Australian Government

Australian Reinsurance Pool Corporation

CYBER TERRORISM AND AUSTRALIA'S TERRORISM INSURANCE SCHEME

PHYSICALLY DESTRUCTIVE CYBER TERRORISM IS A GAP IN CURRENT INSURANCE COVERAGE

ARPC, March 2016

Australian Government
Australian Reinsurance Pool Corporation

17 March 2016

Introduction

This paper presents a discussion on cyber terrorism and its impact on commercial infrastructure and property and issues for insurance coverage.

This paper is provided for discussion purposes and should not be relied upon for making commercial decisions.

Should you have any questions or require further information please do not hesitate to contact ARPC.

Yours sincerely,

Dr Christopher Wallace
Chief Executive Officer

Correspondence to: PO Box Q1432 Queen Victoria Building NSW 1230
T +61 2 8223 6777 | **F** +61 2 9241 1887 | **E** enquiries@arpc.gov.au
www.arpc.gov.au | ABN 74807136872

Executive Summary

This paper seeks to define “cyber terrorism” and highlights various examples. The paper outlines the coverage provided by conventional property insurance policies in Australia and the emerging market for cyber insurance.

It also analyses how the *Terrorism Insurance Act 2003* (TI Act) and the reinsurance scheme administered by the Australian Reinsurance Pool Corporation (ARPC), responds to property damage and business interruption arising from terrorism.

This analysis proposes that “cyber terrorism” is currently not covered by Australia’s terrorism insurance scheme because it is defined as a computer crime which is currently excluded by the TI Act. Standard cyber insurance policies also exclude losses from terrorist activities meaning there is no cyber cover provided by the commercial market or via the TI Act for cyber losses from terrorist activities.

The paper concludes there is a gap in the property insurance market in situations where a cyber-attack, by terrorists (or indeed others), may inflict major physical damage by primarily cyber means. Even if insurers were to include cyber-attack coverage for physical property, the ARPC scheme does not provide reinsurance cover for this type of attack as it would be considered computer crime under the Australian Criminal Code.

Contents

1. Synopsis

In her address to the Insurance Council of Australia on 4 March 2016, The Honourable Kelly O'Dwyer MP Minister for Small Business and Assistant Treasurer said that cyber terrorism is a significant risk for the insurance industry.

This paper seeks to define "cyber terrorism" and highlights various examples. Some types of cyber terrorism have the potential to damage Australian commercial property and/or infrastructure and therefore impact wider economic activity. The paper outlines the coverage provided by conventional property insurance policies in Australia and the emerging market for cyber insurance. It also analyses how the *Terrorism Insurance Act 2003* (TI Act) and the reinsurance scheme administered by the Australian Reinsurance Pool Corporation (ARPC), responds to property damage and business interruption arising from terrorism.

Cyber insurance is a relatively new product and it is expected that the industry will develop the product over time to ensure that loss exposure can be accurately quantified and adequate reinsurance is placed.

This analysis proposes that "cyber terrorism" is currently not covered by Australia's terrorism insurance scheme because it is defined as a computer crime which is currently excluded by the TI Act. However, the increase in incidents of cybercrime, and its growing sophistication mean there is the potential for it to physically damage commercial property and impact the wider economy. Therefore we believe that physically destructive cyber terrorism is a gap in current insurance coverage as provided by the TI Act.

2. Definition

What is cyber terrorism?

According to Major General Stephen Day[1], a significant cyber terrorist attack occurred in August 2013 when the websites of media companies such as the New York Times, the Huffington Post and Twitter were allegedly hacked by a Syrian group known as the Syrian Electronic Army. During that specific attack, users who clicked onto those respective websites were redirected to a server controlled by the Syrian group.

The November 2014 cyber attack on Sony Pictures by a hacker group which identified itself as "OurMine" initially released confidential information such as employees' names, addresses and salaries and also caused physical damage to a substantial number of computers. This was followed one month later by a demand to cancel a comedy film called *The Interview* to which Sony partially complied. Intelligence officials alleged that this cyber attack was state sponsored.

So, what constitutes an act of terrorism and what is the range of potential cyber terrorist activities?

In an article for the US-based *Combating Terrorism Centre (CTC) Sentinel* in August 2012, Jonalan Brickey[2] sets out a useful classification scheme titled "Clusters of cyber terrorism" as a "qualitative approximation" and it is represented in Figure 1.

[1] Australia at growing risk of cyber terrorism: cyber security head (News Ltd 17 Feb 2015).
[2] Jonalan Brickey, Defining Cyberterrorism: Capturing a broad range of activities in cyberspace, Combating Terrorism Centre at West Point, CTC Sentinel Journal, August 2014.

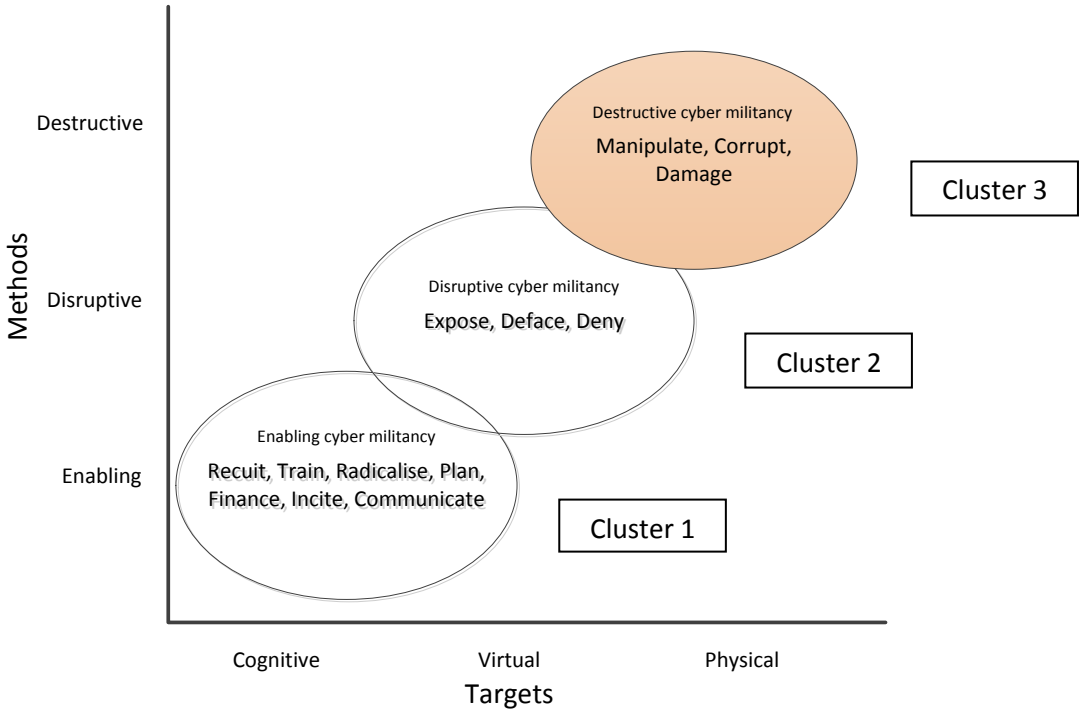


Figure 1: Clusters of cyber terrorism
(Defining Cyberterrorism: Capturing a broad range of Activities in Cyberspace, Jonalan Brickey, CTC Sentinel, August 2012, VOL 5, Issue 8)

Brickey sees terrorism targets as, "cognitive" (the minds of people), "virtual" (resources in cyberspace) and "physical" (the physical things connected with and via cyberspace). Terrorist methods to attack targets are seen as "enabling", "disruptive" and "destructive". Brickey references US Cyber Command which has reported on the evolution of cyber-attacks on US information networks which started as exploitative, moved onto disruptive and more recently, entered the realm of physically destructive.

Cluster 1:

The enabling/cognitive cluster contains activities such as use of email, social media, and YouTube. These activities aim to radicalise, recruit, train, incite and generally communicate and may or may not be legal.

Cluster 2:

Next in Brickey's scheme is the disruptive/virtual cluster. Activities in this cluster include denial of service type attacks, website defacement, unauthorised access and transactions, theft or disclosure of confidential or personal information.

Cluster 3:

Finally in Brickey's scheme is the destructive/physical cluster in which terrorists use cyber as a means to manipulate and corrupt information system functions in order to cause physical damage or destruction to physical targets.

Brickey's diagram focusses on terrorists as actors but he also makes the point that other actors such as nation states, organised criminals and general hackers may also carry out activities in the same clusters and these could be represented as different planes on another third dimensional axis.

He ultimately presents a definition of cyber terrorism 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 in the pursuit of political change*".

The Syrian Electronic Army attack on media outlets and twitter referred to by Major General Stephen Day would certainly fit into the disruptive/virtual cluster. Other media coverage of alleged cyber terrorism incidents to date would generally fit into either the enabling/cognitive or disruptive/virtual clusters. Technical ability and specialist resources represent a barrier in this area and media reports of destructive/physical cyber-attacks that have occurred have generally been carried out with sophisticated knowledge and significant resources suggesting backing by nation states. Russia, China, North Korea, the USA and Israel have all been attributed as the source of such attacks. The danger is that as the associated malware is distributed and more widely understood, terrorist technical experts may be able to employ similar techniques.

A major concern to governments worldwide, including the Australian Government, is the possibility that a terrorist group could develop the ability to carry out destructive physical attacks by cyber means.

The definition of terrorism in Australian law

Terrorism is defined in Australia in the *Criminal Code Amendment (Terrorism) Act 2003 (CCA Act)*, Section 100.1:

> **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.*
>
> *(2) Action falls within this subsection if it:*
>
> *(a) causes serious harm that is physical harm to a person; or*
>
> *(b) causes serious damage to property; or*
>
> *(c) causes a person's death; or*
>
> *(d) endangers a person's life, other than the life of the person taking the action; or*
>
> *(e) creates a serious risk to the health or safety of the public or a section of the public; or*
>
> *(f) seriously interferes with, seriously disrupts, or destroys, an electronic system including, but not limited to:*
>
> *(i) an information system; or*
>
> *(ii) a telecommunications system; or*
>
> *(iii) a financial system; or*
>
> *(iv) a system used for the delivery of essential government services; or*
>
> *(v) a system used for, or by, an essential public utility; or*
>
> *(vi) a system used for, or by, a transport system.*
>
> *(3) Action falls within this subsection if it:*
>
> *(a) is advocacy, protest, dissent or industrial action; and*

(b) is not intended:

(i) to cause serious harm that is physical harm to a person; or

(ii) to cause a person's death; or

(iii) to endanger the life of a person, other than the person taking the action; or

(iv) to create a serious risk to the health or safety of the public or a section of the public.

(4) In this Division:

(a) a reference to any person or property is a reference to any person or property wherever situated, within or outside Australia; and

(b) a reference to the public includes a reference to the public of a country other than Australia.

To be classed as terrorism, an action needs to cause harm or serious risk to people or serious damage to property or it may cause serious interference, disruption or destruction. In addition, the action can't be advocacy, protest or dissent where there was no intention to cause harm or risk or damage. The action must also be done with the intent of advancing a political, religious or ideological cause and the action must be done with the intent of coercing or influencing by intimidation a government, Federal, State or Territory or the general public or a foreign country. In Appendix 1, "Is an action terrorism?" shows a flowchart derived from the relevant section of the CCA Act.

Brickney's disruptive/virtual and destructive/physical clusters for terrorist actors would likely qualify as terrorism under Australian law as these attacks either cause disruption or damage to electronic systems or actual physical damage. The enabling/cognitive cluster activities by terrorists would probably not be classed as terrorism although they may still be criminal activities.

3. Background

"Australia at growing risk of cyber terrorism: cyber security head"

This was the headline of a February 2015 media article[3] featuring an interview with Major General Stephen Day, head of the Australian Government's new Cyber Security Centre (ACSC) established in November 2014.

In the article Major General Day stated that:

"Australia remains susceptible to the threat of cyber terrorist attacks and as terrorist organisations become more tech-savvy, the risk of a cyber-attack on the country becomes 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."

In a recent global survey[4], PwC estimated the annual global cost of cyber-attacks at between US$375 billion and US$575 billion. PwC stated that a true figure is ultimately unknowable as many attacks go unreported and costs such as the theft of secrets and intellectual property, are largely unquantifiable. The PwC survey reported a dramatic increase in security incidents detected between 2013 and 2014, with a dramatic 41% jump in Europe, 11% in North America and 5% in the Asia

[3] Australia at growing risk of cyber terrorism: cyber security head (News Ltd 17 Feb 2015).

[4] Managing cyber risks in an interconnected world: key findings from *The Global State of Information Security Survey, 2015*, PwC, www.pwc.com/gsiss2015.

Pacific. PwC also asked survey respondents to nominate the likely source of incidents. Current and former employees were the most commonly reported sources overall (30% of survey respondents). Hackers (25%), competitors (24%), organised crime (17%), activists/activist organisations/hacktivists (16%) and unknown sources (18%) had the highest reporting rates for external sources. Terrorists were reported by 10% of respondents as an external source of (at least one) attack, a two per cent increase compared to 2013. Unfortunately, the survey does not provide information on the frequency or percentage of incidents that respondents attribute to the various incident sources, including terrorism.

The PwC survey report also flagged increasing cyber risks in the form of major banking fraud and theft, major economic espionage and major identity and personal information theft. The report also identified the growing risk of major attacks on critical infrastructure including public utilities. This development is a particular area of concern to the property insurance market.

Ernst & Young's (EY) Global Information Security Survey 2014[5] contains similar trends but it concludes that external threats have now overtaken internal threats as the most likely source of cyber risks.

Evolution: Cyber attacks turn physical

The risk of catastrophic physical property and infrastructure losses has increased as the physical world and cyberspace become more interconnected. In a March 2015 report[6], the UK Government emphasised this issue, using an example where hackers compromised the electronic control system for a German steel mill and were then able to shut down a blast furnace resulting in "massive damage". This attack was reported in December 2014 by the German Federal Office for information Security (BSI).

In December 2014, Bloomberg[7] reported a previously secret 2008 cyber-attack on a Turkish crude oil pipeline which caused an explosion and major fire. Allegedly, Russian hackers had "shut down alarms, cut off communications and super-pressurized the crude oil in the line. The main weapon at valve station 30 on the 5th August 2008 was a keyboard."

The control systems for power and water utilities, industrial plants, pipelines and transportation networks are all potentially vulnerable to cyberattacks. Indeed, a 2014 Financial Times article reported that "sophisticated state-backed cyber adversaries employed powerful malware to infect the industrial control systems of hundreds of energy companies across the US and Europe".[8]

Awareness of the potential vulnerability of computer-controlled infrastructure was first raised significantly in 2010 with the discovery of the Stuxnet computer worm which was designed to attack programmable logic control units in an industrial plant and which was reportedly responsible for ruining around one fifth of Iran's nuclear centrifuges by causing them to spin out of control.

Actors such as governments, businesses and criminals are locked in a race as they seek to variously exploit, damage or protect resources in cyberspace. Included in the mix are terrorists who seek to exploit the opportunities of technology and cyberspace for their own agendas. Potentially, cyberspace offers the cyber terrorist advantages such as global reach, anonymity, remoteness from targets, access and control and media shock value.

[5] Get ahead of cybercrime, EY's *Global Information Security Survey* October 2014.
[6] UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk, HM Government, Marsh, March 2015.
[7] Mysterious 2008 Turkey Pipeline Blast Opened New Cyberwar, Bloomberg, December 10, 2014.
[8] Financial Times, Energy companies hit by cyber-attack from Russia- linked group, June 30 2014.

4. Insurance cover

How does the general property insurance market respond to cyber risk including cyber terrorism?

In Australia, the Mark IV and Mark V Industrial Special Risks (ISR) policies are industry standard wordings that are the most commonly used starting point for property insurance contracts for large businesses. This would include big businesses with infrastructure such as power stations, chemical plants, dams and refineries. The standard may be modified with parts removed or added, but the unmodified Mark IV policy contains the section below:

> ***PERILS EXCLUSIONS***
>
> *7. Physical loss, destruction or damage occasioned by or happening through:*
>
> *(a) (ii) Access by any person(s) **other than** the Insured or the Insured's employee(s) to the Insured's computer system via data communication media that terminate in the Insured's computer system.*

As a consequence of this exclusion, cyber-attack scenarios causing physical loss and damage such as the Turkish pipeline blast or the German steel furnace shutdown, are **unlikely** to be covered if this exclusion remains. If such incidents were carried out as terrorist acts and were declared as such by the Australian Government, then any terrorism exclusion clause in the policy would be struck out, however, because exclusion 7 (a) (ii) is not a terrorism exclusion, it would remain and in this scenario there would be no effect to the liability of the insurer by the declaration of a terrorism incident.

Insurers also offer "Business Package" products to small and medium sized enterprises and these normally have property and business interruption sections of cover. In line with the Mark IV ISR standard policy, many of these business package products have exclusions for physical loss as a consequence of malicious external access to the insured's computer systems. For example, below:

> ***EXAMPLE INSURER A - BUSINESS PACKAGE - EXCLUSIONS***
>
> *We will not pay You under this section for physical loss, destruction or Damage caused by, or as a consequence of:*
>
> *24. Computer access - The gaining of access by any person other than You or Your employees to Your computer system via data communication media.*
>
> ***EXAMPLE INSURER B - BUSINESS PROPERTY - Policy section exclusions***
>
> *2. We will not cover You for loss or damage caused by:*
>
> *r) the gaining of unauthorised access to Your computer via any communication system by any person other than You or Your directors, partners, Employees, officers or any other person who has an interest in the property.*

Again, because these exclusions are not terrorism exclusions, they would remain and in this scenario there would be no effect to the liability of the insurer by the declaration of a terrorism incident.

How does the terrorism insurance scheme respond to malicious physical damage by remote electronic means?

Although it appears that malicious physical property damage by remote electronic means is excluded from many ISR and business pack policies, this may not always be the case as individual policies can be modified and there are other types of policies potentially eligible for the terrorism insurance scheme. If there is not a relevant exclusion for this type of peril, how does the terrorism insurance scheme respond?

The terrorism insurance scheme was set up as a response to insurance market failure and a need to protect the economy from the financial impact of terrorist attacks. Following the September 11 terrorist attacks, insurers withdrew coverage for terrorism from the commercial property insurance markets and this impacted the Australian economy with the subsequent withdrawal of funding for commercial property development and the consequent heightened risk borne by the commercial sector. In response to lobbying by key stakeholders in the property and banking industries, the Government passed the *Terrorism Insurance Act 2003* (TI Act) which renders terrorism exclusions in eligible insurance contracts ineffective if a terrorism incident is declared by the relevant government minister. The Act also established ARPC as a source of Australian terrorism reinsurance.

There are a range of limitations on the coverage and operation of the ARPC scheme and these are set out in the *Terrorism Insurance Act 2003*, the *Terrorism Insurance Regulations 2003* (Regulations) and the *Assistant Treasurer to Australian Reinsurance Pool Corporation (Premiums) Directions 2015*.

Computer crime is excluded from eligible contracts of insurance

Appendix 2 shows a flowchart stepping through the tests to determine if an insurer's contract/policy is eligible under the ARPC scheme. In brief, the scheme covers policies which insure construction sites, commercial property and tangible contents (in Australia) for loss or damage, business interruption and liability as an owner or occupier of eligible property. The scheme covers the additional liability that an insurer incurs if a terrorism incident is declared by the relevant government minister as this has the effect of striking out terrorism exclusion clauses in an eligible insurance policy.

However, there are several exclusions to the reinsurance coverage provided by the terrorism insurance scheme and these are primarily established in Schedule 1 of the Regulations.

Notable exclusions are war, nuclear explosion and radioactive hazard (such as the effects of a dirty bomb). Attacks on ships, aircraft, residential buildings and motor vehicles are also excluded.

Specifically in the context of this paper, "**loss arising from computer crime**" is one of the 40 exclusions specified in Schedule 1 of the Regulations. Exclusion 32 of Schedule 1 of the regulations states:

> *32 A contract of insurance to the extent that it provides cover for loss arising from computer crime.*

What does "computer crime" then mean for the purposes of the scheme?

What is Computer Crime?

The section below is extracted from the Federal Attorney Generals' Department website:

> *"In Australia, the term 'cybercrime' is used to describe both:*
>
> - *crimes directed at computers or other information communications technologies (such as hacking and denial of service attacks)*
> - *crimes where computers or ICTs are an integral part of an offence.*
>
> *Criminal offences*
>
> *The Commonwealth has enacted a comprehensive set of offences to address cybercrime, contained in the Criminal Code Act 1995 (Criminal Code). These offences are based on model laws agreed to by Commonwealth, State and Territory governments in 2001. The offences are consistent with those required by the Council of Europe Convention on Cybercrime and are drafted in technology-neutral terms to accommodate advances in technology.*
>
> *Key Commonwealth offences are contained in Part 10.6 and Part 10.7 of the Criminal Code, which contains offences criminalising the misuse of telecommunication networks, 'carriage services' (a term which includes the internet and online services, as well as wired and mobile services) and computers.*
>
> *The Commonwealth computer offences are complemented by state and territory laws which criminalise the misuse of data and computer systems."*[9]

It was the *Cybercrime Act 2001* which specified several telecommunications and computer offences (or crimes) to be included into the Australian Criminal Code. Part 10.6 of the Code deals with telecommunications offences and part 10.7 deals with computer offences. Appendix 3 is the relevant extract relating to computer offences.

Therefore, even if an insurer's property policy does cover malicious physical property damage as a result of remote computer access, then that act will likely be defined as "computer crime" under the Australian Criminal Code and therefore any loss arising would be excluded from coverage by the terrorism insurance scheme.

[9] http://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Pages/default.aspx.

Interactions: Cybercrime, IT use, terrorism and terrorism insurance scheme cover

Figure 2 indicates the relationship between terrorism, the ARPC scheme, cybercrime and terrorists' general use and exploitation of information and communications technology (ICT).

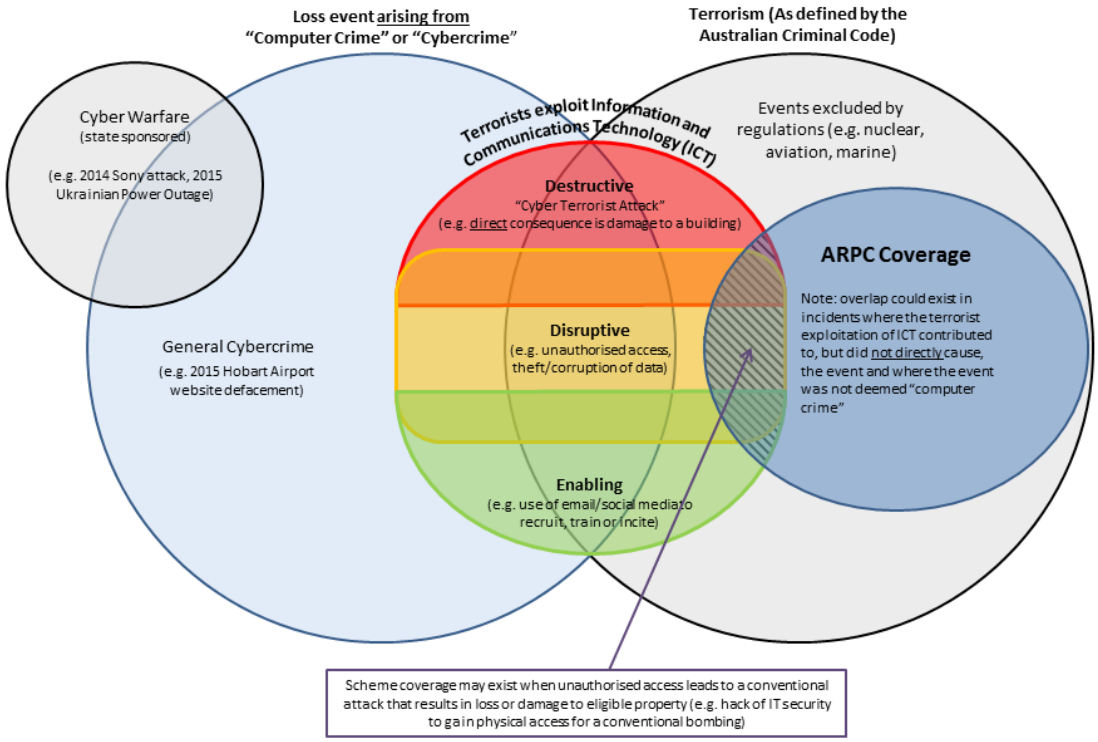


Figure 2: Terrorism, Cybercrime, Information and Communications Technology exploitation, the APRC Scheme

As per the computer crime exclusion in the Regulations, there should be no overlap between cybercrime/computer crime loss and ARPC scheme cover.

Both of Brickey's "destructive" and "disruptive" clusters of cyber terrorism (Figure 1) would likely qualify as terrorism as set out in the criminal code. A "destructive" attack could potentially cause major property damage and business interruption but because both destructive and disruptive attacks also qualify as "computer offences", losses from these actions would be excluded from coverage under the terrorism insurance scheme. The "enabling" cyber terrorism cluster is different however, in that these sorts of cyber activities may not be computer crimes. Additionally, they are unlikely to qualify as terrorism under the Australian criminal code.

"Cyber warfare" is shown as outside computer crime and terrorism although there may be a grey area where espionage and disruption activities are conducted with nation state backing. This could be considered as an act of war due to state backing and would therefore not be covered under the scheme because insurance policies generally exclude acts of war and in any case, under the TI Act, acts of war cannot be declared as terrorism incidents.

A major point in the declaration of a cyber based terrorist incident is that Australia applies a 'non-disclosure' policy for cyber crimes that have state backing. This reduces the possibility that a major cyber attack could be officially declared as terrorism for the purposes of the TIA as such a declaration would be contrary to government policy.

As highlighted previously in the references to the PwC and E&Y global cyber risk surveys (Ref: page 1, paragraph 4), cybercrime is increasing and terrorists may become engaged in criminal activities such

as identity theft, money theft and money laundering in support of their agendas and these terrorist committed cyber-crimes may not qualify as terrorism themselves.

An area which raises a question mark is the overlap of the circle for terrorists' exploitation of ICT and terrorism insurance scheme coverage. It is conceivable, for example, that terrorists may use a cyber-attack to compromise a physical security system, which then enables a physical attack to take place, such as the bombing of a commercial property.

In a March 2011 report, the US Congressional Research Service noted that:

> *"A future cyber-attack could be effective if directed against a portion of the U.S. critical infrastructure, and if timed to amplify the effects of a simultaneous conventional physical or chemical, biological, radiological, or nuclear terrorist attack."*[10]

Would the terrorism insurance scheme respond to this terrorism scenario? In this scenario, was the loss arising from a computer crime? Unauthorised access to compromise an electronic security system would likely fall under section 10.7 (computer offences) of the criminal code and may not be covered by the scheme.

This would likely be contrary to the current expectations of the insurance industry and policy holders.

5. Latest products

New cyber insurance policies

In the cyber sphere, assets are mostly intangible and in the form of electronic information. There are a growing number of insurance products in the area of "cyber insurance" which aim to cover electronic data assets damage or loss and/or the business interruption and response costs that may arise. Cyber policies may also cover the costs of responding to cyber breaches, such as notifying customers or owners of information and/or responding to regulators as may be required by local laws which vary from country to country.

In Australia "cyber" products are offered by most large insurers. The detail of coverage varies considerably. However, cyber insurance products don't generally address physical damage to tangible property caused by a cyber attack other than perhaps damage to computer hardware.

In a December 2014 article PartnerRe reported that:

> *"Despite the vulnerability and significant loss potential, cyber insurance cover is almost totally absent for physical damage and limited for business interruption (non-physical damage and property damage). For these there remains a lack of clarity amongst insureds over the exact exposure potential, irritation about the limited availability of protection and confusion linked to non-standardized covers. The result of all these factors is that insureds are increasingly asking for cyber protection to be added to their existing liability and property covers either through endorsement, or (and where we have particular concern), by removing the cyber exclusion."*[11]

For the purpose of terrorism risk reinsured with ARPC and as previously noted, if the relevant cyber exclusion is removed from property damage policies then, in the event of a terrorism incident, any terrorism exclusion will be struck out and the insurer will be liable for any loss arising. Importantly,

[10] Terrorist Use of the Internet: Information Operations in Cyberspace, Congressional Research Service Report for Congress, C. A. Theohary and J Rollins, March 2011.
[11] Markus Bassler, What Isn't Vulnerable to Cyber Attack? , PartnerRe views, December 2014.

the insurer will not be able to reinsure a cyber terrorist perpetrated risk with ARPC because of the current computer crime exclusion in the Regulations.

Although the ARPC scheme excludes computer crime it is technically possible for cyber insurance policies to be "eligible insurance contracts" under the scheme. One example of a cyber-insurance product analysed for this paper could be classified as an eligible insurance contract because it covers an eligible property and loss type combination, being business interruption loss arising from damage to tangible computer hardware property. However, after the exclusion of computer crime as a source of loss, the only remaining insured sources of loss are accidents and omissions and it is unclear how these might possibly arise from a terrorism incident which is, by definition, deliberate.

6. Global responses

Coverage for cyber terrorism in terrorism insurance pools

Major terrorism pools globally have not yet expanded their coverage to include cyber terrorism. And, although insurance coverage for cyber risk is an emerging market, there are no terrorism risk insurance pools that explicitly cover cyber attacks. In the USA, the *Terrorism Risk Insurance Act* which provides for a post-event funded scheme, does not specifically address the issue either as covered or excluded.

7. Conclusion

Cyber-attacks are increasing globally. Some sophisticated attacks aimed at disrupting and/or damaging infrastructure covered by the terrorism insurance scheme have occurred, however, these have not yet been attributed to terrorist groups. There is a danger that terrorists and others may develop the required skills and methods as more and more examples of sophisticated hacking tools and malware become available.

The most commonly used property policy structure for Australian large business (the Mark IV ISR policy), excludes major physical damage caused by a cyber-attack type event. Business package property sections likewise would appear to generally exclude this type of peril.

The ARPC scheme follows the reinsured's coverage but does not respond to any terrorism loss arising from a "computer crime" even if the insurer's policy provides such cover. The Australian criminal code contains descriptions of computer offences/crimes and cyber-attacks on property and infrastructure which would likely be considered as computer crimes and thus excluded from the scheme.

There is a gap in the property insurance market in situations where a cyber-attack by terrorists (or indeed others), may inflict major physical damage by primarily cyber means. Even if insurers were to include cyber-attack coverage for physical property, the ARPC terrorism reinsurance does not provide reinsurance cover for this type of attack as it would be considered computer crime under the Australian Criminal Code.

8. Other resources:

The Australian Cyber Security Centre: "Partnering for a Cyber Secure Australia". http://www.asio.gov.au/ASIO-and-National-Security/Partners/The-Australian-Cyber-Security-Centre.html

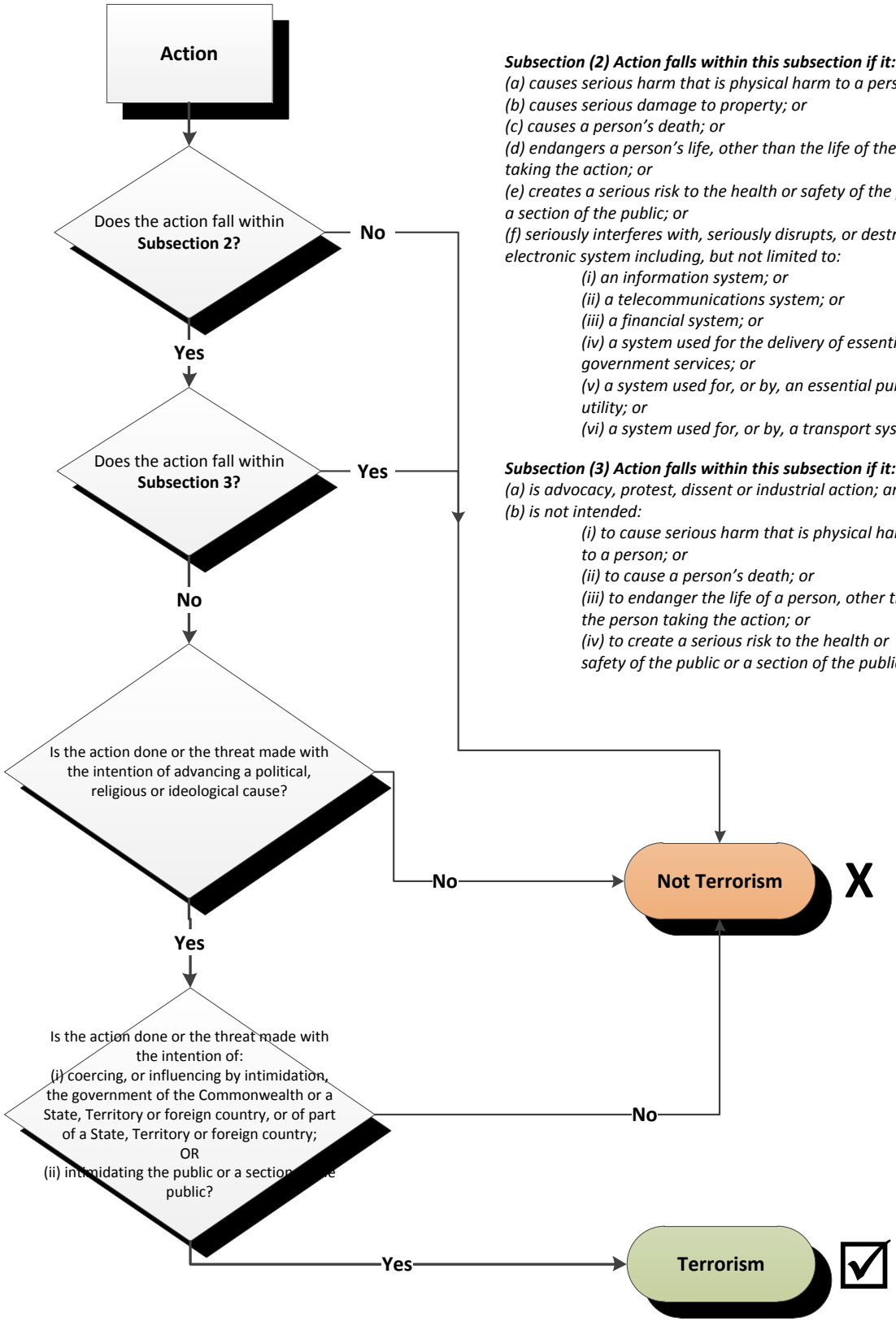
9. Acknowledgement

ARPC thanks Mr Norris Robertson for his original authorship of this paper in his capacity as ARPC's Manager of Insurance Audit & Research. Further refinements have been made to this ARPC discussion paper by Dr Christopher Wallace, Mr Michael Pennell, Ms Anna Fenech and Mr Daniel Wright since its original authorship.

Appendix 1

Is an Action Terrorism?

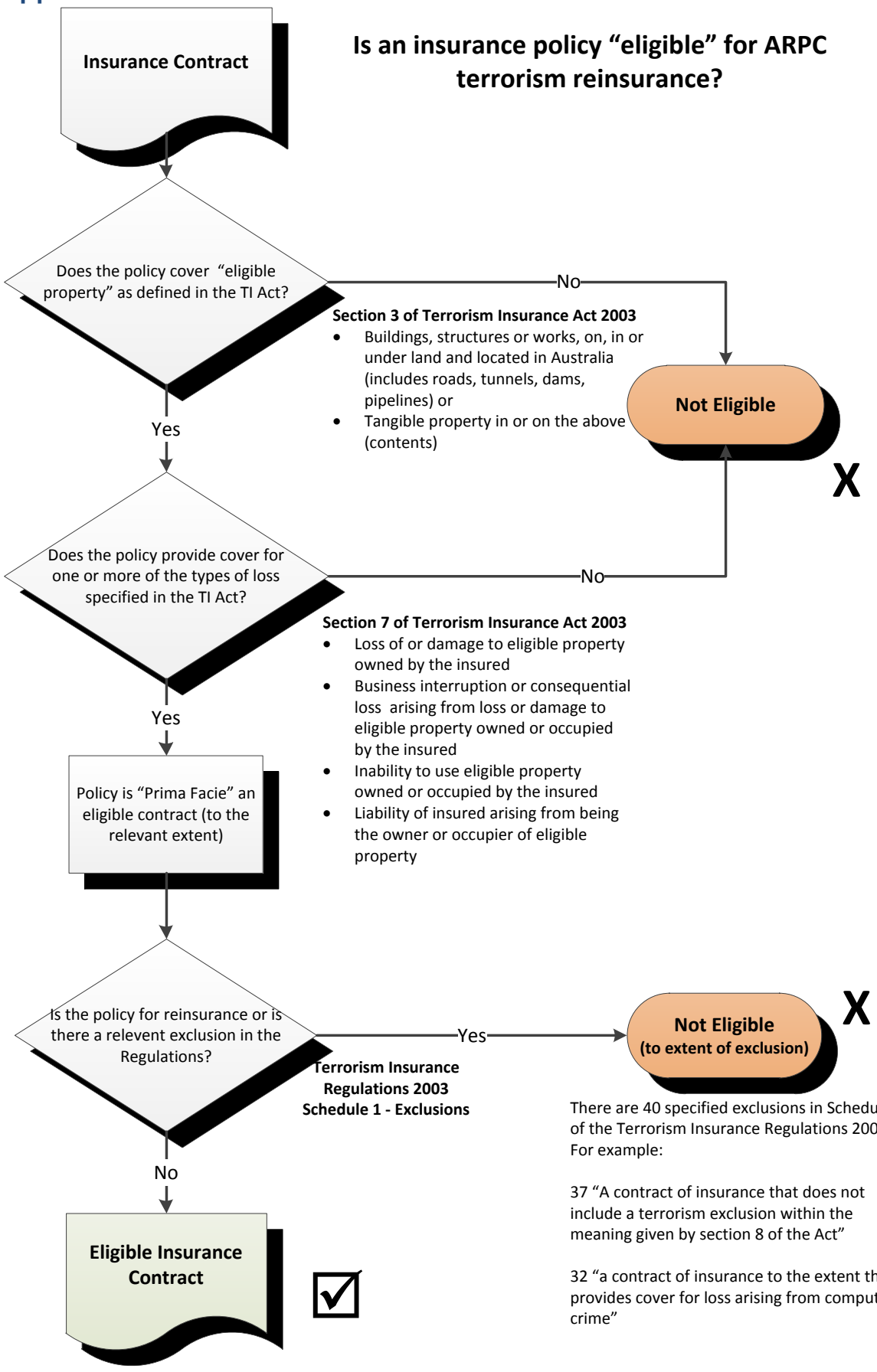
Terrorism is defined in Australia in the Criminal Code Amendment (Terrorism) Act 2003.



Subsection (2) Action falls within this subsection if it:
(a) causes serious harm that is physical harm to a person; or
(b) causes serious damage to property; or
(c) causes a person's death; or
(d) endangers a person's life, other than the life of the person taking the action; or
(e) creates a serious risk to the health or safety of the public or a section of the public; or
(f) seriously interferes with, seriously disrupts, or destroys, an electronic system including, but not limited to:
(i) an information system; or
(ii) a telecommunications system; or
(iii) a financial system; or
(iv) a system used for the delivery of essential government services; or
(v) a system used for, or by, an essential public utility; or
(vi) a system used for, or by, a transport system.

Subsection (3) Action falls within this subsection if it:
(a) is advocacy, protest, dissent or industrial action; and
(b) is not intended:
(i) to cause serious harm that is physical harm to a person; or
(ii) to cause a person's death; or
(iii) to endanger the life of a person, other than the person taking the action; or
(iv) to create a serious risk to the health or safety of the public or a section of the public."

Appendix 2


Is an insurance policy "eligible" for ARPC terrorism reinsurance?
Insurance Contract
Does the policy cover "eligible property" as defined in the TI Act?
No
Section 3 of Terrorism Insurance Act 2003
Buildings, structures or works, on, in or under land and located in Australia (includes roads, tunnels, dams, pipelines) or
Tangible property in or on the above (contents)
Not Eligible
X
Yes
Does the policy provide cover for one or more of the types of loss specified in the TI Act?
No
Section 7 of Terrorism Insurance Act 2003
Loss of or damage to eligible property owned by the insured
Business interruption or consequential loss arising from loss or damage to eligible property owned or occupied by the insured
Inability to use eligible property owned or occupied by the insured
Liability of insured arising from being the owner or occupier of eligible property
Yes
Policy is "Prima Facie" an eligible contract (to the relevant extent)
Is the policy for reinsurance or is there a relevent exclusion in the Regulations?
Yes
Not Eligible
(to extent of exclusion)
X
Terrorism Insurance Regulations 2003
Schedule 1 - Exclusions
There are 40 specified exclusions in Schedule 1 of the Terrorism Insurance Regulations 2003. For example:
37 "A contract of insurance that does not include a terrorism exclusion within the meaning given by section 8 of the Act"
32 "a contract of insurance to the extent that it provides cover for loss arising from computer crime"
No
Eligible Insurance Contract
☑

Appendix 3

Part 10.7 of the Australian Criminal Code

The *Cybercrime Act 2001* was a bill to amend the *Criminal Code Act 1995* (Criminal Code) by adding a new Part 10.7, which contains new updated computer offences based on the January 2001 Model Criminal Code *Damage and Computer Offences Report* developed through Commonwealth, State and Territory cooperation as a model for national consistency. The existing offences in Part VIA of the *Crimes Act 1914* (Crimes Act), which were enacted in 1989 and pre-date existing technology, would be repealed.

Below is an extract relating to computer offences.

"Division 477—Serious computer offences

477.1 Unauthorised access, modification or impairment with intent to commit a serious offence

(1) A person is guilty of an offence if:

(a) the person causes:

(i) any unauthorised access to data held in a computer; or

(ii) any unauthorised modification of data held in a computer; or

(iii) any unauthorised impairment of electronic communication to or from a computer; and

(b) the unauthorised access, modification or impairment is caused by means of a carriage service; and

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

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