PROMOTING THE
**NEXT GENERATION**
OF AUSTRALIAN LEADERS

MENZIES
FOUNDATION

# Regional Cyber Futures Initiative:
# The Future of Risk, Security and the Law

Threatcasting Project Report | 2020

# Contents

# Executive Summary

*The coming decade will see heightened challenges at the intersection of cyber and security in Australia and the broader region. The community and the law will need to take steps to address these threats and risks.*

## Threat Futures

The Threatcasting Lab agreed that threats impacting the law fall in three major areas:

**Data**: Manipulation and exploitation of public data by criminals, state actors and others will have physical and financial impact on citizens. Use of Artificial Intelligence (AI) to process and analyse data will open organisations to misuse and theft.

**Trust**: Inability to navigate false news and deep fake content will give rise to distrust of the government and public sector. In this environment the individual radicalisation of citizens will threaten the stability of the region.

**Workforce**: Corporations will advance physical and digital automation technologies. These changes will bring about greater efficiencies however the effect on human labour will produce widespread cultural and economic instability.

## Warning Signs to Avoid

Signals that will show that Australia and the region is heading to an undesired future:

- Governments enact laws and regulations that are conceived with the problem or threat of today and are out of date even before they can be implemented.
- Governments create laws that are unhelpful and unenforceable in the future, especially on the transnational stage.
- Governments and private industry place the culpability for or recovery from threats on the individual citizen and not on the entity, service or product upon which the threat was enacted.
- Australia and allied developed countries make decisions, laws and regulations that don't include the region, and block these players from any involvement because of gaps in capability or other inability to participate.

## Recommendations for Action

**Academia has a Role:** To deepen understanding of the implications of cyber risk and security, the consequent legal implications and remediation.

**Collaboration is Key:** New forms of collaboration to deepen understanding of current and future technological capabilities and the implications of this for the community and the law

**Train the Next Generation:** To **e**nsure that the next generation of lawyers have the systems thinking, computational, strategic and behavioural skillset to engage with cyber concepts and language.

# Introduction

The Menzies Foundation's vision is to raise the profile and importance of outstanding leadership for Australia. One of the Foundation's key strategic platforms is supporting law specialists to help shape Australia's response to increasingly complex global issues. Appendix 1

In 2019, the Foundation undertook a consultation with key legal experts across Australia, exploring legal cyber challenges, skills required to grapple with cyber complexity, and the training platforms most likely to effectively build capability.

It found lawyers are finding it increasingly difficult to respond to these challenges, in particular:

- Emergent technologies (artificial intelligence, quantum computing, big data and cybersecurity processes) are challenging traditional legal structures and creating increasing complexities for law practice.
- The emergence of AI means that software platforms will complete more data and administrative tasks and lawyers will have to focus on value adding skills to stay ahead of the changing landscape.
- Cyber is a multi-faceted system which impacts all aspects of society, across the political, cultural and economic spheres. This obscures which bodies of law may regulate a matter (such as criminal, human rights, constitutional) or in which jurisdiction.

In partnership with the University of Melbourne, as part of the new Menzies Oration Series, the Foundation partnered with futurist and Director of Arizona State University's Threatcasting Lab, Professor Brian David Johnson to explore the future of risk, security and the law, particularly within Australia and the Indo-Pacific.

In October 2019, Professor Johnson ran a Threatcasting Lab and delivered the Menzies Oration.

This report captures the findings of the subject matter experts, general public, and practitioners contributing to the project, with analysis and recommendations for action by Professor Johnson.

# What is Threatcasting?

The Future of Risk, Security and the Law project used threatcasting to look a decade into the future, identify relevant risks and possible steps to disrupt, mitigate and recover from the identified threats.

Threatcasting is a conceptual framework and process that enables groups to envision and plan systematically against threats ten years in the future. Groups explore how to transform the future they desire into reality while avoiding an undesired future.

Threatcasting uses multidisciplinary inputs which allow the creation of potential futures - focused on the fiction of a person in a place doing a thing. Some of these futures are desirable while others are to be avoided. It guides people to imagine what needs to be done today and then three years into the future to empower or disrupt the targeted future scenario. The framework also illustrates what flags, or warning events, could appear in society that indicate the progress toward the threat future. This project took the following steps:

- Interviews were conducted with subject matter experts in risk, security and the law. These interviews were analysed and summarised and used as inputs to two Workshops.
- Workshop 1 was held with members of the general public to understand and explore current general sentiment around cyber issues. The group also explored possible steps that might be taken and who should take them.
- Workshop 2 was more in-depth and conducted with risk, security and law practitioners. These were individuals who are actively working in these areas and whose organisations could take substantial action to disrupt, mitigate and recover from the threats that were identified.

*For many, future threats seem unimaginable and insurmountable. This threatcasting report seeks to envision these threats and empower people and organisations to act. These possible futures, based on facts and modelled by professionals, can dispel the myths and clear the fog for pragmatic, action-based dialogue.*

### // About Professor Brian David Johnson, Project lead and facilitator

As a futurist Brian works with organisations to develop an actionable 10 -15-year vision and what it will feel like to live in the future. His work is called futurecasting, using ethnographic field studies, technology research, cultural history, trend data, global interviews and even science fiction to provide a pragmatic road map of the future.

Professor Johnson has worked with governments, trade organisations, start-ups and multinational corporations to not only help envision their future but specify the steps needed to get there. Johnson is currently the futurist in residence at Arizona State University's Center for Science and the Imagination, a Professor in the School for the Future of Innovation in Society, and the Director of the ASU Threatcasting Lab. He is also a Futurist and Fellow at Frost and Sullivan.

# Cyber Challenges of the Law Today

## Are laws fit for purpose?

Australian laws relating to cyber sit within a multitude of regulations built up over more than a century, with applicability determined as a series of responses to issues.

Internationally, jurisdictions have their own unique drivers, whether in response to specific cyber threats or the promotion of cyber resilience, but it is clear there is no 'one size fits all'.

Laws are often criticised for best governing people and organisations in respect of yesterday's analogue world, while staring down a future where digital information is 'exploding' or expected in an impending 'tsunami'.

### // Smart Contracts: Jurisdiction-Free Future?

Blockchain smart contracts aim to circumvent the need for trust in humans, or a court. Intended to be standalone agreements not subject to interpretation or jurisdiction, the code is the arbiter.

Parties must ensure the code is 100% correct: in 2016, an error in the smart contract to establish the cryptocurrency venture fund *The DAO,* allowed US$50M to be "hacked" from it (Van Rijmenham & Ryan, 2019).

Debate followed on whether legal recourse was possible on an instrument that mimicked a business entity but lacked the convention of executives, directors, and legal jurisdiction of incorporation or physical location. The owners/investors decided to effectively rewrite the code to prevent the release of cryptocurrency to the hacker, demonstrating that code was not yet ready to be law (Hinkes, 2016).

## Who is actually the 'victim'?

*The acknowledgement of these challenges that has shifted the perception of organisations as hackers' victims; to one where organisations are at fault for not properly securing assets or policing use (Gilbert + Tobin, 2020).*

Legal contests in recent years have not been about prosecuting perpetrators, but disputes between a breached organisation and the intermediaries interacting with them (Wolff, 2018, p. 239) (Pappalardo & Suzor, 2018, p. 474) (Zittrain, 2019).

As the more intractable cyber threats have moved from "viral malware to viral mis- and disinformation", the role of platforms that amplify content have come under greater legal and regulatory scrutiny (Zittrain, 2019).

## Where the liability lies

Australian civil law holds product manufacturers responsible for the safety of a product where it contains inbuilt AI (Corrs Chambers Westgrath, 2019). Likewise, under human rights laws, discrimination by an algorithm is still discrimination for which its deployer must be held to account (Eyres, 2019). The recent Australian Federal Court rulings against the Commonwealth regarding the Robodebt scheme have reinforced that Government cannot escape responsibility for its use of automated decision-making (Leins, 2019).

However, Australian common law is unclear on liability when an intermediary creates a technology or system that allows another party to commit a wrongdoing.  It is often determined by the Court on the degree to which the intermediary is seen to be active in the wrong. Determining the intention, passivity and knowledge of an intermediary in an action however still lacks a clear framework, creating uncertainty (Pappalardo & Suzor, 2018).

As intermediaries are more often expected to help enforce laws and uphold social norms, addressing who is best placed to reduce or redress harm is becoming more relevant than asking who it is 'fair' to blame (Wolff, 2018, pp. 2018-209).

## The boundary-less world

There are no boundaries on the internet, expanding the legal complexity of stakeholder roles.

Digital technology enables people to act in and exert influence anywhere around the world, often operating in multiple jurisdictions at once (Young & Meli, 2019). And international law can make the issue of legal attribution where a state actor is involved highly complex. (Finlay & Payne, 2019).

The Indo-Pacific is growing in its digital connectivity, with Malaysia, Indonesia and Vietnam as global hotspots for major blocked web activities. Hackers are 80% more likely to attack organisations in Asia due to its high volume of cross-border data transfers and weak regulations (Oliver Wyman, 2017) (AT Kearney, 2018). Computer servers connected across countries via undersea cable have the potential to turn countries into intermediaries for attack (Rudolph, 2018).

There are a prevalence of cyber related laws, bills and policies across Pacific Island states including Papua New Guinea, Tonga, Nauru and Samoa, and a growing acknowledgement of the need to build capacity across justice systems to enforce these laws. (PICISOC Board, 2019).

The globalisation of data mobility, and cultural norms under which data is governed, challenges domestic law application and reform (The Law Society of NSW, 2017).

## // Cross Border Cyber Crime

**Vanuatu and China**

In mid-2019 Vanuatu was placed under scrutiny for arresting and allowing deportation to China of six people, including dual citizens. The Vanuatu Minister of Internal Affairs reported the arrests were made at the request of Chinese law enforcement which had evidence of an internet scam targeting Chinese citizens (Power & Tobin, 2019).

The Minister was criticised for not considering his own responsibilities under Vanuatu law. If a crime was committed in China from Vanuatu, the Vanuatuan legal systems should still have taken precedent for the individuals holding Vanuatuan passports. Instead it appeared that China was able to act as though Vanuatu was an extension of its own system (McGarry, 2019) (Wyeth, 2019). Later the Minister advised that the individuals were appropriately deported under Vanuatu's immigration law to face criminal proceedings in China for security reasons (Wasuka, 2019). This raised several unanswered questions and demonstrates how state interests can increase the lack of transparency about who or what is being protected when addressing cybercrime.

**Australia, Canada and the US**

The 2015 data breach of the Ashley Madison website involved approximately 36 million user accounts across 45 countries. Australia, Canada and the United States subsequently cooperated in the legal treatments of the breach.

The Australian Privacy Commissioner and Canadian counterpart undertook a joint investigation to examine whether parent Avid Life Media (ALM) had taken reasonable steps to protect the information of the Australian citizens to whom the Canadian company marketed and provided service. It was found to have not. ALM was particularly called out for its poor governance and escaped financial penalty in Australia (OAIC, 2016).

In the US, the Federal Trade Commission acted against ALM due to what it alleged was "deceptive and unfair acts or practices" by the company. Ashley Madison had marketed privacy and security as an explicit marketing tool which was found to have limited basis in fact. The case was settled out of court with a financial penalty of US$1.6M (FTC, 2016).

Class actions totalling US$1B launched in the US were depleted when it was ruled that all litigants must be named in proceedings. Ashley Madison provided a service to facilitate discreet extramarital affairs, and many litigants dropped out of action rather than risk further public humiliation. Damages of up to US$3,500 per named litigant to cover "unreimbursed documented losses" were awarded eventually, out of a total settlement fund of US$11.2M. However, the award clearly sidestepped the much greater losses that were non-monetary and non-physical.

While Ashley Madison was the nominative 'victim' of the hack, there was scant attention paid to finding or seeking redress against the hackers from either government authorities or class action litigants. ALM was found culpable for its role in the breach, however its customers, and in this case their families, suffered the more substantial harm and enduring consequences despite best intents of the law (Wolff, 2018).

# Cyber Challenges for the Law Tomorrow

The coming decade will see heightened challenges at the intersection of cyber and general security in Australia and the broader region. The Australian community and the legal sector will need to prepare for and address these threats and risks.

Technological advances in artificial intelligence (AI), machine learning (ML), quantum computing, the internet of things (IoT), smart cities, and autonomous vehicles in land, sea and air are quickly developing, largely funded by private transnational corporations with uneven oversight and regulation.

This constellation of technologies is expanding vulnerabilities and increasing the capabilities of bad actors, nation states and criminals. The multidimensional attack surface will present an increasingly complex environment to police, regulate and monitor.

Australia and the region will need to expand traditional legal actions as well as explore new and novel cultural, collaborative, normative and regulatory mechanisms to promote security, stability and growth.

Criminal and state actors along with corporations, governments, special interest groups, communities and average citizens will have an unprecedented ability to act.

The public sector (including Government, defence, and the community) will experience more challenges in understanding, preparing, monitoring and enforcing the law.

This complexity will also be increased by the transnational nature of the region; enforcing laws and communicating across borders with entities in countries that have their own laws and regulations, different culture, and varying levels understanding of both the risks and threats.

This will be exacerbated by uneven technological and enforcement capabilities between these entities and varying abilities to act.

The public sector will be forced to react when “surprised” or taken off guard by threats that they are not prepared for. Reacting for the public good will mean that these actions could fall into four specific warning events.

### Warning Events

- Governments will enact laws and regulations that are conceived with the problem or threat of today and will be out of date even before they can be implemented.
- Governments will create laws that will be unhelpful and unenforceable in the future, especially on the transnational stage.
- Governments and private industry will place the culpability for threats or at least the recovery from them on the individual citizen and not on the state or government or even on the corporation’s products and/or services upon which the threat was enacted.
- Australia and many more developed countries could make decisions, laws and regulations that not only don’t include many of the other players in the region but also might block these players from any involvement because of a capability gap, or the other entities’ inability to participate.

## Future Threats

**Threats** (intent x capability) in this future environment will increase in number, complexity and under diminished ability for the public sector to act. **Risks** (probability x consequence) will also increase. The probability of a wide variety of risks in this environment and the consequence of these risks also increases. The connected digital and data centric nature of this future environment means that the consequences have greater depth inside of Australia as well as breadth, across the region.

**The Public Perils of Digital Consolidation and Artificial Intelligence:** The continued digitisation and consolidation of public record will generate massive pools of public data that will become targets for criminals, state actors and potentially corporations and other organisations. From personal healthcare to transnational banking, the manipulation and exploitation of this data will have physical and financial impact to citizens. The use of AI to better streamline the analysis and processing of this public data opens up organisations to potential misuse and theft, when the programming of AI is not transparent and addressable, and private corporations are used for public services.

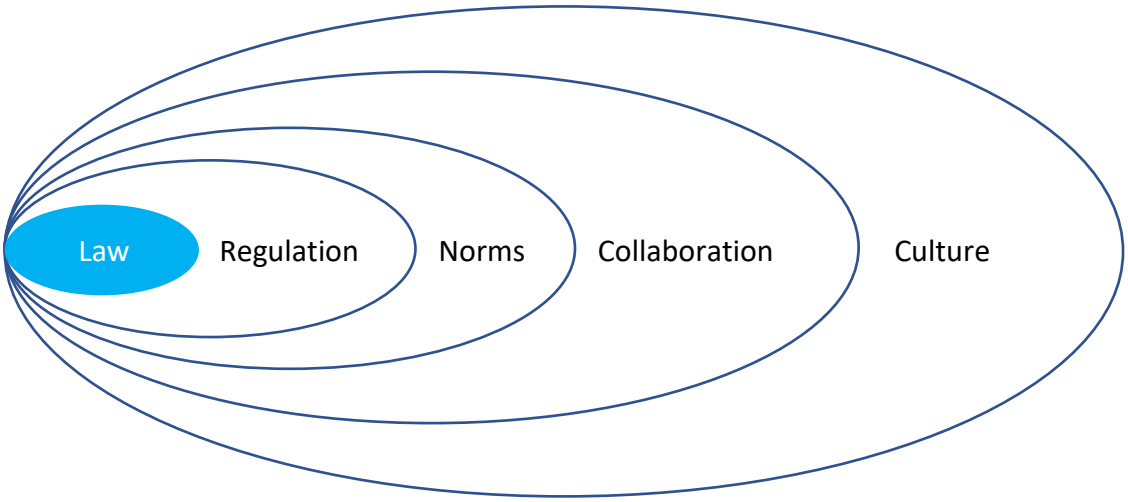
**Who Accounts for the Truth?** Technological and cultural changes in the region have seen and will continue to see an erosion of the truth and citizen's ability to navigate a world of false news and deep fake content giving rise to distrust of the government and public sector. Additionally, in this environment the individual radicalisation of citizens will threaten the stability of the region.

**Human Labour's Seismic Shift:** Over the next decade private corporations will fund and advance both physical and digital automation technologies (e.g. AI, robots, autonomous vehicles) that will have a dramatic effect on the workforce. Although these changes will bring about greater efficiencies the effect on human labour cannot be underestimated, potentially producing widespread cultural and economic instability.

### // Digital Sweatshops

The burgeoning gig economy is being helped by better digital connections and new online labour marketplaces where employment can be sold in parcels. While this creates opportunities for work unlimited by geographical location, it also raises concerns about the increasing commodification of work, particularly in parts of the world with weak employment protections (Wood & Graham, 2019). Facebook is currently facing class actions in the US and Ireland from contractors suffering post-traumatic stress disorder (PTSD), allegedly as a result of moderating social media content. In the wake of this, Accenture, which employs content moderators for Facebook, Google and YouTube has admitted to providing contracts for employees to acknowledge that their jobs may cause PTSD. While employment law experts comment that this does not remove liability for providing an unsafe workplace, it does show how companies are testing ways of passing their risk to the more vulnerable, even in developed nations (Newton, 2020).

# Action Framework




The following framework explores the relationship and impact from different types of actions that can be taken.

Typically, traditional legal actions are effective, but their reach can be limited. **Regulations**, as an extension of the law, can have a wider impact especially across borders and transnational issues.

**Norms** can be particularly helpful as they allow people, organisations, businesses and communities to self-regulate themselves. This "non-official" form of regulation can be particularly effective in the business sector as the value of having social licence becomes greater.

*"A norm is a social rule that does not depend on government for either promulgation or enforcement. Examples range from table manners and the rules of grammar to country club regulations and standard business practice. Norms may be independent of laws, as in the examples just given, or may overlap them; there are norms against stealing and lying, but also laws against these behaviors." (Posner & Rasmusen, 1999)*

### // Cyberspace International Norms

The United Nations Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) has set out the voluntary non-binding norms for the responsible behaviour of states in cyberspace.

The 11 norms provide a framework for Australia to advance democratic action in coalition with its partners in ASEAN – and importantly lift international dialogue beyond cybercrime and terrorist use of the internet (Noor, 2018) (Commonwealth of Australia, Department of Foreign Affairs and Trade, 2017).

Some fear the group is becoming a mechanism to help authoritarian regimes advance their own agendas on military use of information technology (Sherman & Raymond, 2019). However while the statement has not been fully endorsed by all UN members states, it still remains the best forum to share international understanding (Sukumar, 2017).

**Collaborations** expand the ecosystem of participants across borders, domains, expertise and multiple sectors. These collaborations will help to inform norms, regulations and laws.

Finally, the broadest area of influence is **culture**. Creating a culture change is slow and can be convoluted and complex as it is decentralised. But if a culture change can be achieved the effect on the public and private sector as well as average citizens can be broad.

## Implementation

As we explore the specific actions that can be taken by different sectors and domains across the Indo-Pacific it is helpful to view each action through this framework to expand and broaden impact.

### Academia

The academy will need to explore the implications, perils and potential for increased collaboration, as well as new ways of thinking and operating.

The academy can provide tools, frameworks and research that explores wider implications and ramifications as well as processes and procedure to begin the pragmatic application of these ideas.

The academy can also work to educate the next generation of lawyers in technological implications and capabilities, so that lawyers can enact better laws and policy.

This includes training not just in understanding technology, but also in understanding how and when to communicate and collaborate with technologists and corporations as they develop new technologies.

The academy is also an ideal place to explore and research the potential risks and threats from the multidimensional attack space in Australia, but more importantly how it could and will play out across the Indo-Pacific region.

It is a neutral, evidence-based environment to convene all parties involved in this complex future to explore solutions and communications. Including:

- Legal Profession
- Local Government
- Foreign Government
- Defence
- Corporations
- Political Parties
- Special Interest Groups
- Other Organisations
- Communities

### Corporations: *The Great Unknown*

Over the next decade corporations will find themselves increasingly challenged by their position as technological leaders and providers to citizens and governments.

Because of a lack and inability to enforce global regulations corporations will be continually caught between profit and public good. This is more complex because the definition of “public” and “good” will be different in different countries and regions across the globe.

It is unclear what role private corporations will see themselves as playing in the multidimensional attack space versus the role that will be regulated or forced upon them. How much will this impact on profit incentives and ability to meet shareholders demands? What will the push back be against regulatory change that negatively affects profit?

### // Corporations: A Strange Bedfellow

The advances in technologies will be fuelled and funded by private transnational corporations who to date, and in the foreseeable future, have remained largely unregulated. This lack of regulation and oversight arguably has led to rapid development and innovation but also means that bad actors may use these technologies to commit crime and cause harm to citizens. Government will need to partner with private corporations to build critical public infrastructure. This will create a "strange bedfellows" relationship between these corporations and the public sector. The public sector will both be reliant on these corporations while at the same time be required to monitor, enforce and regulate them. The complexity of this relationship will move beyond a simple conflict of interest. It could produce a cognitive gap for practitioners inside of the public sector to be able to do the public good.

**Industry Associations**

Industry associations should act as a bridge between academia, the public sector, private corporations, start-ups and the general public to facilitate conversations, enable business and encourage cross-functional sharing.

**The General Public**

There is a strong need for public outreach in this area in order to educate average citizens of all ages to these possible threats. It is important that these threats are not seen as overwhelming and unapproachable and that the focus is on the development of pragmatic, simple steps that can be taken for people to protect themselves, their families and communities from these possible and potential threats.

This empowerment will allow for average citizens to participate more robustly with all other members of this complex ecosystem.

To confront and prepare for these possible and potential threats the law will need to expand thinking past traditional legal frameworks, modes of thought, possible collaborations and potential actions.

# Conclusion

The Threatcasting Workshops identified a range of possible ways to disrupt, mitigate, and recover from these possible threats. A single organisation cannot meet these threats. Over the next decade each domain will need to learn to inform, collaborate, and support the others.

Although the law can accomplish a great deal, other mechanisms will be needed to support actions that will fall outside the ethical and legal parameters of what the law can do.

### Academia has a Role to Play

Several of the threat futures developed for this report should be explored in academia, to understand the risk, security and legal implications of these threats as well as what actions can be taken. Academia is the ideal location to convene all relevant players to act.

### Collaboration is Key

To confront the threats of the next decade a wide range of collaboration will be needed. Adding to academia and legal practitioners, technological expertise is needed to understand current technological capabilities and the possible and potential capabilities that will arrive in the coming years. This expertise together can better inform policy makers of trends, likely impacts and preventative (or permissive) action under the law.

### Train the Next Generation

The next generation of lawyers needs to be prepared and have a working knowledge of technological advancements. They will not need to be technology practitioners but will need to understand the concepts and language so that they may better collaborate with and add value to the broader ecosystem in the region.

Best practice systemic change initiatives suggest that solutions are not likely to be derived from any one sectoral perspective, but rather a cross-sector government and business partnership model to co-create solutions at the national and regional level. Philanthropy may play a role in brokering these collaborations.

The Australian Government's own development policies, and International Cyber Engagement Strategy, reflect the value of closer relationships with partners, enabling learning and leveraging of experience and expertise.

# Acknowledgments

We would like to acknowledge the Wurundjeri people who are the Traditional Custodians of this Land. We would also like to pay respect to the Elders of the Kulin Nation, both past and present.

We would like to extend our gratitude to the University of Melbourne Chancellery for their support and commitment to the Menzies Oration Series. We would like to thank the Melbourne Law School for their contribution to the 2019 Menzies Oration – The Future of Risk, Security and the Law.

# Appendix 1

The Menzies Foundation aspires to raise the profile and importance of 'outstanding' leadership.

To achieve this, the Foundation identifies leadership challenges and supports initiatives to support these challenges.

One of the Foundation's key areas of focus is supporting law specialists who can help shape Australia's response to increasingly complex global issues. For the next three years, this will focus on cyber security.

The Foundation's Regional Cyber Futures Initiative supported the Future of Risk, Security and the Law Threatcasting Project in partnership with the University of Melbourne.

The Foundation is proud to support several interrelated projects aimed at lifting domestic and international capability in cyber law. The results of the threatcasting project will feed into a number of these initiatives to ensure the learning is used. This includes:

**Research** identifying:

- sectoral, transnational partners which block or enable progress in cyber law
- strategic cyber law priorities of the broader Indo-Pacific region
- model laws and international guidelines to serve as a basis for treaty potential

**Training** program delivering:

- an immersive training platform based on real time; problem-centred legal challenges set in a global context
- support to develop cultural awareness and a global perspective in law

**Stakeholder** program communicating:

- thought leadership to develop a community of interest, and encourage discourse across the community of interested stakeholders
- real world context and potential case studies for Australian lawyers to engage in cyber legal challenges in the region
- an oration and speaker series

Partners in the Regional Cyber Futures Initiative include The Menzies Foundation, The Australian National University and AustCyber.

# References


AT Kearney. (2018). *Cybersecurity in ASEAN: An Urgent Call to Action.* Retrieved from Kearney: https://www.kearney.com/documents/1781738/1782318/Cybersecurity+in+ASEAN%E2%80%94An+Urgent+Call+to+Action.pdf/80a880c4-8b70-3c99-335f-c57e6ded5d34

Australian Cyber Security Centre. (2018, September 13). *Strengthening cyber security across the Pacific*. Retrieved from Australian Signals Directorate: https://www.cyber.gov.au/news/pacific-islands

Bennett, M., & Johnson, B. D. (2016, September 12). *Dark Future Precedents: Science Fiction, Futurism and Law.* Retrieved from Creative Science: https://www.creative-science.org/wp-content/uploads/2015/05/2016_CS16DarkFuturePrecedentswithHeaders.pdf

Bowers, J., & Zittrain, J. (2020, January 14). *Answering impossible questions: content governance in an age of disinformation*. Retrieved from Harvard Kennedy School of Government (HKS) Misinformation Review: https://doi.org/10.37016/mr-2020-005

Commonwealth of Australia, Department of Foreign Affairs and Trade. (2017). *Australia's International Cyber Engagement Strategy.*

Corrs Chambers Westgrath. (2019, November 1). *Liability for AI: considering the risks*. Retrieved from Corrs Chambers Westgrath: https://corrs.com.au/insights/liability-for-ai-considering-the-risks

Espinoza, J., & Fleming, S. (2020, February 18). *EU rejects Facebook's proposals for online regulation*. Retrieved from Financial Times: https://www.ft.com/content/81ae47b0-51a9-11ea-8841-482eed0038b1

Eyres, J. (2019, March 15). *Call for 'AI policy council' to govern how algorithms use personal information*. Retrieved from Australian Financial Review: https://www.afr.com/technology/call-for-ai-policy-council-to-govern-how-algorithms-use-personal-information-20190315-h1cej1

Finlay, L., & Payne, C. (2019, February 20). *Why international law is failing to keep pace with technology in preventing cyber attacks*. Retrieved from The Conversation: https://theconversation.com/why-international-law-is-failing-to-keep-pace-with-technology-in-preventing-cyber-attacks-111998

FTC. (2016, December 14). *Operators of AshleyMadison.com Settle FTC, State Charges Resulting From 2015 Data Breach that Exposed 36 Million Users' Profile Information*. Retrieved from US Federal Trade Commission: https://www.ftc.gov/news-events/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting

Gilbert + Tobin. (2020). *Cyber Security*. Retrieved from Gilbert + Tobin: https://www.gtlaw.com.au/expertise/cyber-security

Hinkes, D. (2016, June 21). *A Legal Analysis Of The DAO Exploit and Possible Investor Rights*. Retrieved from Bitcoin Magazine: https://bitcoinmagazine.com/articles/a-legal-analysis-of-the-dao-exploit-and-possible-investor-rights-1466524659

International Comparative Legal Guides. (2019, October 22). *Cybersecurity Laws and Regulations - Australia.* Retrieved from ICLG: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/australia

Leins, K. (2019, December 4). *What is the law when AI makes the decisions?* Retrieved from University of Melbourne: https://pursuit.unimelb.edu.au/articles/what-is-the-law-when-ai-makes-the-decisions

McGarry, D. (2019, July 11). *Vanuatu Is Not China*. Retrieved from Vanuatu Daily Post: https://dailypost.vu/news/vanuatu-is-not-china/article_14fe0983-e06f-599c-8504-a235dcb67129.html

MinterEllison. (2019, March 26). *Perspectives on Cyber Risk 2019*. Retrieved from MinterEllison: https://www.minterellison.com/articles/2019-perspectives-on-cyber-risk

Newton, C. (2020, January 24). *YouTube moderators are being forced to sign a statement acknowledging the job can give them PTSD*. Retrieved from The Verge: https://www.theverge.com/2020/1/24/21075830/youtube-moderators-ptsd-accenture-statement-lawsuits-mental-health

Noor, E. (2018, October 4). *ASEAN Takes a Bold Cybersecurity Step*. Retrieved from The Diplomat: https://thediplomat.com/2018/10/asean-takes-a-bold-cybersecurity-step/

OAIC. (2016, September 24). *Ashley Madison data breach: joint findings released*. Retrieved from Office of the Australian Information Commissioner: https://www.oaic.gov.au/updates/news-and-media/ashley-madison-data-breach-joint-findings-released/

Oliver Wyman. (2017). *Insights: Cyber Risk in Asia-Pacific: The Case for Greater Transparency.* Retrieved from Oliver Wyman: https://www.oliverwyman.com/our-expertise/insights/2017/may/cyber-risk-in-asia-pacific.html

Pappalardo, K., & Suzor, N. (2018). The liability of Australian online intermediaries. *The Sydney Law Review, 40*(4), 469-498.

PICISOC Board. (2019, November 24). *Cybersecurity: state of play in the region and current priorities*. Retrieved from Internet Society: https://www.picisoc.org/2019/11/24/cybersecurity-state-of-play-in-the-region-and-current-priorities/

Posner, R., & Rasmusen, E. (1999, September). Creating and Enforcing Norms, with Special Reference to Sanctions. *International Review of Law and Economics, 19*(3), 369-382.

Power, J., & Tobin, M. (2019, July 10). *Is Vanuatu's deportation of six Chinese nationals an erosion of its democratic rights at Beijing's bidding?* Retrieved from South China Morning Post: https://www.scmp.com/week-asia/geopolitics/article/3018076/vanuatus-deportation-six-chinese-nationals-erosion-its

Rudolph, C. (2018, August 27). *Turning the cybersecurity spotlight on the Pacific*. Retrieved from Monash University: https://lens.monash.edu/2018/08/26/1358125/cybersecurity-in-the-pacfic

Sherman, J., & Raymond, M. (2019, December 4). *The U.N. passed a Russia-backed cybercrime resolution. That's not good news for Internet freedom.* Retrieved from The Washington Post: https://www.washingtonpost.com/politics/2019/12/04/un-passed-russia-backed-cybercrime-resolution-thats-not-good-news-internet-freedom/

Sukumar, A. M. (2017, July 4). *The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?* Retrieved from Lawfare: https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well

The Law Society of NSW. (2017). *Future of Law and Innovation in the Profession.* Retrieved from Law Society of NSW: https://www.lawsociety.com.au/sites/default/files/2018-03/1272952.pdf

Van Rijmenham, M., & Ryan, P. (2019). *Blockchain: Transforming Your Business and Our World.* Milton Park, Oxford: Routledge.

Wasuka, E. (2019, July 9). *Vanuatu government breaks silence over deportation of alleged criminals to China*. Retrieved from ABC Radio Australia: https://www.abc.net.au/radio-australia/programs/pacificbeat/vanuatu-government-defends-criminals-deportation-to-china/11290786

Wolff, J. (2018). *You'll see this message when it is too late: The Legal and Economic Aftermath of Cybersecurity Breaches.* Cambridge, MA: MIT Press.

Wood, A. J., & Graham, M. (2019, February 28). *Networked but Commodified: Digital Labor in the Remote Gig Economy*. Retrieved from New Internationalist: https://newint.org/features/2019/02/28/networked-commodified-digital-labour-remote-gig-economy

Wyeth, G. (2019, July 11). *The Long Arm of Chinese Law Reaches Vanuatu, Again*. Retrieved from The Diplomat: https://thediplomat.com/2019/07/the-long-arm-of-chinese-law-reaches-vanuatu-again/

Young, R., & Meli, O. (2019, May). *Trusted, ethical, fast-moving and effective future police.* Retrieved from ANU National Security College: https://nsc.crawford.anu.edu.au/publication/14221/trusted-ethical-fast-moving-and-effective-future-police

Zittrain, J. (2019, September 23). *Three Eras of Digital Governance*. Retrieved from SSRN: https://ssrn.com/abstract=3458435