Australian Government
Australian Reinsurance Pool Corporation

The University of Queensland
Australia
CREATE CHANGE

Analysis of Identified Gaps in Australia's Terrorism Insurance Environment

Authors: ARPC, Professor Paula Jarzabkowski, University of Queensland and Dr Elisabeth Krull, City, University of London.

December 2020

Contents

Executive Summary

Since ARPC's establishment in 2003, the global terrorism environment has continued to evolve. In particular, there has been an increased risk of low-sophistication attacks carried out by lone actors using knives, firearms, and motor vehicles. The experience of relatively unsophisticated attacks overseas has highlighted gaps in insurance cover, such as where business interruption losses have occurred despite the absence of physical damage to property. At the same time, the risk of sophisticated attacks causing catastrophic damage remains unchanged.

In 2020, ARPC partnered with University of Queensland Business School to investigate the extent of insurance coverage for losses attributable to acts of terrorism in Australia and potential insurance coverage gaps. This report outlines the impact of six terrorism-based scenarios on the three pillars of Australian society: People, Property and Economic Performance. The scenarios were developed and analysed to identify and illustrate insurance gaps and coverage within the *Terrorism Insurance Act 2003 (TI Act 2003)*[1], and its associated Regulations, including broader impacts on market operation and coverage under public schemes of terrorist attacks. All scenarios refer to a Declared Terrorism Incident (DTI), meaning an incident which the Treasurer is satisfied was a terrorist attack after conferring with the Attorney General, and which is declared to be a DTI by the ARPC Minister.

While terrorism-related risks are widely covered in Australia, potential insurance gaps and inconsistencies could be identified for each pillar. The overall findings indicate that some types of losses from terrorism are not covered by existing arrangements or are covered imperfectly or inconsistently. At a high-level, these gaps include:

- Physical property damage caused by cyber terrorism;
- Business interruption insurance uptake by SMEs;
- Compulsory Third Party (CTP) motor insurance schemes;
- Inconsistencies in Workers' Compensation schemes;
- Inconsistencies in Victims of Crime schemes;
- Coverage of State and Commonwealth assets.

The purpose of this report, in identifying and presenting these existing gaps, is to inform future discussions on insurance coverage, such as what risks should be covered, and by whom within the commercial or public sector. The report concludes with some recommendations that might inform these future discussions.

Section 1

Background and Purpose

Section 1: Background and Purpose

Australian Reinsurance Pool Corporation (ARPC)

Australian Reinsurance Pool Corporation (ARPC) was established in 2003 in response to a gap in the Australian commercial property terrorism insurance market following the 9/11 terrorist attacks in the United States in 2001. ARPC's vision is to be an effective provider of terrorism risk insurance that facilitates private participation, supports national resilience, and reduces losses arising from catastrophic events caused by terrorism. ARPC is a corporate Commonwealth entity within the Treasury portfolio and with a Commonwealth solvency guarantee designed to be limited to $10bn. Similar Government-backed schemes exist in, for example, the UK (Pool Re)[2], France (GAREAT)[3] and Germany (EXTREMUS)[4]. The ARPC scheme covers eligible terrorism losses including commercial property, associated business interruption, and public liability. In July 2017, the scheme was expanded, following a review by the Treasury, to include mixed-use buildings where floorspace is at least 20% commercial and high-value mixed-use and residential buildings valued at more than $50 million.

Who should read this report

ARPC commissioned this report to identify current gaps in insurance coverage as a result of a declared terrorism incident (DTI).The report aims to raise awareness and increase understanding of potential gaps in DTI insurance cover to support informed decision-making by four key stakeholders:

1. Insurers – to help prevent unintended or hidden exposure to ('silent') risks;
2. Policy-holders – to help identify and select appropriate insurance policies that optimises protection according to their needs;
3. State authorities – to help consider and evaluate the liabilities and risks on their own balance sheets;
4. Policy makers – to help develop policies on managing and reducing gaps that are grounded in informed debate about their risks to Australian society.

We have concluded that there are some types of losses from terrorism that are either not covered by existing arrangements or are covered imperfectly or inconsistently. These findings are presented as a 'Perils-on-a-Page' framework based on the implications of current risks and potential insurance gaps for People, Property and Economic Performance, and then expanded upon through illustrative scenarios. While these scenarios and gaps are not exhaustive, the framework is intended to serve as a sensitising tool to raise stakeholders' awareness of protection gaps for a DTI, and to assess and reflect on their compounded impact on the three pillars of Australian society. The scope of the report excludes any issues and impacts outside of a DTI and any reasons for non-coverage of perils by private insurers.

Section 2

Terrorism Threat and Insurance Cover

Section 2: Terrorism Threat and Insurance Cover

Terrorism Threat in Australia

Terrorism remains a threat in Australia. In recent years, Australia has seen several terrorist incidents prevented, varying from actions by lone actors to harm individuals, to an attempt to load a chemical bomb onto an aircraft departing Sydney.[5] The former incidents show that terrorism tactics have evolved and include unsophisticated attacks. The latter attempt shows that large-scale terrorism remains a significant threat. The potential magnitude of a large-scale attack would be unlikely to be fully covered by the global reinsurance capital market. Terrorism insurance pools such as ARPC provide a mechanism to provide such cover, with risk shared between policy-holders, insurers, the global reinsurance market, and the government of a country.[6] At the same time, terrorism tactics have evolved, resulting in lone actor events witnessed in Australia and abroad, such as knife attacks or the use of vehicles and attacks on “soft” targets, like crowds. In addition, non-conventional attacks involving cyber can pose a potential threat.[7] The ongoing evolution in these tactics makes it necessary to consider the broader financial impacts of new forms of attack.

On 26 November 2015, the Australian Government launched the National Terrorism Threat Advisory System (NTTAS) to inform the public about the likelihood of an act of terrorism occurring in Australia. NTTAS has five levels to indicate the national threat level as shown in Table 1.

Table 1: National Terrorism Threat Advisory System (NTTAS)

Certain	Red is the highest level and means that a terrorist action is certain.
Expected	Orange means a terrorist action is expected.
Probable	Yellow indicates that a terrorist action is probable. This is the current threat level in Australia.
Possible	Blue indicates that a terrorist action is possible.
Not expected	Green is the lowest category of threat and means a terrorist action is not expected.

At the time of writing this report, NTTAS threat level is ‘Probable’, which indicates individuals or groups have developed the intent and capability to conduct a terrorist attack in Australia. The current level has not been introduced in response to a specific threat but rather indicates that there is a probable level of risk that, like other probable perils, should be considered in terms of the potential implications of gaps in insurance cover.[8]

Terrorism Cover in Australia

Insurance cover for property damage and financial losses caused by a DTI is not widely available in Australia. Any cover for terrorism is generally excluded in insurance policies but is written back into policies by the TI Act 2003 in the event of a DTI. Policies that include Industrial Special Risk (ISR),[9] an ‘all-risks’ property policy for assets which are valued at more than $5 million and covers material damage to property, and business interruption; and Business Packs, where businesses choose the cover that is relevant to them (e.g. public & product liability and / or business interruption) but where no minimum or maximum asset limit applies.[10]

The majority of commercial property excludes cover but transfers it through reinsurance by ARPC. Where insurance policies state a terrorism exclusion clause, in the event of a DTI that policy will still respond and those policies with a terrorism exclusion clause in them can be reinsured with ARPC. The decision to reinsure with ARPC lies with the primary insurer. In Australia, the majority of primary insurers have reinsured with ARPC, providing a wide coverage overall. However, while ISR uptake is generally high, Business Interruption insurance uptake by small- to medium-sized businesses (SMEs) remains comparably low.

Personal insurance such as life insurance, income protection, and health insurance policies typically do not have terrorism exclusions. Hence, individuals who have purchased personal cover would be covered in the event of a terrorist attack. However, not all people have purchased these covers. Such people may be relying on other insurance products such as Workers' Compensation or Victims of Crime compensation or may simply be unaware of the risks posed by, or cover available for, a DTI.

Section 3

Gaps in Terrorist Attack Cover

Section 3: Gaps in Terrorist Attack Cover

This section provides an overview of the current gaps in cover for terrorist attacks in Australia and their implications for three pillars of society: Australian people, property and the economic performance of Australian-based businesses.

- People, meaning individuals affected by the attack in form of death or injury;
- Property, meaning damage to or destruction of commercial property;
- Economic Performance, meaning financial losses through, e.g. loss of attraction, denial of access, loss of goodwill, and loss of markets as a consequence of a DTI.

This overview is followed by a detailed presentation of the gaps for each pillar. Presentation of these gaps is illustrated using six detailed terrorist attack scenarios with further scenarios available in Appendix 2. The scenarios, listed in Table 2, include non-conventional and conventional terror attacks:

Table 2: Scenarios for non-conventional and conventional terror attacks

Non-conventional terror attacks	Conventional terror attacks
1. Cyber-attack with physical building damage	1. Mass gathering attack via truck
2. Ransomware	2. Explosion with commercial building collapse
3. Chemical explosion in crowded public place	
4. Drones releasing toxic chemicals in CBD	

Our analysis showed that damage and losses resulting from DTIs are widely covered in Australia. Nevertheless, we have identified some gaps in insurance cover that might result in moderate to severe losses if they are not addressed.

Sensitising tool: Perils-on-a-page

Figure 1 provides a 'Perils-on-a-Page' sensitising framework for assessing the extent of current cover and gaps. This framework shows the impact of each of the six scenarios on the three pillars (People, Property, and Economic Performance) by assessing the degree of cover or non-cover (Table 3) in relation to two types of gaps. The scenarios that we present are not exhaustive and illustrative only.

Figure 1: Perils-on-a-Page

Tactics of Terror		Act of Terror	People COVER	People GAP	Property COVER	Property GAP	Economic Performance COVER	Economic Performance GAP
Non-Conventional	Cyber	1) *Cyber attack with physical building damage*	PI ($$$); WCI ($)*	I & II	X	I & II	X	II
Non-Conventional	Cyber	2) *Ransomware attack*	PI ($$$); WCI ($)	I & II	n/a	n/a	CI ($)	I & II
Non-Conventional	Chemical or Biological (CB)^	3) *Chemical explosion in crowded public place*	PI ($$$); WCI ($)	I & II	CI ($$$)	II	CI ($)	I
Non-Conventional	Chemical or Biological (CB)^	4) *Drones releasing toxic chemicals in CBD*	PI ($$$) WCI ($)	II	CI ($$$)	II	CI ($)	I
Conventional	Lone actor	5) *Mass gathering attack via truck*	PI ($$$); CTP ($)	II	CI($$$)	II	CI ($)	I
Conventional	Explosives	6) *Explosion with commercial building collapse*	PI ($$$)** WCI ($)	I & II	CI ($$$)	II	CI ($)	I
		Impact on:	**People**		**Property**		**Economic Performance**	

^ Events of Nuclear and Radiological (NR) nature are uninsurable and excluded
* Only covers if victims are in a commercial building. Does not include travel / passing of building
** There are gaps in in terms of cover for 'victims of crime' schemes, incurring losses to (some) states / territories

Severe gaps / lack of cover | Some gaps / lack of cover | No gaps / lack of cover

Cover

The Perils-on-a-Page framework, accounts for the different types of cover. These include personal (non-commercial) cover, which is outside of ARPC's remit. However, in order to provide a complete picture of the current insurance landscape, gaps or inconsistencies in non-commercial cover are taken into consideration where appropriate.

Table 3: Key for Cover in Perils-on-a-Page

Key	Conventional terror attacks
$$$	Full cover
$	Some cover but either (1) a majority of losses are not insured; or (2) coverage differs between States / Territories.
X	No cover
CI	Commercial Insurance, e.g. **Industrial Special Risk (ISR),** also known as Property Insurance, an 'all-risks' property policy for assets >$5,000,000 which covers property, i.e. material damage, and business interruption, often a form of contingent business interruption based on a disruption that affects the policy-holder's suppliers and/or customers[11]; **Business Packs** including Business Interruption insurance that helps protect businesses from losses due to a closure of business as a result of an insured event. In Australia, ~40% of businesses do not have adequate business interruption insurance.[12]
PI	Private Insurance (e.g. life insurance, income protection, private health insurance, compulsory third party [CTP], travel insurance).
WCI	Workers' Compensation (WC) Insurance, a compulsory insurance for any business that employs staff to cover for workplace injuries or disease. WC is governed on a State government basis and rules, regulations including roles of insurers differ between States and Territories.[13]

Gaps

Our analysis has revealed two types of gaps, which are specified in the Perils-on-a-Page framework.

- Type I: Not covered in an underlying insurance policy. ARPC cannot reinsure as there must be an eligible contract of insurance covering the impact.
- Type II: ARPC is unable to reinsure due to the nature of the Declared Terrorist Incident ('DTI'). That is, an impact that would otherwise be covered by the scheme but is specifically excluded by the Terrorism Insurance Regulations 2003.[14]

This categorisation of gaps outlines that for some classes of business, not all policies offer standardised cover, and there can be large disparities between the policy terms and conditions in the market. As ARPC offers reinsurance, for the scheme to cover the loss, the initial risk must be covered in the underlying primary market policy. This means that businesses and individuals must purchase cover in order for such cover to come into effect. As the Perils-on-a-Page framework shows, property currently has most cover, followed by people and then economic performance. The following sections detail some of the gaps by drawing on selected scenarios to illustrate them. While we present the scenario analyses specifically for each pillar to illustrate the gaps, the impacts of a DTI are, of course, compounding.

3.1 Property

Commercial property damage as a result of a DTI is excluded in policies but written back in through the TI Act 2003. The majority is reinsured by ARPC. However, we identified some gaps especially with regards to the:

- **Type of property,** i.e. is it commercial, residential, or dual-occupancy property; and
- **Type of ownership,** i.e. is it privately / commercially owned, Commonwealth- or State-owned property.

To illustrate these gaps, we draw on scenarios 1, and 6 from the Perils-on-a-Page (Figure 1):

1) Cyber-attack with physical building damage;

6) Explosion with commercial building collapse.

Type of property

The cover for damage to buildings caused by acts of terror depends on the type of property. The majority of commercial property in Australia is reinsured by ARPC. Residential property buildings are outside of ARPC's remit with the exception of high-value residential buildings valued at more than $50 million and mixed-use buildings with at least 20% commercial floorspace.[15] For residential property, wide-ranging private insurance options are available which, unless specifically stated, do not exclude damage resulting from terrorist attacks.

Scenario

(1) Cyber-attack (DTI) with physical building damage:

A cyberterrorist attack on a dam causes widespread flooding, resulting in flood damage to property, both commercial and residential, in the nearby township.

Analysis of Gap

This scenario is exposed to both Type I and Type II gaps:

Type I gap for residential property: A Type I gap exists where flood damage that results from a malicious action is not covered in the relevant insurance contracts. This is a subset of insurers; most do not have this exclusion.

Type II gap for commercial property: In this event, commercial property would not be covered under reinsurance if an ISR is in place. The current regulations stated in the TI Act 2003 exclude computer crime, restricting ARPC to reinsure any cyber-attacks.

In this scenario, residential buildings are mainly covered albeit some minor exceptions may exist, which highlights the importance of examining carefully the policy wording. Nonetheless, generally cover is available. However, due to the nature of the attack and the current regulations in the TI Act 2003, no cover is available for commercial property in the event of a terrorist cyber-attack with physical building damage (see Figure 1), even where an ISR is in place. Had the dam been damaged via a physical attack using, for example, explosives, the commercial building would be reinsured by ARPC provided a commercial property insurance (or ISR) was in place. While standalone cyber insurance is available in Australia, the uptake remains relatively low compared to property and general liability insurance[16] and where they are taken up the physical property damage cover is sub-limited, primarily aimed at covering damaged computer equipment. Furthermore, definitions of cyber-terrorism in the policy wordings differ across individual insurers.[17] In addition, stand-alone cyber insurance policies do not cover property damage (except for computer equipment),[18] which poses a significant risk to commercial properties and businesses in the event of a cyber terrorist attack with physical damage.

Type of ownership

The cover for damage to buildings caused by DTIs also depends on the type of ownership. State and Commonwealth assets are not reinsured by ARPC and the risk is often carried by the States themselves, albeit without an explicit insurance policy for that risk.

Scenario

(6) Explosion with commercial building collapse

An explosion causes the collapse of a major city hotel containing numerous function and meeting rooms, one of which is hosting the AGM for a major listed company; a high number of individuals who were not employed at the site die. The adjacent Government office was also destroyed in the explosion.

Analysis of Gap

This scenario is exposed to a Type II gap:

Type II gap for Commonwealth or State property: The hotel building is a commercial property and would be covered by an ISR policy. The ISR would be eligible to be reinsured with ARPC. However, the adjacent Government office is a publicly owned enterprise. The outlet would be covered by the Commonwealth but would not be eligible to be reinsured with ARPC since contracts of insurance covering the Commonwealth are excluded by the TI Act Regulations 2003.

This scenario demonstrates that there is potential high risk of financial losses to the public sector for State and Commonwealth-owned properties. Two buildings standing side-by-side may suffer identical damage from the same event, but one will be covered and the other not. The costs for the damage of such risk to public sector buildings, if uninsured, ultimately, would be carried by the Australian public as taxpayers.

Property Summary and Recommendations

As these analyses show, while a lot of Property cover exists because of write-backs due to TI Act 2003 (see Figure 1), there are inconsistences in cover arising from the Type 1 and 2 gaps. First, for policy holders it is important to recognise that physical building damage resulting from a DTI cyber-attack is not covered by existing ISR insurance policies as the risk cannot be reinsured by ARPC. However, where stand-alone cyber policies exist, these typically do not cover physical building damage. Hence, there is a market gap in suitable cover for such physical damage from cyber-attack.

Second, many State and Commonwealth owned properties are self-insured, purchasing reinsurance to protect their own insurance schemes, without coverage from ARPC. While such cover is usually for the threat of natural catastrophe damage to publicly-owned assets and infrastructure, such schemes might be further explored in terms of the extent of cover for damage to publicly-owned property from terrorist attacks.

These two points mean that, in the event of a DTI, it is important to be aware that similar damages will result in different or inconsistent payments to recover from loss. Even where cover is comparatively strong and appears comprehensive, nonetheless, clarity about the specific nature of that cover and its implications post-event is needed. We recommend an awareness-raising campaign for commercial, high-value residential, and mixed-use property owners to ensure that they make informed choices about the extent of their cover. These examples are not exhaustive but rather intended to raise such awareness.

3.2 Economic Performance

Business interruptions can be caused by both physical building damage that interrupts business operations, and also 'non-damage' events that nonetheless cause interruption through, for example, loss of attraction or prevention of access. Most business interruption caused by terrorism events is excluded in ISR policies. However, should a DTI be declared, this exclusion is written back in as the majority of commercial property in Australia is reinsured by ARPC. Some gaps were identified especially with regards to the

- **Duration of interruption** i.e. short-term or long-term; and
- **Type of damage,** i.e. physical or non-physical.

To illustrate these gaps, we draw on scenarios 1, 2 and 3 from the Perils-on-a-Page framework (Figure 1):

1) Cyber-attack with physical building damage;
2) Ransomware attack;
3) Chemical explosion in a crowded public place.

Duration of interruption

The duration of business interruption, for example through lack of access to the physical business site, IT systems, or vital information, can, in addition to the (physical) damage caused by a DTI, have an effect on a business' profitability and economic performance.

Scenario

(1) Cyber-attack with physical building damage:

A cyberterrorist attack on a dam causes widespread flooding, resulting in damage on the ground floor of a three-storey commercial property. The entire building is closed for two weeks and none of the businesses located in the property are able to operate during that time.

Analysis of Gap

This scenario is exposed to a Type I gap:

Type I gap for business interruption caused by damage to a commercial property: In this event, commercial property would **not** be covered under reinsurance. The resulting interruption to business would also not be covered. The current regulations stated in the TI Act 2003 exclude computer crime, restricting ARPC from reinsuring any cyberattacks.

This scenario demonstrates that in the event of physical damage to a business caused by a cyber terror attack, business interruption would not be covered. If the dam structure had been damaged as the result of a physical terror attack (e.g. using explosives), all businesses, whether physically damaged or not, would be covered provided they had a BI policy. Of note, while cyber insurance is available in the market, policies typically only cover costs of recovering data and systems, assisting to manage reputational damage, and liability claims. Physical building damage is typically not covered, exacerbating the gap in cover for this type of scenario.[19]

Scenario

(2) Ransomware attack:

A ransomware attack cripples a major Australian bank; 40% of the bank's systems cannot be accessed, and screens display pro-extremist videos and demand payments to an anonymous location. This significantly impacts customer and investor confidence in the bank along with cyber losses impacting many commercial entities and individuals.

Analysis of Gap

This scenario is exposed to both Type I and Type II gaps:

(Partial) Type I gap for loss of attraction: This could occur if there is a sentiment in the marketplace immediately after a cyberattack that the bank's security systems are inferior to competitors (this would likely be more significant in the case of a DTI due to the heightened psychological impact terrorism has compared to standard criminality). This would have a negative impact on customer retention and acquisition, impacting revenue. Insurance products purporting to cover this kind of loss are still in their infancy. To date, standard insurance policies tend not to protect any form of business interruption without linked property damage, unless explicitly stated via a policy extension. There is no property damage in this scenario, therefore it is very likely that the bank will be facing a gap in insurance cover.

Type II gap for cyber losses of the bank: The impact of a ransomware attack would impact many commercial entities and individuals. The majority of these entities and individuals would not have insurance cover and would seek indemnity from the bank. Cyber insurance policies are beginning to emerge in higher numbers.[20] However, terms and conditions can vary significantly between different insurers' products and coverage is currently not very broad. A prudent bank with strong risk management practices should have tailored cyber insurance policies to protect their customers and themselves. Regardless of the products on offer, ARPC cannot reinsure this kind of coverage since "computer crime" is excluded in the TI Act Regulations.

This scenario demonstrates the importance of awareness regarding computer crime. While, as stated in the scenario, a bank would likely have comprehensive cyber insurance in place, it is typically not included in standard insurance policies. This highlights the need for careful review of policy wording to optimise adequate cover. The scenario also draws attention to types of losses that may not be covered by standard business interruption policies (e.g. loss of attraction). It is therefore important to be aware of the various products that are available and to be able to assess their adequacy for the respective businesses.

Type of damage

Interruptions to business operations can have severe economic impacts. This can be caused by both damage-based interruptions, arising from damage to or destruction of the physical site where the business is located, or non-damage interruptions such as restricted customer or employee access to the business physical site as the result of an incident.

Scenario

(3) Chemical explosion in crowded public place:

A chemical release/explosion in a crowded railway station in a large city during peak hour causes mass casualties. Some businesses in the immediate vicinity of the explosion are physically damaged albeit most businesses are damage free. A large number of people, customers, passengers, and employees, are injured and killed.

Analysis of Gap

This scenario is exposed to a Type I gap:

Type I gap for businesses with non-physical damage business interruption (BI): For most BI contracts, some amount of property damage is a precondition for an insurer paying a claim. Many policies require physical damage within the vicinity for a business interruption claim to be paid. In the case of a mass casualty attack of this nature, many businesses would experience economic impact, yet the access to insurance payments will be varied. For example, an explosion would cause physical damage, which would make some businesses eligible to claim for business interruption, but other businesses located further from the incident may not be able to claim.

This scenario demonstrates that despite a wide variety of cover available, the policies and terms can differ significantly. For businesses, it is important to consider these differences in order to be able to make informed decisions. For example, many businesses could be disrupted by the unexpected loss of a number of key staff, yet most businesses would be unable to claim for business interruption if a chemical attack impacted people but not property. Businesses within the exclusion zone that had denial of access cover would be able to claim business interruption for denial of access, but unlikely for the extended disruption caused during the period to source and train new staff. For a small number of businesses that had key person insurance there would be cover for the loss of those named individuals, but for most businesses there would be no cover for the economic impact of losing staff.

Economic Performance Summary and Recommendations

These gap analyses show that cover for Economic Performance exists, albeit that there is less coverage than for Property (see Figure 1). However, even where cover exists, it is inconsistent, especially where insurance policies require physical damage within the vicinity for a BI claim to be paid. This means that businesses impacted by the same DTI might not receive the same cover, which will cause unequal post-event hardship to ostensibly similar business attempting to recover from the same event, generating perceptions of inequity. These inconsistencies in cover again raise awareness that clarity about the specific nature of any particular cover and its implications post-event is needed, so that those who will be affected can make informed decisions about both legislating and/or purchasing risk cover. Over and above this inconsistency, while BI insurance products are available, they have low uptake by SMEs. In Australia, approximately 40% of SMEs do not have adequate business insurance packages, let alone BI insurance, making them vulnerable in the event of significant financial impacts.[21]

To mitigate these risks, we suggest the development of targeted education campaigns for SMEs, primary insurers, and insurance brokers in order to aid informed decision-making. This could be complemented by a set of (digital) tools that help SMEs identify their key risks, the possibilities to cover those risks, and provide guidance regarding essential cover and possible implications of non-cover.

Another solution to increase the uptake of BI insurance by SMEs which could be investigated is the bundling of BI products into general business insurance products, potentially coupled with compulsory cover. Sometimes SMEs do not buy products because they are either unaware of their benefits or are required to opt into the purchase of additional cover at an extra cost. While bundling of multiple risks, including terrorism, into a single product would come at an extra cost, if all SMEs were offered terrorism in their general insurance bundle, this would increase both the diversification and also the amount of cover being purchased by all SMEs, so lowering the price for any individual SME. A combination of bundling combined with compulsory cover, in which SMEs were required to take out BI cover on all risks, including terrorism, would ensure both the widest spread of protection, and also, due to combined effects of risk diversification and risk pooling across all SMEs in Australia, would lower the price for all.[22]

However, before such solutions can be designed it is important to gain a better understanding of what prevents SMEs from taking out BI insurance in the first place. A 2015 survey by the Insurance Council of Australia showed that key reasons for not taking out BI insurance included policies being 'too expensive' (25.9%), and the risk was seen as too low (23.1%).[23] Further research to understand whether these reasons are still valid and to identify any additional barriers for non-uptake, could provide insights into SME motivations for purchasing insurance. Such research could clarify whether this is due to affordability of the products, which could be mitigated by different risk-sharing strategies, ignorance of the products available and the risks associated with non-cover, which could be addressed by an education campaign, or whether there are other currently unidentified barriers to uptake.

3.3 People

People are a key target for terrorist attacks. In the unfortunate event of injuries and deaths occurring from DTIs, there are a range of policies that could hold and cover such horrific events. These include, for example, life insurance, private health insurance, travel insurance, and income protection. However, there is wide inconsistency in the uptake of such cover.

To illustrate these gaps, we draw on scenarios 1, 4, 5, and 6 from the Perils-on-a-Page:

1) Cyber-attack with physical building damage;
4) Drones releasing toxic chemicals in CBD;
5) Mass gathering attack;
6) Explosion with commercial building collapse.

Scenario

(1) Cyber-attack with physical building damage:

A cyberterrorist attack on a dam causes widespread flooding, resulting in damage on the ground floor of a three-storey commercial property. Unfortunately, some people are caught in the magnitude of the flooding and either injured or killed. Among those injured are some whose injuries are so severe that they will need life-long physical support and have also lost their means of livelihood and ability to work. The victims include employees and workers who were located in the building or on their way to work, and members of the public who were passing by.

Analysis of Gap

This scenario is exposed to both Type I and Type II gaps:

Type I gap for private cover. While private insurance is available and typically does not exclude terrorism, people may not have purchased private insurance. While Victims of Crime schemes may hold, compensation for individuals differs across States (see Appendix 3).

Type II gap for Workers' Compensation Insurance (WCI). While WCI does cover victims who are employed at the respective business and, at the time of the attack, in the commercial building, those victims travelling to and from work are covered in some States but not in others (see Appendix 3). which would make some businesses eligible to claim for business interruption, but other businesses located further from the incident may not be able to claim.

This scenario shows that while individuals are generally covered, compensation for bystanders via Victims of Crime schemes and regulations of cover regarding WCI differ across States (see Appendix 3). However, in the event of a cyber terrorist attack, cover is generally available.

Scenario

(4) Drones releasing toxic chemicals in CBD

A multi-drone flight across a central business district (CBD) in a large city releases toxic biological/chemical substances. This results in implications for all three pillars in terms of injury and deaths, interruption to business, and damage to property. The implications for people are both loss of life, but also varying degrees of injury including some significant periods of medical care and rehabilitation to get some of those injured to a stage where they are able to resume any type of employment.

Analysis of Gap

This scenario is exposed to a Type II gap:

Type II gap for Worker's Compensation Insurance (WCI) schemes: There are significant inconsistencies in the application of WCI schemes across States. For example, if a large amount of the contaminant enters buildings adjacent to the drone flight paths and spreads through many businesses for a prolonged amount of time, many workers in a geographically defined area could be affected, either fatally or severely injured. This would trigger a large payout under that State or Territory's WCI scheme, incurring large financial cost to the insurers involved (for schemes including private providers) or the responsible State organisation (for state-administered schemes). In addition, an exclusion exists for workers travelling to or from work in some jurisdictions.

This scenario shows a large financial impact on either insurers or the State in the event of a DTI. Workers' compensation is currently excluded under the TI Act Regulations, and would not be covered by ARPC. Furthermore, terrorism is not specifically mentioned in the legislation in many States. We believe that workers' compensation in those jurisdictions would be used in the event of a high casualty DTI. State Governments would be impacted from claims under Workers' Compensation schemes and Victims of Crime schemes.

Scenario

(5) Mass gathering attack via truck

A lone assailant drives a truck into a mass gathering during a town festival. A large number of people are injured or killed. These include people who were at the premise as guests (including students, travellers, and the general public) and those who were there for work-related reasons (e.g. food stall employees, council workers, and volunteers). Injuries range from relatively minor stays in hospital to major, life-changing injuries that will result in needing life-long care, as well as loss of ability to work.

Analysis of Gap

This scenario is exposed to a Type II gap:

Type II gap for Compulsory Third Party (CTP) cover: The majority of victims would be covered by some form of insurance policy such as private (e.g. life insurance, private health insurance, travel insurance, and income protection), compulsory (i.e. compulsory third party (CTP) cover), and public (Medicare, workers' compensation, victims of crime compensation, and National Injury Insurance Scheme (NIIS) in some States). However, CTP differs in coverage where terrorism is excluded from State CTP arrangements. With the exception of Victoria and WA (partially), all other States and Territories exclude terrorism from their CTP schemes.

This scenario demonstrates that while victims would generally be covered (either through their private or public insurance schemes), CTP, which is the typical means of paying personal injury claims from motor vehicles, would not apply in most States due to the exclusion of terrorism. While property policies with terrorism exclusions are covered by ARPC in the event of a DTI, there is no similar pooling mechanisms or reinsurance scheme to cover exclusions from personal injury policies. As vehicle-based attacks are increasingly shown to be a source of lone-actor terrorist attacks overseas, such as the 2016 vehicle-ramming attack on a German Christmas Market,[24] this exclusion is an area of increasing concern, where awareness is needed.

Scenario

(6) Explosion with commercial building collapse

An explosion causes the collapse of a major city hotel containing numerous function and meeting rooms, one of which is hosting the AGM for a major listed company. A high number of individuals (some who were employed at the site and many who were not, e.g. hotel guests, meeting attendees, and bystanders) die. The adjacent Australia Post outlet was also destroyed in the explosion and many individuals (Australia Post employees and members of the public) were either permanently injured or killed.

Analysis of Gap

This scenario is exposed to a Type II gap as well as to inconsistencies in victims of crime schemes:

Type II gap as there are losses to the State via interaction with 'victims of crime' schemes and the State. The large number of deaths would trigger a large number of primary victim claims (from families of the deceased to help pay for funeral costs and other sudden expenses, and from people seriously injured in the attack), and potentially a large number of secondary victim claims from bystanders who witness the collapse or attempt to help people trapped in the rubble. This means incurring a large and unexpected payment from the State or Territory in which the attack happens, representing an uninsured risk.

Type II gap for Workers' Compensation Insurance (WCI). While WCI does cover victims who are employed at the hotel and, at the time of the attack, in the commercial building, those victims travelling to and from work are covered in some States but not in others (see Appendix 3).

This scenario demonstrates that the impact of such a DTI would cause significant costs to the State or Territory regarding Victims of Crime schemes, which are uninsured. There are also significant differences between State schemes (Appendix 3) and so a state-by-state analysis is necessary. The equity of such variability between State arrangements is questionable given the similar physical and psychological consequences across State lines for people impacted in such an attack. The State schemes are post-funded and the States have indicated they are content to carry these exposures.

People Summary and Recommendations

These scenarios illustrate the complexity regarding cover in an event that results in loss of lives or permanent injuries. For people who are on site due to work-related matters, cover is typically provided via Workers' Compensation Insurance (WCI). In Australia, any business that employs staff is legally obliged to have WCI in place to cover for workplace injuries or disease. WC is governed on a State basis and rules and regulations, including roles of insurers differ between States and Territories.

A wide range of private cover to protect against healthcare costs, or loss of income for victims or beneficiaries of deceased or permanently injured victims is available, all which typically do not exclude terrorist attacks. Such private cover includes health insurance, income protection cover, life insurance and permanent disability insurance. However, the uptake of these types of private insurances tends to be skewed towards higher socio-economic strata or older generations.[25] As a result, not all Australians are equally covered, leaving many of those who are already more vulnerable financially exposed should they or their family member fall victim to a terrorist attack. While it may be possible to make such cover compulsory this would a) constitute a financial burden on many individuals; and b) insistence on compulsory personal insurance to alleviate the possible damages arising from a terrorist attack could generate undesirable heightened levels of fear within the general population.

Where people do not have private insurance and are not covered under an employment scheme, publicly funded cover and compensation would normally come into effect. However, there are many inconsistencies across States and Territories especially with regards to Victims of Crime schemes and Workers' Compensation Insurance. In the event of permanent injury, different outcomes for individuals suffering similar injuries from the same event, or different outcomes in different jurisdictions for individuals suffering largely similar injuries from similar events, will generate perceived inequities. We recommend a review of such inconsistencies, alongside an awareness campaign, so that the implications of such inconsistencies are clearly understood.

Awareness of these gaps and inconsistences in cover provides an opportunity to revisit the current schemes more carefully and potentially develop new, innovative solutions. For example, France's Fonds De Garantie Des Victimes[26] (Guarantee Fund for Victims of Terrorist Acts and Other Offences [FGTI]) scheme provides comprehensive compensation for victims of terror attacks or their beneficiaries, should the victim decease. Such compensation does not arise from an insurance product per se. However, it nonetheless follows insurance principles of solidarity and mutualisation, as the fund arises from a small levy on all personal insurance policies which, collectively, across insureds, provides the fund to enable such compensation while not requiring any individual to take out a specific policy for protection from such events.

3.4 Summary of Protection Gaps to Three Pillars

Our findings indicate that despite comprehensive coverage of DTIs, some gaps exist in the current terrorism insurance landscape. By developing six scenarios and analysing them through the lens of Australia's three pillars of society (Property, People, and Economic Performance), we have presented some of those gaps in this report. We found that while Property is generally well covered, significant inconsistencies, especially regarding the type of property and type of ownership, still exist. In order to avoid problems arising from different loss payments to comparable properties following similar events, such inconsistencies need to be properly understood through an awareness campaign.

There are also significant inconsistencies in coverage of Economic Performance, particularly in BI coverage, that require further analysis. In particular, a key concern for SMEs is non- or underinsured businesses, even where cover is available. This can be mitigated with education campaigns, innovations to support small business with risk analysis and decision-making, and product innovations, such as bundled products that provide full cover, alongside further analysis of the reasons for lack of demand for available cover.

People had the most inconsistencies in coverage, partially as a result of inconsistencies of (public) schemes such as Workers' Compensation or Victims of Crime schemes across States and Territories. Such inconsistencies could result in perceptions of social inequality should events occur. Such perceptions will be exacerbated where a DTI might cross State lines, or involve multiple people from different State jurisdictions. It is important to recognise that a terrorist attack is typically an attack on the values of the society and peoples of a whole country (see definition in Criminal Code Act 1995),[27] rather than on the particular states or regions within that country. Hence, inconsistencies in cover by state will likely be seen as indefensible should a DTI, particularly one with large-scale loss of life and injury, such as Scenarios 3 and 4, lead to differential outcomes for individuals. While an awareness campaign may be of value, gaps in cover for people would benefit particularly from innovative approaches to providing cover, including ways of mutualising risk to ensure that all individuals can be confident should a terrorist attack occur on their country.

These scenarios and gaps are illustrative only and most DTIs would likely affect all three pillars of society at once. For example, our analysis of the cyber-attack scenario illustrates that DTIs (can) have a compounding effect, meaning that they impact multiple pillars; Property, Economic Performance, and / or People. While extensive cover may be available for one pillar, as shown by our findings on Property (with the exception of cyber-attack), the extent and consistency of cover available for others, such as People may not have been considered (yet), or may be available, but have low awareness and uptake, such as for impacts on Economic Performance . Hence, a single event, particularly a large-scale event, may expose the pillars of Australian society to significant and compounding risk from which there is only ex-ante financial protection. This calls for a more holistic and systematic assessment of the implications of terrorist attacks to ensure adequate cover is available and awareness and understanding of remaining gaps, and how they will be paid for is addressed.

A summary of the key findings includes:

1. The exclusion of computer crime in the TI Act 2003 (and resulting inability to reinsure via ARPC) could result in significant exposure for Property and Economic Performance. The ARPC scheme currently excludes computer crime. This means that physical damage to property and consequential business interruption from a cyber terrorist attack is not covered. The scenario involving flooding due to a compromised dam revealed a significant exposure for homeowners with flood insurance, from one major insurance company, that excludes deliberate damage to a dam. While not strictly an exclusion for terrorist attacks, in practice the impacts of a terrorist attack involving a dam or reservoir would be excluded.
2. There is a gap in the insurance market in the event of business interruption with no corresponding property damage (e.g. Scenario 3: Chemical explosion in a crowded public place). For DTIs that cause a business to stop trading, but which do not cause physical damage to property, business interruption insurance is available in the market, including cover extensions for terrorism. However, a gap in the market remains, as SME uptake of business interruption insurance remains low or inadequate.
3. Compulsory third party (CTP) insurance only covers terrorism risk in some jurisdictions, having an impact on coverage for injuries to people (e.g. Scenario 5: Mass gathering attack via truck).
4. The applicability of Workers' Compensation is highly inconsistent between States, leaving some Australian workers covered and others not (e.g. Scenario 4: Drones releasing toxic chemicals in CBD). Especially the regulations regarding travel to and from work is inconsistent, leading to potential inequalities across States.
5. Victims of Crime schemes are inconsistent across jurisdictions (e.g. Scenario 6: Explosion with commercial building collapse). While the regulations are clear in that terrorism is classified as a crime and therefore Victims of Crime cover comes into effect whenever an injury is caused to victims, the compensations and regulations are not coherent across Australia (see Appendix 3).
6. State and Commonwealth assets are not reinsured by ARPC (e.g. Scenario 6: Explosion with commercial building collapse). State governments have indicated that they effectively self-insure against risks to their physical assets or have other insurance and reinsurance arrangements. There is no gap while these arrangements remain in force, but it is worth noting that these States cannot currently reinsure their risk with ARPC due to exclusions in the Regulations. The Territories do not have their own arrangements but are covered by the Commonwealth.

Section 4
Conclusion

Section 4: Conclusion

Increasing awareness and understanding of potential gaps in DTI insurance cover, and their separate but also compounding effects on the three pillars of Australian society, Property, Economic Performance and People, is important for informed decision making by the four key stakeholders: insurers in offering policies, policy-holders including people and businesses in purchasing policies, State authorities in evaluating coverage, and policy-makers in developing policy and legislation to address protection gaps.

For insurers, it helps them prevent the dangers of unintended or hidden exposure to risks they have not accounted for when offering their policies. Such hidden risks can lead to unexpected claims that have not been priced into policies, and for which there are, therefore, inadequate capital reserves to cover these 'silent' risks. Indeed, the financial impact of such silent terrorism risk on insurance companies and their capacity to pay claims following the 2001 attacks on the World Trade Centre was one dominant reason for establishing reinsurance pools such as ARPC in many countries around the world.

For policy-holders, both individuals and businesses, it helps them identify and select appropriate policies to get optimal protection. This is particularly important where insurance cover exists and is fairly priced and affordable by many policy-holders, but lacks uptake because of a lack of knowledge of the risks to which they are exposed, or consideration of how they might pay for losses arising from these risks.

For State authorities, it helps them to consider the liabilities and risks on their own balance sheets and how they might meet the costs on under-insured areas or gaps. This is particularly important as, alongside losses to the assets that such authorities own, they are typically the insurer of last resort for any uncovered losses to the wider business and society within their jurisdiction.

For policy-makers, it provides insights into those areas where no cover exists, or where cover is available but has little uptake. In addition, it indicates areas where hidden exposures and underinsurance may impact on the three pillars of Australian society in the event of a DTI. Such insights can support informed debate over legislation and policy making to address protection gaps.

To conclude, damage caused by DTIs in Australia is well covered. Nevertheless, we have identified several gaps that would benefit from further in-depth analysis, in order to ensure that such protection gaps are factored into prior planning for, and legislation of, financial and social recovery from terrorist events.

Appendices

Appendices

Appendix 1 – Key terms

Term	Definition
Business interruption (BI)	A category of losses occurring when a business is unable to trade due to some unforeseen disaster; for the purposes of this Paper, BI occurs when a business is directly shut down by a DTI.
Cyber-attack	Physical damage and business interruption following a terrorism cyber-attack is excluded from the ARPC scheme.
Declared terrorist incident (DTI)	An incident which the Treasurer is satisfied to be a terrorist attack after conferring with the Attorney General, and which is declared to be a DTI by the Minister.
Denial of access	A category of losses occurring when a business premises cannot be entered in the course of commerce due to a security incident or danger; this might be because a business is located within an exclusion zone set up in the immediate aftermath of a DTI that prevents access for a significant period of time.
Goodwill	Businesses that rely in large part on an established base of trust with the public are at risk of significant financial damage from a DTI that reduces public trust. Consistent media headlines naming a business in connection with an attack may greatly reduce the willingness of consumers to engage with that business. Such a loss would be sustained and very real but difficult to precisely quantify and would certainly be more difficult than quantifying physical property damage. Some of this loss may be recoverable under business interruption coverage, although goodwill itself is not currently insured. Nonetheless, such losses may be significant for a business to wear and so deserves to be more closely examined.
Loss of attraction	In terrorism insurance this is a class of losses that stem from a reduction in consumers' comfort in attending a place of business or interacting with that business due to some perceived risk that has come about because of a past incident. Insurance cover for loss of attraction due to terrorist attacks is a highly specialised product, is not offered widely and must constantly change in order to keep apace of evolving tactics of assailants. While this is a kind of BI loss, BI usually does not cover it since it is difficult to quantify and does not stem directly from property damage; it is closer to reputation damage which is more difficult to insure against.
Loss of markets	Some types of economic disruption to a business are well covered by existing insurance arrangements, but others are harder to precisely quantify or are otherwise imperfectly covered. For example, temporary interruption of a business' trading can be insured against with business interruption insurance. However, permanent interruption to trading caused by the destruction of or substantial decrease in a market is normally considered a standard business peril and so is not covered. This might include situations like when a DTI causes extensive and lasting water pollution to a previously thriving marine area; businesses that relied on fishing or eco-tourism in the area would lose the basis for the business activity. The result of this element of loss of markets arrangements is that businesses relying on a fragile market that can be severely disrupted with a DTI are carrying a large and uninsured risk.
Victims of crime compensation	Compensation is available to persons affected either directly or indirectly by crime. Since terrorism is a criminal offence, victims of terrorism could claim this compensation. The extent of the compensation varies state to state and are paid out in different ways. This means compensation varies in quantity from a total of $40,000 in the Northern Territory through to $100,000 in South Australia and varies in the wording of what compensation is paid for and to whom (most states and territories pay compensation to secondary victims, i.e. witnesses or family of the victim, up to a lower threshold than the primary victims).

Appendix 2 - Scenarios

Scenario 1 – Cyber-attack

Scenario: Cyber-attack on a dam causing widespread flooding.

Consequence: Flood damage to commercial property, residential homes and office buildings; severe injuries and deaths

Impact	Analysis	Gaps/Inconsistencies
Property *Commercial*	• ARPC excludes computer crime therefore damage caused by flooding as a result of a cyber-attack would not be reinsurable.	**Type II gap** exists as cyber terrorist attacks are excluded from ARPC.
Property *Residential*	• There is an anomaly in the market in residential home insurance. Home insurance policies do not generally exclude terrorism. While most contracts provide flood cover that would be relevant to this scenario, some insurance contracts specifically exclude damage caused by malicious actions interfering with dams and reservoirs. This potentially represents a Type I insurance gap as ARPC believes that many houses covered by such contracts sit within at-risk areas.	**Potential Type I gap** exists where flood damage that results from a malicious action is not covered in the relevant insurance contracts. This is a subset of insurers, most do not have this exclusion.
Economic Performance *Business interruption*	• Business interruption caused by damage to a commercial property: In this event, commercial property would not be covered under reinsurance. The resulting interruption to business would also not be covered. The current regulations stated in the TI Act 2003 exclude computer crime, restricting ARPC from reinsuring any cyber-attacks.	**Type I gap** for business interruption
People *Private cover & WCI*	• Private cover: While private insurance is available and typically does not exclude terrorism, people may not have purchased private insurance. While Victims of Crime schemes may hold, compensation for individuals differs across States (Appendix 3); • Workers' Compensation Insurance (WCI). While WCI does cover victims who are employed at the respective business and, at the time of the attack, in the commercial building, those victims travelling to and from work are covered in some States but not in others (Appendix 3).	**Type I gap** for private cover; **Type II gap** for WCI

Scenario 2 – Ransomware attack

Scenario: A ransomware attack cripples a major Australian bank; 40% of the bank's systems cannot be accessed, and screens display pro-extremist videos and demand payments to an anonymous location.

Consequence: Impacts customer/investor confidence in bank along with cyber losses impacting many commercial entities and individuals.

<table>
<tr><th>Impact</th><th>Analysis</th><th>Gaps/Inconsistencies</th></tr>
<tr><td>Economic Performance
Goodwill lost</td><td>Quantifying the risk and amount of losses of goodwill would likely be exceptionally difficult in cases of a deliberate and sudden event like this, whether or not it was a DTI; goodwill is normally accounted for during the sale of a business, but no mechanism exists for measuring it otherwise. It is therefore considered to be uninsurable with current insurance mechanisms, so represents a Type I gap for businesses.</td><td>Type I gap for businesses where goodwill is significant.</td></tr>
<tr><td>Economic Performance
Loss of attraction</td><td>In this case, loss of attraction could occur if there is a sentiment in the marketplace immediately after a cyber-attack that a bank's security systems are inferior to competitors (this would likely be more significant in the case of a DTI due to the heightened psychological impact terrorism has compared to normal criminality). This would have a negative impact on customer retention and acquisition, impacting revenue. Such losses could be roughly quantifiable through the usual method of comparing the period of time in question to a period of "normal profits" over an analogous 12-month period. Insurance products purporting to cover this kind of loss are still very much in their infancy and only some insurers offer these kinds of products, although the insurance industry continues to innovate.
Typically, these policies currently only offer this cover to the following industries:
Hotels
Retailers
Entertainment venues
Museums and Galleries
Restaurants, cafes and bars
Tourist attractions
Theme Parks
Standard insurance policies tend not to protect any form of business interruption without linked property damage. There is no property damage in this scenario, therefore it would be very likely that the bank will be facing a gap in insurance cover.</td><td>Partial Type I gap for businesses, since these products are limited;

Type II gap because "computer crime" is excluded by the TI Act 2003.</td></tr>
<tr><td>Economic Performance
Cyber losses</td><td>The impact of a cyber terrorist attack of this kind would impact many commercial entities and individuals. The majority of these entities and individual would not have insurance coverage and would seek indemnity from the bank.
Cyber insurance policies are beginning to emerge in higher numbers. However, terms and conditions can vary significantly between different insurers' products and coverage is currently not very broad. A prudent bank with strong risk management practices, should have tailored cyber insurance policies to protect their customers and themselves.
Regardless of the products on offer, ARPC cannot reinsure this kind of coverage since "computer crime" is excluded in the Regulations. While by no means the only factor, this is potentially holding back development of these kinds of insurance products since insurers are no doubt aware that they cannot be reinsured through ARPC.</td><td>Type II gap because computer crime is excluded in the TI Act 2003.</td></tr>
</table>

Scenario 3 – Chemical explosion in crowded public place

Scenario: A chemical release/explosion in a crowded railway station in a large city during peak hour causes mass casualties.

Consequence: A number of people are injured and killed.

Impact	Analysis	Gaps/Inconsistencies
Property	• Damage to property is covered to the extent it is privately owned and insured with an eligible Industrial Special Risk (ISR) or Business Package policy. If it is a state or Commonwealth public asset, it is excluded by the TI Act 2003 and outside ARPC's remit. However, the government owning the asset can insure through the relevant state scheme or self-insure.	**Minor Type II** gap exists for state or Commonwealth public assets, not able to be reinsured with ARPC.
Economic Performance *Business interruption*	• For most Business Interruption (BI) contracts, some amount of property damage is a precondition for an insurer paying a claim. Many policies require physical damage within the vicinity for a business interruption claim to be paid. In the case of a mass casualty attack, many businesses could be disrupted by the unexpected loss of a number of key staff. Such an incident would have a financial impact on affected businesses but may not involve any direct physical damage to the insureds property or property in the vicinity. • An explosion would cause physical damage, which would make some businesses eligible to claim for business interruption, but other businesses located further from the incident may not be able to claim. • Most businesses would be unable to claim for business interruption if a chemical attack impacted people but not property. Businesses within the exclusion zone that had denial of access cover would be able to claim business interruption for denial of access, but unlikely for the extended disruption caused during the period to source and train new staff. • For a small number of businesses that had key person insurance there would be cover for the loss of those named individuals, but for most businesses there would be no cover the economic impact of losing staff.	**Type I gap** for non-physical damage business interruption.
	• An imposition of an exclusion zone for a period of time would affect businesses in that zone. Prevention of access cover, a sub class of BI, normally has time retention periods and will pay as long as a building is damaged 'in the vicinity' of the incident.	**No gap** in this scenario regarding prevention of access cover.
People *Private insurance*	• Victims will rely on insurance such as, life insurance, private health insurance, Medicare, workers compensation, income protection, victims of crime compensation. Life insurance, income protection (depending on the policy) and private health insurance normally pay out regardless of the cause of death or injury and these flows of payments fall within normal business for insurers, so we consider that there is no gap. • Workers' Compensation is analysed below, and victims of crime compensation is analysed in scenario 6.	**No gap** regarding life insurance/income protection/private health insurance.
People	• Worker's compensation schemes in Queensland and the ACT cover workers who are in transit between their residence and their place of work. In New South Wales, Tasmania, South Australia, Western Australia and Victoria an	**Type I** gap exists for workers in jurisdictions where workers'

Impact	Analysis	Gaps/Inconsistencies
Payouts under WC	employer is generally not liable if an employee is injured on the way to or from work. In Victoria, workers who are injured on this journey are able to apply for compensation under a separate transport accident compensation scheme. This means in other states, an attack such as this at a train station during peak hour will likely impact a large number of persons who would be eligible for worker's compensation. The financial impact here is therefore on the state responsible. This large and unexpected payout may put stress on a state or territory's worker's compensation scheme.	compensation cover excludes the journey to or from the workplace.

Table 4: Analysis. Workers compensation insurance gap coverage (refer to Appendix 3 for further details)

State	Summary	Gap (Y/N)
Victoria	Victoria covers terrorist attacks under the *Workplace Injury Rehabilitation and Compensation Act 2013 (Vic)*, does not cover workers while commuting.	Yes
NSW	Under the *Workers Compensation Act 1987 (NSW) NSW covers terrorist attacks*, NSW takes the risk but is compensated through a state reinsurance scheme with limitations on state exposure, and does not cover workers while commuting, therefore gap for commuters.	Yes
Queensland	*Workers' Compensation and Rehabilitation Act 2003 (Queensland)* doesn't exclude terrorism, does cover workers while commuting.	No
South Australia	South Australia likely exposed without ability to reinsure under *Return to Work Act 2014 (SA)*, and does not cover workers while commuting.	Yes
Western Australia	The extent of coverage including the operation of the *Workers' Compensation and Injury Management (Acts of Terrorism) Act 2001 (WA)* seems to be partial but this is unclear, also does not cover workers while commuting, so potentially a gap but requires deeper analysis to make conclusions.	Possible
Tasmania	Included in the *Workers Rehabilitation and Compensation Act 1988 (Tas)* Tasmania has a built-for-purpose body with mechanism to protect the state, although does not cover workers while commuting.	Yes
ACT	Under the *Workers Compensation Act 1951 (ACT),* risk is reinsured through a legislated agency and injuries/deaths of workers while commuting are covered.	No
Northern Territory	Under the Return to Work Act (NT), NT potentially has exposure and isn't reinsured, and does not cover workers while commuting.	Yes

Scenario 4 – Drones releasing toxic chemicals in CBD

Scenario: A multi-drone flight across a central business district of a major city releases toxic biological/chemical substances.

Consequence: Some people are injured and killed, interruption of business, and damage to property.

Impact	Analysis	Gaps/Inconsistencies
Property	• Damaged property (including contaminated property) is covered to the extent it is privately owned and insured with an eligible ISR or Business Package type of policy. If it is a State or Commonwealth government owned asset then it is excluded by the TIA Regulations.	**Type II** gap for Commonwealth or state property, since it is excluded, although may be self-insured or insured by other commercial contracts.
Economic Performance *Business interruption*	• For most business interruption contracts, some amount of property damage is a precondition for an insurer to pay a claim; the property damage can be in the vicinity of the insured's business (i.e. not their own property). For a drone attack using contaminating chemicals, where physical damage occurs, a business interruption claim is triggered. For chemicals only impacting people, business interruption losses would occur despite there being no physical damage in the vicinity. This would mean the insureds are not covered.	**Type I** gap in coverage for non-property damaging business interruption.
	• An imposition of an exclusion zone for a period of time would affect businesses in that zone. Prevention of access cover, a sub class of BI, will pay as long as a building is damaged 'in the vicinity' of the incident. If there is no property damage, normal time retention periods would apply meaning prevention of access cover would take effect after a set period of time. If attacks like this are likely to impact an area for longer than this, and in a case where no property damage occurred, this would mean businesses would not be covered.	**No gap** is present except for businesses that remain closed for longer than the time retention period after an attack in which no property damage is caused; Minor Type I gap.
People *Losses to state from large payouts under CI*	• A large amount of the contaminant in this scenario could enter buildings adjacent to the drone flight paths through air intakes, spreading through many businesses in an attack that could go on for some time. Many workers in a geographically defined area could be affected, triggering a large payout under that state or territory's worker's compensation scheme. • In the event of a high casualty attack occurring at a place of work, the state or territory government of that jurisdiction will be under pressure to provide worker's compensation for the victims. This is likely to be at large financial cost to the insurers involved (for schemes including private providers) or the responsible state organisation (for state-administered schemes). Worker's compensation is excluded under the TIA Regulations. • Terrorism is not specifically mentioned in the legislation in many states so in these jurisdictions we believe worker's compensation would be used in the event of a high casualty DTI. State Governments would be impacted from claims under workers compensation schemes and victims of crime schemes. Furthermore, an exclusion exists for workers travelling to or from work in some jurisdictions.	**Significant inconsistencies** in the application of workers compensation schemes, further detailed investigation is required to confirm any potential gaps.

Impact	Analysis	Gaps/Inconsistencies
	• Additionally, in the states where cover excludes commuting, an exception is made for travel that occurs on the instruction of the employer. These are likely to be lower impact, however, since such trips would not tend to occur all at the same time in the same way that commuting during rush hour does.	

Scenario 5 – Mass gathering attack via truck

Scenario: A lone assailant drives a truck into a mass gathering during a town festival.

Consequence: A number of people are injured or killed, including but not limited to students, travellers, workers and general public.

Impact	Analysis	Gaps/Inconsistencies
People *Compulsory Third Party (CTP)*	• Damaged property (including contaminated property) is covered to the extent it is privately owned and insured with an eligible ISR or Business Package type of policy. If it is a State or Commonwealth government owned asset then it is excluded by the TIA Regulations.	**Type II** gap for Commonwealth or state property, since it is excluded, although may be self-insured or insured by other commercial contracts.

CTP insurance gap coverage (see Appendix 3 for further details)

State	Summary	Gap (Y/N)	State	Summary	Gap (Y/N)
Victoria	Victoria is liable to pay claims, but cannot reinsure with ARPC due to exclusion in the Regulations	No	**Western Australia**	CTP partially applies; for victims suffering "catastrophic" injury there is no CTP support	Partial
NSW	NSW CTP excludes terrorism	Yes	**Tasmania**	Tasmanian CTP excludes terrorism	Yes
Queensland	Qld excludes terrorism	Yes	**ACT**	ACT CTP excludes terrorism	Yes
South Australia	SA CTP excludes terrorism	Yes	**Northern Territory**	NT CTP excludes terrorism	Yes

Impact	Analysis	Gaps/Inconsistencies
Economic Performance *Business interruption (BI)*	• An exclusion zone is likely to be imposed on the area by police responding to the incident, affecting businesses located within the exclusion zone. If there is property damage to any eligible buildings caused by the incident, the commercial occupants of that building and occupants of commercial buildings in the "vicinity" will be insured for business interruption. • There is some limited cover available for "prevention of access" where authorities have blocked areas not immediately associated within the location of the attack. This amount is often small in value and has a one or two-day exclusion or waiting period. However, if there is no property	**Type I** gap exists as business interruption with no property damage is an insurance coverage gap as it is not covered in the underlying insurance policy.

Impact	Analysis	Gaps/Inconsistencies
	damage, there is no business interruption cover, even under the "prevention of access" sub clause. This means many businesses are carrying an uninsured risk, potentially creating localised economic disruption in the event of a DTI.	

Scenario 6 – Explosion with commercial building collapse

Scenario: An explosion causes the collapse of a major city hotel containing numerous function and meeting rooms, one of which is hosting the AGM for a major listed company; a high number of individuals who weren't employed at the site die

Consequence: Many people are injured and killed, damage to hotel and surrounding properties

Impact	Analysis	Gaps/Inconsistencies
Property *Publicly owned enterprises*	• The building is a commercial property and would be covered by an ISR policy, which is an eligible risk, and in turn covered by reinsurance with ARPC. • If an adjacent Australia Post outlet was also destroyed in the explosion, such a business would be covered by the Commonwealth but would be unable to be reinsured with ARPC since contracts of insurance covering the Commonwealth are excluded by the Regulations. This would apply to any property of the Commonwealth's that was destroyed, as well as business interruption or any other financial impact.	**Type II** gap exists only for State or Commonwealth public assets.
People	• International hotel guests will not be protected in Australia but generally will be covered by travel insurance, if taken. • Local hotel guests would rely on life insurance, private health insurance, Medicare, workers compensation, income protection, victims of crime compensation.	**No gap** regarding life insurance/income protection/private health insurance.
Public liability	• ARPC reinsures public liability associated with the eligible buildings involved in the terrorist incident.	**No gap**
People *Losses to state via interaction with 'victims of crime' schemes*	• In this scenario, the large number of deaths would trigger a large number of primary victim claims (from families of the deceased to help pay for funeral costs and other sudden expense, and from people seriously injured in the attack), and potentially a large number of secondary victim claims from bystanders who witness the collapse or attempt to help people trapped in the rubble. This means incurring a large and unexpected payment from the state or territory in which the attack happens, representing an uninsured risk. These are state schemes and so a state-by-state analysis is necessary; • The equity of such variability between State arrangements is questionable given the similar physical and psychological consequences across State lines for people impacted in such an attack. • The State schemes are post-funded and the States have indicated they are content to carry these exposures.	**Inconsistent cover** between states for victims of terrorism with different levels of compensation. **Type II** gap exists as the state cannot reinsure the risk with ARPC.

Table 5: Analysis. The State schemes are post-funded and the States have indicated they are content to carry these exposures.Victims of Crime schemes (see Appendix 3 for further details)

State	Summary
Victoria	• Victims covered • State holds financial responsibility
NSW	• Far lower compensation available than other jurisdictions • State holds financial responsibility but less risk than other states due to lower caps
Queensland	• Victims covered • State holds financial responsibility
South Australia	• Victims covered • State holds financial responsibility
Western Australia	• Victims covered • Possibly greater risk due to high cap for all victims
Tasmania	• Lower compensation available than other jurisdictions • State holds financial responsibility but less risk than other states due to lower caps
ACT	• Lower compensation available than other jurisdictions • Territory holds financial responsibility; less risk than other states due to lower cap/restricted eligibility
Northern Territory	• Lower compensation available than other jurisdictions • Territory holds financial responsibility; less risk than other states due to lower cap/restricted eligibility

Appendix 3 – Summary tables

Workers’ Compensation (WC) schemes – State by State

State	DTI coverage and terms	Conclusions
Victoria[28]	Workers are likely covered but arrangement unclear	Victoria likely carries uninsured risk; possible gap
NSW[29]	Covers workers; insurers are reinsured by a state fund above a threshold total loss	NSW takes the risk but is compensated, therefore no gap
Queensland[30]	Likely to have a dependence claim and “Nervous Shock” claim[31]; civil claims may also be applicable (not excluded)	Compensation available to victims at little risk to state; no gap
South Australia[32]	Does not exclude terrorism; payout to victims likely but it remains unclear as cover for terrorism is not specifically referred to	South Australia likely exposed without ability to reinsure; gap
Western Australia[33]	Insurers sometimes allowed to exclude terrorism; partial coverage	Unclear the extent of coverage, so potentially a partial gap
Tasmania[34]	Minister may declare an event to be a terrorist event; a public “Nominal Insurer” which may limit state exposure pays compensation instead of employer	Tasmania has built-for-purpose body with mechanism to protect state; no gap
ACT[35]	Addressed with a public reinsurance fund; insurers are required to obtain reimbursement for terrorist attacks	Risk is reinsured; no gap
Northern Territory[36]	Seems to cover terrorism; no explicit exclusion, remains unclear	NT potentially has exposure and isn’t reinsured; potential gap

Victims of Crime schemes – State by State

State	Compensation offered	ARPC conclusions
Victoria[37]	Cap on payment to primary victim = $60k Cap on payment to secondary victim = $50k Cap on payment to related victims = $50k Max per death = $100k	Victims covered, risk not reinsurable
NSW[38]	Cap on the package of benefits = $5k Cap on funeral costs = $9,500k Cap on assist. for economic loss = $30k Cap on ‘recognition’ payment = $15k	Far lower compensation available than other jurisdictions; risk not insurable but lesser than other states due to lower caps

State	Compensation offered	ARPC conclusions
Queensland[39]	Cap on payment to primary victim = $75k Cap on payment to secondary victim = $50k Cap on payment to related victims = $10k	Victims covered, risk not reinsurable
South Australia[40]	Cap on non-financial loss comp. = $100k Cap on financial loss comp. = $2k + 75% of excess of first $2k lost, capped at $100k	Victims covered, risk not reinsurable
Western Australia[41]	Cap on payment to victim = $75k Cap of $150k if a number of offences committed by the same offender	Higher compensation available. Victims covered, risk not reinsurable, possibly greater risk due to high cap for all victims (depends on practical application of this scheme)
Tasmania[42]	Cap on payment to primary victim = $30k Cap on payment to secondary victim = $20k Cap on payment to relation = $10k (limit on multiple related claims = $50k)	Lower compensation available than other jurisdictions; risk not insurable but lesser than other states due to lower caps
ACT[43]	Cap on payment to primary victim = $50k Cap on payment to primary victim for a non-physical offence = $10k	Lower compensation available than other jurisdictions; risk not insurable but lesser than other states due to lower cap and restricted eligibility. Separate payments are provided to homicide victims and witnesses.
Northern Territory[44]	Cap on payment to victim of violent crime = $40k Cap on payment for financial loss = $10k Cap on payment to witness of violent crime = $40k for injury, $10k for financial loss	Lower compensation available than other jurisdictions; risk not insurable but lesser than other states due to lower cap and restricted eligibility

Compulsory Third-Party (CTP) schemes – State by State[45]

State	DTI coverage and terms	Conclusions
Victoria[46]	Does not exclude CTP coverage of damage/injury from acts of terrorism	Victoria is liable to pay claims, but cannot reinsure with ARPC due to exclusion in the Regulations; gap
NSW[47]	Excludes coverage of damage/injury from acts of terrorism	CTP does not pay out and so ARPC cannot reinsure; gap
Queensland[48]	Excludes coverage of damage/injury from acts of terrorism	CTP does not pay out and so ARPC cannot reinsure; gap

State	DTI coverage and terms	Conclusions
South Australia[49]	Excludes coverage of damage/injury from acts of terrorism	CTP does not pay out and so ARPC cannot reinsure; gap
Western Australia[50]	Excludes coverage of “catastrophic” damage/injury from acts of terrorism; otherwise included. Western Australia allows claims under the compulsory third party insurance scheme for personal harm caused directly by the driving of a motor vehicle in an act of terrorism.	CTP partially applies; for victims suffering “catastrophic” injury there is no CTP support; partial gap
Tasmania[51]	Excludes coverage of damage/injury from acts and threats of terrorism	CTP does not pay out and so ARPC cannot reinsure; gap
ACT[52]	Excludes coverage of damage/injury from acts of terrorism	CTP does not pay out and so ARPC cannot reinsure; gap
Northern Territory[53]	Excludes coverage of damage/injury from acts of terrorism	CTP does not pay out and so ARPC cannot reinsure; gap

Appendix 4 – Research process and methodology

Background

In 2017, ARPC began a research project with the aim of examining the extent of insurance coverage for losses attributable to acts of terrorism in Australia. FPL Advisory acted in a project management capacity to help organise the project and also conducted an 'alternative analysis' in parallel to ARPC's research. By approaching questions of insurance coverage from a first principles perspective that is not based on previous insurance industry experience, FPL was able to identify broad areas not previously considered in strategic reviews and refer them to subject matter experts for a technical analysis. Through this process, ARPC was able to analyse coverage in unorthodox areas such as victims of crime compensation and certain kinds of loss of attraction (which had previously not been on the agenda). In 2020, ARPC collaborated with the University of Queensland to produce the framework for evaluating the gaps identified, generate recommendations, and produce this report. The project has moved through four distinct phases:

1. Refining the scope

   The original intention of the Paper was to create a thought leadership piece for use as an aid to discussing with the states and territories how they can better protect themselves. As initial engagement with the states and territories showed, there was little appetite for change at the state level. This iteration of the Gaps Project has instead opened up a broader discussion regarding the operation of terrorism reinsurance in Australia, shining a light on some issues for further discussion with interested parties.

2. Initial exploration of potential issues

   Initially, there were two main options for the core of the Paper. The first was to develop a set of scenarios for potential DTIs and to analyse the likely current insurance response to each. The second was to examine the existing exclusions in the Regulations and consider which ones could be amended. After considering these alternate strategies, ARPC decided on the first approach as it takes a more holistic view of the current terrorism reinsurance environment and so more appropriately covers the realm of potential gaps in the insurance response. A list of potential scenarios was developed and worked through in several iterations to ensure a wide variety of likely insurance responses would come of them to ensure our analysis had adequate coverage.

3. Detailed exploration of identified issues

   Once the list of terrorist attack scenarios was approved by ARPC internal stakeholders, project managers from both ARPC and FPL delved into the background analysis already existing on the fields concerned with the scenarios. Overseas terrorism reinsurance schemes were examined and elements of them were compared to Australia's scheme, and terrorist attacks that have occurred in overseas jurisdictions were analysed from an Australian insurance viewpoint. A few areas were identified which have not received much attention in the Australian context, such as attacks involving the use of vehicles as weapons, or attacks where a large number of people are injured in a locality. This analysis provided much of the basis for subsequent focus on the mechanisms through which losses are insured.

4. Refinement and external engagement

   After the list of scenarios and likely insurance responses were narrowed down, ARPC and FPL project managers met to review the status of different areas of analysis. After this, ARPC began drawing in industry experts in these distinct areas to gain deeper insights into the extent and manner of coverage available in these areas. Through this process and benefiting from previous work done to uncover areas that have not been examined in this way, the subject matter of the Paper relating directly to insurance mechanisms was drafted. At this stage, ARPC also engaged with Professor Paula Jarzabkowski at University of Queensland, an expert in partnerships for addressing global protection gaps, to develop a framework for evaluating the gaps identified, and propose recommendations.

Methodology

Early in the piece, ARPC decided to keep the scope of the Paper focused squarely on a small number of carefully selected scenarios. This was because ARPC, in collaboration with Professor Jarzabkowski, aimed to produce specific recommendations to improve Australia's response to losses occurring from terrorism, rather than a more high-level or abstracted paper report that was less likely to produce actionable recommendations. As part of this approach and utilising the iterative methodology FPL brought to the Project, the following process was used to narrow down the field of inquiry dealt with by this Paper:

- An assessment of the current Exclusion list in the Schedule 1 of the Regulations was undertaken to identify how each exclusion may be dealt with elsewhere (for example Item 3 relating to sickness is dealt with through other means),
- The exclusion list was then filtered to identify those areas that there may be a gap (as in specifically excluded but not covered elsewhere), building on the assessment by Mike Stallworthy (General Manager, Insurance Audit) earlier in the year,
- Of those, the scheme interaction framework (which highlights the incidents and types of terrorism events) was overlaid, exploring how related losses related to will be dealt with currently,
- It was thought that this would have been likely to be heavily focussed on a state by state comparator as the particular exclusions are dealt with differently by state legislation (for example CTP etc) although many turned out to be nationally consistent,
- From that, we received a fair indication of what gaps exist and how they may be dealt with.

In particular, it was decided that the Paper would focus in on several areas like Workers' Compensation and Compulsory Third-Party schemes, requiring a state by state analysis to uncover current gaps in the response to losses from terrorism.

Once these areas of focus were decided upon, a few scenarios were eliminated, and the final list of DTI scenarios used in this Paper was decided on.

For most of the scenarios, there are a range of potential impacts of different kinds and on different actors; so as to not repeat sections, this Paper places the category of impact under the most relevant scenario. For example, a discussion of loss of attraction occurs under Scenario 1, but the same impacts may be applicable to other scenarios as well. This reflects the intention of the Paper's use of the scenarios as a tool for shining a light on impacts of unorthodox kinds of DTIs.

Footnotes

[1] Terrorism Insurance Act 2003 (https://www.legislation.gov.au/Details/C2018C00176)

[2] Pool Reinsurance Limited (Pool Re): https://poolre.co.uk

[3] Gestion de l'Assurance et de la Réassurance des risques Attentats et actes de Terrorisme (GAREAT): https://www.gareat.com/en/who-are-we/

[4] Extremus Versicherungs-AG (EXTREMUS): https://www.extremus.de/?jjj=1592556422622

[5] ARPC (2019), *Annual Report 2018-2019,* https://arpc.gov.au/wp-content/blogs.dir/3/files/2020/05/ARPC-Annual-Report-2018-2019-Final.pdf

[6] Jarzabkowski P, Chalkias K, Cacciatori E and Bednarek R (2018). *Between State and Market: Protection Gap Entities and Catastrophic Risk*. London: Cass Business School, City, University of London: https://www.paulajarzabkowski.com/downloads/

[7] OECD (2020), *Insurance Coverage for Cyber Terrorism in Australia*, www.oecd.org/finance/insurance/Insurance-Coverage-for-Cyber-Terrorism-in-Australia.htm

[8] ARPC (2019), *Annual Report 2018-2019,* https://arpc.gov.au/wp-content/blogs.dir/3/files/2020/05/ARPC-Annual-Report-2018-2019-Final.pdf

[9] ISR is also known as Property Insurance in other countries

[10] Lantern Insurance Advisers (2020), *What's the difference between an Industrial Special Risks policy and a Business Pack policy?,* https://lanterninsurance.com.au/resources/knowledge-base/whats-difference-industrial-special-risks-policy-business-pack-policy/

[11] OECD (2020), *Insurance Coverage for Cyber Terrorism in Australia*, www.oecd.org/finance/insurance/Insurance-Coverage-for-Cyber-Terrorism-in-Australia.htm; Insurance Advisernet (2019), *Property Insurance,* https://insuranceadviser.net/business-insurance/property-insurance; Lantern Insurance Advisers (2020), *What's the difference between an Industrial Special Risks policy and a Business Pack policy?,* https://lanterninsurance.com.au/resources/knowledge-base/whats-difference-industrial-special-risks-policy-business-pack-policy/

[12] Insurance Advisernet (2019), *Business Interruption Insurance,* https://insuranceadviser.net/business-insurance/business-interruption-insurance; Lantern Insurance Advisers (2020), *What's the difference between an Industrial Special Risks policy and a Business Pack policy?,* https://lanterninsurance.com.au/resources/knowledge-base/whats-difference-industrial-special-risks-policy-business-pack-policy/

[13] Insurance Council of Australia (2020), *Understand Insurance: Workers' Compensation,* http://understandinsurance.com.au/types-of-insurance/workers-compensation

[14] The Terrorism Insurance Regulations 2003 can be viewed at: https://www.legislation.gov.au/Details/F2020C00124

[15] ARPC (2020), *Media Fact Sheet,* https://arpc.gov.au/publications/media-fact-sheet/

[16] OECD (2020), *Insurance Coverage for Cyber Terrorism in Australia*, www.oecd.org/finance/insurance/Insurance-Coverage-for-Cyber-Terrorism-in-Australia.htm

[17] ibid

[18] ibid

[19] OECD (2020), *Insurance Coverage for Cyber Terrorism in Australia*, www.oecd.org/finance/insurance/Insurance-Coverage-for-Cyber-Terrorism-in-Australia.htm

[20] OECD (2020), *Insurance Coverage for Cyber Terrorism in Australia*, www.oecd.org/finance/insurance/Insurance-Coverage-for-Cyber-Terrorism-in-Australia.htm

[21] Insurance Advisernet (2019), *Business Interruption Insurance,* https://insuranceadviser.net/business-insurance/business-interruption-insurance

[22] European Commission Ernst & Young Report (2014). Study on (co)reinsurance pools and on ad-hoc (co)reinsurance agreements on the subscription market. https://ec.europa.eu/competition/sectors/financial_services/KD0414707ENN.pdf

[23] Insurance Council of Australia (2015). *2015 Non insurance in the small to medium sized enterprise sector,* https://www.insurancecouncil.com.au/issue-submissions/reports/2015-non-insurance-in-the-small-to-medium-size-enterprise-sector

[24] ABC News (2016), *Suspected Terrorist Attack Kills at Least 12 at Christmas Market in Berlin, I*https://abcnews.go.com/International/truck-drives-public-square-berlin-injuring-pedestrians/story?id=44287616

[25] Roy Morgan (2019), *Declining importance of private health insurance to fund members,* http://www.roymorgan.com/findings/7908-private-health-insurance-201903220158

[26] Fonds de Garantie des Victims, https://www.fondsdegarantie.fr/en/home-2/

[27] As per Criminal Code Act 1995, a terrorist act "means an action or threat of action where: (a) the action falls within subsection (2) and does not fall within subsection (3); and (b) the action is done or the threat is made with the intention of advancing a political, religious or ideological cause; and (c) the action is done or the threat is made with the intention of: (i) coercing, or influencing by intimidation, the government of the Commonwealth or a State, Territory or foreign country, or of part of a State, Territory or foreign country; or (ii) intimidating the public or a section of the public." https://www.legislation.gov.au/Details/C2020C00120

[28] http://www.legislation.vic.gov.au/Domino/Web_Notes/LDMS/PubStatbook.nsf/51dea49770555ea6ca256da4001b90cd/3629925065cdb2a6ca257c210015979b/$FILE/13-067abookmarked.pdf

[29] https://www.legislation.nsw.gov.au/inforce/6967ac98-632d-c3a0-81b8-f6cba965a6ab/1987-70.pdf

[30] https://www.legislation.qld.gov.au/view/html/inforce/current/act-2003-027

[31] https://www.thepersonalinjurylawyers.com.au/faqs-do-victims-of-terrorism-have-a-right-to-claim-injury-compensation/

[32] https://www.legislation.sa.gov.au/LZ/C/A/WORKERS%20REHABILITATION%20AND%20COMPENSATION%20ACT%201986/2015.06.30/1986.124.UN.PDF

[33] https://www.slp.wa.gov.au/statutes/swans.nsf/5d62daee56e9e4b348256ebd0012c422/737198f00849324e48256b3500185c74/$FILE/Workers%20Compensation%20and%20Injury%20Management%20(Acts%20of%20Terrorism)%20Act%202001.PDF

[34] http://www5.austlii.edu.au/au/legis/tas/consol_act/wraca1988400/s131c.html

[35] https://www.legislation.act.gov.au/a/1951-2/current/pdf/1951-2.pdf

[36] https://legislation.nt.gov.au/en/Legislation/RETURN-TO-WORK-ACT-1986

[37] https://www.victimsofcrime.vic.gov.au/going-to-court/compensation-and-financial-assistance

[38] http://www.victimsservices.justice.nsw.gov.au/Documents/bk19_vss-guide-details.pdf

[39] https://www.qld.gov.au/law/crime-and-police/victims-and-witnesses-of-crime/financial-assistance/victims-categories

[40] https://www.legislation.sa.gov.au/LZ/C/A/VICTIMS%20OF%20CRIME%20ACT%202001/CURRENT/2001.58.AUTH.PDF

[41] http://www.courts.dotag.wa.gov.au/C/compensation.aspx?uid=1894-2822-6966-4703

[42] http://www.justice.tas.gov.au/victims/financialassistance/awards_and_payments

[43] https://www.victimsupport.act.gov.au/financial-assistance-scheme/new-financial-assistance-scheme-1-july-2016/frequently-asked-questions

[44] https://legislation.nt.gov.au/en/Legislation/VICTIMS-OF-CRIME-ASSISTANCE-ACT-2006

[45] https://www.thepersonalinjurylawyers.com.au/faqs-do-victims-of-terrorism-have-a-right-to-claim-injury-compensation/

[46] https://treasury.gov.au/sites/default/files/2019-03/Document-2-7-1.pdf

[47] https://www.legislation.nsw.gov.au/inforce/b11aa4c4-1420-c25e-ad1e-9cb036ae4b9e/1999-41.pdf

[48] http://www8.austlii.edu.au/cgi-bin/viewdoc/au/legis/qld/consol_act/maia1994243/s5.html

[49] http://insurancenews.com.au/local/sa-excludes-terrorist-acts-from-third-party-cover

[50] https://www.icwa.wa.gov.au/data/assets/pdf_file/0030/97851/Insurance-Commission-Annual-Report-2019_hi-res.pdf

[51] https://www.legislation.tas.gov.au/view/whole/html/inforce/current/act-1973-071

[52] https://legislation.act.gov.au/DownloadFile/a/2008-1/20181023-69836/PDF/2008-1.PDF

[53] https://legislation.nt.gov.au/en/Legislation/MOTOR-ACCIDENTS-COMPENSATION-ACT-1979