policies normally acquired by commercial entities. Public or general liability policies will cover the costs of defending against a liability claim and any compensation that might be awarded to a third party - including coverage for claims resulting from property damage sustained by a third party.

As in the case of commercial property/ISR coverage, take-up of public/general liability coverage is fairly high. Larger companies will generally purchase specific public/general liability policies while smaller companies will often acquire this coverage through package (or business package) policies that include both property and liability coverage. According to APRA data, insurers wrote approximately AUD 2.4 billion in premiums for the Public (and Product) Liability class of business in 2018 (APRA, 2019[21]).

1.3.1. Coverage for cyber risk in public/general liability policies

As noted above, stand-alone cyber insurance policies provide coverage for a number of different types of liability claims (particularly network security, media and privacy) as some of these types of liability have been excluded from coverage provided by public/general liability policies in many countries. In addition to the CL380 exclusion for cyber-attacks (which is applied across a number of business lines), some specific exclusions have been developed for liability lines:

- In the United States standard commercial general liability forms published by the Insurance Services Office (ISO) apply an exclusion for “damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data” (Insurance Services Office (ISO), 2006[35]) (which has since been expanded to exclude damages related to privacy liability).
- There is also a Lloyd’s market exclusion wording for “cyber losses” (LMA5274), developed for casualty treaty reinsurance that is used in some types of liability policies. In this exclusion, cyber loss is defined as “all actual or alleged loss, damage, liability, injury, compensation, sickness, disease, death, medical payment, claim, cost, defence cost, expense or any other amount incurred by or accruing to the Company, including but not limited to any mitigation cost or statutory fine or penalty, directly or indirectly caused by, contributed to by, resulting from, arising out of or in connection with any Cyber Act perpetrated by any person or group(s) of persons not covered under the original insurance or reinsurance” (where “Cyber Act” is defined as “an unauthorised or malicious act or series of related unauthorised or malicious acts, regardless of time and place, or the threat or hoax thereof involving access to, processing of, use of or operation of any Computer System or any data by any person or group(s) of persons” (Lloyd’s Market Association, 2016[36]).

As in the case of commercial property policies, how frequently cyber exclusions are applied is unclear. For the US market, broker and legal analyst assessments suggest that cyber-related losses would mostly be excluded from commercial general liability policies (and, where used, that the ISO exclusion would likely be effective in excluding malicious cyber- attacks and viruses) (ProWriters Insurance, n.d.[37]), (Watkins, n.d.[38]). A recent Lloyd’s market review of the use of cyber exclusions found some application of both the CL 380 cyber-attack and the LMA 5274 cyber loss exclusions in general liability policies (although with no indication of how often) (Lloyd’s Market Association, 2018[39]).

In Australia, market participants indicated that most public liability policies are silent about the coverage of cyber risks – i.e. there is neither affirmative coverage nor an exclusion for losses resulting from a cyber incident. As a result, costs for defending a claim and any awarded compensation resulting from a cyber incident could arguably be covered under a public liability policy in Australia.
1.3.2. Treatment of terrorism as a peril in public/general liability insurance policies

Terrorism is normally (if not always) excluded as a peril in public/general liability policies across the world. In a few countries (Belgium, Netherlands, United States), the terrorism (re)insurance programmes provide co-insurance or reinsurance for losses incurred through liability coverage. As a result, coverage for liability claims resulting from terrorism attacks must be included (Belgium), must be offered (United States) or may be included (Netherlands) in general/public liability policies.

In Australia, public liability policies normally (if not universally) exclude terrorism as a peril. However, public liability policies are eligible insurance contracts under the Terrorism Insurance Act 2003 which means that any exclusion for terrorism would be made ineffective in the event of a DTI (and primary insurers can reinsure that risk through ARPC). As in the case of ISR policies (and as discussed in chapter 4), the wording of the exclusion could have an impact on whether it would be effective in excluding coverage for cyber-terrorism claims.

It should be noted that, while liability is included in the coverage provided by terrorism (re)insurance programmes, the risk of liability claims arising from a terrorist attack is generally perceived to be remote (in Australia and elsewhere). A terrorism-related loss on a general/public liability policy would only occur if the (commercial) victim of a terrorist attack was reasonably believed – and ultimately found in a judicial proceeding – to have been responsible for the resulting losses due to negligence. As a result of the low risk, some terrorism (re)insurance programmes (including ARPC) do not assess an additional premium for the terrorism reinsurance coverage that they provide for public/general liability policies.

1.4. Stand-alone terrorism insurance policies

Companies may also purchase coverage for property damage through specialty stand-alone insurance policies designed to protect against terrorism and often other types of political violence. These types of policies are often acquired by larger companies with multinational operations in order to address any gaps in coverage (potentially as a difference-in-conditions or difference-in-limits policy) that may arise due to: (i) the lack of any coverage for terrorism risk in commercial property policies in some countries (particularly those without a terrorism (re)insurance programme); (ii) differences in the coverage provided by terrorism (re)insurance programmes in different countries (as reflected in primary policies); and/or (iii) limitations in the scope of incidents and losses covered (see Box 1.2). In Australia, very limited amounts of stand-alone terrorism (or political violence) coverage is acquired, suggesting a level of market comfort with the current coverage available through ARPC for conventional terrorist attacks.

The major stand-alone terrorism insurance providers offer coverage for terrorism and other political violence risks for first-party (own property) and often third party (liability) losses, with a variety of coverage and limits available for different types of political violence perils, including: terrorism and sabotage; nuclear, chemical, biological and radiological (NCBR); war or civil war; insurrection, revolution, rebellion; and strikes, riots and civil commotion (SRCC). Most advertise stand-alone capacity of USD 100 million to USD 1 billion per risk although a reported maximum capacity of USD 4.3 billion is possible to secure with amounts of USD 1.5 billion to USD 2.5 billion readily available (depending on location) (Marsh, 2018[40]).

While the specific wordings for stand-alone terrorism insurance policies are not generally available, most companies write these policies based on Lloyd’s Market Association wordings for “Physical Loss or Physical Damage Risks, Strikes, Civil Commotion, Malicious Damage, Terrorism and Sabotage Insurance” (LMA 3092) (Lloyd’s Market Association, 2010[41]) or “Terrorism Insurance: Physical Loss or Physical Damage Wording” (LMA 3030) (Lloyd’s Market Association, 2006[42]). An extension of coverage for business interruption (resulting from covered physical damage) is also normally available based on the
Lloyd’s Market Association standard business interruption wording (LMA 5039) (Marangos and Redden, 2018[43]). A recent analysis for the Lloyd’s market found that 25% - 50% of stand-alone terrorism insurance policies use one of these standard wordings (Lloyd’s Market Association, 2018[39]).

1.4.1. Coverage for cyber risk in stand-alone terrorism insurance policies

The Lloyd’s Market Association terrorism-related wordings contain an exclusion for “Loss or damage by electronic means including but not limited to computer hacking or the introduction of any form of computer virus or corrupting or unauthorised instructions or code or the use of any electromagnetic weapon” (Lloyd’s Market Association, 2010[41]), (Lloyd’s Market Association, 2006[42]) which is also applied in a further 0%-25% of policies that do not use the standard LMA 3030 or LMA 3092 wording (Lloyd’s Market Association, 2018[39]). A review of the online marketing material of the major stand-alone terrorism insurance providers found only one company that specifically advertised coverage for cyber-attacks (physical damage only) (Liberty Specialty Markets, 2017[44]) although market consultations indicated that other insurers may be willing to provide coverage for cyber-attacks on a case-by-case basis as an endorsement. While the coverage for cyber-related risks is limited, the stand-alone terrorism market has recently expanded to provide coverage for other forms of loss not directly resulting from physical damage, including coverage for loss of attraction, denial of access, threat/hoax and, in at least one case, broad contingent business interruption coverage – see Box 1.2).

Box 1.2. Coverage for losses without physical damage

In response to an evolution in terrorist tactics - and in recognition of the broader impact of terrorist incidents on local businesses - the stand-alone terrorism insurance market has developed new forms of protection for businesses that are affected by terrorism but have not sustained direct damage to their property.¹ These new forms of coverage provide protection against the business interruption losses that can be incurred in the aftermath of a terrorist incident that occurs in proximity to the operations of the insured or as a result of a credible threat to the insured, such as:

- loss of attraction: business interruption losses that result from a loss of customers/turnover due to a terrorism incident nearby;
- denial of access: business interruption losses due to an inability of employees or customers to access the insured’s premises due to the establishment of a restricted area in the aftermath of a terrorism incident nearby; and
- threat/hoax: business interruption losses due to a need to respond to a threat to the insured by closing or evacuating the insured’s premises.

Many of the major providers of stand-alone terrorism insurance have expanded their coverage to include these types of non-material business interruption losses – and at least one insurer is providing broad coverage for contingent business interruption (including a utility interruption) (Chubb, 2019[45]).

¹ As outlined in the annex, a number of the terrorism (re)insurance programmes have also implemented changes to their coverage to address these non-material business interruption risks.
1.5. Reinsurance

Reinsurance provides insurance coverage to primary insurers (or cedants) through a contractual arrangement to indemnify losses or otherwise provide a payout to the cedant based on the occurrence of a triggering event, such as a loss incurred by the cedant. The reinsurance arrangement may be established on a facultative (individual policy/risk) or treaty basis (portfolio of policies/risk) and may provide proportional coverage (i.e. where premiums and claims are shared on a proportional basis) or non-proportional coverage (i.e. where the reinsurer provides indemnification only for losses above a given threshold).

Insurance companies providing coverage under commercial property/ISR, public/general liability and stand-alone cyber and terrorism insurance policies will often secure reinsurance coverage to reduce volatility in underwriting results, increase underwriting capacity or protect against catastrophic losses (e.g. in the event of a natural catastrophe or terrorist incident) (OECD, 2018[46]).

In general, reinsurers will follow the wording (and losses incurred) under the policies that they reinsure (i.e. if a reinsured primary policy provides coverage and incurs losses (or losses above an agreed threshold), the reinsurance policy will also provide coverage and incur losses). However, reinsurers may also apply exclusions in the coverage that they provide for cyber and/or terrorism risks (or require that the insurers they reinsure apply such (or similar) exclusions):

- The Lloyd’s Market Association has model exclusion clauses for use in property treaty reinsurance that aim to exclude all cyber losses (LMA 5240) or all cyber losses except physical damage to the insured property (LMA 5241) (Lloyd’s Market Association, 2015[25], Lloyd’s Market Association, 2015[47]). As noted above, a cyber act exclusion has also been developed for casualty treaty insurance (LMA 5274) (Lloyd’s Market Association, 2016[36]). However, a recent assessment of the use of these clauses in the Lloyd’s market found limited (less than 5%) application of these exclusions to property and casualty reinsurance treaties (Lloyd’s Market Association, 2018[39]).

- There are also model terrorism exclusions for application in property treaty reinsurance (NMA 2930c) and casualty treaty reinsurance (NMA 2929) (RDG and the Institute, 2012[48]) although the extent to which they are applied is not known.
2. ARPC coverage for cyber-terrorism risk

2.1. Operation of the scheme

ARPC was established in 2003, in the aftermath of the September 11th terrorist attacks in the United States. Its mission is to provide the market with confidence that claims will be paid in the event of a terrorism incident in Australia. ARPC is a public financial corporation backed by a government guarantee of up to AUD 10 billion for a single event. ARPC is funded by the premiums it collects from its policyholders which are used to acquire retrocession coverage and also to pay fees and dividends to the government to compensate for the guarantee and capital provided. It makes reinsurance coverage available to primary insurers for losses resulting from a DTI affecting the properties they insure. A DTI is a terrorist act (or acts) that has occurred in Australia and that has been declared as such by the responsible Minister (in consultation with the Minister responsible for administering the Australian Security Intelligence Organisation Act 1979).

Similar to other terrorism reinsurance programmes, the reinsurance coverage provided by ARPC is focused on commercial property, subject to some coverage exclusions outlined in regulation (including for computer crime, see section 2 below). The Terrorism Insurance Act 2003 defines the types of insurance policies that are subject to the Act and that may be reinsured through ARPC (“eligible insurance contracts”) as those providing insurance cover for any or all of the following types of losses: (i) loss of or damage to eligible property; (ii) business interruption and consequential loss resulting from loss of, damage to or inability to use eligible property; and (iii) liability that arises out of the insured being the owner or occupier of an eligible property. In addition, the Terrorism Insurance Regulations 2003 sets out a set of exclusions to the types of insurance policies that are deemed eligible insurance contracts, including policies that would normally be considered as life or accident insurance policies as well as policies that provide coverage for mainly residential buildings, motor vehicles, marine and aviation as well as various forms of liability insurance (professional indemnity, directors and officers and product liability). Insurance policies that provide coverage for machinery and electronic equipment breakdown (on a stand-alone basis) are also excluded, along with “a contract of insurance to the extent that it provides cover for loss arising from computer crime.” In addition, a policy that “provides cover only for loss or liability arising from terrorism” (i.e. a stand-alone terrorism insurance policy) and any policy that does not contain a terrorism exclusion are also excluded.

The Terrorism Insurance Act 2003 voids any terrorism exclusion contained in an eligible insurance contract, meaning that the insurer must pay claims that result from a DTI (for which ARPC makes reinsurance coverage available). In 2017, an amendment to the legislation extended the scope of exclusions that will be voided in the event of a DTI to clarify that losses resulting from biological and chemical terrorism would also be covered.
ARPC’s reinsurance coverage is available for eligible insurance contracts and is triggered by the declaration that an incident is a DTI. ARPC coverage follows the terms and conditions of the underlying policy and makes payments to insurers for claims they have incurred above their retention (see below). As a result, losses normally covered in commercial property/ISR policies (property damage, business interruption and contingent business interruption) and public liability policies (compensation for injuries to third parties) would also be covered by ARPC.

Primary insurance companies that have a reinsurance agreement with ARPC would be responsible for losses (above the policyholder deductible) up to AUD 100 000 or 5% of the Fire and ISR premium collected by that insurer (to a maximum of AUD 12.5 million). There is also an industry maximum retention of AUD 200 million for a single event which, if exceeded, would reduce the retentions of individual affected insurers on a proportionate basis. The Terrorism Insurance Act Review: 2018 indicated that approximately 99% of all risks (i.e. commercial properties) are reinsured through ARPC (Australian Government: The Treasury, 2018[49]).

Primary insurers are charged a premium for ARPC coverage set as a percentage of the premium collected from the policyholder. For policies insuring properties located in the postcodes covering central business districts of cities with over 1 million in population (Tier A), the rate is 16%. For policies covering properties located in postcodes covering other significant urban areas (state capitals and cities with a population over 100 000 – Tier B), the rate is 5.3%. Other policies (not in Tier A or Tier B) are reinsured at a rate of 2.6% of the premium charged to the policyholder. ARPC’s reinsurance premium rates are not otherwise adjusted based on risk although the premiums charged by primary insurers to their policyholders (which impact ARPC rates) may have taken account the level of terrorism risk and/or mitigation efforts by the policyholder.18

ARPC funds the losses that it incurs by securing retrocession coverage in international markets. The Corporation has approximately AUD 285 million in net assets for use as a deductible on retrocession coverage of up to AUD 3.315 billion. The Australian Government provides a guarantee of up to AUD 10 billion for losses not covered by the retrocession programme. Figure 2.1 provides an overview of the overall funding of the scheme.

Figure 2.1. Funding of losses under the ARPC scheme

<table>
<thead>
<tr>
<th>Commonwealth guarantee (up to AUD 10 bn)</th>
<th>Funding provided through the guarantee is limited to AUD 10 billion. If losses exceed the amount of the guarantee, a reduction percentage would be applied to all claims on a pro rata basis.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retrocession coverage (AUD 3.315 bn)</td>
<td>Retrocession coverage is provided by international reinsurance markets</td>
</tr>
<tr>
<td>ARPC deductible (AUD 285 mn)</td>
<td>Funded by ARPC net assets</td>
</tr>
<tr>
<td>Industry retention (up to AUD 200 mn)</td>
<td>Primary insurer retentions are set based on collected ISR premiums, with a maximum industry-wide retention of AUD 200 million</td>
</tr>
<tr>
<td>Policyholder deductibles</td>
<td>Policyholders deductibles established in primary policy</td>
</tr>
</tbody>
</table>

Note: As of 1 January 2019
Source: (ARPC, n.d.[50])
2.2. ARPC coverage for cyber-terrorism risk

As noted above, there are three main criteria that must be met in order for a loss incurred by a primary insurer with an ARPC reinsurance coverage to be reimbursed by ARPC: (i) that the loss resulted from a DTI; (ii) that the loss was incurred under an eligible insurance contract; and (iii) that the primary insurer’s aggregate losses are greater than its calculated retention.

There is no specific definition of a terrorist act in the Terrorism Insurance Act 2003 although a reference is made to the definition provided in Part 5.3 of the Criminal Code Act 1995 where a terrorist act is defined as an act that meets both of the following criteria: “(i) it intends to coerce or influence the public or any government by intimidation to advance a political, religious or ideological cause; and (ii) it causes one or more of the following: death, serious harm or danger to a person; serious damage to property; a serious risk to the health or safety of the public; serious interference with, disruption to, or destruction of critical infrastructure such as a telecommunications or electricity network” (Attorney-General’s Department, n.d.[51]). Similar to most other countries, the legal definition is focused on motivation and impact, and does not specify which types of attack could be considered terrorist acts - cyber-attacks are neither specifically included or specifically excluded as attacks that could be terrorist acts. If the Minister is “satisfied that…a terrorist act has happened in Australia”, then the Minister must declare the terrorist act as a DTI subject to the Act. As a result, it is expected that a cyber-attack that meets the conditions on motivation and impact under the legal definition of terrorism would be identified as a DTI.

However, a policy, “to the extent that it provides cover for loss arising from computer crime” is not an eligible insurance contract under the Terrorism Insurance Act 2003. Computer crime is not defined in the Act or the Terrorism Insurance Regulations 2003. However, Part 10.7 of the Criminal Code Act 1995 (Division 477) indicates that a person is committing a serious (criminal) offence when the following conditions are met:

(a) the person causes: (i) any unauthorised access to data held in a computer; or (ii) any unauthorised modification of data held in a computer; or (iii) any unauthorised impairment of electronic communication to or from a computer; and

(c) the person knows the access, modification or impairment is unauthorised; and

(d) the person intends to commit, or facilitate the commission of, a serious offence against a law of the Commonwealth, a State or a Territory (whether by that person or another person) by the access, modification or impairment.

A plain reading of the Terrorism Act Regulations 2003 exclusion for contracts covering computer crime and the Criminal Code Act 1995 definition of computer crime suggests that any insurance policy providing coverage for losses that result from criminal activities implemented through unauthorised access or manipulation of data or impairment of electronic communication would not be considered an eligible insurance contract (or at least not the elements of the policy providing coverage for those losses).

It is therefore expected that the Terrorism Act Regulations 2003 would exclude stand-alone cyber insurance policies as well as coverage provided by ISR policies for fire/explosion following a cyber-attack as eligible insurance contracts:

- The coverage provided by stand-alone cyber insurance policies is specifically meant to address losses resulting from unauthorised access to - or modification of - data and network interruption. For example, one policy reviewed defined an insured “security event” as “any unauthorised access to, unauthorised use of, introduction of malicious code into, or denial of service attack upon, the company’s computer system, that results in...an interruption of service; or ...the theft, alteration, modification, corruption or destruction of digital assets” (Zurich (Australia), 2018[16]). Another policy.
provides coverage for various losses resulting from a “network compromise” defined as “any unauthorized: access to, use or misuse of, modification to the computer system, and/or denial of computer system resources by attacks perpetuated through any electronic means” (AXA XL Insurance (Australia), 2019[18]).

- The (write-back) coverage provided by ISR policies in Australia for losses due to a fire or explosion following a cyber-attack specifically refers to “access by any person(s) other than the Insured or the Insured’s employee(s) to the Insured's computer system via data communication media that terminate in the Insured's computer system.”
- An intentional effort motivated by terrorism to access and/or modify data or interrupt a network would likely meet the other criteria of the definition of computer crime.

As a result, the provisions of the Act, including the voiding of terrorism exclusions and the availability of reinsurance coverage through ARPC, would not be expected to apply in the case of coverage provided for losses resulting from cyber-terrorism.
3. Assessment of coverage gaps

There are a number of cyber vulnerabilities that could be exploited by terrorist organisations for the purposes of causing damage to property, personal injury and loss of life or widespread economic disruption. The ARPC invited the University of Cambridge Centre for Risk Studies (CCRS) to undertake an assessment of cyber-terrorism risk, develop plausible (if unlikely) scenarios and quantify the financial and economic impacts that could result should any of those scenarios materialise. CCRS has developed two scenarios: a Laptop Battery Fires attack and a Building Management Systems attack, as described below (Evan et al., 2020[52]). This chapter will provide a brief description of these scenarios and an assessment of the insurance coverage that would likely be available to respond to the losses that could be incurred.

3.1. CCRS Scenarios

3.1.1. Laptop Battery Fires attack

Lithium batteries are ubiquitous in computers, smart phones and other technological equipment and also (highly) flammable. The scenario developed by CCRS examines three variants of a Laptop Battery Fires attack: (i) a severe (S1) scenario where attackers cause multiple lithium batteries to overheat and cause fires in a variety of commercial properties; (ii) a more severe (S2) scenario involving a greater number of devices and buildings; and (iii) an extreme (X1) scenario that incorporates additional factors such as the potential for the battery fires to impact buildings constructed with – or containing – harmful materials/compounds.

The scenario considers a number of possible attack methods, including remote tampering through a firmware update (original scenario), specific targeting of older laptops that are likely more susceptible, targeting of batteries in connected devices (which are often unsecured) and tampering with the batteries at the point of manufacture (with overheating of the batteries triggered remotely). Table 3.1 provides an overview of the types of losses that could be incurred as a result of the different scenario variants.

Table 3.1. Laptop Battery Fires attack losses

<table>
<thead>
<tr>
<th></th>
<th>Maximum loss (AUD billions)</th>
<th>Average loss (AUD billions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property damage to buildings</td>
<td>$54.8</td>
<td>$1.4</td>
</tr>
<tr>
<td>Property damage to contents</td>
<td>$11.4</td>
<td>$0.1</td>
</tr>
<tr>
<td>Business interruption</td>
<td>$17.1</td>
<td>$0.5</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>$83.3</strong></td>
<td><strong>$2.0</strong></td>
</tr>
</tbody>
</table>

Source: (Evan et al., 2020[52])
### 3.1.2. Building Management Systems attack

The systems that control heating, cooling, lighting, water and other services within buildings have become increasingly automated and are often accessible remotely in order to allow for monitoring and control from an external location. These remote connections could provide malicious actors with the ability to cause a fire or explosion by disabling air conditioners that keep servers cool or taking control of boilers and causing an explosion.

The scenario developed by CCRS examines three variants of a Building Management Systems attack: (i) a severe (S1) scenario involving a data centre fire in a single building; (ii) a more severe (S2) scenario involving a boiler explosion at a single building; and (iii) an extreme (X1) scenario that involving multiple boiler explosions. The scenario is designed based on a remote access to the building management systems through a known vulnerability. Table 3.2 provides an overview of the types of losses that could be incurred as a result of the different scenario variants.

#### Table 3.2. Building Management Systems attack losses

<table>
<thead>
<tr>
<th></th>
<th>Maximum loss (AUD billions)</th>
<th>Average loss (AUD billions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property damage to buildings</td>
<td>$27.0</td>
<td>$0.9</td>
</tr>
<tr>
<td>Property damage to contents</td>
<td>$6.5</td>
<td>$0.01</td>
</tr>
<tr>
<td>Business interruption</td>
<td>$8.3</td>
<td>$0.3</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>$41.8</strong></td>
<td><strong>$1.3</strong></td>
</tr>
</tbody>
</table>

Source: (Evan et al., 2020[52])

### 3.2. Potential insurance coverage for scenario losses

As outlined in chapter 2, coverage for property damage and business interruption losses resulting from cyber-attacks may be found in commercial property insurance policies (ISR), cyber insurance policies, public liability policies and stand-alone terrorism insurance policies. The following sections will assess the level of likely coverage, both from private (direct) insurers as well as terrorism (re)insurance programmes, for losses from the scenarios based on market practices in Australia and elsewhere. An important assumption in the forthcoming assessment is that the incidents described are declared as DTIs (which, as noted above, would likely be the case if there was sufficient evidence of a terrorist motivation).

#### 3.2.1. Potential coverage in commercial property insurance policies

As noted in chapter 2, commercial property insurance/ISR policies normally cover property damage and consequential business interruption, with many policies providing coverage for contingent business interruption due to disruption at suppliers, customers and/or public utilities. In a number of countries, property damage and consequential business interruption resulting from a cyber-attack may be excluded. However, in Australia, ISR policies provide a write-back of coverage for property damage and business interruption losses resulting from a cyber-attack that cause an otherwise covered peril such as a fire or explosion.

Under the Laptop Battery Fires attack and Building Management Systems attack scenarios, the cyber-attack leads to a fire and/or explosion which ultimately causes property damage. As a result, it is expected that the property damage and consequential business interruption losses would normally be covered by ISR policies in Australia under these attack scenarios.
However, if the attack is identified as a terrorist attack (and, therefore, a DTI), terrorism exclusions contained in the policy would be triggered and insurance coverage for the losses would not be provided. As noted above, the provisions of the Terrorism Insurance Act 2003, including the annulment of terrorism exclusions and the availability of reinsurance coverage through ARPC, would only apply to the extent that the contract of insurance is eligible under the Act. The coverage provided under ISR policies for losses resulting from cyber-attacks is unlikely to be considered an eligible insurance contract and therefore any terrorism exclusion would remain valid. Therefore, we expect that primary insurers would, in general, be able to successfully exclude coverage for losses from a cyber-terrorism event when declared as a DTI.

It should be noted, however, that some forms of terrorism exclusions found to be (or found to have been) in use in Australia by ARPC (ARPC, n.d.[34]) may be ambiguous and might (unintentionally) provide coverage. For example, a terrorism exclusion wording that alerts the policyholder to the invalidity of that exclusion in the event of a DTI declaration could inadvertently be providing coverage for a DTI that does not lead to an annulment of the terrorism exclusion clause.19 Another example is a wording that provides a list of the types of terrorist act for which the exclusion will still apply after the declaration of a DTI, made up of terrorist attacks, such as nuclear or radiological attacks, that would not be covered by ARPC (although without any mention of cyber-attacks).20 The ARPC has discouraged the use of terrorism exclusions that describe how the Act may apply, due to the potential for ambiguity and unintended consequences. This advice is also pertinent in the case of cyber-terrorism attacks.

As a result, losses resulting from property damage – as well as consequential business interruption losses that are only triggered if there is property damage from a covered peril – would not generally be covered under ISR policies in Australia – with the exception of losses covered by a policy using an ambiguous terrorism exclusion.

The coverage of contingent business interruption losses is not normally conditional on the occurrence of a covered peril and therefore such losses may be covered under ISR policies. The Laptop Battery Fires attack and Building Management Systems attack scenarios would also create contingent business interruption losses for the suppliers and customers of those affected by the attack. The ISR policies of those customers and suppliers would generally provide coverage for the contingent business interruption losses incurred. However, most of the policies would contain sub-limits for contingent business interruption coverage and some might only be triggered if the victim of the attack was a pre-identified supplier/customer.

Both of the scenarios would likely be considered a “computer crime”. As a result, ARPC reinsurance coverage would not be available for any of the losses incurred by primary insurers.

### Table 3.3. ISR coverage of scenario losses

<table>
<thead>
<tr>
<th></th>
<th>Property damage</th>
<th>Business interruption</th>
<th>Contingent business interruption</th>
<th>ARPC reinsurance coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptop Battery Fires attack</td>
<td>Excluded as terrorism</td>
<td>Excluded as terrorism</td>
<td>Covered (with sub-limits)</td>
<td>Not available (computer crime)</td>
</tr>
<tr>
<td>Building Management Systems attack</td>
<td>Excluded as terrorism</td>
<td>Excluded as terrorism</td>
<td>Covered (with sub-limits)</td>
<td>Not available (computer crime)</td>
</tr>
</tbody>
</table>

#### 3.2.2. Potential coverage in cyber insurance policies

As noted in chapter 2, cyber insurance policies normally provide coverage for losses resulting from cyber-attacks (and incidents), including both first party costs related to incident response, data restoration, network interruption and contingent business interruption as well as defence costs and compensation in...
response to various possible third party liability claims. Internationally, some cyber insurance policies include coverage for property damage although none of the reviewed policies offered in Australia provided such coverage.21

Cyber insurance coverage may respond to some of the business interruption losses incurred by companies affected under the Laptop Battery Fires and Building Management Systems attack scenarios. Cyber insurance policies generally cover loss of revenue and extra expense incurred as a result of an interruption to the operation of the insured’s computer system22 which might be considered the proximate cause23 of some (if not all) of the business interruption losses that would be incurred under both scenarios. As noted above, cyber insurance policies often provide coverage for cyber-terrorism so the identification of an event as a DTI is unlikely to lead to an exclusion of subsequent losses.

The contingent business interruption losses incurred by suppliers and customers of affected companies under the scenarios may be covered under some cyber insurance policies, depending on the scope of the contingent business interruption coverage provided. A number of policies limit the scope of such coverage to suppliers of information technology services24 and therefore the coverage would only be triggered if the affected company was a provider of such services. Other policies appear to provide broader contingent business interruption coverage for any external supplier that is affected by a cyber incident that would have been covered under the insured’s cyber insurance policy.25

As in the case of contingent business interruption coverage under ISR policies, such coverage under cyber insurance policies is usually subject to sub-limits. It should also be recalled that both the take-up of cyber insurance policies and the limits applied to such policies is relatively low.

Both of the scenarios would be considered a “computer crime” while all of the policies would be considered policies covering computer crime. As a result ARPC reinsurance coverage would not be available for any of the losses incurred by primary insurers.

<table>
<thead>
<tr>
<th>Table 3.4. Cyber insurance coverage of scenario losses</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Laptop Battery Fires attack</strong></td>
</tr>
<tr>
<td>Not covered</td>
</tr>
<tr>
<td><strong>Building Management Systems attack</strong></td>
</tr>
</tbody>
</table>

**3.2.3. Potential coverage in public liability insurance policies**

As noted in chapter 2, public liability policies provide coverage for defence costs and compensation awarded to third parties for liability claims made against the insured. Third parties might make a claim against the insured for property damage or bodily injury suffered as a result of the actions (or inactions) of the insured. Third party claims against an insured affected by a terrorist attack are generally perceived to be unlikely although conceivable. Among the scenarios presented here, it is conceivable that a claim could be made against companies targeted by the Laptop Battery Fires attack and Building Management Systems attack scenarios under variants that involve a spread of fires to other buildings/premises.26

Public liability insurance policies are often silent on whether cyber risk is covered as a peril and the vast majority apply a terrorism exclusion. Similar to the case of ISR policies, the terrorism exclusions would apply if the incidents are declared as DTIs (and not annulled by the Act). As a result, losses resulting from any claims made against the affected insured would not be covered by their public liability policies.
Both of the scenarios would be considered a “computer crime”. As a result ARPC reinsurance coverage would not be available for any of the losses incurred by primary insurers.

Table 3.5. Cyber insurance coverage of scenario losses

<table>
<thead>
<tr>
<th></th>
<th>Liability claims</th>
<th>ARPC reinsurance coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptop Battery Fires attack</td>
<td>Excluded as terrorism</td>
<td>Not available (computer crime)</td>
</tr>
<tr>
<td>Building Management Systems attack</td>
<td>Excluded as terrorism</td>
<td>Not available (computer crime)</td>
</tr>
</tbody>
</table>

3.2.4. Potential coverage in stand-alone terrorism insurance policies

As noted in chapter 2, stand-alone terrorism insurance policies provide coverage for property damage and business interruption resulting specifically from terrorist attacks. These types of policies are mostly acquired by companies with multinational operations or with operations in countries where terrorism is excluded as a peril from commercial property insurance policies (and where support from a terrorism (re)insurance programme is not available). In Australia, there is very limited take-up of stand-alone terrorism coverage given that the Terrorism Insurance Act 2003 effectively obliges commercial property insurers to provide coverage for terrorism risks (with ARPC reinsurance available).

Most stand-alone terrorism insurance policies apply an exclusion for losses resulting from cyber-attacks although we did identify at least one policy offered internationally that advertises coverage for cyber-attacks. We expect that a company with a stand-alone terrorism insurance policy that provides coverage for cyber-attacks would be insured for the property damage – and potentially the business interruption losses27 – incurred under both scenarios.

A contract of insurance that provides cover only for loss or liability arising from terrorism (or that does not contain an exclusion of terrorism risk) is not an eligible insurance contract under the Terrorism Insurance Act Regulations 2003. As a result ARPC reinsurance coverage would not be available for any of the losses incurred by primary stand-alone terrorism insurers.

Table 3.6. Stand-alone terrorism insurance coverage of scenario losses

<table>
<thead>
<tr>
<th></th>
<th>Property damage</th>
<th>Business interruption</th>
<th>ARPC reinsurance coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptop Battery Fires attack</td>
<td>Mostly excluded as cyber attack</td>
<td>Mostly excluded as cyber attack</td>
<td>Not available for terrorism insurance policies</td>
</tr>
<tr>
<td>Building Management Systems attack</td>
<td>Mostly excluded as cyber attack</td>
<td>Mostly excluded as cyber attack</td>
<td>Not available for terrorism insurance policies</td>
</tr>
</tbody>
</table>

3.2.5. Overall assessment

Overall, a large share of all of the losses from the two examined scenarios would be borne by affected companies, including their customers and suppliers.

Companies that are directly affected by cyber-attacks would:

- Only recover costs of property reinstatement if they: (i) had acquired a stand-alone terrorism insurance policy with cyber coverage included (only one policy offering such coverage was identified); or (ii) the terrorism exclusion clause in their ISR policy was poorly drafted, unintentionally providing some coverage;
• Only recover costs of business interruption if they: (i) found coverage for property damage under an ISR or stand-alone terrorism insurance policy that met the conditions outlined above; or (ii) had acquired a cyber insurance policy with sufficiently broad network interruption coverage (and limits);

• Unlikely recover defence and compensation costs incurred as a result of any liability claim (although, as noted, the risk of a liability claim is remote).

Companies that are indirectly affected by cyber-attacks would:

• Recover some contingent business interruption losses (up to applicable sub-limits) through their ISR policies under both scenarios and from their cyber insurance policies in certain circumstances (potentially only if the supplier is a technology service provider).

ARPC reinsurance coverage would not respond to losses incurred under any of the policies for any of the scenarios.

Table 3.7 provides an overall view of the likely coverage for losses across business lines.

Table 3.7. Overall insurance coverage for scenario losses

<table>
<thead>
<tr>
<th>Scenario</th>
<th>ISR policies</th>
<th>Cyber insurance policies</th>
<th>Public liability policies</th>
<th>Stand-alone terrorism policies</th>
<th>ARPC reinsurance coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptop Battery Fires attack</td>
<td>No coverage for PD or BI (terrorism exclusion)</td>
<td>Coverage for PD not normally provided</td>
<td>No coverage for liability claims (terrorism exclusion)</td>
<td>Coverage for PD and BI unlikely (cyber exclusion)</td>
<td>Not available (computer crime exclusion)</td>
</tr>
<tr>
<td>Building Management Systems attack</td>
<td>No coverage for PD or BI (terrorism exclusion)</td>
<td>Coverage for PD not normally provided</td>
<td>Coverage for PD and BI unlikely (cyber exclusion)</td>
<td>Coverage for PD and BI unlikely (cyber exclusion)</td>
<td>Not available (computer crime exclusion)</td>
</tr>
</tbody>
</table>

Note: PD: property damage; BI: business interruption; CBI: contingent business interruption

Box 3.1 provides a brief overview of how insurers and terrorism (re)insurance programmes in selected countries might respond to these scenarios (a more detailed analysis of terrorism (re)insurance programme coverage of cyber-terrorism is provided in Annex).
Box 3.1. Scenario losses – the insurance response in other countries

Property damage and consequential business interruption

Three of the terrorism (re)insurance programmes reviewed (Germany, Spain, South Africa) provide direct insurance coverage for terrorism (and sometimes other) risks. In all three cases, property damage and consequential business interruption resulting from a cyber-terrorism incident would likely be covered as there are no specific exclusions applied for cyber risks and as the definition of terrorism used to trigger coverage is broad enough to include the cyber-terrorism scenarios considered here.

In most of programmes that provide co-insurance or reinsurance (Austria, Belgium, France, India, Netherlands, United Kingdom and United States), a cyber-terrorism incident would be covered by the programme to the extent that losses are covered in the underlying commercial property policy (and where other triggering conditions, such as loss thresholds, are met). Some of the programmes could also respond if property damage and business interruption losses were incurred under stand-alone cyber insurance policies (Netherlands, France, Spain, United States).\(^1\)

As outlined in chapter 2, the application of cyber exclusions in commercial property policies – and the inclusion of property damage coverage in cyber insurance policies – varies across countries. As a result, the extent to which private insurance and terrorism (re)insurance would respond to the cyber-terrorism scenarios is somewhat unknown. In France, coverage for terrorism risk in commercial property (and other) policies is compulsory and cyber-terrorism is specifically included in the definition of terrorism – as a result, coverage for cyber-terrorism is likely to be included in primary commercial insurance policies.\(^2\) In the United Kingdom, coverage for cyber-terrorism is being offered (with some conditions) in the reinsurance coverage provided by Pool Re which may encourage coverage of this risk in underlying commercial insurance policies (to the extent it was otherwise excluded).

In Russia, losses resulting from cyber-attacks are specifically excluded from the reinsurance provided by the terrorism (re)insurance programme and are likely to also be excluded from commercial property policies as a result.

Contingent business interruption

Most of the terrorism (re)insurance programmes will only provide coverage for business interruption that is consequential to property damage to the premises of the insured. The terrorism (re)insurance programmes in Austria, Germany and Spain either do not provide such coverage in the insurance, co-insurance or reinsurance that they provide or are prohibited from providing such coverage (either in legislation or as part of their agreements with government guarantee providers). Only the programmes in the Netherlands, the United Kingdom (in certain circumstances) and the United States will provide coverage for contingent business interruption if such coverage is included in the underlying policy.

Liability

Only three of the terrorism (re)insurance programmes reviewed (Belgium, Netherlands, United States) will respond to a claim against an insured for liability related to a terrorism incident. In the unlikely event that the victim of a terrorist incident is found liable for property damage or bodily injury to a third party, the terrorism (re)insurance programmes in these countries may respond.

1. In the Netherlands, the terrorism (re)insurance programme (NHT) indicated that it would be unlikely that a cyber-attack would meet the definition of a terrorist attack under the terms of their coverage. In France and Spain, it was noted that coverage for property damage is not normally included in cyber insurance policies.
2. In the United States, terrorism insurance must be offered to policyholders in all lines of business subject to the Program although policyholders are not required to acquire that coverage.
4. Providing coverage to cyber-terrorism: options and considerations

The assessment of the insurance coverage available for a cyber-terrorism incident, based on the two scenarios developed by CCRS, found limited coverage in Australia for the property damage, business interruption and contingent business interruption losses that would be incurred. As a result, commercial policyholders would likely be required to absorb a significant share of the losses. This chapter outlines some of the issues that the Government of Australia may wish to consider as part of any decision on whether to extend ARPC coverage to include cyber-terrorism. It will also examine some options for providing greater coverage of cyber-terrorism and the practicalities for extending such coverage.

4.1. Extending ARPC coverage to cyber-terrorism: some considerations

4.1.1. Is there a market failure for cyber-terrorism insurance coverage

The Government decision to intervene in the terrorism insurance market in the aftermath of the September 11th terrorist attacks was driven by concerns about the impact of terrorism exclusions on the commercial property market. As noted in the Terrorism Insurance Act Review: 2018, “the Government was concerned that forcing property owners to assume their own risk for terrorism would lead to a reduction in financing and investment in the Australian property sector, including a substantial reduction in commercial building activity” (Australian Government: The Treasury, 2018[49]). The Act, and the availability of reinsurance through ARPC, was established as a temporary measure subject to triennial reviews to determine whether there is a continued need for the scheme. These reviews examine, amongst other issues, whether the level of private insurance market capacity for terrorism risk is sufficient to meet the needs of the Australian commercial property market. The most recent review found that there continues to be a market failure in terrorism insurance markets that warrants the continued need for the Act and the reinsurance capacity provided by ARPC (Australian Government: The Treasury, 2018[49]).

An assessment of whether a similar market failure exists in the case of insurance for cyber-terrorism should consider: (i) if there is insurance coverage available for cyber-terrorism risk to commercial properties; and (ii) if not, whether the lack of insurance coverage is having – or could have – an impact on activity in the commercial property sector.

The assessment of the insurance coverage available for losses resulting from a cyber-terrorism attacks suggests that, similar to the situation after the September 11th terrorist attacks, commercial property owners would be uninsured for many of losses resulting from a cyber-terrorist attack and would therefore need to absorb the associated costs. As outlined in chapter 4, insurers of property damage and consequential business interruption under ISR policies would be expected to rely on terrorism exclusions to deny coverage for the subsequent losses (and they would likely be successful if the event were declared a DTI under the Act).
Coverage for cyber-terrorism provided in cyber insurance policies will not provide a meaningful alternative as property damage is not covered in policies offered on the Australian market, coverage for business interruption might only be triggered under certain conditions - and overall insured limits remain low. Given that there is broad coverage for property damage in the case of a fire or explosion resulting from cyber incidents in ISR policies (for incidents where a terrorism or war exclusion would not apply), it is not expected that significant demand will emerge for property damage coverage in cyber insurance policies.\(^{28}\) As noted, only one provider of coverage for property damage resulting from cyber-terrorism on international markets was identified. Coverage for contingent business interruption might broadly respond to a cyber-terrorism event (although subject to the sub-limits applied in most policies for this type of loss).

Currently, there is no evidence to suggest that the lack of insurance coverage for losses due to cyber-terrorism is having a material impact on commercial property markets in Australia. While there is a potential for a cyber-terrorism incident to lead to significant damages and losses (as described in the CCRS scenarios), the probability of such an attack occurring is largely unknown and may not be significant (cyber-terrorism is, at the time of writing, a hypothetical risk only, with no known occurrences). In addition, we expect that commercial policyholders are generally unaware that they may be faced with uninsured losses as a result of a cyber-terrorism event (or even that they could be targeted by a cyber-attack motivated by terrorism). While the vast majority of insurance companies that were consulted clearly expect losses from a cyber-terrorism to be excluded from the coverage provided by ISR policies, there was some uncertainty even among insurance companies.\(^{29}\) Activity in commercial property markets would not normally be affected by a risk that is largely unknown.

\[4.1.2.\textit{ Would ARPC displace private coverage of cyber-terrorism losses}\]

A related issue is whether ARPC coverage would become a substitute for coverage that would otherwise be provided by the private insurance market. As a provider of reinsurances, ARPC’s coverage could conceivably serve as a direct alternative to private reinsurance of cyber-terrorism or to primary insurers’ retention of cyber-terrorism risk. It could also provide an indirect substitute for specialty cyber-terrorism insurance coverage where such coverage is not provided in standard commercial property policies (as any ARPC reinsurance coverage for cyber-terrorism would encourage coverage in standard commercial property policies).

The reinsurance companies that were consulted during the development of this report consistently demonstrated a preference for providing coverage for terrorism risk by assuming risk from ARPC (i.e. as reinsurance) rather than as direct reinsurers of terrorism risk in primary policies (this was also a finding of the 2018 review of the Act (Australian Government: The Treasury, 2018\(^{[49]}\)). They indicated that, given the challenges in modelling and underwriting cyber-terrorism risk, assuming a portion of the aggregate risk of ARPC’s portfolio of individual insured properties was likely the most effective and cost-efficient means to manage potential cyber-terrorism losses in Australia. Reinsurers are providing coverage for property damage resulting from cyber-attacks through the primary ISR policies that they reinsure although they have limited appetite to assume cyber-terrorism risk (or terrorism risk in general) without ARPC involvement.

As noted above, primary commercial property insurers are unlikely to face significant exposure to cyber-terrorism risk under ISR policies, with the exception of coverage provided for contingent business interruption. As a result, ARPC reinsurance coverage would not displace coverage in the primary property market – in fact, it could encourage some private property market coverage by imposing industry retentions consistent with retention requirements for other forms of terrorism. It is conceivable that some private market coverage in cyber insurance policies for cyber-terrorism business interruption losses could be displaced by ARPC reinsurance coverage, to the extent that those losses are currently retained by cyber
insurers and/or transferred to private reinsurers. However, the coverage provided by cyber insurers may only be available under certain conditions and is constrained by relatively low insured limits.

ARPC reinsurance coverage (or more accurately, the Terrorism Insurance Act 2003) likely acts as an indirect alternative to stand-alone terrorism insurance coverage from the private market by requiring that commercial property insurers provide coverage for terrorism risk (by annulling terrorism exclusions) and providing reinsurance coverage. The same impact would likely occur if the scope of the Act (and ARPC’s reinsurance coverage) were extended to include cyber-terrorism. However, as noted, there are very few coverage options available for cyber-terrorism in the private market (only one policy advertising such coverage was identified).

4.1.3. Reputational risks

A lack of awareness among commercial policyholders of uninsured cyber-terrorism exposures would likely lead to significant reputational risks for insurers, ARPC as the terrorism reinsurance provider in Australia and the Government should a cyber-terrorist attack leave policyholders liable for most losses incurred. An illustrative example might be the experience following the 2010-11 floods in Queensland where a lack of policyholder awareness of flood exclusions in property policies led (at least in part) to numerous government reviews and inquiries at both the federal and state level.\(^{30}\)

A significant portion of the reputational impacts will likely be borne by the ARPC and the Government, as it will be difficult to explain to the general public why an incident declared as a terrorism incident by the Government is not reinsured by the government reinsurer with a mission support recovery and ensure that claims are paid after a terrorism event. Most imaginable cyber-terrorism attack scenarios, including variants of the two CCRS scenarios, could conceivably be implemented as a conventional (physical) attack without accessing a company’s network remotely which will exacerbate the challenges in explaining why cyber-terrorism is sufficiently different from other types of terrorism and warrants a different (less favourable) level of support from government.

It should be noted that these reputational risks are not unique to Australia. As outlined in the Annex, other countries with terrorism (re)insurance programmes may not provide much coverage for cyber-terrorism, either because of an exclusion in the programme’s reinsurance agreements (Russia) or as a result of exclusions for cyber-attacks applied in the underlying policies that are co-insured or reinsured by the terrorism (re)insurance programmes (Austria, Netherlands). Even countries where specific steps have been taken to clarify or even encourage coverage for cyber-terrorism in commercial property policies (France, United Kingdom, United States), there are only limited mechanisms\(^{31}\) to ensure that underlying commercial property policies provide the coverage necessary to trigger programme co-insurance or reinsurance.

However, Australia is unique in that it is the legislation that establishes an exclusion for cyber-terrorism (steering the reputational impacts more directly to the government). As outlined below, Australia is also unique in having the legislative tools to ensure broad and effective coverage for cyber-terrorism losses.

4.2. Enhancing insurance coverage of cyber-terrorism losses

Should a decision be made to address the gaps in coverage for cyber-terrorism losses, a number of approaches might be available.
4.2.1. Invalidating terrorism exclusions for all DTIs

The Terrorism Insurance Act 2003 has two practical implications for the insurance market once an incident is declared a DTI: (i) it annuls terrorism (and other) related exclusions contained in eligible insurance contracts; and (ii) it triggers the reinsurance coverage made available by ARPC for eligible insurance contracts that have been reinsured with ARPC. Currently, these two impacts occur concurrently – if an insurance coverage is an eligible insurance contract then terrorism exclusions are annulled and ARPC reinsurance coverage is triggered. However, it may be possible to make amendments to the legislation to annul terrorism exclusions in insurance policies without making ARPC reinsurance coverage available for cyber-terrorism incidents.

Such a change would force insurance companies to provide coverage for such losses (instead of policyholders) – although potentially without the protection of reinsurance if private reinsurers are unwilling to accept cyber-terrorism risk. This approach would likely face significant resistance from insurance companies who would (reasonably) consider it unfair to force them to cover a risk without making reinsurance available. Compulsory coverage requirements are usually (if not always) backed by a government insurance arrangement.

This approach might not, however, significantly increase the private insurance market’s exposure to property damage resulting from cyber-attacks given that a significant portion of that risk is already covered under ISR policies. All property damage resulting from cyber-attacks is covered except for incidents motivated by terrorism or excluded based on the war exclusion – although, as noted in Box 4.3, the insurance market is increasingly working to exclude and/or limit politically-motivated (state-backed) cyber-attacks from cyber and property insurance coverage through the refinement of exclusion wordings and litigation.

4.2.2. Integrating cyber-terrorism coverage into ARPC terrorism reinsurance coverage

Another option would be to make ARPC reinsurance coverage available for losses resulting from cyber-terrorism under the same terms as reinsurance coverage provided for other terrorism losses. Under this approach, a cyber-attack that is deemed to be motivated by terrorism and identified as a DTI would lead to the annulment of any exclusions in primary insurance policies and trigger reinsurance coverage for incurred losses above insurer retentions under policies reinsured with ARPC. This approach would provide reinsurance coverage for cyber-terrorism that is similar to the coverage that was recently extended by Pool Re in the United Kingdom (see Box 4.1). It would also provide effective coverage for cyber-terrorism losses as there would be no risk that such losses might not be covered in the underlying policies (given that any relevant exclusions would be annulled).
Box 4.1. Pool Re coverage for cyber-terrorism

In November 2017, Pool Re, the UK terrorism reinsurance programme, announced that it would extend its terrorism reinsurance coverage to offer coverage, with some conditions, for property damage and consequential business interruption resulting from a cyber-terrorism attack beginning 1 April 2018. This followed an extensive assessment of the risk of cyber-terrorism and the agreement of the UK Treasury as the provider of a government guarantee for Pool Re losses in excess of its reserves and retrocession coverage.

The extended coverage was provided by amending Pool Re’s reinsurance agreement to include coverage for “remote digital interference” resulting in property damage at the premises of the insured and business interruption at the affected premises (and consequential to the property damage). The extended coverage is being provided at no additional charge (Willis Towers Watson, 2018).

Similar to ARPC, Pool Re purchases retrocession coverage. In 2019, Pool Re successfully integrated its cyber-terrorism exposure into its GBP 2.3 billion retrocession placement (up from a GBP 2.1 billion placement in 2018) (Pool Re, 2019).

1. It should be noted that the scope of coverage for cyber-terrorism provided in Pool Re’s reinsurance agreement is similar to the scope of cover that is provided for cyber-attacks in ISR policies in Australia, so there would not likely be a need to establish specific conditions in ARPC’s reinsurance agreement.

Legislative and regulatory amendments

An extension of coverage to cyber-terrorism could likely be achieved through amendments to the Terrorism Insurance Act 2003 and the Terrorism Insurance Regulations 2003. Any amendments to legislation would need to be drafted by legal experts in the Australian Government although the following provides an overview of some of the considerations:

- In the Terrorism Insurance Regulations 2003, item 32 in Schedule 1 would likely need to be repealed or amended. In amending item 32, the government may want to consider whether to allow stand-alone cyber insurance policies to be considered eligible insurance contracts. This may not be necessary if the main objective is to address the gap in coverage for property damage and consequential business interruption (and to limit ARPC’s intervention to those types of losses). As noted above, cyber insurance policies may currently respond to business interruption losses resulting from a cyber-terrorism incident under certain conditions and therefore ARPC coverage would potentially displace existing market coverage. In addition, making ARPC reinsurance coverage available for all types of losses that may be incurred under cyber insurance policies (subject to any exclusions in the Regulation) could force ARPC to cover losses resulting from privacy breaches or cyber-extortion (for example) if motivated by terrorism. However, excluding cyber insurance policies could preclude the possibility of providing ARPC reinsurance coverage for any property damage coverage in cyber insurance policies that may emerge, should the market evolve in that way.

- In addition, Section 8, paragraph (2) of the Terrorism Insurance Act 2003 would likely need to be amended to ensure that any cyber exclusions applied in ISR policies are annulled in the same way as terrorism exclusions. This amendment would be required to ensure that cyber-terrorism is not excluded from ISR policies as the result of any exclusion applied for cyber-attacks or incidents. The same approach was taken to ensure that biological and chemical attacks were not excluded in these policies as a result of a pollution or contamination exclusion clause.
Implementation issues

Implementing such a change would raise a number of operational issues for ARPC and for the government. An extension of ARPC’s reinsurance coverage to include cyber-terrorism would increase ARPC’s overall exposure to losses (even if the likelihood of a cyber-terrorist attack is currently remote). As a result, ARPC would need to determine whether to collect any additional premium from cedants to cover this additional exposure and how to most cost-effectively acquire retrocession coverage for its greater level of risk. While not new (or driven by any extension of ARPC coverage for cyber-terrorism), the government must also address the challenges in confirming a cyber-attack as a cyber-terrorist attack (and a DTI).

As noted in chapter 3, ARPC reinsurance premiums are established as a share of the premium charged for the underlying coverage with a different rate charged for properties located within post codes covering central business districts in the largest cities, other significant urban areas and other locations. This premium structure reflects the likely greater level of risk of a conventional (physical) terrorist attack in central business districts and other significant urban areas where larger groups of people are likely to congregate. As it is based on the (all-risk) premium rate charged by primary insurers, it would reflect any risk differentiation imposed by the primary insurer (i.e. if a primary insurer charges a lower premium rate for a well-secured property, the reinsurance premium charged by ARPC would also be lower).

It is difficult to ascertain whether the same differentiation of risk would be relevant for cyber-terrorism (i.e. that central business districts in the largest areas are more likely to be affected/targeted by a cyber-terrorist attack). It is also less likely that primary (property) underwriters are applying differentiated premium rates based on the cyber security measures applied by insureds.\(^{33}\) As a result, it is likely not desirable to charge differentiated premiums for cyber-terrorism coverage at this time. If ARPC wishes to charge primary insurers for the additional reinsurance coverage provided, the best approach might be a consistent increase in premium rates across all policies. One option for calibrating any additional charge could be to base it on any additional cost for retrocession coverage (as discussed below). Improvements in the modelling of property damage from cyber-attacks might allow ARPC to design a risk differentiated premium structure in the future (see Box 4.2).

Box 4.2. Challenges in assessing exposure to cyber risk

A lack of historical experience with cyber incidents combined with the constantly changing nature of cyber risk due to the adoption of new technologies, the identification of new vulnerabilities and the development of new attack methods creates significant challenges for assessing cyber risk and underwriting insurance coverage (OECD, 2017[3]). These challenges are likely to be even greater in the case of cyber-attacks aimed at property damage given that there have only been a small number of successful attacks.\(^1\) An assessment of cyber-terrorism risk faces the additional complexity of understanding the motivation and capability of terrorist actors.

There has been significant investment into modelling cyber risk in recent years, by both traditional catastrophe modelling firms as well as by new entrants, often with links to the major cyber security firms. In 2018, the two major catastrophe modelling firms released their first probabilistic cyber risk models for use in underwriting (AIR Worldwide, 2018[55]), (RMS, 2019[56]). The model developed by Risk Management Solutions incorporates a number of property damage scenarios, including a power blackout, property fire, marine cargo port, industrial facilities and upstream energy (RMS, 2019[56]). AIR Worldwide’s probabilistic model also incorporates a power blackout, among other scenarios (AIR Worldwide, 2018[55]). New
entrants, such as Guidewire Cyence and CyberCube, focus on company cyber security controls and network activity to provide data on exposure to cyber risks at the company and/or portfolio level.

The continued development of these models, further experience with actual incidents as well as investments by terrorism (re)insurance programmes into understanding their exposure to cyber-terrorism should eventually allow a better understanding of this risk – providing an opportunity to differentiate premiums and promote better cyber risk management.

1 There are only a few reported examples of cyber-attacks leading to property damage, including a malware attack in 2010 that sabotaged the operation of centrifuges used for uranium enrichment in Iran (Kelley, 2013[62]) and a late 2014 attack on a German steel mill that led to significant damages as the control systems for blast furnaces failed (Zetter, 2015[59]). There have also been a few disruptions to critical infrastructure caused by cyber-attacks, including two direct attacks that disrupted the power grid in the Ukraine (Zetter, 2016[91]), (Condliffe, 2016[92]) as well as the disruption to the UK National Health Service caused by the WannaCry ransomware (Field, 2018[93]).

If ARPC wished to include the additional coverage for cyber-terrorism into its existing retrocession coverage, the premium rate applied to that coverage is likely to increase (or the amount of capacity made available may decline). In 2018, ARPC acquired AUD 3.065 billion of retrocession coverage at a rate-online of 1.9% for a premium cost of AUD 58.3 million (Australian Government: The Treasury, 2018[49]). In its report to inform the 2018 review of the Terrorism Insurance Act 2003, Finity Actuarial and Insurance Consultants estimated that overall market capacity for assuming ARPC terrorism risk had declined by approximately AUD 1 billion as a result of the clarification/confirmation of ARPC coverage for chemical and biological attacks made in 2017 (Australian Government: The Treasury, 2018[49]). Similar capacity constraints may emerge as a result of the inclusion of cyber-terrorism coverage. A number of the reinsurance sector representatives consulted suggested that ARPC may want to seek separate retrocession coverage for its cyber-terrorism exposure in order to avoid adverse pricing impacts or limit constraints on its existing retrocession programme. That said, Pool Re was able to successfully integrate its cyber-terrorism exposure into its existing retrocession programme for its 2019 renewal and was able to secure higher overall limits than in the past (Pool Re, 2019[54]).

A potentially more significant implementation challenge – which also exists under the current framework – could be the difficulty in identifying a cyber-attack as a terrorist attack – for at least two reasons: (i) it is likely much more difficult to identify (in a timely way) the source of a cyber-attack relative to conventional terrorist attacks; and (ii) it may be difficult to clearly identify the perpetrators as terrorists (and not other politically-motivated actors).

The attribution of cyber-attacks to specific individuals or organisations is challenging. A cyber-attack can be launched from any location, including from public networks (Cook et al., 2016[62]) and can make use of a variety of tools to mask the point of origin of the attack. The coding of the malware used to execute a cyber-attack can be deliberately manipulated to mask the identity of the attacker and/or to attempt to deceive investigators into believing that the attack originated from a different perpetrator (O’Brien, 2018[83]). Cyber-attacks on industrial control systems, the systems whose compromise would most likely lead to property damage, may be even more difficult to attribute given some of the technical differences between these systems and other enterprise networks (Cook et al., 2016[62]).

However, there is some evidence that these difficulties are being overcome. A number of recent cyber-attacks have been publicly attributed by one or more governments, including the WannaCry ransomware attack (attributed to North Korea), the NotPetya malware and the BadRabbit ransomware (attributed to the Russian military) and the theft and release of information from the US Democratic National Committee (attributed to the Russian military) (The White House, 2017[84]), (The White House, 2018[85]), (Burgess, 2017[66]), (Kovacs, 2018[87]), (Office of the Director of National Intelligence, 2017[68]). A number of cyber-
attacks have also led to criminal charges against specific individuals, suggesting a level of confidence in attribution that could meet the standards of a criminal trial.34

Intelligence agencies – which can provide critical intelligence data to complement the findings of a forensic investigation – have shown some reluctance in the past to attribute cyber-attacks to specific organisations or countries. This reluctance is partly due to concerns about inadvertently disclosing intelligence methods and investigative techniques although this may also be changing. The Office of the Director of National Intelligence in the United States has released guidance for attributing cyber-attacks that clearly encourages attribution as a first step to discouraging future cyber-attacks (Office of the Director of National Intelligence, 2018[69]). The head of the UK’s National Cyber Security Centre suggested that the United Kingdom will similarly provide attribution when it is in the public interest and where there is a high enough level of confidence in the findings of its investigation (Ashford, 2018[70]). The Government of Australia has made public attributions for the WannaCry, NotPetya and BadRabbit attacks (Prime Minister of Australia, 2018[71]) although a more recent breach of the networks of the Australian Parliament were attributed only to a “sophisticated state actor” (Van Graver, 2019[72]).35

The definition of a terrorism act under the Criminal Code Act 1995 considers the motivation of the actor (“with the intention of advancing a political, religious or ideological cause” and “with the intention of coercing, or influencing by intimidation, the government… or intimidating the public or a section of the public”) and the impact of the act (“causes serious harm that is physical harm to a person”, “causes serious damage to property”, “creates a serious risk to the health or safety of the public” “seriously interferes with, seriously disrupts, or destroys, an electronic system” amongst other impacts).36 The definition specifically excludes acts that are “advocacy, protest, dissent or industrial action” and that are not intended to cause some of the impacts outlined above (notably, serious damage to property and serious interference of - or disruption to - an electronic system are not included in the list of impacts). Acts of advocacy or dissent that are intended to cause serious property damage or interfere with an electronic system such as a telecommunication network or other public utility – or that unintentionally cause bodily harm – would therefore not appear to meet the definition of a terrorist act. This may create some challenges in determining whether a cyber-attack that is not obviously aimed at causing serious bodily harm is an act of terrorism or an act of advocacy/dissent.

The requirement that a DTI not be an act of war could also create some challenges in declaring a cyber-attack a DTI. While an in-depth discussion of the legal definition of an “act of war” is outside the scope of this report, some observations can be made:

- While there is currently no international legal guidance on whether (or when) a cyber-attack should be considered an act of war, a number of countries and international organisations have indicated that certain types of cyber-attacks could meet that threshold.37 For example, in 2017, the Council of the European Union released a set of guidelines for the development of a framework for responding to malicious cyber-attacks that indicated that “malicious cyber activities could amount to a use of force or an armed attack within the meaning of the Charter of the United Nations” (General Secretariat of the Council of the European Union, 2017[74]). In the United Kingdom, the Attorney General confirmed in a speech in May 2018 that the United Kingdom would consider...
“cyber operations that result in, or present an imminent threat of, death and destruction on an equivalent scale to an armed attack will give rise to an inherent right to take action in self-defence, as recognised in Article 51 of the UN Charter” (Attorney General’s Office, 2018[75]). The G7 made a Declaration on Responsible States Behavior in Cyberspace in 2017 that included a similar conclusion (G7, 2017[76]) while the North Atlantic Treaty Organization (NATO) confirmed in 2014 that a cyber-attack could invoke the organisation’s collective defence agreement (NATO, 2014[77]).

- A cyber-attack can be considered to be a state-sponsored attack where it can be demonstrated that it is authorised by a state (Okereke-Fisher, 2018[78]). In 2002, the United Nations General Assembly adopted a resolution on the Responsibility of States for internationally wrongful acts that includes a principle indicating that “the conduct of a person or group of persons shall be considered an act of a state under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of that State in carrying out the conduct” (United Nations, 2002[79]).

- Most current assessments of capability to execute destructive (or significantly disruptive) cyber-attacks suggest that only actors with links to – or backing of – nation-states have such capability. The cyber-attacks that have caused destruction or major disruption in recent years, such as the NotPetya and WannaCry ransomware attacks in 2017, the power disruptions in the Ukraine in 2016, the attack on Saudi Aramco in 2012 and the destruction of uranium enrichment equipment in Iran in 2010 have all been linked (sometimes loosely) to nation-states or actors backed by nation-states (either as the source of the attack, the source of the malware used or both) (Cambridge Centre for Risk Studies, 2017[73]). In the near-term, it is unlikely that an organisation would have the capability to execute a destructive cyber-attack without some kind of support from a nation-state or without attack tools that have been developed by a nation-state.

### 4.2.3. Expanding the scope of the Act to include malicious cyber attacks

The lack of insurance coverage for destructive or significantly disruptive cyber-attacks motivated by terrorism also (likely) exists for other types of politically-motivated cyber-attacks – particularly for attacks with nation-state involvement.

ISR policies in Australia (and commercial property policies elsewhere) usually (if not always) apply a war exclusion indicating that the policy will not provide any coverage for damage to the insured property “directly or indirectly occasioned by or happening through or connected with war, invasion, act of foreign enemy, hostilities (whether war be declared or not), civil war, rebellion, revolution, insurrection, military or usurped power.” As outlined above, the legal framework for conflict between countries (United Nations Charter, Geneva Conventions) does not explicitly include destructive cyber-attacks in the definition of an act of war although a number of countries have indicated that they would consider a destructive cyber-attack as a use of force/armed attack that could trigger their right to self- (or collective-) defence. As a result, insurance companies would likely have some basis for excluding losses resulting from a destructive cyber-attack attributed to a nation-state (or nation-state-backed actor) under the war exclusion. This issue is currently being tested in US courts (see Box 4.3). If the war exclusion is deemed to be applicable to these types of attacks, policyholders would be uninsured and forced to absorb the resulting losses.
Box 4.3. Litigation on the applicability of war exclusions to cyber-attacks

The NotPetya malware attack in 2017 affected a number of companies around the world. It was disseminated through a corrupt software update in a Ukrainian tax software application and resulted in the corruption of data in affected systems (Levine and Ellis, 2019[80]). The attack was attributed by a number of governments (including Australia, Canada, United Kingdom and the United States) to Russian attackers – and specifically in statements to the “Kremlin” as an “effort to destabilize the Ukraine” as part of an “ongoing conflict” (Bershidsky, 2019[81]).

One of the affected companies, Mondelez International, reportedly faced losses of over USD 100 million as a result of damages to equipment and interruption to its business after being affected by NotPetya. Mondelez had property insurance coverage through Zurich America Insurance for physical loss or damage to electronic data as well as for non-physical losses due to a failure of electronic processing equipment as a result of a cyber-attack (Shooter, 2019[82]). The claim was (eventually) denied by Zurich as the policy excluded losses resulting from an act of war (the definition of which included “hostile or warlike action in time of peace or war”) (Bershidsky, 2019[83]). Mondelez has launched litigation against Zurich which, at the time of writing, remains before the courts.

However, cyber insurance policies do not consistently apply a war exclusion. Among the eight cyber insurance policies offered in the Australian market that were reviewed, four apply a war exclusion that is similar to the exclusion applied in ISR policies (similarly, some of the international policies reviewed apply a war exclusion while others do not). Leading cyber insurers in the London market are reportedly developing a common wording for war exclusions that will allow for some coverage of smaller scale state-backed attacks while excluding large-scale damage (Spoerry, 2019[84]). If successful, this wording could potentially be applied more broadly across the cyber insurance market. However, even in cases where acts of war would be covered under cyber insurance policies, a gap in coverage would remain for physical damage.

As a result of the consistent application of war exclusions in ISR policies, the limited (or non-existent) coverage for property damage in cyber insurance policies and the current efforts to limit exposure to significant state-backed attacks in those policies, we expect that the losses resulting from a destructive cyber-attack linked to a nation-state would not generally be covered by insurers.

A decision by Government of Australia to introduce changes to the Terrorism Insurance Act 2003 and the Terrorism Insurance Regulations 2003 to address the lack of insurance coverage for cyber-terrorism risk could also provide an opportunity to address the lack of coverage for destructive nation-state attacks or even all politically-motivated, destructive cyber-attacks (which could be executed for political motivations but not meet the definition of terrorism under the Criminal Code, as discussed above).

Legislative and regulatory amendments

Such a change would require further amendments to the Terrorism Insurance Act 2003 and Terrorism Insurance Regulations 2003, in addition to those described above. Any amendments to legislation would need to be drafted by legal experts in the Australian Government although the following provides an overview of some of the considerations:

- Terrorism Insurance Act 2003:
o Additional definitions for malicious cyber-attacks and losses would likely need to be added to section 3 in Part 1
o A section would likely need to be added to Part 2 to outline the process for declaring an incident (similar to the provisions in section 6 setting out the process for declaring a DTI although without an exclusion for acts of war). There would likely be a requirement to provide a more expansive definition of the types of malicious cyber-attacks that would be covered and/or a referral to a specific definition in the Criminal Code Act 1995.

- A paragraph would likely need to be added to section 8 in Part 2 to annul the effect of war exclusions in eligible insurance contracts. Consideration could be given to mirroring the wording that is commonly used in such exclusions. The annulment should only apply when an incident is declared and not in other circumstances where the war exclusion would be applied.

- An additional ARPC role would likely need to be added to Part 3, Division 1, section 10, providing ARPC with a role in providing insurance for malicious cyber-attack losses.

- Terrorism Insurance Regulations 2003:
  o Schedule 1 – Exclusions would likely need to be amended to exclude contracts without war exclusions or that only cover war (as in the case of terrorism currently).

A broader expansion of the Act and ARPC reinsurance coverage to include malicious (destructive) cyber-attacks executed by other politically-motivated actors, including nation-states, would respond to a gap (or an emerging gap) in insurance market coverage for losses from these types of attacks. It could also address some of the challenges related to attribution raised above, particularly where there is uncertainty about the level of involvement of nation-states in a given attack.

While ARPC would be unique among terrorism (re)insurance programmes in providing specific reinsurance coverage for a broader set of politically-motivated cyber-attacks, other countries will likely be forced to at least examine this emerging risk and the role of terrorism (re)insurance programmes in the future. The continued involvement of nation-states in executing destructive or significantly disruptive cyber-attacks, combined with the increasing number of targets that can be attacked by digital means, is likely to lead to continued insurance market reluctance to cover these risks and increasing uninsured losses for policyholders.

**Implementation issues**

An expansion of the reinsurance coverage provided by ARPC would unquestionably increase ARPC’s exposure to losses (as well as the government’s exposure as guarantor). A number of nation-state (or nation-state-backed) actors currently have the capability to execute destructive and/or significantly disruptive cyber-attacks. This would have implications for the pricing of ARPC reinsurance coverage and the cost for retrocession coverage secured by ARPC. While cyber-terrorism remains a hypothetical risk, destructive and significantly disruptive cyber-attacks by nation-states have occurred and therefore the likelihood of incurring losses is higher (and potentially higher than conventional terrorism). In addition, unlike conventional physical attacks, cyber-attacks have the potential to create significant accumulation risk as multiple targets can be attacked simultaneously by one or few attackers without any geographical constraints (see Box 4.4).

As outlined above, we expect it would currently be very difficult to develop an ARPC pricing approach for the additional coverage that reflects different levels of risk at the level of individual policyholders. This may change as experience with destructive cyber-attacks grows and as models for underwriting such risks continue to be developed.
The most efficient approach for securing retrocession will need to be discussed with ARPC’s broker and retrocession market participants. As noted above, a number of reinsurance companies suggested that it would be more efficient to secure a separate coverage tower for cyber-attacks in order to avoid price increases in the existing (conventional) terrorism retrocession coverage. We expect that an expansion of ARPC coverage to include other politically-motivated cyber-attacks (including nation-state attacks) might further the case for a separate tower – or even a separate entity– although, in the primary insurance market, these types of political violence risks are often covered in a single policy.

Box 4.4. Mitigating cyber accumulation risk

The potential for an accumulation of losses from a single event is a key concern for providers of cyber insurance coverage. Dependence on the same information technology infrastructure, software and services across countries and sectors limits the ability to build a diversified portfolio and leaves insurance - and particularly reinsurance - companies exposed to accumulation risk related to vulnerabilities in commonly-used software, hardware and/or operating systems and disruptions to cloud service, domain name system and other common service providers. While the business model of reinsurers depends on building a portfolio of risks from across regions and sectors (which provides diversification benefits), the drivers of cyber accumulation and the potential scope of catastrophic losses are not well understood and are not bound by geography making it difficult to build a portfolio of risks that is not exposed to accumulation risk (OECD, 2018[85]). This risk is equally present for ARPC as a reinsurance provider and the Government of Australia as guarantor of ARPC obligations.

One approach to managing this risks could be to provide any ARPC reinsurance coverage for “declared [malicious] cyber-attack” losses through a separate legal entity, possibly a subsidiary of ARPC. The reinsurance coverage could be provided on different terms than the coverage provided for DTI losses, based on a separate premium structure and independent retrocession programme. Industry retentions could be established at levels to limit ARPC losses (see Box 4.5, for example) while a ceiling on government exposure could be established at a level lower than AUD 10 billion (with a reduction percentage applying to losses above that lower ceiling). This approach would provide some coverage for a risk not generally covered in the market while limiting ARPC and the government’s exposure and limiting the impact of the expanded coverage on ARPC’s existing programme.

4.2.4. Reducing the frequency of ARPC losses

The proposals to expand the scope of the Act and the reinsurance coverage provided by ARPC would unquestionably involve an increase in the exposure of ARPC - and ultimately, the government - to losses. One means to mitigate this increased exposure could be increase the thresholds (or loss levels) that must be reached before triggering ARPC coverage.

A number of changes were made in 2017 to the retention that ARPC cedants are required to incur before ARPC coverage is triggered. Individual insurance company retentions have increased from 4% of ISR and Fire premiums collected to 5%, with a minimum retention of AUD 100 000 (relative to no minimum retention before 2017) and a maximum per company retention of AUD 12.5 million (up from AUD 10 million). The industry-wide retention (i.e. the maximum amount that the industry as a whole would retain for a DTI) has increased from AUD 100 million to AUD 200 million. These increases should reduce the frequency of ARPC
claims by ensuring that ARPC reinsurance coverage is only triggered for less frequent larger events (or for events with large impacts for one or a few smaller insurers).

While terrorism (re)insurance programmes use different approaches to establishing industry retentions, some countries appear to impose a higher threshold for triggering programme reinsurance or co-insurance. In the United States, for example, individual insurers are responsible for first losses up to 20% of their direct earned premium in the prior calendar year in insurance lines eligible for the Terrorism Risk Insurance Program (TRIA) co-insurance coverage (which includes a number of insurance lines in addition to commercial property insurance). Insurers are also responsible for 19% of losses incurred above their retention/deductible (increasing to 20% in 2020) (Federal Insurance Office, 2018 [86]). In addition, the co-insurance provided by TRIA is only triggered if aggregate industry losses from a terrorism event exceed USD 180 million (as of 2019, increasing to USD 200 million in 2020). These deductible and co-insurance arrangements could require insurance companies to bear a significant share of the costs from a terrorism incident in the United States. As a result, a private reinsurance market has developed in order to provide reinsurance coverage for primary insurers’ exposure to TRIA deductibles and co-insurance obligations – providing another layer of coverage that allows primary insurers to manage their retentions and co-insurance while ensuring that the public co-insurance is only triggered for the largest events.

ARPC could similarly aim to limit the coverage that it provides to only the largest events – and reduce the frequency of its losses. Individual primary insurer retentions could be increased significantly (towards levels in the United States), although this would likely require a lengthy transition period to allow the market to adapt (and a reinsurance market for individual insurer retentions to develop). An alternative could be to transform the ARPC into a provider of “overspill” reinsurance where ARPC coverage would only be triggered once primary insurer retentions and private reinsurance coverage have been exhausted. For example, a primary insurer could be required to retain or acquire reinsurance coverage for losses up to a specific threshold, such as a given share of written premiums or a given return period [41], and then seek overspill reinsurance coverage from ARPC. ARPC would only be responsible for losses above that threshold (see Box 4.5).

**Box 4.5. Overspill reinsurance example**

Some specialised markets, particularly marine insurance, provide an “overspill” coverage for losses that exceed insurer retentions and reinsurance protection. For example, the clubs that pool marine risks will normally seek traditional excess-of-loss reinsurance to cover amounts up to a certain limit and the either acquire (or obligate members to provide) overspill coverage for losses that exceed reinsurance coverage up to a (higher limit) (IGP&I, 2019 [87]), (The Shipowners’ Club, 2017 [88]). For most marine clubs, the overspill coverage has never been triggered as the thresholds have been set at amounts that signify a truly systemic event.

ARPC’s coverage for cyber-terrorism (or terrorism or malicious cyber-attacks or other catastrophe perils) could be provided on an overspill basis that would only be triggered once losses exceed a truly catastrophic level (i.e. above insurer retentions and the excess-of-loss reinsurance coverage that insurers would normally acquire to manage catastrophe risks). This would make the likelihood of losses at ARPC (and the government) extremely remote – while still providing the insurance industry and policyholders with confidence that claims would be paid in the event of a truly systemic event.
Annex A. International approaches to ensuring the availability of coverage for cyber terrorism

Overview of terrorism (re)insurance programmes

A number of countries have established terrorism (re)insurance programmes (or pools), particularly in the years following the September 11th terrorism attacks in the United States (although some of these programmes pre-date those events). In most cases, these programmes were established to address a gap in the availability of insurance coverage for terrorism risk that emerged as insurers (and reinsurers) began applying a terrorism exclusion in their policies.

While there are some significant differences in the coverage provided by terrorism (re)insurance programmes in different countries (see Table A.A.1), most are specifically focused on providing coverage for commercial property damage and consequential business interruption (although some also provide coverage for residential property, life and personal accident and/or certain types of liability). In most of these programmes, the state plays a role in assuming some of the risk, either as insurer, co-insurer, reinsurer or as a provider of a backstop/guarantee for extreme losses (including losses incurred by a public insurer or reinsurer).

In most cases, the programme defines when an incident is a terrorism event for which losses will be covered by the programme. In some cases (Belgium, France, Spain), the programme will refer to a statutory definition of terrorism when determining when an event is eligible for coverage. In other cases (Austria, India, Germany, Netherlands, South Africa), the programme has established a definition of terrorism events eligible for coverage, normally based on prevailing industry definitions (or exclusions). In the United Kingdom and United States, an event must be specifically certified as an act of terrorism by the treasury department (based on a programme-specific statutory definition) before it is eligible for programme coverage (see Table A.A.2).
Table A A.1. Overview of terrorism (re)insurance programmes

<table>
<thead>
<tr>
<th>Country</th>
<th>Arrangement</th>
<th>Types of damages/losses covered</th>
<th>Private insurance market role</th>
<th>Public sector role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>Industry co-insurance and reinsurance pool</td>
<td>Commercial and residential property damage and consequential business interruption</td>
<td>Distribution, retention, co-insurance, reinsurance</td>
<td>None</td>
</tr>
<tr>
<td>Belgium</td>
<td>Industry co-insurance and reinsurance pool</td>
<td>Commercial and residential property damage and third party liability, consequential business interruption, motor vehicle, life, personal accident and health, liability, workers compensation</td>
<td>Distribution, retention, co-insurance, reinsurance</td>
<td>Explicit state guarantee</td>
</tr>
<tr>
<td>France</td>
<td>Industry co-insurance and reinsurance pool backed by state reinsurer</td>
<td>Commercial and residential property damage and consequential business interruption, motor vehicles</td>
<td>Distribution, retention, co-insurance, reinsurance</td>
<td>Reinsurance (state-owned reinsurer with explicit state guarantee)</td>
</tr>
<tr>
<td>Germany</td>
<td>Industry-owned insurance company</td>
<td>Commercial property damage, consequential business interruption and contingent business interruption</td>
<td>Retention, reinsurance</td>
<td>Explicit state guarantee</td>
</tr>
<tr>
<td>India</td>
<td>Industry co-insurance and reinsurance pool</td>
<td>Commercial property damage and consequential business interruption</td>
<td>Distribution, retention, reinsurance</td>
<td>None</td>
</tr>
<tr>
<td>Netherlands</td>
<td>Industry reinsurance pool</td>
<td>Commercial and residential property damage, consequential business interruption, life and health, liability</td>
<td>Distribution, retention, reinsurance</td>
<td>Explicit state guarantee</td>
</tr>
<tr>
<td>Russia</td>
<td>Industry co-insurance and reinsurance pool</td>
<td>Commercial and residential property damage and consequential business interruption</td>
<td>Distribution, retention, reinsurance</td>
<td>None</td>
</tr>
<tr>
<td>South Africa</td>
<td>Public insurance company</td>
<td>Commercial and residential property damage and consequential business interruption, motor vehicles</td>
<td>Reinsurance</td>
<td>No explicit state guarantee</td>
</tr>
<tr>
<td>Spain</td>
<td>Public insurance company for extraordinary risks</td>
<td>Commercial and residential property damage, consequential business interruption, motor vehicle, life and health</td>
<td>Distribution, retention</td>
<td>Explicit state guarantee</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>Industry reinsurance pool</td>
<td>Commercial property damage and business interruption</td>
<td>Distribution, retention, retrocession</td>
<td>Explicit state guarantee</td>
</tr>
<tr>
<td>United States</td>
<td>Public-private co-insurance arrangement</td>
<td>Commercial property damage and consequential business interruption, liability, workers compensation</td>
<td>Distribution, retention, co-insurance, reinsurance</td>
<td>Co-insurance</td>
</tr>
</tbody>
</table>

Note: Terrorism (re)insurance programmes also exist in other countries, such as Denmark and Switzerland. The programme in Denmark only provides coverage for incidents involving nuclear, biological, chemical and radiological (NBCR) weapons and was therefore excluded from the analysis. For other countries, sufficient information on the programme structure and coverage was not available.

Source: (OECD, 2016[89]), (IFTRIP, 2017[30])
### Table A A.2. Definitions of terrorism applied by terrorism (re)insurance programmes

<table>
<thead>
<tr>
<th>Country</th>
<th>Definition</th>
<th>Source</th>
<th>Interpreting Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>Terrorist acts are all acts of persons or groups of persons with a view to achieving political, religious, ethnic, ideological or similar goals, and which are apt to put the public or sections of the public in fear, thereby influencing a government or public bodies</td>
<td>Industry association/ programme</td>
<td>Programme committee</td>
</tr>
<tr>
<td>Belgium</td>
<td>An act or threatened act organized in secret for ideological, political, ethnic or religious ends, performed individually or in groups and intended as an attempt at the lives of individuals or to either partially or completely destroy the economic value of tangible or intangible property whether to impact on the public, create a climate of insecurity or put pressure on the authorities in a bid to impede the running and normal operation of a service or business.</td>
<td>Legislation (Loi relative à l'assurance contre les dommages causés par le terrorisme)</td>
<td>Programme committee</td>
</tr>
<tr>
<td>France</td>
<td>Acts of terrorism, when intentionally connected with an individual or collective enterprise for the purpose of seriously disturbing public order by intimidation or terror, include the following offenses: (i) voluntary attacks on life, willful attacks on the integrity of the person, kidnapping and sequestration and the hijacking of aircraft, vessels or any other means of transport; … (ii) theft, extortion, destruction, damage and deterioration, as well as computer offenses…</td>
<td>Legislation (Code pénal - Article 421-1)</td>
<td>Programme/ policy language</td>
</tr>
<tr>
<td>Germany</td>
<td>Any acts committed by persons or groups of persons to achieve political, religious, ethnic or ideological purposes that are likely to spread anxiety or fear amongst the population or parts of the population and thereby influence any government or government institution.</td>
<td>Industry association/ programme</td>
<td>Programme/ policy language</td>
</tr>
<tr>
<td>India</td>
<td>An act or series of acts, including but not limited to the use of force or violence and/or the threat thereof, of any person or group(s) of persons, whether acting alone or on behalf of or in connection with any organisation(s) or government(s), or unlawful associations, recognized under Unlawful Activities (Prevention) Amendment Act, 2008 or any other related and applicable national or state legislation formulated to combat unlawful and terrorist activities in the nation for the time being in force, committed for political, religious, ideological or similar purposes including the intention to influence any government and/or to put the public or any section of the public in fear for such purposes.</td>
<td>Industry association/ programme</td>
<td>Programme/ policy language</td>
</tr>
<tr>
<td>Netherlands</td>
<td>Any violent act and/or conduct – committed outside the scope of one of the six forms of acts of war as referred to in 3.38 of the Financial Supervision Act [Wet op het Financieel toezicht] – in the form of an attack or a series of attacks connected together in time and intention as a result whereof injury and/or impairment of health, whether resulting in death or not, and/or loss of or damage to property arises or any economic interest is otherwise impaired, in which case it is likely that said attack or series – whether or not in any organisational context – has been planned and/or carried out with a view to effect certain political and/or religious and/or ideological purposes</td>
<td>Industry association/ programme</td>
<td>Programme committee</td>
</tr>
<tr>
<td>South Africa</td>
<td>(i) Any act (whether on behalf of any organisation, body or person, or group of persons) calculated or directed to overthrow or influence any State or government, or any provincial, local or tribal authority with force, or by means of fear, terrorism or violence; (ii) Any act which is calculated or directed to bring about loss or damage in order to further any political aim, objective or cause, or to bring about any social or economic change, or in protest against any State or government, or any provincial, local or tribal authority, or for the purpose of inspiring fear in the public, or any section thereof; (iii) riots, strikes, public disorder; (iv) Any attempt to perform any act referred to in clause (i), (ii) or (iii) above; (v) The act of any lawfully established authority in controlling, preventing, suppressing or in any other way dealing with any occurrence referred to in clause (i), (ii), (iii) or (iv) above.</td>
<td>Insurer</td>
<td>Programme/ policy language</td>
</tr>
<tr>
<td>Spain</td>
<td>Every violent act committed with the object of destabilizing the established political order or generating fear or insecurity in the social environment in which it is perpetrated.</td>
<td>Regulation (Reglamento del seguro de riesgos extraordinarios)</td>
<td>Programme/ policy language</td>
</tr>
</tbody>
</table>
## Coverage of cyber-terrorism by terrorism (re)insurance programmes

The terrorism (re)insurance programmes established in the aftermath of September 11th (or prior) were unlikely to have seriously considered the potential for damages and losses to result from a cyber-terrorism attack at the time of their establishment. As in the private market, some terrorism (re)insurance programmes may be exposed to silent (or non-affirmative) cyber risk. Others have taken steps to provide clarity on the extent of coverage provided by the programme. This section provides an overview of the potential coverage of terrorism (re)insurance programmes for: (i) property damage and consequential business interruption under property insurance policies; (ii) property damage and consequential business interruption under cyber insurance policies; (iii) business interruption without material damage (including contingent business interruption); and (iv) third party liability.

### Property damage and consequential business interruption under property insurance policies

The potential coverage provided by terrorism (re)insurance programmes depends on a number of factors including whether the programme provides primary insurance or co-insurance/reinsurance and whether the scope of coverage offered is defined by the programme or by legislation, regulation or an agreement with government.

Terrorism (re)insurance programmes in Germany, South Africa and Spain provide primary insurance and therefore their exposure to cyber-terrorism is governed solely by the terms and conditions established in their insurance policies:

- In Germany, the insurer (Extremus AG)\(^4\) has defined the coverage provided and is also responsible for defining when an incident should be considered a covered terrorism incident. A cyber-terrorism incident could potentially meet the definition of a terrorism incident. In such cases, physical damage and consequential business interruption losses (i.e. business interruption incurred as a direct consequence of physical damage) resulting from a named peril (such as fire or explosion) due to a cyber-attack would be covered.

- In South Africa, there is no government involvement in providing a backstop which means the terrorism insurer (SASRIA) is able to define the extent of coverage for cyber-terrorism. The definition of terrorism, as included in SASRIA policy wording, would likely include a cyber-terrorism incident as a covered event and would pay claims for covered loss types (property damage and consequential business interruption).

---

Source: (OECD, 2016\[^{[89]}\]), (IFTRIP, 2017\[^{[30]}\]), (Sasria, 2016\[^{[90]}\])
In Spain, the primary insurance coverage provided by state-owned insurer (Consorcio de Compensación de Seguros (CCS)) is defined by statute although CCS is responsible for determining when an incident should be considered a covered terrorism incident, with reference to the definition of terrorist offenses in the criminal code (which was amended in 2015 to include cyber-related offenses within the definition of possible terrorism offenses) (Government of Spain, 2015[91]). The CCS would treat physical damages and consequential business interruption resulting from cyber-terrorism in a similar way as damages and losses from other types of terrorism incidents (and extraordinary risks more generally).

Figure A A.1. Primary coverage for physical damage and consequential business interruption by terrorism (re)insurance programmes

A cyber-attack could be considered a terrorist incident (based on the definition of terrorism)  
Yes  
No  
Not covered by terrorism insurance programme

The insurance policy excludes physical damage and consequential business interruption resulting from a cyber-attack  
Yes  
No  
Not covered by terrorism insurance programme

Could be covered by terrorism insurance programme.

Extremus (Germany)  
SASRIA (South Africa)  
CCS (Spain)

The other terrorism (re)insurance programmes provide co-insurance and/or reinsurance of terrorism-related losses which means that their exposure to cyber-terrorism will depend on both the terms and conditions of the underlying (co-insured or reinsured) policy as well as any conditions applied by the programme to the co-insurance or reinsurance coverage provided (which may be established by the programme alone or through legislation, regulation or agreement with the government).

The programmes in Austria, India and Russia are not backed by any form of state guarantee. The programmes themselves are responsible for defining the terms and conditions of the co-insurance and/or reinsurance coverage provided and determining when an incident is a terrorism event covered by the programme:

- In Austria and India, physical damage and consequential business interruption from an incident that meets the definition of terrorism would be eligible for coverage by the terrorism (re)insurance programmes (Österreichischer Versicherungspool zur Deckung von Terrorrisiken (OVDT) and the Indian Market Terrorism Risk Insurance Pool (IMTRIP)). The current definitions of terrorism applied in Austria and India would not necessarily exclude cyber-terrorism and therefore physical damage and consequential business interruption from cyber-terrorism could be eligible for programme coverage (where covered in the underlying primary insurance policy).
In Russia, the Russian Anti-Terrorism Insurance Pool (RATIP) coverage excludes “loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system” (i.e. the commonly-used Institute Cyber Attack Exclusion Clause – CL 380) (IFTRIP, 2017[30]). Therefore, any damages and losses (including property damage and consequential business interruption) resulting from a cyber-terrorism event are likely to be excluded from programme coverage.

The terrorism (re)insurance programmes in Belgium, France, Netherlands, the United Kingdom and the United States involve loss-sharing with government (through a backstop or co-insurance) and therefore the scope of the co-insurance and/or reinsurance that they provide is defined to some extent in either legislation or regulation or through an agreement with the government. In addition, the co-insurance and/or reinsurance coverage provided by these programmes would only be triggered if claims were incurred based on the policy terms and conditions of the underlying policy:

- In Belgium (Terrorism Reinsurance and Insurance Pool or TRIP) and the Netherlands (Nederlandse Herverzekeringsmaatschappij voor Terrorismeschaden or NHT) a cyber-terrorism incident could potentially meet the definition of a terrorism event and is not specifically excluded from the coverage provided by the terrorism (re)insurance programmes. Therefore, losses resulting from cyber-terrorism and covered by the programmes (physical damage to commercial properties and consequential business interruption as well as damage to residential property and motor vehicles in Belgium) would likely be eligible for coverage if payments are made under the terms and conditions of the underlying policies. The determination of whether an incident is a terrorism incident eligible for programme coverage is made by the programme independently in the Netherlands and by a committee comprising representatives from the government and the insurance sector in Belgium.

- In France, the legal definition of terrorism (for which coverage must be included in property and motor vehicle insurance policies) specifically includes “computer offenses” and coverage under the terrorism (re)insurance programme (Gestion de l’assurance et de la réassurance des risques attentats et actes de terrorisme or GAREAT) is based on whether an incident meets that legal definition (with no specific need for a government declaration). As a result, physical damage and consequential business interruption resulting from cyber-terrorism would be eligible for coverage and should be included in underlying policies given that coverage for terrorism (including cyber-terrorism) is mandatory and policy wordings generally refer to the legal definition of terrorism.

- In the United Kingdom, the terrorism (re)insurance programme (Pool Re) only provides coverage for incidents certified as terrorism incidents by the UK Treasury, based on a statutory definition. A cyber-terrorism incident causing physical damage and consequential business interruption losses could meet the requirements of certification, and in April 2018, Pool Re began offering coverage for physical damage and consequential business interruption due to cyber-terrorism (with certain conditions). This was implemented by revising a general exclusion of cyber-attacks previously applied in its policies to extend coverage to acts of terrorism using “remote digital interference”. However, as a reinsurance provider, Pool Re would only pay claims to cedants if losses were covered in the underlying policy (which is not mandatory, as in France).

- In the United States, the co-insurance provided by the Terrorism Risk Insurance Program (commonly referred to as TRIA (Terrorism Risk Insurance Act)) is only available for incidents
certified by the US Treasury Secretary, based on a number of conditions including that the incident meets a statutory definition of terrorism and that a certain level of industry-wide losses are incurred. A cyber-terrorism incident could meet the criteria for certification as a terrorism act eligible for coverage. However, terrorism losses must be incurred by the insurer before TRIA co-insurance would be provided which means that TRIA coverage would not be available in the case of insurance policies that exclude cyber-attacks. TRIA’s requirement that terrorism coverage be offered to property insurance policyholders extends to cyber-terrorism where cyber-attacks are covered in the property policy.

Box A A.1. Damages to computer hardware, software and data

As described in Box 1.1 above, there are a number of cyber-related exclusions that may be applied to commercial property insurance policies - which may exclude cyber-attacks as a covered peril and/or damages to data and software as a covered loss. The terrorism (re)insurance programmes that provide co-insurance and/or reinsurance would normally follow the coverage provided in underlying policies (including endorsements) unless a specific exclusion or condition has been applied to their co-insurance or reinsurance agreements.

Similar to standard market practices, most terrorism (re)insurance programmes (OVDT (Austria), Extremus (Germany)\(^1\), GAREAT (France)\(^2\), CCS (Spain)) will only provide coverage for data and software losses (and any consequential business interruption) where that loss is the result of physical damage to computer hardware. Pool Re (United Kingdom) excludes damage to information technology equipment generally, including data and software, along with any consequential business interruption (as long as there is no other physical damage that would trigger coverage). These limitation would apply even in cases where coverage for data and software is provided by an underlying or co-insured policy (e.g. in a computer equipment or other machinery and equipment endorsement that provides coverage for data and software).

In the United States, TRIA does not apply any limitations or exclusions for data and software on the co-insurance that it provides and therefore coverage for data and software (without damage to hardware) may be co-insured by TRIA if other programme conditions are met. In South Africa, SASRIA’s material damage regulations, which define the coverage provided for property, allow for coverage to be provided for damage or losses to software and data.

\(^1\) Extremus AG’s terrorism insurance policy specifically excludes losses to data or programs caused by computer viruses, worms and Trojan horses (Extremus Versicherungs-AG, 2016\(^[5]\)).

\(^2\) As outlined below, GAREAT (France) has issued a specific clarification on what type of damages should be considered physical damage (based on jurisprudence) which clarifies that coverage excludes simple harm to data, loss of data, or the denial of access to data when not accompanied by technically irreversible damage to any computer hardware and/or equipment.
**Figure A A.2. Co-insurance/reinsurance coverage for physical damage and consequential business interruption by terrorism (re)insurance programmes: property policies**

**Property damage and consequential business interruption under cyber insurance policies**

As noted in chapter 2, there are some cyber insurance policies that include coverage for property damage resulting from cyber incidents (particularly outside Australia), either as part of standard coverage or, more commonly, as a possible endorsement or add-on to standard cyber insurance coverage. Some terrorism (re)insurance programmes (OVDT (Austria), Pool Re (United Kingdom)) will only provide co-insurance or reinsurance for property insurance policies and therefore a stand-alone cyber insurance policy would not be eligible for co-insurance or reinsurance through the programme (even where property damage coverage is provided).

In other countries, stand-alone cyber insurance policies that cover losses eligible for programme coverage (such as property damage) are not explicitly excluded as policies eligible for the programme’s co-insurance or reinsurance coverage:

- In Belgium, TRIP provides co-insurance and secures reinsurance for insurance policies that provide coverage for property damage to buildings, contents and other tangible assets and therefore a stand-alone cyber insurance policy that provides this type of coverage could...
conceivably be eligible for TRIP coverage (a stand-alone cyber insurance policy that does not include coverage for property damage would not be eligible for coverage under the programme).

- In France, GAREAT’s rules do not explicitly exclude stand-alone cyber insurance policies from programme co-insurance and reinsurance coverage and therefore a stand-alone cyber insurance policy providing coverage for property damage could potentially be eligible and would likely trigger the compulsory coverage for terrorism (and natural catastrophes). However, coverage for property damage is not normally included in stand-alone cyber insurance policies in France.

- In the Netherlands, NHT provides co-insurance and secures reinsurance for almost all lines of insurance that provide coverage for terrorism as a peril. A stand-alone cyber insurance policy providing coverage for property damage resulting from cyber-terrorism could therefore be eligible for the co-insurance and reinsurance provided by the programme.

- In Spain, CCS provides primary coverage for extraordinary risks as an extension to the primary policies underwritten by private insurers. A stand-alone cyber insurance policy that provide coverage for property damage would be subject to the extraordinary risk extension and receive coverage from CCS.

In the United States, stand-alone cyber insurance policies are (with some exceptions) explicitly eligible for programme coverage. The US Treasury issued guidance in 2016 confirming that cyber liability insurance written in any line of insurance included in the Program is subject to TRIA (Department of the Treasury, 2016[92]). This clarification was provided in light of confusion over the status of cyber liability insurance written as a professional liability insurance policy, which is not subject to the Program because professional liability insurance is not an eligible insurance line. Therefore, coverage provided for cyber-terrorism related property damage and consequential business interruption in a cyber insurance policy could be co-insured under TRIA (where other programme conditions are met). In addition, the requirement to offer terrorism coverage in lines of business subject to the Program extends to eligible cyber insurance policies (Department of the Treasury, 2016[92]).
Figure A.A.3. Co-insurance/reinsurance coverage for physical damage and consequential business interruption by terrorism (re)insurance programmes: cyber policies

1. A cyber-attack could be considered a terrorist incident (based on the definition of terrorism)
   - Yes: Stand-alone cyber insurance policies can be co-insured/reinsured with the programme
     - Yes: The stand-alone cyber insurance policy provides coverage for physical damage and consequential business interruption
       - Yes: The co-insurance/reinsurance policy of the programme excludes physical damage and consequential business interruption resulting from a cyber-attack
         - No: Not covered by terrorism co-insurance/reinsurance programme
       - No: Not covered by terrorism co-insurance/reinsurance programme
     - No: Not covered by terrorism co-insurance/reinsurance programme
   - No: Not covered by terrorism co-insurance/reinsurance programme

2. Stand-alone cyber insurance policies can be co-insured/reinsured with the programme
   - Yes: The stand-alone cyber insurance policy provides coverage for physical damage and consequential business interruption
     - Yes: The co-insurance/reinsurance policy of the programme excludes physical damage and consequential business interruption resulting from a cyber-attack
       - Yes: Could be covered by terrorism co-insurance/reinsurance programme
     - No: Not covered by terrorism co-insurance/reinsurance programme
   - No: Not covered by terrorism co-insurance/reinsurance programme

Countries mentioned:
- OVDT (Austria)
- IMTRIP (India)
- Pool Re (UK)
- GAREAT (France)
- CCS (Spain)
- RATIP (Russia)
- TRIP (Belgium)
- NHT (Netherlands)
- TRIA (US)
**Business interruption without physical damage (including contingent business interruption and business interruption resulting from damages to intangible assets)**

Business interruption coverage in property policies is normally triggered by the occurrence of damage to property that is insured within the scope of the policy. However, businesses could face business interruption losses as a result of cyber-terrorism incidents that do not involve damage to tangible property at their premises, such as: (i) business interruption as the result of a disruption at a supplier or customer (including a supplier of infrastructure services such as electricity or telecommunications); (ii) business interruption as the result of an incident in close proximity to a business’ operation that leads to access restrictions; and (iii) business interruption as the result of damages to intangible assets such as software or data not normally covered by a property insurance policy.

Coverage for business interruption without physical damage can generally be acquired in the private market for a variety of perils. Coverage for business interruption losses resulting from supplier/customer disruption (i.e. contingent business interruption) or loss of access may be available in property insurance policies or specialty policies for specific risks (such as political violence), either as specific endorsements/add-ons to standard policies or as stand-alone coverage. Coverage for business interruption resulting from damage to software or data (system/network business interruption) is normally included in cyber insurance policies and is sometimes added to property insurance policies.

As in the case of other loss types, terrorism (re)insurance programmes that provide co-insurance or reinsurance will normally reimburse losses incurred in underlying policies unless specifically excluded in their co-insurance and reinsurance agreements. Therefore, the terrorism (re)insurance programme may reimburse losses incurred if the underlying policy is: (i) eligible for coverage through the programme (which may not be the case if it is a cyber insurance policy, as noted above); and (ii) provides coverage for contingent business interruption, loss of access or system/network business interruption — and if these types of losses are not specifically excluded from the co-insurance/reinsurance coverage provided by the programme.

A number of terrorism (re)insurance programmes will only co-insure or reinsure business interruption losses that are consequential to physical damage to tangible property incurred directly by the insured (OVDT (Austria), Extremus (Germany)). As noted above, GAREAT (France) made a change to its internal rules in 2017 to provide greater clarity on what would (not) be considered direct physical damage (“Pure financial losses caused by acts of cyber terrorism defined by Article 421-1 point 2 and Articles 323-1 to 323-8 of the Penal Code, and particularly those caused by malicious software, viruses and cryptolockers, computer hacking and by computer attacks and denial of service attacks, as well as by any data breaches. Coverage therefore excludes simple harm to data, loss of data, or the denial of access to data when these are not accompanied by technically irreversible damage to any computer hardware and/or equipment”).

In Spain, CCS also generally only provides coverage for business interruption that is consequential to direct physical damage although some coverage may be provided for business interruption from loss of access due to an administrative order arising in relation to an “extraordinary risk” covered by the programme and that eventually materialises as physical damage (this coverage would apply for both commercial property and cyber insurance policies, although it would only be triggered in the event of physical damage). CCS does not provide coverage for any other form of business interruption without direct damage to the tangible property of the insured.

In the United Kingdom, the legislation governing the coverage that can be provided by Pool Re (and specifically, the liability of the UK Treasury as backstop provider) only, until recently, allowed for business interruption coverage to be provided as a direct consequence to property damage at the insured. A recent amendment to that legislation allows Pool Re to provide coverage for business interruption without direct physical damage which Pool Re will provide as coverage for loss of access and loss of attraction due to a terrorism incident (cyber terrorism will be excluded from that coverage).
Figure A A.4. Coverage for business interruption without material damage by terrorism (re)insurance programmes

The terrorism (re)insurance programmes in the Netherlands and the United States do not have a specific requirement for direct damage to tangible property of the insured to be incurred in order for business interruption coverage to be triggered. If an underlying policy provides coverage for contingent business interruption without physical damage (CBI, loss of access, damage to intangible assets), the co-insurance and reinsurance available through NHT and under TRIA would be available as long as other programme conditions are met.

**Liability (physical damage and bodily injury)**

A few terrorism (re)insurance programmes (TRIP (Belgium), NHT (Netherlands), TRIA (United States)) provide coverage for third party liability, in addition to the coverage provided for first party losses. Public liability (also referred to as general liability or civil liability) insurance will normally provide coverage for claims made by third parties for physical damage and bodily injury for which the insured may be liable. Workers’ compensation insurance provides liability coverage for employers for bodily injury claims made by its employees.

Similar to other types of losses – and to the extent that a liability claim could be made against a company on account of the cyber-terrorism event (which, as discussed above, is probably unlikely) - these
(re)insurance programmes would provide co-insurance or reinsurance for physical damage or bodily injury from a cyber-terrorism attack where a claim is paid under the underlying policy (and subject to other programme conditions). As outlined in chapter 2, cyber risks are sometimes excluded from liability insurance policies. However, workers’ compensation and civil liability policies in Belgium and workers’ compensation policies in the United States are required to include coverage for terrorism-related losses (general liability policyholders must also be offered terrorism coverage in the United States).

Figure A A.5. Co-insurance/reinsurance coverage for liability by terrorism (re)insurance programmes

A cyber-attack could be considered a terrorist incident (based on the definition of terrorism)

Yes

Liability insurance policies can be co-insured/reinsured with the programme

Yes

The liability insurance policy excludes physical damage and bodily injury resulting from a cyber attack

Yes

The co-insurance/reinsurance policy of the programme excludes physical damage and consequential business interruption resulting from a cyber-attack

No

Could be covered by terrorism co-insurance/reinsurance programme

No

Not covered by terrorism co-insurance/reinsurance programme

No

Not covered by terrorism co-insurance/reinsurance programme

No

Not covered by terrorism co-insurance/reinsurance programme

No

Not covered by terrorism co-insurance/reinsurance programme

No

Not covered by terrorism co-insurance/reinsurance programme

No

OVDT (Austria)
GAREAT (France)
CCS (Spain)
Pool Re (UK)

TRIP (Belgium)
NHT (Netherlands)
TRIA (US)
References


market-updates-brochure.pdf


ARPC (2016), Cyber Terrorism and Australia’s Terrorism Insurance Scheme: Physically destructive cyber terrorism is a gap in current insurance coverage, Australian Reinsurance Pool Corporation, http://www.arpc.gov.au


Department of Justice (2019), Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 million People, Department of Justice, https://www.justice.gov/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including


Evan, T. et al. (2020), Insurance Assessment of Cyber Terrorism in Australia, Centre for Risk Studies, University of Cambridge.


G7 (2017), G7 Declaration on Responsible States Behavior in Cyberspace, Group of Seven.


Government of Spain (2015), Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo, Boléntin Oficial del Estado.


House of Representatives, S. and G. Perrett (2012), In the wake of disasters: The operation of the
insurance industry during disaster events (Volume 1), Parliament of Australia,


Insurance Services Office (2011), Building and Personal Property Coverage Form (Commercial Property - CP 00 10 10 12), http://dx.doi.org/InsuranceServicesOffice


https://www.huntoninsurancerecoveryblog.com/2019/01/articles/cyber/zurich-invokes-war-exclusion-in-battle-over-coverage-for-notpetya-attack/#page=1

Liberty Specialty Markets (2017), War and Terrorism, Liberty Specialty Markets,  


Lloyd’s and the University of Cambridge Centre for Risk Studies (2015), Business Blackout: The insurance implications of a cyber attack on the US power grid, Lloyd’s,  

Lloyd’s Market Association (2018), Cyber Risks and Exposures: Model Clauses - Class of Business Review, Lloyd’s Market Association,  
http://www.lmalloyds.com/AsiCommon/Controls/BSA/Downloader.aspx?iDocumentStorageKey=c3910476-c5d4-47b1-bf3c-8b7e12e08299&iFileTypeCode=PDF&iFileName=cyber%20clauses%20review


Lloyd’s Market Association (2015), Cyber Loss Exclusion (Property Treaty Reinsurance) - LMA5240, Lloyd’s Market Association,  
http://www.lmalloyds.com/CMDownload.aspx?ContentKey=1ed03787-6264-4085-8bd5-45e91d09234f&ContentItemKey=5a47b8c5-9654-48b5-9a69-d25e3c4cad30

Lloyd’s Market Association (2015), Cyber Loss Limited Exclusion (Property Treaty Reinsurance), Lloyd’s Market Association,  
https://www.lmalloyds.com/CMDownload.aspx?ContentKey=8abfb611-baf8-4d3c-b2bc-eedaf278ad80&ContentItemKey=5a47b8c5-9654-48b5-9a69-d25e3c4cad30

Lloyd’s Market Association (2015), Electronic Data Endorsement C, Lloyd’s Market Association,  
https://www.lmalloyds.com/AsiCommon/Controls/BSA/Downloader.aspx?DocumentStorageKey=f980fb6-52d3-4d3a-87c5-d63052a926b6&FileTypeCode=DOC&FileName=NMA2914A

Lloyd’s Market Association (2015), Electronic Data Endorsement D, Lloyd’s Market Association,  
https://www.lmalloyds.com/AsiCommon/Controls/BSA/Downloader.aspx?DocumentStorageKey=c8892553-d64d-4fc6-8f71-39a668695fbb&FileTypeCode=DOC&FileName=NMA2915A

Lloyd’s Market Association (2010), Physical Loss or Physical Damage Riots, Strikes, Civil Commotion, Malicious Damage, Terrorism and Sabotage Insurance (LMA3092), Lloyd’s Market Association,  

Lloyd’s Market Association (2006), Terrorism Insurance Physical Loss or Physical Damage Wording


OECD (2017), *Enhancing the Role of Insurance in Cyber Risk Management*, OECD,


OECD (n.d.), The contribution of reinsurance markets to managing risk, OECD.


Pool Re (2019), Pool Re completes £2.3 billion terrorism retrocession placement, Pool Reinsurance, https://www.poolre.co.uk/pool-re-completes-2-3-billion-terrorism-retrocession-placement/

Pool Re (n.d.), Pool Re completes £2.3 billion terrorism retrocession placement, Pool Reinsurance, https://www.poolre.co.uk/pool-re-completes-2-3-billion-terrorism-retrocession-placement/


RDG and the Institute (2012), A review of typical reinsurance clauses currently used in Australia and
New Zealand market treaty documents (3rd edition), The Reinsurance Discussion Group and The Australian and New Zealand Institute of Insurance and Finance.


Watkins, J. (n.d.), Is there a Cyber Gap in your Coverage for Bodily Injury and Property Damage Claims?, Thompson Hine,


Notes

1 The survey was conducted in October and November 2017. A more recent survey by the same company (conducted between October and December 2018) saw an increase in the overall share of companies that had adopted cyber insurance (to 41% from 33%) although a breakdown by country and company size was not provided (Hiscox, 2019).

2 The policy may also be offered in other markets.

3 The policies reviewed provided affirmative coverage only for a defined or named set of service providers and/or applied a specific exclusion for utility service providers.

4 The cyber DIC policies identified include: AIG Cyber Edge PC (AIG, 2014); Chubb Global Cyber Facility – property endorsement and casualty endorsement (Chubb, 2017); and Aegis Cyber Resilience Plus (AEGIS Insurance Services, n.d.).

5 In the marketing material for one of the thirteen policies, coverage for terrorism was advertised as included in the policy although the specific policy wording was not available.

6 For the other companies, only marketing material (i.e. not specific policy wording) was available.

7 For example, contingent business interruption may include coverage for loss of access or loss of attraction where access to the insured’s premises is impeded or depressed because of property damage or other incident in proximity.

8 For example, a recent analysis of the use of cyber exclusions in the Lloyd’s market estimated that the most common broad cyber exclusion (CL380) was applied in less than 5% of UK property insurance coverage (although the exclusions of coverage for electronic data (NMA 2914 and 2915) were applied in 75% to 100% of coverage) (Lloyd’s Market Association, 2018). An analysis of a US power outage scenario also assumed that all-risk property policies in that market are commonly silent on whether cyber-related losses would be paid, suggesting similarly limited use of broad cyber exclusions in US commercial property policies (Lloyd’s and the University of Cambridge Centre for Risk Studies, 2015). One of the major international brokerage firms has also suggested that “there are currently no widespread cyber exclusions in the property market” (JLT Specialty, 2017).

9 A loss resulting from a cyber-attack that does not lead to a peril covered by the policy would not be insured. For example, a cyber-attack that corrupts data leading to business interruption would not lead to coverage for the business interruption loss as data corruption is an excluded peril.
The transfer of terrorism risk to GAREAT is not a legal obligation although all members of the Fédération française de l’assurance have committed to transfer large risks (sum insured above EUR 20 million) to GAREAT.

A breakdown between public liability and product liability is not available.

In our review of publicly-available policy wordings offered for the Australian market, we identified one company that applied an exclusion in its business package and combined general liability policies for a cyber-related incident, specifically “any liability of whatsoever nature directly or indirectly caused by, in connection with or contributed to by or arising from…the insured’s internet operations” (Zurich (Australia), 2014[111]), (Zurich (Australia), 2018[113]). We were also informed during meetings with market participants that at least one company provides affirmative (explicit) coverage for cyber-related losses under its public/general liability policies in Australia.

The company websites reviewed for this section include: AIG, AXA XL, Beazley, Chubb, Hiscox, Liberty Specialty Markets, Lockton and QBE (Europe).

For 2018-19 to 2020-21, this includes (annually) an AUD 55 million fee for the government guarantee, AUD 35 million capital holding fee and an AUD 10 million dividend (Australian Government: The Treasury, 2018[49]).

The responsible Minister is the Minister responsible for administering the Terrorism Insurance Act 2003, currently the Assistant Treasurer.

ISR policies will often apply an exclusion for damages and losses resulting from pollution or contamination which, if applied in the event of a biological or chemical attack, could serve to exclude the resulting losses. The legislative amendment extends the scope of exclusions that would become ineffective in the event of a DTI to exclusions of “acts that are described using the word ‘chemical’, ‘biological’, ‘polluting’, ‘contaminating’, ‘pathogenic’, or ‘poisoning’ or words of similar effect.”

The amount of the deductible that would be applied in the event of a DTI is not mandated by the Act and would normally be the same deductible that would apply to the policyholder for losses from any peril covered by the policy.

The 2018 review of the Terrorism Insurance Act 2003 considered whether to allow ARPC to offer premium discounts for risk mitigation for policyholders although concluded that there was insufficient information to determine what types of measures would be effective in mitigating terrorism risk (Australian Government: The Treasury, 2018[49]).

The example wording provided by ARPC is the addition of the following sentence to a general terrorism exclusion: “This terrorism exclusion will not operate in the event that the Treasurer declares an act to be a declared terrorist incident under the Terrorism Insurance Act” (ARPC, n.d.[34]).

The example wording provided by ARPC is the addition of the following sentence to a general terrorism exclusion: “in the event that the Treasurer declares an act to be a declared terrorist incident under the Terrorism Insurance Act we will not apply this exclusion unless the act of terrorism was directly or indirectly caused by, contributed to by, resulting from or arising out of or in connection with biological, chemical, radioactive, or nuclear pollution or contamination or explosion.” (ARPC, n.d.[34])

Some policies provided some limited coverage for computer hardware, which would normally be considered tangible property. One policy reviewed offered some coverage for hardware betterment costs when such costs were incurred in order to improve security (Zurich (Australia), 2018[16]). Another policy offered an optional endorsement for “tangible property cover” that would reimburse costs related to the
repair or replacement of IT infrastructure damaged as a result of a covered cyber event (Emergence, 2018[19]).

22 For illustrative purposes, one policy defines the trigger for its business interruption coverage as “interruption, suspension, failure, degradation or delay in the performance of the company’s computer system” (Zurich (Australia), 2018[16]).

23 The principle of proximate cause serves as a guide for determining whether a loss is covered under an insurance policy in cases where the loss results from multiple or concurrent causes. It has been defined in UK jurisprudence as the “active, efficient cause that sets in motion a train of events which brings about a result, without the intervention of any force started and working actively from a new and independent source” (iEduNote, n.d.[105]) or the dominant or effective cause of loss (Cooper, 2015[104]).

24 For example, one policy defines a “dependent business” whose interruption would trigger an insured’s contingent business interruption coverage as “any entity from which the Insured obtains technology services” (AXA XL Insurance (Australia), 2019[18]).

25 One policy provides contingent business interruption coverage (as an endorsement) that is triggered by a covered cyber incident at an “external supplier” (without defining what types of external suppliers) (Emergence, 2018[19]). Another policy provides coverage that is triggered by a covered cyber incident at a “service provider” and lists examples of technology service providers as service providers (while not limiting the definition of service providers to that list) (Zurich (Australia), 2018[16]).

26 Under the Building Management Systems attack, if building management is contracted to a third party, that contractor could potentially be targeted by liability claims from affected clients although this type of liability would normally be covered under a professional indemnity insurance policy rather than a public liability insurance policy. A professional indemnity insurance contract is not an eligible insurance contract under the Terrorism Insurance Regulations 2003.

27 As noted above, the specific stand-alone terrorism insurance policy advertising coverage for cyber-attacks only advertised coverage for property damage, not business interruption (Liberty Specialty Markets, 2017[44]).

28 A number of insurance company representatives suggested that it would be inefficient to provide property damage coverage in cyber insurance policies given that there would be a need to develop expertise in calculating the likely cost of property damage (expertise that already exists and is applied to underwriting property insurance policies).

29 One insurance company that was consulted indicated that they expected to cover cyber-terrorism losses as the terrorism exclusion they apply indicated that the terrorism exclusion would be annulled in the event of a DTI.

30 This includes the Queensland Floods Commission of Inquiry (Queensland Floods Commission of Inquiry, 2012[18]), Natural Disaster Insurance Review (Natural Disaster Insurance Review Panel, 2011[121]), an inquiry into the operation of the insurance industry after disaster events by the House of Representatives’ Standing Committee on Social Policy and Legal Affairs (House of Representatives and Perrett, 2012[120]) and the Northern Australia Insurance Premiums Taskforce (Northern Australia Insurance Premiums Taskforce, 2016[119]) (amongst others).

31 Insurance coverage for terrorism (including cyber-terrorism) must be provided in commercial property policies in France and must be offered in commercial property policies in the United States although property damage from cyber-attacks is not as consistently covered in those countries as they are covered in Australian ISR policies.
The Terrorism Insurance Act 2003 includes a broad definition of eligible insurance contracts (“loss of, or damage to, eligible property…business interruption and consequential loss arising from loss of, or damage to, eligible property….or inability to use eligible property…liability of the insured that arises out of the insured being the owner or occupier of eligible property.”). The definition of eligible insurance contract is then narrowed in scope through the Terrorism Insurance Regulations 2003 although with different approaches to different types of policies (some are excluded “to the extent that” they provide a given coverage while other policies are excluded when they provide cover “only” for a given loss). A detailed legal analysis of the types of distinct coverage provided in cyber insurance policies would be required to determine what should be excluded (or not) under the Act.

In the United Kingdom, for example, the Bank of England Prudential Regulation Authority found in a recent survey of insurance companies that “firms’ quantitative assessments of non-affirmative [cyber] risk are not well-developed and mostly rely on stress scenarios and expert elicitation” (PRA, 2019[131]).

This includes a criminal charges in California against a North Korean individual related to the Sony Pictures, WannaCry and the Bangladesh Bank attacks, criminal charges in Pennsylvania against seven military officers from Russia for the theft and release of athletes’ medical records from the World Doping Agency and an indictment in Indiana against a Chinese national for the theft of customer records from Anthem (Posa, n.d.[126]), (Department of Justice, 2019[127]).

It has also been suggested that the Government of Australia may be more reluctant to attribute cyber-attacks perpetrated by China (Cave, 2018[128]).

In some countries (e.g. United Kingdom), the definition of terrorism connects the act to an organisation with terrorist motivations which requires both the attribution of the act to an individual organisation as well as a determination of the actor’s motivation (Cambridge Centre for Risk Studies, 2017[73]).

Article 51 of the United Nations Charter authorises countries to exercise (or more specifically, does not inhibit countries from exercising) the “inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations” (United Nations, 1945[129]).

Some policies, used most often in the marine sector, provide a more narrow exclusion that applies only to war between the five powers (China, France, Russia, United Kingdom, United States).

The Consorcio de compensacion de seguros (CCS) in Spain provides coverage for damages related to other politically-motivated incidents (rebellion, sedition, riot and turmoil as well as actions by military or security forces in times of peace. Sasria (South Africa) provides coverage for damages due to riots, strikes, civil commotion and public disorder. However, neither organisation provides coverage for acts of war.

For example, according to estimates by the US Treasury, through their deductibles and co-insurance obligations, larger insurers could be accountable for close to 50% of the approximately USD 27 billion in losses covered under their policies for a modelled loss scenario based on an attack in New York City (Federal Insurance Office, 2018[86]).

One possible threshold could be the 0.5% probability (1-in-200 year return period) that is used by APRA for the purposes of establishing capital requirements (APRA, 2013[132]).

In Spain, an incident must meet the definition of a terrorism event under the regulations governing insurance coverage provided by the Consorcio de Compensación de Seguros (CCS) for “extraordinary risks”, with reference to the definition of terrorism under the criminal code. A procedure has been established for the attribution of an incident as a terrorist incident based on consultations with the Ministry of the Interior and/or the application of the terrorism-related provisions of the criminal code to the perpetrators.
Other private insurance companies in Germany also provide coverage for terrorism based on their own underwriting standards although only Extremus AG’s coverage is backed by a government guarantee.

CCS coverage for extraordinary risk is provided as primary coverage although it is exclusively attached to the insurance policies in eligible business lines underwritten by private insurers. As a result, CCS coverage will also be included in the discussion of co-insurance and reinsurance below.

In the Netherlands, an incident must involve an act of violence to be considered a terrorism event.

In some policies, damages to data and software may be covered by the property insurance policy or endorsement although business interruption resulting solely from such damage may be excluded.

Extremus AG does provide coverage for contingent business interruption and business interruption due to loss of access outside the scope of its agreement with the government (i.e. without a government backstop) which could be triggered as a result of physical damage due to a cyber-attack. Most of the coverage currently provided is for loss of access.

In addition to third party liability coverage for bodily injury, coverage for bodily injury due to terrorism in personal accident and life insurance policies is available under the terrorism (re)insurance programmes in Belgium, Netherlands and Spain and would likely be covered through the co-insurance and reinsurance provided as cyber risks are not normally excluded from personal accident or life insurance policies.