

The World of Terrorism Risk Insurance

How Australia Shapes Up

The Australian terrorism reinsurance scheme, administered by the Australian Reinsurance Pool Corporation (ARPC) under the *Terrorism Insurance Act 2003* (TI Act), is designed to cover property damage, business interruption and liability losses associated with a terrorism event causing damage to construction sites, commercial property and tangible contents in Australia. The ARPC scheme, supported by a guarantee from the Commonwealth Government of Australia, was established following the 2001 terrorist attacks in the U.S. and the resulting failure in the private insurance market to be able to provide terrorism insurance coverage in its own right.

A number of other countries have established similar schemes to support the private market with a Government backstop for catastrophic terrorism losses, while in other jurisdictions exposures are typically excluded from coverage by the private market. The TI Act provides for the override of any terrorism exclusions in insurance policies written in the Australian market, subject to the declaration of a terrorist incident by the Treasurer of Australia.

Is Australia at risk?

The current terrorism threat level in Australia is currently classified by the Australian National Security department of the Australian Government as 'Probable', being the third highest level on a scale of 5 on the National Terrorism Threat Advisory System.

The ARPC scheme has been utilised on only one occasion since its inception in respect of business interruption losses associated with the Sydney Lindt Café siege in 2014.

In addition to the devastating impact of such events on human lives, terrorism related activities also have the potential to cause material financial losses in the order of billions of dollars to the Australian community as well as the insurance industry. For example, a blast attack in Melbourne or Sydney could result in losses of over \$8 billion, while an attack involving the use of a biological agent could result in losses of over A\$30 billion. While terrorism losses could exceed \$8 billion in the event of a blast attack in Melbourne or Sydney,

the private insurance market is well protected with an aggregate industry retention of A\$100 million before losses are transferred to the terrorism reinsurance pool.

Following the most recent triennial review of the ARPC, with the report being released in December 2018, the Government is not expected to make any major changes to the existing terrorism reinsurance pool arrangements over the short-medium term. As part of the prior review in 2015, changes to the industry retention levels were under consideration which could have had an adverse impact on the financial positions of Australian insurance companies. No such recommendations have been made in the 2018 report. There are some longer-term opportunities for the scope of the terrorism reinsurance pool to be extended to cover emerging terrorism risk exposures, such as cyber-terrorism attacks, though no changes have been recommended at the current time.

Maturity of the Terrorism Pool Arrangements in Australia

The ARPC scheme is reasonably mature in respect of the coverage of property damage and business interruption (PDBI) losses associated with conventional terrorist attacks. As shown in Table 1 in Appendix A, the coverage of the ARPC scheme is broadly comparable to that of the majority of major international peer schemes. The schemes included in Table 1 are those that are monitored by the OECD to evaluate developments in national terrorism risk insurance programs across OECD countries.

There are, however, potential opportunities for expansion of the ARPC to cover additional sources of losses from non-traditional terrorist attacks, including: the use of chemical, biological, nuclear and radiological (CBNR) materials; and cyber terrorism, which may be defined as “the use of cyber capabilities to conduct enabling, disruptive, and destructive militant operations in cyberspace to create and exploit fear through violence or the threat of violence”¹.

Tables 2 and 3 in Appendix A demonstrate how the coverage of the ARPC scheme is broadly comparable to that of selected major international terrorism insurance schemes in respect of CBNR terrorism risks.

Large Scale Terrorist Blast Event in Sydney or Melbourne

Geoscience Australia (GA) is an Australian Federal Government agency that is engaged to assist the ARPC in estimating gross losses that may be experienced due to blasts in larger Australian cities. GA modeling indicates exposures associated with a large-scale terrorist blast event (i.e. 500-3000 kg charge size) could be

¹ *Defining Cyberterrorism: Capturing a broad range of activities in cyberspace*, CTC Sentinel Journal, Combating Terrorism Centre at West Point, Brickey, J., Aug. 2014.

considerable, with estimated insured losses of A\$8.6 billion in Sydney or A\$8.2 billion in Melbourne for a 3,000 kg charge².

Probabilities have not been specifically assigned as part of the GA research, with the modeled scenarios being assumed to be possible but low probability events. The assignment of specific probabilities is made difficult by the lack of historical data available (in comparison to natural catastrophes) and other attributes of terrorism risk (e.g. psychological and social factors).

Notwithstanding the substantial potential losses noted above, Australian commercial property insurers are well protected, relative to APRA regulatory capital surplus measures and ratings agency capital requirements, by the A\$10 million maximum retention that applies to all individual insurers reinsured via the ARPC scheme. An aggregate industry retention of A\$100 million also applies, as per the ARPC scheme structure detailed in Table 4 in Appendix A.

What could insurers be liable for without the ARPC?

Key players in the commercial insurance sector could be liable for exposures in the order of A\$0.8–2.9 billion in the event that they ceased their coverage through the scheme, as per ARPC estimates¹.

Under the ARPC scheme, there is no coverage for terrorism incidents associated with acts of war, events involving aircraft, or exposures under life and health insurance policies, including group life insurance policies made available via superannuation funds. In such scenarios, the associated exclusions within the primary insurance policies would not be overridden by the declaration of a terrorist incident under the terms of the TI Act. The significant losses that could be experienced by the Australian economy would need to be dealt with under separate arrangements by the Commonwealth Government, such as post event compensation and economic recovery schemes.

Chemical, Biological, Nuclear and Radiological (CBNR) Events

Chemical and biological attacks are covered under the ARPC scheme, where there is property damaged involved (depending on the nature of the agent and delivery mechanism used), and business interruption and liability losses are triggered under commercial/business package covers.

GA has completed some modeling on the impact of CBNR incidents, but the detailed results have not been made public due to the sensitive nature of the information. However, the ARPC has estimated the gross

² A Blast Loss Estimation Capability for the Australian Government, 2016, Geoscience Australia, Australian Government, Record 2016/22, eCat 101902, www.ga.gov.au, Dale, K. W., Edwards, M. R., and Kay, R. D.

losses of an event involving the use of a biological agent in a central business district location as being in the order of A\$30 billion³.

An event of this scale would exceed the capacity of the ARPC scheme, including the associated A\$10 billion government guarantee. The surplus losses incurred above the government guarantee would fall back to the underlying insured rather than the primary insurance company. There is a potential opportunity for insurers to underwrite excess coverage for potential losses exceeding the government backstop, however this does not appear to have been explored by the industry to date and the appetite for such cover amongst relevant corporate groups is unknown.

Nuclear and radiological events have been excluded in the ARPC scheme. Significant losses could be sustained by the Australian economy in this respect, which would need to be dealt with under separate arrangements by the Commonwealth Government. However, there is minimal use of nuclear energy facilities in Australia and the war exclusion would apply in respect of state actors.

Cyber Terrorism

There have been no known successful cyber-attacks attributed to terrorist activities to date. However, this is considered by market participants to be feasible over the medium term, particularly in the U.S. “ISIS [Islamic State of Iraq and Syria] is ‘waking up’ to the idea of using sophisticated malware to cyber-attack critical infrastructure in the U.S.”⁴. Other jurisdictions are not immune to such risks.

Is Australia at risk for cyber terrorism?

“Australia remains susceptible to the threat of cyber terrorist attacks and as terrorist organizations become more tech-savvy, the risk of a cyber-attack on the country become more likely. Some terrorist groups are very well resourced and it is an absolute possibility that they could create significant troubles for national security or economic prosperity”¹.

Potential losses from cyber terrorism attacks may include: business interruption due to denial of service (DoS) and loss of consumer confidence, material property damage and bodily injury due to cyber attack; data/systems damage due to cyber attack; and contingent business interruption stemming from a critical infrastructure/supply chain event (i.e. utility outage). Likewise, material losses can arise from third party risk including shareholder claims.

³ Actuaries Institute General Insurance Seminar 2014 materials, *Terrorism Risk Insurance in Australia*, ARPC, Dr Christopher Wallace, Michael Pennell and Norris Robertson, Nov. 2014.

⁴ James Comey, Federal Bureau of Investigations (FBI) Director, May 2015.

Is any cover available for cyber terrorism risk?

There is essentially no coverage being provided for cyber terrorism losses by the Australian primary insurance sector at present, given the nature of cyber security policies, cyber extensions under other insurance policy types, and the associated exclusions.

Commercial property damage policies (e.g. Mark IV and V industrial special risk policies for large enterprises, business package products for small-medium enterprises, etc.) are typically subject to exclusions for losses caused by cyber-attack, but may be extended to cover the risk of malicious external access to information systems by policy endorsement.

Cyber security policies provide coverage to corporate insurers in respect of the direct and indirect losses arising from a cyber security breach. Direct losses can include: incident response costs, information asset losses, regulatory fines and remediation costs, cyber extortion expenses and loss of income from business interruption. Indirect losses can include: data privacy liabilities, media liabilities and network security liabilities. Cyber security policies typically include a standard exclusion for losses attributable to terrorist activities.

Further, cyber security policies and cyber extensions to other policy types do not generally contemplate the potential for damages to physical property as a result of cyber-attack. “Even if insurers were to include cyber-attack coverage for physical property, the ARPC ... does not provide reinsurance cover for this type of attack [cyber terrorism] as it would be considered computer crime under the Australian Criminal Code”⁵. Losses caused by computer crime are excluded from coverage of the ARPC scheme under the *Terrorism Insurance Regulations 2003* (Regulations).

There could however be some potential overlap with the ARPC scheme where a terrorist attack occurred, but cyber-attack was not considered to be the primary cause of PDBI losses (e.g. conventional terrorist bombing attack subsequent to cyber terrorism attack) and the event was not deemed to be caused by computer crime.

Table 5 in Appendix A provides further detail on the level of cyber insurance cover ordinarily provided under various insurance policy types.

Given the limitations in coverage under the ARPC scheme and the private insurance market at present, significant losses could be sustained by the Australian economy in respect of any cyber terrorism events, which would need to be separately borne by the Commonwealth Government.

⁵ *Cyber Terrorism And Australia's Terrorism Insurance Scheme – Physically Destructive Cyber Terrorism Is A Gap In Current Insurance Coverage*, www.arpc.gov.au, ARPC, Mar. 26.

There have been no studies released in relation to the potential costs of a cyber terrorism event in Australia. Lloyds and the University of Cambridge's Center for Risk Studies have estimated the cost of a 1 in 200 year event involving a cyber-attack on the US power grid as ranging between US\$21.4 billion and US\$71.1 billion, with the majority of losses incurred in respect of commercial insurance lines (www.lloyds.com/businessblackout, Jul.15.).

The ARPC has highlighted the need for consideration to be given by the Commonwealth Government to extending the ARPC scheme to cover cyber terrorism losses as an emerging risk area. Such an extension could make more effective use of the existing ARPC scheme arrangements and provide a greater level of certainty to the insurance and corporate markets in Australia in respect of potential cyber-terrorism attacks in the future.

Concluding Remarks

The Australian terrorism risk insurance scheme is currently well placed relative to its international peers to manage the commercial exposures associated with a potential large-scale terrorism event.

However, the arrangements in Australia, along with those in all other jurisdictions, will need to continue to evolve in line with emerging terrorism risks in the future.

Contact Details

www.halladvisory.com

Melbourne: +61 3 9653 6493 | Level 27, 101 Collins Street, Melbourne

Sydney: +61 2 8035 4400 | Level 36, Gateway, 1 Macquarie Place, Sydney

Singapore: +65 6679 6146 | Level 24, Capita Green, 148 Market Street, Singapore



Appendix A: Comparative Tables

Table 1: Terrorism Program Insurance Cover For (Conventional) Terrorist Attacks – Selected Countries⁶

| | Property Damage | Business Interruption | Data/Systems Reinstatement | Bodily Injury | Liability |
|--|-----------------|-----------------------|----------------------------|---------------|-----------|
| Australia - ARPC | ✓ | ✓ | ?* | ?** | ✓ |
| Austria – Österreichischer Versicherungspool zur Deckung von Terrorisiken | ✓ | ✓* | ✓ | ✗ | ✗ |
| Belgium – Terrorism Reinsurance and Insurance Pool (TRIP Belgium) | ✓ | ✓ | ✓ | ✓ | ✓ |
| Denmark – Terrorism Insurance Pool for Non-Life Insurance (TIPNLI) | ✓^ | ✓^ | ✓^ | ✗ | ✗ |
| France – Gestion de l'Assurance et de la Reassurance des Risques Attentats et Actes de Terrorisme (GAREAT) and Caisse Centrale de Reassurance (CCR) | ✓ | ✓ | ?* | ✗^^ | ✗ |
| Germany – Extremus Versicherungs-AG | ✓ | ✓ | ?* | ✗ | ✗ |
| India – Indian Market Terrorism Risk Insurance Pool | ✓ | ✗ | ✗ | ✗ | ✗ |
| Israel – Compensation Fund according to the Israeli <i>Property Tax Act</i> | ✓ | ✓ | ?* | ✗^^^ | ✗ |
| Netherlands – Nederlandse Herverzekeringsmaatschappij voor Terrorismeschaden N.V. (NHT) | ✓ | ✓ | ✓ | ✓ | ✓ |
| Russia – The Russian Anti Terrorism Insurance Pool (RATIP) | ✓ | ✓ | ✓ | ✗ | ✓ |
| Spain – Consorcio de Compensacion de Seguros (CCS) | ✓ | ✓ | ✓ | ✓ | ✗> |
| UK – Pool Reinsurance Company Ltd. (Pool Re) | ✓ | ✓ | ?>> | ✗ | ✗ |
| US – Terrorism Risk Insurance Program (TRIP) | ✓ | ✓ | ?>>> | ?>> | ✓ |

* Material damage to tangible assets (e.g. equipment, such as servers and automated data processing systems) may be covered but not damages to intangible assets such as data or software. In respect of Israel, intangible assets are similarly not covered, but the Finance Minister can determine which type of assets can be covered under the *Property Tax Act*.

** Bodily injury covered under the liability policies of an owner or occupier of eligible property with terrorism insurance coverage would be eligible for coverage by ARPC. Life and health insurance lines are not eligible for ARPC coverage.

*** Arising from direct consequential property damage only.

^ Where losses caused by a nuclear, biological, chemical and radioactive (NBCR) terrorist attack.

^^ Bodily injury is separately covered by the Fonds de Garantie des victimes des actes de Terrorisme et autres Infractions (FGTI). It is not included in the GAREAT + CCR.

^^^ Bodily injury is separately covered under the National Insurance system and the *Compensation for Victims of Hostilities Act*.

> Except for compulsory third party motor liability, for which CCS coverage was introduced in 2016.

⁶ Primary Source: Adapted from ARPC-OECD Global Terrorism Risk Insurance Conference 2016 materials; *The Coverage of Cyber-Terrorism Insurance Programmes*; Leigh Wolfom (Policy Analyst, Director for Financial and Enterprise Affairs, OCED).
Secondary Source: OECD International Platform on Terrorism Risk Insurance, <http://www.oecd.org/daf/fin/insurance/terrorism-risk-insurance-programmes.htm>

>> Bodily injury covered under liability policies with terrorism insurance coverage or under workers' compensation policies would be eligible for coverage. Life and health insurance lines are not eligible for coverage.

>>> When covered by an eligible underlying policy.

Table 2: Terrorism Program Insurance Cover For Chemical, Biological, Nuclear and Radiological (CBNR) Terrorist Attacks – Selected Countries⁷

| | Material Damage – Nuclear and Radiological (NR) Event | Material Damage to Nuclear Plants | Material Damage – Chemical and Biological (CB) Event | Bodily Injury – CBNR Event |
|--------------------|--|--|---|-----------------------------------|
| Australia | X | X | ✓ | ?* |
| Austria | ✓ | ✓ | X | X |
| Belgium | ✓** | X | ✓ | ✓ |
| Denmark | ✓ | ✓ | ✓ | X |
| France | ✓*** | ✓*** | ✓ | X^ |
| Germany | X | X | X | X |
| India | X | X | X | X |
| Israel | ✓^^ | ✓^^ | ✓^^ | ✓^^^ |
| Netherlands | ✓ | ✓ | ✓ | ✓ |
| Russia | X | X | X | X |
| Spain | ✓ | ✓ | ✓ | ✓ |
| UK | ✓ | ✓ | ✓ | X |
| US | ✓ | ✓ | ✓ | X |

* Bodily injury covered under the liability policies of an owner or occupier of eligible property with terrorism insurance coverage would be eligible for coverage by ARPC. Life and health insurance lines are not eligible for ARPC coverage.

** Losses caused by nuclear bombs can be specifically excluded from coverage. There does not appear to be any provision for the exclusion of losses caused by radiological weapons (i.e. radiological dispersal devices or 'dirty bombs').

*** Losses caused by nuclear arms are excluded, but losses caused by radiological weapons are covered.

^ Bodily injury is separately covered by the FGTL. It is not included in the GAREAT + CCR.

^^ The *Property Tax Act* covers hostile actions (including terrorism) but does not define these terms. Coverage is assumed as no explicit exclusion of CBNR related terrorism events.

^^^ Bodily injury is separately covered under the National Insurance system and the *Compensation for Victims of Hostilities Act*.

² *Defining Cyberterrorism: Capturing a broad range of activities in cyberspace*, CTC Sentinel Journal, Combating Terrorism Centre at West Point, Brickey, J., Aug. 2014.

⁷ Primary Source: Adapted from ARPC-OECD Global Terrorism Risk Insurance Conference 2016 materials; *Interconnections between Terrorism Pools and Nuclear Pools*; Elisabeth Rousseau (Secretary General, GAREAT), Francois Vilnet (Vice Chairman, GAREAT), Oct. 2016.

Secondary Sources: OECD International Platform on Terrorism Risk Insurance, <http://www.oecd.org/daf/fin/insurance/terrorism-risk-insurance-programmes.htm>, 2019.

Table 3: Terrorism Program Insurance Cover For Cyber-Terrorist Attacks – Selected Countries⁸

| | Business Interruption due to Denial of Service | Material Damage due to Cyber Attack | Data/Systems Damage due to Cyber Attack | Contingent Business Interruption due to Utility Outage | Bodily Injury due to Cyber Attack |
|--------------------|---|--|--|---|--|
| Australia | X | X | X | X | X |
| Austria | X | ✓ | X | X | X |
| Belgium | X | ✓ | ✓ | X | ✓ |
| Denmark | X | X | X | X | X |
| France | X | ✓ | ?* | X | X** |
| Germany | X | X | X | X | X |
| India | X | X | X | X | X |
| Israel | X | ✓*** | ?* | X | X^ |
| Netherlands | X | ✓ | X | X | X |
| Russia | X | X | X | X | X |
| Spain | ?^^ | ✓ | ?^^ | X^^ | ✓ |
| UK | X | X | X | X | X |
| US | ?> | ?> | ?> | ?> | ?>> |

* Material damage to tangible assets (e.g. equipment, such as servers and automated data processing systems) would be covered but not damages to intangible assets such as data or software. In respect of Israel, intangible assets are similarly not covered, but the Finance Minister can determine which type of assets can be covered under the *Property Tax Act*.

** Bodily injury is separately covered by the FGTI. It is not included in the GAREAT + CCR.

*** The *Property Tax Act* covers hostile actions (including terrorism) but does not define these terms. Coverage is assumed as no explicit exclusion of computer crime or cyber related terrorism events.

^ Bodily injury is separately covered under the National Insurance system and the *Compensation for Victims of Hostilities Act*.

^^ Business interruption is only indemnified by the terrorism scheme where the underlying policy includes business interruption cover and provided that the business interruption losses arise from direct material damage on properties insured. Losses as a result of the disruption or cutting off of the external supply of electrical power, combustible gasses, fuel oil, diesel oil or other fluids are excluded. Data and systems losses are excluded if they are consequential losses.

> When covered by an underlying eligible policy. The US terrorism scheme technically covers cyber terrorism but attribution is difficult to prove and thus may not be covered in practice. TRIA would apply to cyber liability policies that cover the type of damage addressed by the federal terrorism reinsurance backstop.

>> Bodily injury covered under liability policies with terrorism insurance coverage or under workers' compensation policies would be eligible for coverage. Life and health insurance lines are not eligible for coverage.

⁸ Primary Source: Adapted from ARPC-OECD Global Terrorism Risk Insurance Conference 2016 materials; *The Coverage of Cyber-Terrorism by Terrorism Insurance Programmes*; Leigh Wolfrom (Policy Analyst, Director for Financial and Enterprise Affairs, OECD).
Secondary Sources: OECD International Platform on Terrorism Risk Insurance, <http://www.oecd.org/daf/fin/insurance/terrorism-risk-insurance-programmes.htm>, 2019.

Table 4: ARPC Terrorism Risk Insurance Scheme Structure

| | Underwriter | Limit |
|----------------|---|------------------|
| Layer 6 | Policyholder exposure | Unlimited |
| Layer 5 | Commonwealth Government guarantee | A\$10 billion |
| Layer 4 | Highly diversified retrocession program | A\$3.065 billion |
| Layer 3 | ARPC retention | A\$285 million |
| Layer 2 | Aggregate industry retention | A\$100 million |
| Layer 1 | Policyholder exposure | A\$100,000 |

Table 5: Cyber Insurance Cover in Australia⁹

| | Insurance Policy Type | | | | | | |
|---|------------------------------|------------------------------|---------------------------------|---|---|--------------|---------------------------|
| | Property Damage | General Liability | Management Liability | Professional Indemnity / Directors & Officers' Liability | Information Technology Liability | Crime | Cyber Security |
| First Party Loss | | | | | | | |
| Incident Response | X | X | X | X | X | ?* | ✓ |
| Information Asset Loss | X | X | X | X | X | ?* | ✓ |
| Regulatory | X | X | ✓ | X | X | ?* | ✓ |
| Cyber Extortion Expenses | X | X | X | X | X | ?* | ✓ |
| Loss of Income | X | X | X | X | X | ?* | ?* |
| Third Party Loss | | | | | | | |
| Data Privacy Liability | X | X | ?* | ?* | ?* | X | ✓ |
| Media Liability | X | ?* | ?* | ?* | ?* | X | ✓ |
| Network Security Liability | X | X | X | X | ?* | X | ✓ |

* Uncertain or varied cover.

⁹ Adapted from Actuaries Institute General Insurance Seminar 2016 materials; *Insuring Cyber Risk – Concerns About Coverage*; Peter Yeates (Associate Director, Ernst & Young) and Dean Marcus (Actuary, Taylor Fry), Nov.16.