UNDERSTANDING THE LAW APPLICABLE TO INFORMATION WARFARE

SPGP2020-106-108 - Understanding the Law Applicable to Information Warfare:
the final report of a project funded by Department of Defence Strategic Policy Division.

A REPORT PREPARED BY:

Melissa de Zwart, Stacey Henderson, Melissa-Ellen Dowling, Joel Lisk and Emma Lush

April 2024

THE UNIVERSITY of ADELAIDE
Flinders University
Jeff Bleich Centre for Democracy and Disruptive Technologies

UNDERSTANDING THE LAW APPLICABLE TO INFORMATION WARFARE[*]

REPORT PREPARED BY:

Melissa de Zwart, Stacey Henderson, Melissa-Ellen Dowling, Joel Lisk and Emma Lush

A Case Studies

Disinformation and misinformation pose threats to national security on a number of levels. The existence of both in a State's information environment can lead to dangerous outcomes on a smaller domestic level, and it can pose a potential threat to a State's international security and relations with other States. This is to say that far from being abstract concepts, disinformation and misinformation can have, and have had, tangible consequences.

Domestically, the existence of misinformation and disinformation has led to real-world consequences that range from threats to public health, to growing threats in the form of domestic far-right-wing terrorism. In Australia, the consequences of misinformation and disinformation have been felt on several fronts. During the COVID-19 pandemic, conspiracy theories and the spreading of misinformation pushing the view that COVID-19 was a hoax

[*] SPGP2020-106-108 - Understanding the Law Applicable to Information Warfare: This is the final report of this project funded by Department of Defence Strategic Policy Division.

aimed at controlling the world's population, resulted in widespread rejection of vital health measures such as mask-wearing and vaccinations.[1] The refusal to follow evidence-based health measures can endanger the public, and expose vulnerable members of the community to real danger.

Misinformation and disinformation can also incite violence in the community.[2] The shooting of two police officers in Wieambilla, Queensland is illustrative of the tangible and violent consequences that misinformation and disinformation can have. Constables Rachel McCrow and Matthew Arnold were shot dead by Stacey and Gareth Train in December 2022. The Trains, also killed in the shootout themselves, were close confidants of Donald Day Jr, a far-right extremist from Arizona in the United States.[3] Mr Day was arrested and charged with inciting violence on 1 December 2023. He would often share conspiratorial posts about vaccines and windfarms, amongst other topics, and routinely called for the overthrow of the government by violent means.[4] Mr Day allegedly communicated with the Trains about 'Christian, end-of-days' ideologies prior to the shootout, the Trains and Mr Day often communicated by commenting on one-another's Youtube videos[5] and the mutual sharing of disinformation and misinformation in the form of conspiracy theories and anti-government sentiment has been connected to the events of the shooting in December 2022, which has been described as a 'religiously-motivated terrorist attack.'[6] Mr Day himself stated that he was prepared to die in a 'last stand' with police,[7] and shortly after the Train's shootout with police posted a video online lamenting their deaths.[8] The sharing of disinformation and misinformation on online platforms (here, across jurisdictions) can fuel acts of violence in the

[1] Christine Mikhaeil, 'Conspiracy theories: how social media can help them spread and even spark violence' *The Conversation* (online, 2 August 2023) <https://theconversation.com/conspiracy-theories-how-social-media-can-help-them-spread-and-even-spark-violence-209413>.
[2] Ibid.
[3] Simon Cullen and Jade Macmillan, 'US Government Urges Court not to Drop Charges Against Donald Day, the Extremist Linked to the Wieambilla Shooting' *ABC News* (online, 10 January 2024) <https://www.abc.net.au/news/2024-01-10/qld-donald-day-wieambilla-stacey-train-gareth-nathan-police/103306006>.
[4] Kevin Nguyen et al, 'Inside the God-fearing and Conspiratorial Worldviews of Donald Day Jr' *ABC News* (Online, 8 December 2023) < https://www.abc.net.au/news/2023-12-08/inside-god-fearing-conspiratorial-worldviews-of-donald-day-jr/103204360>.
[5] Kelsie Iorio and Jessica Black 'Man arrested in Arizona over religiously motivated terror attack at Wieambilla sent shooters 'end of days' ideological messages' *ABC News* (online, 6 December 2023) <https://www.abc.net.au/news/2023-12-06/qld-wieambilla-shooting-arrest-arizona-queensland-police/103196120>.
[6] Ibid.
[6] Ibid.
[7] Kevin Nguyen and Emilie Gramenz, 'Donald Day Jr, US sovereign citizen linked to Wieambilla murders, was prepared for deadly 'last stand' with police, court hears' *ABC News* (online, 29 December 2023) <https://www.abc.net.au/news/2023-12-29/donald-day-jr-wieambilla-shootings-court-transcript/103271920>.
[8] Nguyen (n 4).

domestic sphere, showing the harmful, real-world consequences misinformation can manufacture.[9]

But misinformation and disinformation can have more covert consequences for a State's information environment, in the form of influence operations. A recent example of this is the YouTube influence campaign promoting pro-China, anti-US narratives. Operation 'Shadow-play', as it has been called by the Australian Strategic Policy Institute (ASPI) has a strategic goal of shifting the views of those in English speaking countries about the roles of China and the US's roles in 'international politics, the global economy and strategic technology competition.'[10] To do so, the campaign uses artificial intelligence to create voice-overs on videos, which promote portrayals of China's efforts to win the 'US-China technology war' and pushes a pro-Huawei, anti-Apple narrative. The campaign has amassed a large global audience, with their agenda spanning across 30 YouTube channels, with 4,500 videos accumulating over 120 million views and 730,000 subscribers.[11] According to ASPI:

> "The campaign focuses on promoting six narratives. Two of the most dominant narratives are that China is 'winning' in crucial areas of global competition: first, in the 'US–China tech war' and, second, in the competition for rare earths and critical minerals.[2] Other key narratives express that the US is headed for collapse and that its alliance partnerships are fracturing, that China and Russia are responsible, capable players in geopolitics, that the US dollar and the US economy are weak, and that China is highly capable and trusted to deliver massive infrastructure projects."

Whilst the operator of the influence campaign has not been verified, analysis suggests that it is likely to be a commercial actor following some State direction.[12]

This case study highlights a number of causes for concern. It highlights the potential that social media sites such as YouTube, further manipulated via the use of artificial intelligence, holds for the ability to influence public opinion on topics of global significance through the use of

[9] Melissa de Zwart and Sam Hodge, 'Australia domestic terrorism and the sovereign citizen movement' (2022) *Australian National University National Security College* 19, 20.
[10] Jacinta Keast, 'Shadow Play – A pro-China technology and anti-US influence operation thrives on YouTube' *Australian Strategic Policy Institute* (online, 14 December 2023) <https://www.aspi.org.au/report/shadow-play>.
[11] Ibid.
[12] Ibid.

misinformation and disinformation. It also demonstrates how inauthentic actors are able to push content originating from genuine actors to the side, making it difficult for users to discern the credibility of claims made online,[13] and how they are able to gain traction in the wider information environment.[14] Ultimately, such operations can serve to undermine the truth and upend elections through the use of misinformation. In other words, they are able to manipulate real-world events by shaping narratives and opinions, radicalising individuals, and destabilising society by undermining democratic processes.[15] This creates serious threats to the national security landscape.[16]

B Introduction

This project commenced as a consideration of 'information warfare' as a key emerging trend in national security. During the course of this project, however, due to the COVID-19 global pandemic and major upheavals in the global security context, the emphasis of the project had to also shift to encompass to the broader considerations of misinformation and disinformation as key strategies of information warfare. This shift reflected the ongoing uncertainty regarding both the scope of terminology such as 'information warfare' and where the legal boundaries lie and strategically where Australia might like them to be.

This Report will first identify what the defining characteristics of 'information warfare' are and how it is currently applied in Australia. It will then identify the relevant domestic and international laws that apply to its characterisation and use. This information may then be used as the basis of information sharing with Five Eyes partners, to assess the common understanding and application of the legal boundaries of Information warfare.

This is important because the Defence Strategic Review stated that "more attention and resources should be devoted to crucial future-focused joint capabilities such as information

[13] David Tuffley, 'An AI-driven influence operation is spreading pro-China propaganda across YouTube' *The Conversation* (online, 19 December 2023) <https://theconversation.com/an-ai-driven-influence-operation-is-spreading-pro-china-propaganda-across-youtube-219962?utm_medium=email&utm_campaign=Latest%20from%20The%20Conversation%20for%20December%2020%202023%20-%202831928692&utm_content=Latest%20from%20The%20Conversation%20for%20December%2020%202023%20-%202831928692+CID_c2d51a9e64c9ba21ee1a53889fd881c7&utm_source=campaign_monitor&utm_term=An%20AI-driven%20influence%20operation%20is%20spreading%20pro-China%20propaganda%20across%20YouTube>.
[14] Keast (n 10).
[15] Tuffley (n 13).
[16] de Zwart and Hodge (n 9) 28.

warfare, cyber capabilities" and "electronic warfare."[17] This project will make a strong contribution to understanding the complexity of the information warfare domain, its ever shifting and evolving nature and the compelling need for multistate responses to the problems that it creates. In Australia, responsibility for Information Warfare is currently vested in Joint Capabilities Group. [18]

It is noted that the change in terminology also reflects the recognition that the previous perception was that information operations or 'warfare' would only occur in contexts of (or just below the threshold of) warfare. It is clear that the 24/7 news cycle and the persistent influence of social media platforms has forced a reconsideration of this terminology. Operations in the information environment are now used at every phase, so this necessitates an evolutionary approach to identifying and mitigating the effects of information operations. In this report the term 'information warfare' will be used as the catch all term, except where it has been considered appropriate to adopt the more nuanced term 'information operation'.

C What is Information Warfare?

Information warfare (IW) is an umbrella term for strategic conduct that is aimed at manipulating an adversary's information environment. In the contemporary digital era, IW is typically conducted through cyber-attacks and social cyber-attacks. Understanding the scope of these actions and how they can constitute 'information warfare' is pivotal for identifying the most relevant law that is applicable to information warfare in an Australian context.

The Australian Department of Defence defines IW as: "The contest for the provision and assurance of information to support friendly decision-making, whilst denying and degrading that of adversaries".[19] It explains that, "a key objective of information warfare is to achieve information superiority over an adversary and therefore gain an advantage which can be exploited in the traditional air, land and sea domains".[20] While indicative of the circumstances

[17] Australian Government, "National Defence: Defence Strategic Review" <https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review> (2023) 51.
[18] Edward Morgan and Marcus Thompson 'Building Allied Interoperability in the Indo-Pacific Region' Discussion Paper 3, Information Warfare: An Emergent Australian Defence Force Capability, Center for Strategic and International Studies, October 2018.
[19] Department of Defence. Information Warfare Division. <https://defence.gov.au/jcg/iwd.asp>.
[20] Department of Defence. Information Warfare Division. <https://defence.gov.au/jcg/iwd.asp>.

and domains in which IW occurs, the definition must be unpacked to delineate the core components of IW in order to understand the most relevant law.

- We need to know *who* engages in IW to determine what laws are applicable to the actors involved.
- We need to know *where* IW occurs to be able to identify law that pertains to those arenas.
- We need to know *why* IW occurs to identify law that could reduce incentives for IW.
- We need to know *how* IW is conducted to identify law that could enable or constrain offensive and defensive IW actions.
- We need to know *when* IW is conducted to identify when relevant law applies.

Combined, these lines of inquiry allow us to discern *what* constitutes information warfare in a way that enables identification of applicable law.

1. *Actors: who conducts information warfare and against whom?*

Non-State and State actors engage in IW.[21] However, within a military context, at least one party involved in information warfare is typically a State or is acting on behalf of a State.

Non-State actors that are sponsored by States to engage in offensive information operations are termed 'State-sponsored'[22] and can serve as State proxies. For example, the Internet Research Agency conducted information operations against the United States on behalf of the Russian government.[23]

Types of non-State actors that can engage in IW include terrorist organisations, criminal entities, non-governmental organisations, ideological extremists (that are otherwise not proscribed as terrorists), and hacktivists.[24] For example, ISIS regularly deployed propaganda

[21] Daniel Ventre, *Information Warfare* (John Wiley & Sons, 2016).
[22] Savvas Zannettou et al, 'Characterizing the use of images in state-sponsored information warfare operations by Russian trolls on twitter' (2020) 40 in *Proceedings of the International AAAI Conference on Web and Social Media* 774, 774.
[23] Robert Mueller 'Report on the Investigation into Russian Interferences in the 2016 Presidential Election' *US Department of Justice* (Washington D.C, March 2019) 4.
[24] Dorothy Denning,'Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy' in John Arquilla and David Ronfeldt (eds) *Networks and netwars: The future of terror, crime, and militancy* (RAND Corporation, 2001) 239.

to recruit, radicalise, and terrorise.[25] Greenpeace has manipulated information environments as part of a "strategic response" to climate change,[26] Cambridge Analytica engaged in psychological operations, data theft, and disinformation,[27] and the Syrian Electronic Army has hacked human rights' groups websites to advance its pro-regime agenda.[28]

Theoretically, anyone can perpetrate or be a target of IW since it is not "military-specific",[29] but to constitute 'warfare', operations must be pitched at a strategic scale and be undertaken for a strategic and/or political purpose (see 'Aims').

2. Aims: why is information warfare conducted?

The general objective of IW is to achieve a political goal.[30] It is intended to accomplish or maintain a strategic "competitive advantage".[31] IW can therefore be offensive, defensive, or both.[32] It can be conducted to defend and protect one's own information environment, or attack and manipulate an opponent's information environment.

The primary goals of information warfare are to:

- Influence public opinion[33]
- Undermine an adversary's material capabilities[34]
- Disrupt an adversary's communications infrastructure[35]
- Protect one's own information infrastructure[36]

[25] Alexandra Siegel and Joshua Tucker, 'The Islamic State's information warfare: Measuring the success of ISIS's online strategy' (2018) 17(2) *Journal of language and politic*s 258.
[26] Brad MacKay and Iain Munro 'Information Warfare and New Organizational Landscapes: An Inquiry into the ExxonMobil–Greenpeace Dispute over Climate Change' (2012) 33(11) *Organization Studies*, 1508.
[27] Vian Bakir, 'Psychological operations in digital political campaigns: Assessing Cambridge Analytica's psychographic profiling and targeting' (2020) 5, *Frontiers in Communication* 67.
[28] Mike Chapple and David Seidl, *Cyberwarfare: Information operations in a connected world* (Jones & Bartlett Learning, 2021) 43.
[29] Mariarosaria Taddeo, 'Information warfare: A philosophical perspective' (2012) 25 *Philosophy & Technology*, 112.
[30] Yevgeniy Golovchenko, Mareike Hartmann and Rebecca Adler-Nissen 'State, media and civil society in the information warfare over Ukraine: citizen curators of digital disinformation' (2018) 94(5) *International Affairs*, 975.
[31] Catherine Theohary 'Information warfare: Issues for congress' (2018) *Congressional Research Service*, 1.
[32] Dorothy Denning, *Information warfare and security* (Addison-Wesley, 1999); Brajendra Panda and Joseph Giordano 'Defensive information warfare' (1999) 42(7) *Communications of the ACM*, 30, 30-32.
[33] John Arquilla and David Ronfeldt, *Networks and netwars: The future of terror, crime, and militancy* (Rand Corporation 2001); Tiziana Terranova, 'Futurepublic: On information warfare, bio-racism and hegemony as noopolitics' (2007) 24(3) *Theory, Culture & Society*, 125.
[34] Patrick Blannin, Modelling Information Warfare (2021) 20(3) *Journal of Information Warfare*, 90.
[35] Carlo Kopp, 'Shannon, hypergames and information warfare' (2003) 2(2) *Journal of Information Warfare*, 108.
[36] Ibid.

- Support allies' decision-making[37]

As these goals indicate, IW can be directed at hard and soft information targets. Soft targets are ideational and involve influencing populations, whereas hard targets are material and involve direct damage to and/or penetration of information systems. Some commentators refer to these as 'cognitive' and 'physical' domains of information warfare.[38]

3. Arenas: where is information warfare conducted?

IW is conducted in information environments. Such environments are multidimensional and dynamic, and these nuances are captured in Robert Condray and Marc J. Romanych's definition of the information environment as:

> … a construct based upon the idea that the existence and proliferation of information and information systems creates a distinct operating dimension or environment. As a combination of tangible (physical information systems and networks) and intangible elements (information and decision-making), the information environment is both a resource for military operations and a medium in which armed forces operate.[39]

As this definition highlights, information environments are constituted by a combination of tangible and intangible information elements. Some environments that serve as sites of information warfare are therefore ideational and are engaged with to exert cognitive influence (e.g. social media), whereas others (e.g. cyber infrastructure) are physical and are engaged in to exert physical damage.

[37] Department of Defence. Information Warfare Division – Joint Capabilities Group. <https://defence.gov.au/jcg/iwd.asp>; Edward Morgan and Marcus Thompson *Information Warfare: An Emergent Australian Defence Force Capability*, Center for Strategic & International Studies (online, 4 October 2018).
[38] Robert Condray and Marc Romanych, *Mapping the Information Environment* (2005) *IO Sphere: Joint Information Operations Center*, 7.
[39] Ibid.

4. Primary Sites of Information Warfare

- Social Media: information operations can be conducted on social media platforms to spread disinformation and influence perceptions.[40] As Zannettou and colleagues describe it, "[s]ocial networks have become a battlefield for *information warfare*, with different entities attempting to disseminate content to achieve strategic goals, push agendas, or fight ideological battles".[41]

- News Media: news media can also be used to spread disinformation and propaganda to influence public opinion by promoting biased perspectives and narratives.[42]

- Online discussion boards: online forums and discussion boards can be used to spread propaganda, engage in disinformation campaigns, and sow discord among different groups.[43]

- Elections: elections are increasingly targeted by information warfare operations, which can involve the spread of false information, the use of social media bots and trolls, and other tactics aimed at influencing the outcome of an election.[44]

- Cyber infrastructure: cyber networks and information infrastructure, such as transportation systems, financial networks, and databases can be targeted by cyber-attacks.[45]

Conceptualising these different information spaces as sites of information operations allows us to assess the law that applies to these spaces in a context of IW. For example, since political campaigns and elections can be a site of information operations, law pertaining to political

[40] Jarred Prier, 'Commanding the trend: Social media as information warfare' (2017) 11(4) *Strategic Studies Quarterly*, 50-85.
[41] Zannettou (n 22).
[42] Rosanna Guadagno and Karen Guttieri, 'Fake news and information warfare: An examination of the political and psychological processes from the digital sphere to the real world' in *Research anthology on fake news, political warfare, and combatting the spread of misinformation* (IGI Global, 2020) 218-242.
[43] Martin Innes et al, 'Digital (Dis)information Operations and Misinformation Campaigns' in (William Housley et al (eds) *The SAGE Handbook of Digital Society* (SAGE Publications Ltd, 2023) 458-479.
[44] Melissa-Ellen Dowling, 'Cyber information operations: Cambridge Analytica's challenge to democratic legitimacy' (2022) 7(2) *Journal of Cyber Policy*, 230; Martin Innes et al, 'The normalisation and domestication of digital disinformation: on the alignment and consequences of far-right and Russian State (dis) information operations and campaigns in Europe' (2021) 6(1) *Journal of Cyber Policy*, 31.
[45] See Javier Lopez, Roberto Setola and Stephen Wolthusen, (eds) *Critical Infrastructure Protection: Advances in Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense* (Springer, 2012).

campaigning may be relevant for IW as a means of mitigating information warfare or, conversely, finding gaps in the law to enable it.

5. *Actions: how is information warfare conducted in the digital era?*

Social cyber-attacks: According to NATO, social cyber-attacks involve "creating in people's minds a specific image of the world, consistent with the goals of the information warfare".[46] Such attacks are used when IW aims to influence public opinion and/or influence perceptions. 'Attacks' take place in the digital public sphere consisting of discussion boards, social media, and news media.

Often, social cyber-attacks are conducted covertly using disinformation – "the deliberate creation and/or sharing of false information with the intention to deceive and mislead audiences".[47] Common techniques include astroturfing, band wagoning, bots, filter bubbles, forgery (including deep fakes), leaking, malign rhetoric, manipulation, misappropriation, satire and parody, sock puppets, and trolling.

Disinformation scholar Thomas Rid highlights the way in which disinformation is used to influence public perceptions. He explains how, "political passions are inflamed online in order to drive wedges into existing cracks in liberal democracies; perpetrators sow doubt and deny malicious activity in public, while covertly ramping it up behind the scenes".[48] Law pertaining to publishing and circulating disinformation is therefore relevant for an IW context, as is law regarding election advertising and political campaigning.

Cyber-Attacks: information can be acquired or damaged via cyber-attacks. Common techniques include malware, phishing, SQL injection attacks, cross-site scripting (XSS), denial of service (DoS), session hijacking, and credential reuse.[49] The cyber attribution problem, wherein anonymity online often shields cyber attackers from being identified and held to account, complicates the role of law in mitigating cyber warfare, yet, as this report identifies,

[46] NATO, 'Media - (Dis)Information – Security' available at: <https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf>.
[47] Government Communication Service UK, *RESIST 2: Counter-Disinformation Toolkit*, available at: <https://gcs.civilservice.gov.uk/wp-content/uploads/2021/11/RESIST-2-counter-disinformation-toolkit.pdf> 8.
[48] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (Macmillan, 2020) 6.
[49] Ioannis Agrafiotis et al, 'A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate' (2018) 4(1) *Journal of Cybersecurity*, 1; Rapid7, *Common Types of Cybersecurity Attacks* (online, 2023) available at <https://www.rapid7.com/fundamentals/types-of-attacks/>.

legislation aimed at protecting Australia's critical information infrastructure exists, along with law regulating data and privacy to protect information.

6. Activation: when is information warfare conducted?

Unlike conventional warfare, IW can occur during any stage of conflict – even during times of peace.[50] This means that the breadth of applicable law is vast and is not confined to use during hot conflict contexts.

7. What constitutes information warfare?

These five components – actors, aims, arenas, actions, and activation – outline *what* constitutes IW for the purpose of identifying applicable law.

- Actors: IW can manifest asymmetrically and be initiated by both non-State and State actors alike.
- Aims: The overarching objectives of IW are to weaken an adversary's information space or bolster one's own information space.
- Arenas: IW occurs in tangible and intangible information environments.
- Actions: The tactics and techniques employed in IW often involve covert social cyber-attacks that seek to manipulate public opinion and covert cyber-attacks that cause tangible physical damage.
- Activation: It is worth noting that IW need not be limited to times of hot conflict and can be employed during periods of peace as well.

Law pertaining to warfare, privacy, data, foreign interference, elections, political campaigning, and disinformation are therefore potentially relevant and applicable to Australian information warfare scenarios.

[50] Ventre (n 21); Martin Libicki, *What is information warfare?* (1995) National Defense, University Washington D.C. available at <https://apps.dtic.mil/sti/citations/ADA367662>.

D Current applications of IW in Australia

"Cyber-warfare (and other 'grey-zone' operations) are central to the conduct of political and information warfare. As such, cyber warfare was established as a warfighting 'domain' within Defence in 2019."[51]

1. Domestic Laws for Information Warfare and Operations

Dependent on the approach taken to categorisation of law, there are extremely few laws directly focused on the issue of information operations or information warfare. This is despite the matter being an area of security concern for Australia. This Section will examine domestic laws that 'directly' and 'indirectly' capture conduct that falls under the umbrella of information warfare or operations. While this Section will not identify every possible law that may be captured, it will:

- examine laws that have been introduced in recent times to protect Australia's national security from threats associated with foreign interference;
- explore some of the mechanisms being introduced to protect critical infrastructure from foreign threats;
- sample a small but impactful segment of Federal criminal law that applies to conduct that would be considered a threat to national security;
- touch on recent industry led steps to regulate certain conduct on digital platforms; and
- consider how existing instruments with broad or economy wide foci can be directed to the risks that emerge in connection with information operations and warfare.

(a) Direct

There are several instruments that can be applied directly to conduct that falls within what can be categorised as 'information warfare' or 'information operations'. While this section will proceed through a survey of Australian laws that could be applied, it is clear that there are no overtly applicable legislative instruments that have been introduced to exclusively address information operations or warfare (ie there is no prohibition on engaging in information warfare). Despite this, this section will now proceed to survey Australian legislation that can

[51] Major General Susan Coyle, Head of Information Warfare, Department of Defence, *Committee Hansard*, 25 June 2021, p. 9, cited in Inquiry into the Department of Defence Annual Report 2019-20 November 2021, Commonwealth of Australia 2021, 3.2.

be applied to conduct that falls under the umbrella of 'information warfare' or 'information operations' or preventing conduct that may be captured.

(i) Foreign Influence Transparency Scheme

The Foreign Influence Transparency Scheme ('FITS') commenced operation in December 2018 following the passage of the *Foreign Influence Transparency Scheme Act 2018* (Cth). The law has a stated aim of using registration of persons who 'undertake certain activities on behalf of foreign government[s] and other foreign principals' for the purpose of improving 'transparency' of the activities of the registered persons.[52] The underlying concept behind the FITS is that the registration of foreign interests and representations allows for greater awareness of when a foreign entity or State is having its interests represented or promoted.[53]

How does FITS operate?

FITS is a regime that is reliant upon individuals self-registering with the Secretary of the Attorney-General's department when they undertake registrable activities in relation to, or enter into a registerable arrangement with, a foreign principal.[54] Once an individual registers with the Secretary, the registration is entered on to the FITS register which is publicly accessible. Public information includes the name of the registered person or entity, the name of the foreign principal, a description of the registerable activities and other information as required by the FITS regulations.[55]

Failure to apply for registration once being captured by the regime is an offence under the *Foreign Influence Transparency Scheme Act 2018* with the maximum penalty being five years imprisonment.[56]

What does FITS apply to?

[52] *Foreign Influence Transparency Scheme Act 2018* (Cth) s 3.
[53] Explanatory Memorandum, Foreign Influence Transparency Scheme Bill 2017 (Cth) [2] – [5].
[54] *Foreign Influence Transparency Scheme Act* (n 52) s 18(1).
[55] Ibid s 43(1).
[56] Ibid s 57(1)

FITS captures persons (whether individuals or corporations) engaging in registerable activities on behalf of foreign principals. 'Registerable activities' are broadly listed to include conduct such:[57]

- parliamentary lobbying
- general political lobbying
- communications activities
- disbursement activities
- activities undertaken by former Cabinet Ministers on behalf of a foreign principal
- activities undertaken by certain classes of recent public office holders on behalf of a foreign principal

The FITS also includes a range of exemptions to the regime, including for diplomatic and consular activities, provision of legal advice, participation in industry representative bodies, and involvement in charities, amongst other exceptions.[58]

Relevance to IW/IO

While this law does not directly address the conduct of information operations or warfare, it goes some way to increasing the resources an individual may be able to call upon when engaged in business activities so as to identify when they are being subjected to foreign influences which in some cases may amount to information operations, or at least form part of a larger operation targeting Australia. With corporate Australia being heavily involved in Australian Government operations and systems, transparency associated with a business or individual's activities and international connections can allow for comprehensive due diligence assessments to be undertaken which may ultimately assist in identifying involvement in foreign interference activities or information operations.

(ii) Security of Critical Infrastructure

The Security of Critical Infrastructure ('SOCI') regime was introduced into Australia through the *Security of Critical Infrastructure Act 2018* (Cth). The regime was originally introduced to

[57] Ibid ss 20 – 23.
[58] Ibid ss 24 – 30.

'strengthen the [Australian] Government's capacity to manage the ***national security*** risks of espionage, sabotage and coercion arising from foreign involvement in Australia's critical infrastructure' (emphasis in original).[59] In introducing the SOCI regime, the Australian Government recognised critical infrastructure's importance as an essential element of the operation of the Australian society and economy. Further, the Australian Government recognised that foreign involvement in critical infrastructure is also important to ensure Australia remains an attractive destination for foreign investment. Since its introduction in 2018, the SOCI Act has been amended several times, with the most significant of these being in 2022.

How does SOCI operate?

SOCI operates by deeming 11 different sectors (four prior to 2022 amendments) to be critical infrastructure sectors. It then captures classes of critical infrastructure sector assets by their relationship with the broader sector. Broadly, SOCI operates by requiring:

- there to be a register of information related to critical infrastructure assets;
- responsible entities for some of those assets to implement critical infrastructure risk management programs;
- the notification of cyber security incidents to the Australian Government; and
- enhanced cyber security obligations on some systems of national significance.

The SOCI laws also grant powers to the Australian Government to direct the entities responsible for some assets to do certain things or provide certain information.[60] Overall, for the operators of the critical infrastructure assets, the SOCI regime imposes significant compliance obligations in order to ensure the Australian Government can remain confident that those assets are protected and capable of providing services to the wider Australian community. SOCI does not apply equally to all in the critical infrastructure sectors and those owning or operating critical infrastructure assets. Separate statutory rules impact the precise obligations that apply to asset owners and operators.[61] The *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* require certain critical infrastructure asset owners or operators to prepare risk management programs to mitigate

[59] Explanatory Memorandum, Security of Critical Infrastructure Bill 2017 (Cth).
[60] *Security of Critical Infrastructure Act 2018* (Cth) s 4.
[61] See *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023*

against harms that could arise in connection with their assets. These risk management plans must be developed by reference to specified Australian Standards, and guidelines prepared by government agencies including the Australian Signals Directorate and Australian Energy Market Operator.[62]

What does the SOCI apply to?

The SOCI Act specifies 11 sectors that are deemed to be 'critical infrastructure sectors'. These 11 sectors are:[63]

- the communications sector;
- the data storage or processing sector;
- the financial services and markets sector;
- the water and sewerage sector;
- the energy sector;
- the health care and medical sector;
- the higher education and research sector;
- the food and grocery sector;
- the transport sector;
- the space technology sector;
- the defence industry sector.

There is no comprehensive list of critical infrastructure assets, with the definition contained within the SOCI Act deeming anything that 'is an asset that relates to a critical infrastructure sector' to be 'critical infrastructure assets'.[64]

The SOCI regime will apply to the owners or operators within these sectors and that operate these classes of asset.

[62] Ibid reg 8(4).
[63] *Security of Critical Infrastructure Act* (n 60) s 8D.
[64] Ibid s 8E(1); Cyber and Infrastructure Security Centre, 'New Critical Infrastructure (CI) assets captured under the SOCI Act' *Department of Home Affairs* (5 April 2022) <https://www.cisc.gov.au/legislative-information-and-reforms/critical-infrastructure/assets-captured-under-the-bill>.

Further to the above, operators of declared 'Systems of National Significance' are subject to enhanced cyber security obligations due to the interconnected, interdependent and essential nature of those assets/systems.[65]

The provisions of the SOCI regime apply to 'responsible entities'; those with ultimate operational responsibility for a critical asset, and 'direct interest holders' (those with an ownership interest in an asset of more than 10% or that are in a position to influence the control of the asset (either directly or indirectly)).[66]

Relevance to IO/IW

As raised above, the SOCI Act was introduced to specifically address the risk of 'espionage, sabotage and coercion arising from foreign involvement in Australia's critical infrastructure'. Given the importance of the critical infrastructure sector and assets captured by the legislation, the Australian Government – through SOCI – is seeking to reduce the risk of these sectors and assets being negatively impacted through conduct that could be considered information operations or warfare. This includes direct cyber-attacks on infrastructure that has an immediate impact on the operation of the assets (and the Australian population as a consequence), intrusions into systems that may not have an immediately apparent direct impact on the population, or other influence operations that ultimately cause a detriment to Australia. The focus on cyber security risk mitigation and planning is the key aspect of relevance for the SOCI regime and information operations and warfare. While attacks would likely be focused on infiltration and hostile actions as opposed to influence activities, the hardening of computer systems of critical infrastructure also strengthens Australia's broader national security and resiliency settings.

(iii) National Security Laws

There are also a range of laws that have been crafted in respect of national security matters in the criminal context. Australian laws on subjects including terrorism, espionage, foreign threats and influence have rapidly grown since the events of September 11 2001. Legal commentators

[65] *Security of Critical Infrastructure Act* (n 60) pt 2C, s 52B.
[66] Ibid ss 6, 12L.

have described Australia as having a 'hyper-legislation' approach to these areas.[67] Hardy and Williams observed that there have been 92 distinct 'laws' passed by the Australian Parliament between September 2001 and September 2021 directed at terrorism and related matters.[68] While many of these laws are focused exclusively on what may be conceptualised as being 'traditional' terrorist activities, manifested through physical attacks on the general population, some can be directed at conduct that may be considered to be information warfare or operations.

While Australia has a significant volume of criminal laws at the Federal and State levels. This section will consider several of the more recent interventions into the Federal *Criminal Code* after substantial amendments that were introduced in 2018 with the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth) ('*NSLA (Espionage and Foreign Interference) Act*'). This instrument was comprehensive, introducing a range of new offences and amending others to ensure they could be employed to protect Australia against 'foreign adversaries working against Australia's interests through a variety of means'.[69]

(iv) Espionage

The *NSLA (Espionage and Foreign Interference) Act* sought to improve on Australia's existing federal prohibitions on espionage laws for the 'modern threat environment'.[70] From 2018, the Australian Criminal Code now contains a suite of prohibitions on espionage activities. The laws are intentionally broad, capturing dealings with information or articles that have security classifications or concern Australia's national security,[71] or any information or articles where the dealing with the information could prejudice Australia's national security and that information is provided to foreign principals.[72] The laws also expressly and separately capture conduct that is carried out 'on behalf of or in collaboration with, a foreign principal' or conduct that is otherwise 'directed, funded or supervised by a foreign principle' or someone acting on their behalf.[73] The Australian Government also sought to expressly criminalise the soliciting

[67] Keiren Hardy and George Williams, 'Two Decades of Australian Counterterrorism Laws' (2022) 46(1) *Melbourne University Law Review* 34, 36-44, citing Kent Roach, *The 9/11 Effect: Comparative Counter-Terrorism* (Cambridge University Press, 2011) 309.
[68] Hardy and Williams (n 67) 44.
[69] Explanatory Memorandum, National Security Legislation Amendments (Espionage and Foreign Interference) Bill 2017 (Cth), 2 [2].
[70] Ibid 26 [127]
[71] See, *Criminal Code Act 1995* (Cth) sch 1 ('*Criminal Code*') ss 91.1(1)(b), 91.1(2)(b).
[72] See ibid 91.2.
[73] Ibid ss 91.8(1)(d), 91.8(2)(d), 91.8(3)(c).

or procuring of an espionage offences, facilitating espionage offences, and the planning or preparation of espionage activities.[74] These laws were described as enabling law enforcement to pursue foreign principals that receive information as well as (with respect to the solicitation, procuring and preparation offences) enable early intervention to prevent 'harmful conduct occurring.'[75]

Penalties for engaging in espionage vary, with the maximum penalties being imprisonment for life.[76]

When considering these offences in the context of information operations and warfare, these are clearly focused on the acquisition of information, rather than the use of information by foreign actors. Despite this, the collection of information can subsequently enable information operations through the identification of vulnerabilities or approaches to operations, making these provisions significant.

(v) Foreign Interference Offences

In 2017 and as part of the *NSLA (Espionage and Foreign Interference) Act* package of laws, the Australian Government introduced a suite of laws intended to target foreign interference activities. The Explanatory Memorandum stated that:

> Currently, Commonwealth criminal law contains no offences targeting conduct undertake by [a] foreign government that falls short of espionage but is intended to harm Australia's national security or influence Australia's political or governmental process.[77]

The content of the *NSLA (Espionage and Foreign Interference) Act* sought to change this, with offences capturing intentional foreign interference, reckless foreign interference, preparation of foreign interference, knowingly and recklessly supporting foreign intelligence agencies, and knowingly or recklessly being funded or funding foreign intelligence agencies.[78]

---

[74] Ibid ss 91.11, 91.12.
[75] Explanatory Memorandum, National Security Legislation Amendments (n 69) 26 [128].
[76] *Criminal Code* (n 71) s 91.1(1).
[77] Explanatory Memorandum, National Security Legislation Amendments (n 69) 26 [130].
[78] *Criminal Code* (n 71) div 92.

The primary foreign interference offence is set around conduct that will:

- Influence a political or governmental process of the Commonwealth or a State or Territory;
- Influence the exercise (whether or not in Australia) of an Australian democratic or political right or duty;
- Support intelligence activities of a foreign principal; or
- Prejudice Australia's national security.[79]

There are further provisions related to the targeting of persons[80] and preparatory actions.[81] The provisions related to foreign intelligence agencies are focused around concepts of knowingly and recklessly supporting the activities. These offences are not linked to an outcome (ie the cooperation does not need to involve an impact).[82]

These provisions are clearly targeted at influence operations (that would fall within the umbrella of information warfare and operations). The Explanatory Memorandum supporting the legislation sets out that the purpose of these offences was to complement the espionage offences by criminalising a range of other harmful conduct undertaken by foreign principals who seek to interfere with Australia's political, governmental or democratic processes, to support their own intelligence activities or to otherwise prejudice Australia's national security.'[83]

(vi) Sabotage

Much like the offences described above, the Australian Government made substantial changes to the provisions of the Criminal Code applicable to sabotage as part of the *NSLA (Espionage and Foreign Interference) Act.* The Australian Government sought to expand the scope of the laws applicable to sabotage to ensure that more than Defence assets would be protected.[84] The laws introduced in 2018 sought to criminalise damage to critical infrastructure where that could

[79] Ibid ss 92.2(1)(c), 92.3(1)(c).
[80] Ibid s 92.2(2).
[81] Ibid s 92.4.
[82] Ibid ss 92.7, 92.8, 92.9, 92.10.
[83] Explanatory Memorandum, National Security Legislation Amendments (n 69) [130].
[84] Ibid [131].

prejudice Australia's national security as well as criminalise the introduction of vulnerabilities into systems that could be exploited in the future.[85]

The new s 82.3 makes it an offence to engage in conduct that causes damage to public infrastructure that the person intends to prejudice Australia's national security or advantage the national security of another nation and the conduct was engaged in on behalf of, or in cooperation with a foreign principal, or was directed, funded or supervised by a foreign principal.[86] A separate offence replaces the 'intention' threshold with a 'recklessness' threshold.[87] Separate offences exist that capture conduct that prejudices national security or advantages other nations' national security but is not connected with a foreign principal.[88]

The separate offence of 'introducing vulnerability with intention as to national security' criminalises intentional or reckless conduct that results in 'an article or thing, or software' that is or is part of public infrastructure becoming vulnerable to misuse, impairment, or access or modification by a person not entitled to do so.[89]

Much like the preceding discussion, these offences can be employed to address conduct that may fall under the umbrella term of information operations, especially those offences associated with the introduction of vulnerabilities into public infrastructure software that can later be exploited.

(vii) Potential Legislation - Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023

Though it is not yet more than a draft bill, it is worth briefly considering the *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023*[90] ('Draft Bill'), how it operates, what it will apply to, and how it is relevant to IW/IO. The Draft Bill was introduced by the Albanese Government in 2023, and proposes to address the growing challenge in combatting misinformation and disinformation and the threat it poses to the 'safety

[85] Ibid.
[86] *Criminal Code* (n 71) s 82.3(1).
[87] Ibid s 82.3.
[88] Ibid s 82.5-6.
[89] Ibid s 82.7-8
[90] Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023 (Cth) *(*'Combatting Misinformation and Disinformation Bill').

and wellbeing of Australians, as well as our democracy, society, and economy.'[91] The Draft Bill proposes to amend the *Broadcasting Services Act 1992* (Cth), and consequentially, the:

- *Australian Communications and Media Authority Act 2005* (Cth)*;*
- *Online Safety Act 2021* (Cth)*; and*
- *Telecommunications Act 1997* (Cth)*.*

How does the Draft Bill propose to operate?

The main and significant proposed powers contained within the Draft Bill involve giving the Australian Communications and Media Authority (ACMA) reserve powers to act in the event industry efforts to deal with misinformation and disinformation on digital services are inadequate.[92]

The proposed powers are threefold. ACMA would be able to require digital platform providers to keep records about matters regarding misinformation and disinformation.[93] ACMA could also request that the industries the Draft Bill applies to develop codes of practice regarding combatting misinformation and disinformation on digital platforms (and ACMA could register and enforce those codes of practice).[94] Finally, ACMA could create and enforce an industry standard in the event that a code of practice developed by the industries to which the Draft Bill applies is deemed ineffective in combatting misinformation and disinformation on digital services.[95]

However, ACMA would have no power enabling them to request specific content or posts on digital platform services be removed.[96]

What does the Draft Bill propose to apply to?

[91] Australian Government, *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023 – Fact Sheet* Department of Infrastructure, Transport, Regional Development, Communications and the Arts, 1 ('Draft Bill Fact Sheet').
[92] Combatting Misinformation and Disinformation Bill (n 90) cl 3.
[93] Ibid cls 14-19.
[94] Ibid cls 37-38, 44.
[95] Ibid cl 46-50.
[96] Draft Bill Fact Sheet (n 91) 1.

There are three main components to the Draft Bill that are important to unpack for the purpose of understand what the Draft Bill applies to: the definitions the Draft Bill gives to 'digital service,' 'misinformation' and 'disinformation'.

The Draft Bill defines **digital service** as a service that:

> (a) delivers content to persons having equipment appropriate for receiving that content, where the delivery of the service is by means of an internet carriage service; or
>
> (b) allows end-users to access content using an internet carriage service;
>
> where:
>
> (c) the service is provided to the public (whether on payment of a fee or otherwise); and
>
> (d) any of the content accessible using the service, or delivered by the service, is accessible to, or delivered to, one or more end-users in Australia;
>
> but does not include a service to the extent to which it is:
>
> (e) a broadcasting service; or
>
> (f) a datacasting service.

The Draft Bill considers that dissemination of content using a digital service is **misinformation** on the digital service if:

> (a) the content contains information that is false, misleading or deceptive; and
>
> (b) the content is not excluded content for misinformation purposes; and
>
> (c) the content is provided on the digital service to one or more end-users in Australia; and
>
> (d) the provision of the content on the digital service is reasonably likely to cause or contribute to serious harm.[97]

The Draft Bill considers that dissemination of content using a digital service is **disinformation** on the digital service if:

[97] Combatting Misinformation and Disinformation Bill (n 90) sub cl 7(1).

(a) the content contains information that is false, misleading or deceptive; and
(b) the content is not excluded content for misinformation purposes; and
(c) the content is provided on the digital service to one or more end-users in Australia; and
(d) the provision of the content on the digital service is reasonably likely to cause or contribute to serious harm; and
(e) the person disseminating, or causing the dissemination of, the content intends that the content deceive another person.[98]

A note is included under sub clause 7(2), stating that '[d]isinformation includes disinformation by or on behalf of a foreign power.'

For the purposes of the Draft Bill, 'serious harm' is harm that affects a significant portion of the Australian population, economy or environment, or undermines the integrity of an Australian democratic process.'[99]

The powers of ACMA contained in the Draft Bill are proposed to apply to digital platform services that are accessible in Australia, such as social media, search engines, instant messaging services (though not private messages), news aggregators and podcasting services.[100]

Potential Relevance of the Draft Bill to IW/IO.

The Draft Bill does not directly address the conduct of information operations or warfare, but it does increase the ability of ACMA to direct and require digital service providers to better deal with misinformation and disinformation disseminated through their platforms. Of particular relevance to IW/IO is a type of harm outlined in section 2.1.2 of the Guidance Note to the Bill ('Guidance Note'). The Guidance Note specifies one type of harm that could be caused by misinformation and/or disinformation on digital platforms, being '[h]arm to the integrity of Australian democratic processes or of Commonwealth, State, Territory or local government institutions,' caused by '[m]isinformation undermining the impartiality of an

[98] Ibid sub cl 7(2).
[99] Draft Bill Fact Sheet (n 91) 1.
[100] Ibid 2.

Australian electoral management body ahead of an election or a referendum.'[101] This points to one object of the Draft Bill being to attempt to combat misinformation and disinformation spread on digital services such as social media which is intended to influence public opinion in elections, which in some cases may amount to information operations.

Unsurprisingly this Draft Bill has attracted significant opposition from various groups as an imposition on freedom of communication.[102] Whilst there is some consensus on the need to address the spread of misinformation and disinformation via social media, there is little agreement regarding how this may be done. Other suggestions include leaving the responsibility for detection and removal to the media platforms or supporting groups such as Bellingcat to tag information with the provenance of the information.[103]

(viii) Code of Practice on Disinformation and Misinformation

Moving from statutory instruments that are focused on addressing conduct that threatens national security and thereby captures potential information warfare or operations conduct, the Code of Practice on Disinformation and Misinformation ('The Code') is an industry developed document that addresses part of the concerns arising out of the use of digital platforms.[104]

In 2019, the Australian Competition and Consumer Commission ('ACCC') concluded its Digital Platforms Inquiry in which it investigated the role of large social media and technology companies across a range of areas including advertising, consumer data, and journalism.[105] Amongst the recommendations contained in the ACCC's final report was a recommendation for a 'Digital Platforms Code to counter disinformation'.[106] This recommendation was adopted

[101] Australian Government, *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023 – Guidance Note,* Department of Infrastructure, Transport, Regional Development, Communications and the Arts, section 2.1.2.
[102] Australian Human Rights Commission 'Finding balance: combatting misinformation and disinformation without threatening free expression' Submission to the Department of Infrastructure, Transport, Regional Development, Communications and the Arts, 18 August 2023, <https://humanrights.gov.au/our-work/legal/submission/finding-balance-fighting-disinformation-without-threatening-free>.
[103] Charlotte Maher, Separating Fact from Fiction on Social Media in Times of Conflict, Bellingcat, October 26, 2023, https://www.bellingcat.com/resources/how-tos/2023/10/26/separating-fact-from-fiction-on-social-media-in-times-of-conflict/.
[104] Digital Industry Group Inc, *Australian Code of Practice on Disinformation and Misinformation* (22 December 2022) ('*The Code*').
[105] Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, June 2019).
[106] Ibid 22.

by the Federal Government and ultimately led to the creation of the Digital Industry Group Inc ('DIGI'). DIGI subsequently developed The Code.[107]

Unlike the other instruments discussed above, The Code does not have the force of law and industry participants must opt in to comply with The Code. The Code does not specify a means of compliance and as a consequence, the manifestation of its content varies between those industry participants that have opted to comply with The Code. Adopting organisations include Adobe, Apple, Google, Meta, Microsoft, TikTok and Twitter.[108] The Australian Communications and Media Authority's recommended threshold for participation in The Code is 1 million active monthly users in Australia.[109]

The Code has its own definitions of key concepts such as 'disinformation', 'misinformation', and 'harm'.[110]

The Code is structured around several 'objectives' that relate to disinformation and misinformation as follows:

1. Objective 1: Provide safeguards against Harms that may arise from Disinformation and Misinformation.
2. Objective 2: Disrupt advertising and monetisation incentives for Disinformation and Misinformation.
3. Objective 3: Work to ensure the integrity and security of services and products delivered by digital platforms.
4. Objective 4: Empower consumers to make better informed choices of digital content.
5. Objective 5: Improve public awareness of the source of Political Advertising carried on digital platforms.
6. Objective 6: Strengthen public understanding of Disinformation and Misinformation through support of strategic research.
7. Objective 7: Signatories publicise the measures they take to combat Disinformation and Misinformation.

[107] *The Code* (n 104) 2 [1.1].
[108] Digital Industry Group Inc, *2022 Review of The Australian Code of Practice on Disinformation and Misinformation: Response to submissions* (22 December 2022) 3
[109] Ibid.
[110] *The Code* (n 104), 5 [3.2], 6 [3.6] and 6 [3.4] (respectively).

Together, these objectives (along with the explanatory content that accompanies them) are intended to support digital platforms in acting to prevent the spread of disinformation and misinformation on the respective digital platforms. In implementing these objectives, The Code emphasises the importance of 'proportionality' and that measures taken by digital platforms are 'proportionate and relevant to [the] specific context [of content] including the Harm posed by instances of Disinformation and Misinformation.'[111]

Unlike the above discusses statutory instruments that can directly capture conduct that may be considered to fall under the banner of information operations or warfare, The Code is focused on preventing the spread of misinformation and disinformation on digital platforms, ultimately making it a mechanism that can be directed at one of the more common broad-focused manifestations of information operation conduct.

(b) Indirect

While Australia does have a variety of instruments that can be focused directly on conduct or circumstances associated with national security, it also has a number of laws that operate across the entire economy in an intentionally indiscriminate and far-reaching manner. These laws can also be considered in the context of information operations and warfare. This section will now proceed to examine two laws that fit within this category, the *Privacy Act* and the *Australian Consumer Law*.

(i) Privacy Laws

The *Privacy Act 1988* (Cth) is an Australian Federal law that serves several important functions. The most relevant of these roles is how the *Privacy Act* regulates the collection, use, disclosure and storage of 'personal information'.[112]

One of the most significant aspects associated with information warfare and operations is the collection and use of data by malicious actors. A malicious actor may be able to identify a large cache of personal information held by an entity and subsequently undertake a cyber-attack to obtain or interfere with that personal information. This would allow that malicious actor to take

[111] Ibid 19 [6.1].
[112] See generally, *Privacy Act 1988* (Cth) sch 1.

full advantage of the information they have accessed to engage in subsequent operations. This could include influence operations based on the data accessed.

Cyber incidents are becoming a common occurrence in Australia. The Australian Cyber Security Centre reported that for the 2021-22 financial year, there were 76,000 incidents of cyber crime reported in Australia.[113] Further, the Office of the Australian Information Commissioner, responsible for administering the *Privacy Act* and the notifiable data breaches regime it includes, reported 497 data breaches in the six months between July and December 2022. Of these, 70% were attributed to malicious or criminal attacks.[114]

With this background, the obligations within the *Privacy Act* to protect personal information from misuse, interference, loss and unauthorised access, modification or disclosure become more important.[115] While this obligation is principle-based and not prescriptive in nature (allowing for the actual means of compliance to vary between organisations), it can be an important starting point to protecting personal information from malicious actors (both State-based or individuals). If all organisations take appropriate steps to protect their systems and the information they hold from unauthorised cyber intrusions and attack, these systems will become more hardened to intrusions from malicious actors seeking to undertake information operations or preparatory steps for an information operation.

(ii) Consumer Protection

Australia's primary consumer protection instrument, the Australian Consumer Law ('ACL') is contained in the Federal, *Competition and Consumer Act 2010*.[116] These laws cover a wide range of matters including unconscionable conduct, product and service guarantees, prohibitions on unfair practices (including pyramid schemes) and provisions on misleading or deceptive conduct.[117] The prohibitions on misleading or deceptive conduct (contained in s 18 of the ACL) have been utilised across the Australian economy for a wide variety of reasons. The ACCC, the entity responsible for administering the ACL, frequently uses the misleading

[113] Australian Cyber Security Centre, *Annual Cyber Threat Report: July 2021 – June 2022* (Australian Signals Directorate, 4 November 2022) 12.
[114] Office of the Australian Information Commissioner, Notifiable data breaches report July to December 2022 (1 March 2023) https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2022
[115] *Privacy Act 1988* (n 112) sch 1 cl 11.1.
[116] *Competition and Consumer* Act 2010 (Cth) sch 1 ('*Australian Consumer Law*')
[117] See generally, *Australian Consumer Law*.

or deceptive conduct provisions of the ACL to pursue entities for conduct across industry sectors. The only material limitations contained within the prohibition on misleading or deceptive conduct is the requirement that conduct be in trade or commerce.[118]

Recently, the ACCC has commenced proceedings against Meta Platforms Inc (the operator of Facebook) for allegedly misleading or deceptive conduct associated with advertisements it hosted on its platform. The advertisements contained allegedly false celebrity endorsements for investment schemes that the ACCC also allege to be scams.[119] The ACCC are pursuing Meta Platforms as the publisher of these advertisements.[120] Meta is also being pursued through criminal proceedings by one of the individuals in the published advertising campaigns.[121]

This leads to the possibility of these laws being employed by regulators in Australia in a way that would encourage Australian businesses or platforms operating within Australia to limit the sharing of misinformation or disinformation. The versatility of the ACL's prohibitions on misleading or deceptive conduct in this area are yet to be tested, but the recent actions involving the ACCC and Meta Platforms may act as a test case going to the possibility for future applications of the laws to other instances of misinformation and disinformation – potentially including conduct forming part of larger information operations.

2. International Laws affecting information warfare

There is no general prohibition on information warfare or information operations in international law. While not prohibited, and thus permissible,[122] such activities are generally considered to be adversarial psychological manipulation, unfriendly or hostile acts, i.e., conduct which is not contrary to international law but which inflicts a disadvantage, disregard, or discourtesy on another State.[123] While such acts may render relations between States more complex, and may result in unfriendly acts in return, they will not give rise to legal

[118] This limitation arises out of the constitutional limits on the Federal Parliament to enact laws.
[119] Australian Competition and Consumer Commission, 'ACCC takes action over allegedly misleading conduct by meta for publishing scam celebrity crypto ads on Facebook' (Media release, 18 March 2022) https://www.accc.gov.au/media-release/accc-takes-action-over-alleged-misleading-conduct-by-meta-for-publishing-scam-celebrity-crypto-ads-on-facebook; *Australian Competition and Consumer Commission v Meta Platforms, Inc.* [2022] FCA 1062, [1] – [7].
[120] Ibid [7].
[121] Ibid [11] – [19].
[122] *SS 'Lotus' (France v Turkey) (Judgment)* [1927] PCIJ (ser A) No 9, [46].
[123] Tsvetelina van Bentham, Talita Dias and Duncan B Hollis 'Information Operations under International Law' (2023) 55.5 *Vanderbilt Journal of Transnational Law* 1217; Talita Dias 'Limits on Information Operations Under International Law' in Tatiana Jančárkova et al, (eds) (CCDCOE Publications, 2023) 15th International Conference on Cyber Conflict: Meeting Reality NATO, Tallinn.

consequences and do not generally provide a basis for taking countermeasures or self-defence using force.

Information warfare and information operations do not necessarily amount to an internationally wrongful act pursuant to the law of State responsibility, depending on the measure taken and the target of the operation. An internationally wrongful act consists of two elements:

1. A breach of a State's legal obligation through either commission or omission; and
2. The act in question is attributable to the State.

The carrying out of information warfare activities may lead to a violation of specific international law norms, for example, such activities may amount to a violation of the targeted State's sovereignty or breach of the principle of non-intervention. Even in such circumstances, an act of information warfare may not reach the threshold of an internationally wrongful act trigger a response under international law.

(a) Violation of sovereignty

Sovereignty is a primary rule of international law. In the *Island of Palmas* arbitration, the Permanent Court of Arbitration defined sovereignty as follows.

> Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State.[124]

It is generally accepted that the physical penetration of a State's territory without consent amounts to a violation of that State's sovereignty. As such, IW/IO conducted through physical means on another State's territory may constitute a violation of that State's sovereignty or be contrary to the principle of non-intervention. However, it is less clear whether IW/IO conducted by, or attributable to, one State against another State using technological means should also be treated as a violation of sovereignty or breach of the principle of non-intervention. For example, in response to the Russian IO in the context of the 2016 US Presidential election, there was no

[124] *Island of Palmas (United States v Netherlands)* (1928) 2 RIAA 829, 838.

indication from the US that this was viewed to be a violation of international law or internationally wrongful act triggering responses under international law; the IO was referred to as being a breach of international norms rather than a breach of international law.

Engaging in election propaganda is not a violation of international law. Indeed, there is extensive State practice of State's engaging in both truthful and untruthful propaganda during foreign elections.

(b) Interference/intervention

In 1965 in the *Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty*, the United Nations General Assembly declared that:

> …
>
> [n]o State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind.[125]

Further, in 1970, the United Nations General Assembly declared in the *Friendly Relations Declaration* that:

> every State has an inalienable right to choose its political, economic, social and cultural system, without interference in any form by another State.[126]

The 1976 *Declaration on Non-Interference in the Internal Affairs of States* and the 1981 *Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States* outlined prohibited forms of foreign interference. Both include information operations conducted by adversarial States through broadcasting or other media as a prohibited form of

[125] *United Nations Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty*, GA Res 2131 (XX), UN GAOR, 20th sess, 1408th plen. mtg, UN Doc A/Res/20/2131 (21 December 1965).
[126] *United Nations Declaration on the Principles of International Law concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations*, GA Res 2625 (XXV), UN GAOR, 6th Comm, 25th sess, 1883rd plen mtg, Agenda Item 85, UN Doc A/RES/2625 (XXV), annex (24 October 1970) ('Friendly Relations Declaration') para 26.

interference. They denounced 'campaigns of vilification' and 'subversion and defamation',[127] and 'any defamatory campaign, villification or hostile propaganda for the purpose of intervening or interfering in the internal affairs of other States'.[128] However, these General Assembly declarations cannot be considered to be reflective of customary international law and are not a binding source of law.[129]

The International Court of Justice clarified the content of the principle of non-intervention in the case of *Nicaragua*. The Court held that:

> the principle forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States. A prohibited intervention must accordingly be bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State.[130]

For information warfare to amount to unlawful intervention into the internal affairs of another State and thus be an internationally wrongful act, it must:

1. affect a State's *domaine reserve*; and
2. be coercive.

In the absence of one of these elements, the operation will not be unlawful intervention but may be considered to be interference.

---

[127] *Non-interference in the internal affairs of states*, GA Res 31/91, UN GAOR, 31st sess, 98th plen mtg, Supp No 39, UN Doc A/RES/31/39 (14 December 1976)
[128] *Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States*, GA Res 36/103, UN GAOR, 36th sess, 91st plen mtg, UN Doc A/RES/36/103 (9 December 1981) para II(j).
[129] *Charter of the United Nations* art 14.
[130] *Military and Para-military Activities in and against Nicaragua (Nicaragua v United States)* (Judgment) [1986] ICR Rep 14, 107-8 [205].

The *Tallinn Manual 2.0* states that:

> coercion must be distinguished from persuasion, criticism, public diplomacy, propaganda (…) retribution, mere maliciousness, and the like in the sense that, unlike coercion, such activities merely involve either influencing (as distinct from factually compelling) the voluntary actions of the target State or seek no action on the part of the target State at all.[131]

Actions such as espionage, biased media reporting, and the purchase of advertising to sway public opinion, are not coercive and do not amount to a prohibited intervention.

Some scholars have suggested that the threshold of coercion is reached if the use of an information operation is covert, as it deprives the population of the opportunity of forming genuinely informed opinions.[132] However, as Schmitt argues, coercive actions are intended to cause the ***State*** to do 'something', in the sense of taking an action that it would otherwise not have taken or refraining from taking an action that it would otherwise have taken.[133] Disinformation does not amount to a violation of the principle of non-intervention where the will of the State is not subordinated. Discussion during the Workshop indicated that different states may have different attitudes to what may be considered coercive, so even agreement in principle may have differing outcomes in practical approach.

(c) Breach of obligation to exercise due diligence

It has been suggested in scholarship that information operations may be contrary to the obligation to exercise due diligence in certain circumstances.[134] The obligation to exercise due diligence requires that a State take steps to ensure that its territory is not used as the location from which non-State actors or other States launch an IO.

---

[131] Michael Schmitt (Ed) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, (Cambridge University Press, 2017) 318-319.
[132] Henning Lahmann, 'Information Operations and the Question of Illegitimate Interference under International Law' (2020) 53(2) *Israel Law Review* 189, 202.
[133] Michael Schmitt 'Virtual Disenfranchisement: Cyber Election meddling in the grey zones of international law' in Christopher Whyte, A. Trevor Thrall, Brian M. Mazanec (eds) *Information Warfare in the Age of Cyber Conflict* (Routledge, 2020), 186, 197.
[134] Ibid 198-199.

(d) During Armed Conflict

The use of propaganda, misinformation and disinformation are generally considered to be of military value and an acceptable ruse of war provided such measures comply with the applicable rules of international humanitarian law and are not perfidious.[135]

Article 37(2) of *Additional Protocol I* provides that

> Ruses of war are not prohibited. Such ruses are acts which are intended to mislead the adversary or to induce him to act recklessly but which infringe no rule of international law applicable in armed conflict and which are not perfidious because they do not invite the confidence of an adversary with respect to protection under that law. The following are examples of such ruses: the use of camouflage, decoys, mock operations and misinformation.

The 1987 Commentary on Additional Protocol I defines a ruse of war as consisting 'either of inducing an adversary to make a mistake, or of inducing him to commit an imprudent act'.[136] The Commentary includes the circulation of misleading messages as an example of a ruse of war[137] but suggests that ruses must be connected to combat in order to be permissible. This suggests that IW/IOs directed at the civilian population may not be a permissible ruse of war under international humanitarian law unless those civilians are directly participating in hostilities or there is some other connection between the IO and combat.

There is extensive State practice confirming the permissibility of IW/IO in the context of armed conflict and numerous military manuals specifically provide for the use of IW/IO as a ruse of war. Relevant provisions from several military manuals are extracted below.

(i) Australian law of war manual

The Australian law of war manual states that:

---

[135] *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts*, opened for signature 8 June 1977, 1125 UNTS 3 (entered into force 7 December 1978) art 37.
[136] Yves Sandoz et al (eds), *Commentary to the Additional Protocols* (ICRC, 1987), para 1515.
[137] Ibid.

7.2 Ruses of war and the employment of measures necessary for obtaining information about the enemy and the enemy country are permissible. Ruses of war are used to obtain an advantage by misleading the enemy. They are permissible provided they are free from any suspicion of treachery or perfidy. Legitimate ruses include surprises, ambushes, camouflage, decoys, mock operations and misinformation. Psychological operations are also permitted.

8.45 Propaganda for the purposes of inducing enemy combatants to rebel, desert, or surrender is not prohibited. Inducements may take the form of monetary rewards. Although the LOAC sanctions the use of military aircraft and aircrews to deliver propaganda, not all forms of propaganda are lawful. Propaganda that would incite illegal acts of warfare, as for example killing civilians, killing or wounding by treachery or the use of poison or poisonous weapons, is forbidden.[138]

(ii) US law of war manual

The US law of war manual provides that:

5.2.2.1 *Non-Violent Measures That Are Militarily Necessary*. The principle that military operations must not be directed against civilians does not prohibit military operations short of violence that are militarily necessary. For example, such operations may include:

…

- seeking to influence enemy civilians with propaganda.

…..

5.21 Absolute good faith with the enemy must be observed as a rule of conduct. …

…good faith permits:

• ruses of war or other lawful deceptive activities; …

[138] Australia Department of Defence, (2006), *Law of Armed Conflict*, ADDP 06.4, https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/AUS-Manual-Law-of-Armed-Conflict.pdf.

- military information support operations, including propaganda;

…

5.25 RUSES OF WAR AND OTHER LAWFUL DECEPTIONS

Ruses of war are considered permissible. In general, a belligerent may resort to those measures for mystifying or misleading the enemy against which the enemy ought to take measures to protect itself. Apart from ruses of war, certain other deceptions are not prohibited, but may expose combatants employing them to liability as spies and saboteurs.

5.25.1 Definition of Ruses of War. Ruses of war are acts that are intended to mislead an adversary or to induce him to act recklessly, but that do not infringe upon any rule of international law applicable in armed conflict and that are not perfidious because they do not invite the confidence of an adversary with respect to protection under that law.

Ruses of war are methods, resources, and techniques that can be used either to convey false information or deny information to opposing forces. They can include physical, technical, or administrative means, such as electronic warfare measures, flares, smoke, chaff, aerosol material, or dissemination devices.

…

5.25.2 Examples of Ruses. Often, ruses of war operate by misleading the enemy as to the identity, strength, position, or disposition of one's own forces. Ruses of war include, but are not limited to:

….

planting false information in a manner that allows enemy forces to intercept it, such as through the use of

- false messages among one's own forces;
- intensifying or minimizing message traffic; or
- bogus messages, dispatches, or newspapers;

….

5.26.1.2 *Propaganda Generally Permissible*. In general, propaganda is a permissible means of warfare. Propaganda has been disseminated through a variety of

communications media, including printed materials, loudspeakers, radio or television broadcast, aircraft, or the internet. Propaganda is sometimes used with bribery or to support intelligence gathering. Propaganda may be directed at enemy civilians and neutrals.

Propaganda may encourage enemy persons to commit acts that would violate the domestic law of the enemy State. For example, it would be permissible to encourage enemy combatants to defect, desert, or surrender. Similarly, it is generally permissible to encourage insurrection among the enemy civilian population.

5.26.1.3 *Prohibited Types of Propaganda*. Propaganda must not: (1) incite violations of the law of war; nor (2) itself violate a law of war rule.

Propaganda must not incite acts that are prohibited by the law of war. For example, propaganda intended to incite attacks against civilians is prohibited. In certain cases, individuals may be liable for instigating or inciting violations of the law of war.

Propaganda is also prohibited when it would violate other law of war rules. For example, it is specifically prohibited for an Occupying Power to use propaganda that aims at securing voluntary enlistment of protected persons in its armed or auxiliary forces. Similarly, it is prohibited to declare that no quarter will be given, and propaganda in the form of a declaration to the adversary that no quarter will be given would be prohibited. In addition, propaganda would be prohibited if it constituted a measure of intimidation or terrorism against the civilian population, such as the threats of violence whose primary purpose is to spread terror among the civilian population. Similarly, propaganda may not be used to subject a detainee to public curiosity or other humiliating or degrading treatment. Additionally, the delivery of the propaganda should be consistent with other law of war obligations.[139]

(iii) UK law of war manual

The UK law of war manual states that

5.15.1 It is lawful to employ spies; to induce enemy civilians or soldiers to give information, to desert with or without technical equipment, vehicles, or aircraft, to

[139] US Department of Defense, (2016), *Law of War Manual*, https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190.

surrender, rebel, or mutiny; or to give false information to the enemy. It is lawful to incite enemy subjects to rise against the government in power.

5.17 Ruses of war are not prohibited. Such ruses are acts which are intended to mislead an adversary or to induce him to act recklessly but which infringe no rule of international law applicable in armed conflict and which are not perfidious because they do not invite the confidence of the adversary with respect to protection under the law. The following are examples of such ruses: the use of camouflage, decoys, mock operations and misinformation.

5.17.1 Ruses of war are, therefore, measures taken to obtain advantage of the enemy by mystifying or misleading him. They are permissible provided they are not perfidious and do not violate an agreement. Belligerent forces must be constantly on their guard against, and prepared for, legitimate ruses, but they should be able to rely on their adversary's observance of promises and of the law of armed conflict.

5.17.2 Legitimate ruses include: surprises; ambushes; feigning attacks, retreats, or flights; simulating quiet and inactivity; assigning large strong-points to a small force; constructing works or bridges which it is not intended to use; transmitting bogus signal messages and sending bogus despatches and newspapers with a view to their being intercepted by the enemy; making use of the enemy's signals, passwords, radio code signs, and words of command; conducting a false military exercise on the radio while substantial troop movements are taking place on the ground; pretending to communicate with troops or reinforcements which do not exist; moving landmarks; constructing dummy airfields or aircraft; setting up dummy guns or tanks; laying dummy minefields; removing badges from uniforms; issuing to personnel of a single unit uniforms of several units so that prisoners and the dead may give the impression of a much larger force; giving false ground signals to enable airborne personnel or supplies to be dropped in a hostile area, or to induce aircraft to land in a hostile area; and feint attacks to mislead the enemy as to the point of the main attack.[140]

(iv) Canadian law of war manual

The Canadian law of war manual states that:

[140] UK Ministry of Defence, (2004), *The Joint Service Manual of the Law of Armed Conflict*, JSP 383, para 5.15.1, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/27874/JSP3832004Edition.pdf.

1. Ruses of war are measures taken to obtain advantage of the enemy by confusing or misleading them.

2. Ruses of war are more formally defined as acts, which are intended to mislead an adversary or to induce that adversary to act recklessly. Ruses must not infringe any rule of the LOAC. Ruses are lawful if they are not treacherous, perfidious and do not violate any express or tacit agreement.

3. The following are examples of ruses, which are lawful:

…

g. transmitting bogus signal messages, and sending bogus dispatches and newspapers with a view to their being intercepted by the enemy;

h. making use of the enemy's signals, watchwords, wireless code signs, tuning calls and words of command;

…

q. giving false ground signals to enable airborne personnel or supplies to be dropped in a hostile area, or to induce aircraft to land in a hostile area.[141]

(v) New Zealand law of war manual

The New Zealand law of war manual states that:

8.9.1 A ruse of war is a trick intended to confuse or mislead members of the opposing force or cause them to act recklessly. Ruses of war are not prohibited provided they are not perfidious and do not infringe another rule of LOAC.

8.9.2 Members of the NZDF may employ ruses of war provided that:

1. the trick is not intended to lead the opposing force to believe that a protection under LOAC is being relied upon; and
2. the trick is not treacherous, such as the use of the uniforms of the enemy.

[141] Canada, (2001), *Law of Armed Conflict at the Operational and Tactical Level*, para 602 (land), para 705 (air), para 856 (sea), https://usnwc.libguides.com/ld.php?content_id=2998098.

> **8.9.3** A New Zealand force may employ ruses. This includes misleading the enemy as to intended NZDF courses of action, for example constructing dummy positions or formations of vehicles, supplying disinformation as to the time or place of an attack, making use of the enemy's passwords, codes or radio frequencies to find out details of their plans, publishing false news or social media reports, dropping falsely marked maps or notebooks, leading the enemy to believe that NZDF forces are either stronger or weaker than they actually are, or shifting landmarks or road signs or laying dummy minefields.
>
> **8.9.4** To cause an opposing force to cease fighting because they believe that they are outnumbered, outgunned or surrounded, when in fact they are not, is permissible. To call upon them to cease fighting on the grounds that a general armistice had been announced, when it had not, would be treachery.[142]

(vi) German law of war manual

The German law of war manual states that:

> It is permissible to exert political and military influence by spreading – even false – information to undermine the adversary's will to resist and to influence their military discipline (e.g. calling on them to defect, to surrender or to mutiny). It is prohibited to instigate the adversary to commit violations of international law or other general (major) crimes (e.g. manslaughter, bomb attacks, robbery or rape).[143]

It has been suggested that in hybrid warfare in circumstances where civilians are the subject or object of disinformation, such activities may expose a civilian population to grave harm.[144] Potential harms include:

---

[142] New Zealand Defence Force, (2019), *Manual of Armed Forces Law: Law of Armed Conflict*, https://usnwc.libguides.com/ld.php?content_id=47364407.
[143] German Ministry of Defence, *Law of Armed Conflict: Manual, Joint Service Regulation (ZDv) 15/2*, May 2013, para 487 (original emphasis), https://www.bmvg.de/resource/blob/93610/ae27428ce99dfa6bbd8897c269e7d214/b-02-02-10-download-manual-law-of-armed-conflict-data.pdf.
[144] Eian Katz, 'Liar's war: Protecting civilians from disinformation during armed conflict' (2020) 102 (914) *International Review of the Red Cross* 659-682.

- retaliatory violence – fabrications or organised smear campaigns that vilify individuals or groups may foreseeably encourage and legitimate acts of violence against them. This may rise to the level of inducement[145] or incitement[146] under international criminal law;
- distortion of information vital to securing human needs – such activities may disrupt access to and utilisation of services by sowing dissent, undermining the social order, aggravating crises, and discrediting civilian institutions and humanitarian organisations providing relief; and,
- severe mental suffering – disinformation geared towards civilians may arouse extreme fear, grief or other painful emotions, or unsound mental states. It may lead to them developing paranoia or conspiratorial thinking, doubting their continued ability to satisfy their human needs, believing that friends or relatives have been or will be harmed, or developing a reasonable apprehension of death or bodily injury.

While it may be that the existing rules of international humanitarian law do not provide sufficient protection for civilians from IW/IOs in modern conflicts, as the law stands such operations are permitted during armed conflict provided they do not violate any other applicable rules of IHL, such as the rule against perfidy, and are connected to combat.

(e) Responses

International law provides for limited responses by States to a breach of an internationally wrongful act.

Retorsion

An act of retorsion is an unfriendly, but otherwise lawful, measure. The most frequent acts of retorsion are sanctions and expulsion of diplomatic personnel, but may also include 'hack back' or a responsive IO. An act of retorsion is the most common response by a targeted State to an IW/IO.

Countermeasures

[145] *Rome Statute of the International Criminal Court*, opened for signature 17 July 1998, 2187 UNTS 90 (entered into force 1 July 2002) art 25(3)(b) ('*Rome Statute')*.
[146] Ibid art 25(3)(e).

Countermeasures are measures that would be unlawful, either as a breach of treaty or of customary international law, but for the fact that they are taken in response to another State's internationally wrongful act. They must be proportionate to the internationally wrongful act, and are designed to cause the other State to cease its breach or to provide assurances, guarantees, or reparations to remedy the breach. Retaliation or punishment are not permissible purposes for countermeasures. Unless the IW/IO can be classified as an internationally wrongful act and is attributable to the State, countermeasures are not a lawful response.

Necessity

When the essential interests of a State face a grave and imminent peril, States may engage in activities that would otherwise be unlawful where such measures are the only way to defend that essential interest. Under the plea of necessity, the key issue is whether the interest facing grave and imminent peril is an essential interest of the State. The situation must be imminent or ongoing and the threat posed to the essential interest must be extremely serious. IW/IOs will not generally reach the threshold of gravity necessary to trigger necessity.

Self-defence

The use of force may be taken in self-defence pursuant to Article 51 of the *UN Charter* and customary international law in response to an armed attack. It is extremely unlikely that IW/IO would amount to an armed attack triggering the right to self-defence.

E Information Warfare Workshop

[redacted]

[redacted]

[redacted]

2. Conclusions

The key outcome of the Workshop was that there is a strong agreement with respect to the need for more collaborative multilateral discussion on the threat, nature and responses relevant to information warfare. Clearly States will need to reanimate discussion post-COVID to address questions of appropriate responses and measures to information warfare. Whilst there is a strong desire for mutual collaboration, a complicating factor is the range and disparity of civil and defence agencies that are engaged in the regulation and response to information warfare events and activities. This makes co-operation across agencies both domestically and internationally very complex and fragmented. A comparative study of the Five Eyes, with agreement on the core co-ordinating agencies to be involved in this study, would provide the basis for better interagency and international co-operation.

There is consensus that if likeminded States don't resolve these issues, then the core values of democracy will continue to be at stake. States may have differing concepts of what constitutes coercion and interference, but understanding of these differing cultural thresholds is useful. Whilst these thresholds may differ, there is still an underlying agreement that the threat is imminent and pervasive.

There was strong recognition of the constantly changing landscape and context for information warfare, disinformation and misinformation, necessitating an evolving range of responses to remain effective. As the goal posts keep shifting it calls for different legal responses. Current

[redacted].

responses are ineffective and, in some cases, lack public support. However, as AI continues to shape speech, we cannot leave resolution of these issues to the private sector. Whilst there was some recognition of the potential effectiveness of technological (network level) solutions, this does not deal with the broader and pervasive issue of misinformation.

The consensus outcomes were:

1. Articulate elements of the problem: what types of information are we most concerned about, and then prioritise those concerns. Where do we need intervention?
2. Consider issues of intent and incitement: how may this be identified and defined?
3. Address the broader narrative rather than individual pieces of misinformation.
4. Activate citizens to recognise bad actors.
5. Consider how to build up social immunity to these issues.
6. Develop stronger interagency and State collaborative networks and responses.

Above all, there was a strong recognition that this all requires collaborative (Five Eyes) discussion and response. There is a clear capability gap here that demands an urgent response. This was identified as the next step requiring further investigation and action.

Bibliography

A Articles/Books/Reports

Agrafiotis, Ioannis, et al, 'A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate' (2018) 4(1) *Journal of Cybersecurity*, 1

Arquilla, John and David Ronfeldt, *Networks and netwars: The future of terror, crime, and militancy* (Rand Corporation 2001)

Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, June 2019)

Australian Cyber Security Centre, *Annual Cyber Threat Report: July 2021 – June 2022* (Australian Signals Directorate, 4 November 2022)

Bakir, Vian, 'Psychological operations in digital political campaigns: Assessing Cambridge Analytica's psychographic profiling and targeting' (2020) 5, *Frontiers in Communication* 67

Blannin, Patrick, Modelling Information Warfare (2021) 20(3) *Journal of Information Warfare*, 90

Chapple, Mike, and David Seidl, *Cyberwarfare: Information operations in a connected world* (Jones & Bartlett Learning, 2021) 43

Condray, Robert, and Marc Romanych, *Mapping the Information Environment* (2005) *IO Sphere: Joint Information Operations Center*, 7

Cyber and Infrastructure Security Centre, 'New Critical Infrastructure (CI) assets captured under the SOCI Act' *Department of Home Affairs* (5 April 2022) <https://www.cisc.gov.au/legislative-information-and-reforms/critical-infrastructure/assets-captured-under-the-bill>

Denning, Dorothy, 'Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy' in John Arquilla and David Ronfeldt (eds) *Networks and netwars: The future of terror, crime, and militancy* (RAND Corporation, 2001) 239

Denning, Dorothy, *Information warfare and security* (Addison-Wesley, 1999)

de Zwart, Melissa, and Sam Hodge, 'Australia domestic terrorism and the sovereign citizen movement' (2022) *Australian National University National Security College* 19

Dias, Talita ‘Limits on Information Operations Under International Law’ in Tat’ana Jančárkova et al, (eds) (CCDCOE Publications, 2023) 15th International Conference on Cyber Conflict: Meeting Reality NATO, Tallinn

Dowling, Melissa-Ellen, ‘Cyber information operations: Cambridge Analytica’s challenge to democratic legitimacy’ (2022) 7(2) *Journal of Cyber Policy*, 230

Golovchenko, Yevgeniy, Mareike Hartmann and Rebecca Adler-Nissen ‘State, media and civil society in the information warfare over Ukraine: citizen curators of digital disinformation’ (2018) 94(5) *International Affairs*, 975

Guadagno, Rosanna, and Karen Guttieri, ‘Fake news and information warfare: An examination of the political and psychological processes from the digital sphere to the real world’ in *Research anthology on fake news, political warfare, and combatting the spread of misinformation* (IGI Global, 2020) 218-242

Hardy, Keiren, and George Williams, ‘Two Decades of Australian Counterterrorism Laws’ (2022) 46(1) *Melbourne University Law Review* 34

Innes, Martin, et al, ‘Digital (Dis)information Operations and Misinformation Campaigns’ in William Housley et al (eds) *The SAGE Handbook of Digital Society* (SAGE Publications Ltd, 2023) 458-479

Innes, Martin, et al, ‘The normalisation and domestication of digital disinformation: on the alignment and consequences of far-right and Russian State (dis) information operations and campaigns in Europe' (2021) 6(1) *Journal of Cyber Policy*, 31

Katz, Eian, ‘Liar’s war: Protecting civilians from disinformation during armed conflict’ (2020) 102 (914) *International Review of the Red Cross*

Kopp, Carlo, ‘Shannon, hypergames and information warfare’ (2003) 2(2) *Journal of Information Warfare*, 108

Lahmann, Henning, ‘Information Operations and the Question of Illegitimate Interference under International Law’ (2020) 53(2) *Israel Law Review* 189

Libicki, Martin, *What is information warfare?* (1995) National Defense, University Washington D.C. available at <https://apps.dtic.mil/sti/citations/ADA367662>

Lopez, Javier, Roberto Setola and Stephen Wolthusen, (eds.) *Critical Infrastructure Protection: Advances in Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense* (Springer, 2012)

MacKay, Brad, and Iain Munro 'Information Warfare and New Organizational Landscapes: An Inquiry into the ExxonMobil–Greenpeace Dispute over Climate Change' (2012) 33(11) *Organization Studies*, 1508

Morgan, Edward, and Marcus Thompson *Information Warfare: An Emergent Australian Defence Force Capability*, Center for Strategic & International Studies (online, 4 October 2018)

Mueller, Robert, 'Report on the Investigation into Russian Interferences in the 2016 Presidential Election' *US Department of Justice* (Washington D.C, March 2019)

Office of the Australian Information Commissioner, Notifiable data breaches report July to December 2022 (1 March 2023) https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2022

Panda, Brajendra and Joseph Giordano 'Defensive information warfare' (1999) 42(7) *Communications of the ACM*, 30

Prier, Jarred, 'Commanding the trend: Social media as information warfare' (2017) 11(4) *Strategic Studies Quarterly*, 50

Rid, Thomas, *Active Measures: The Secret History of Disinformation and Political Warfare* (Macmillan, 2020) 6

Roach, Kent, *The 9/11 Effect: Comparative Counter-Terrorism* (Cambridge University Press, 2011) 309

Sandoz, Yves, *et al* (eds), *Commentary to the Additional Protocols* (ICRC, 1987)

Schmitt, Michael, (Ed) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, (Cambridge University Press, 2017)

Schmitt, Michael, ' Virtual Disenfranchisement: Cyber Election meddling in the grey zones of international law' in Christopher Whyte, A. Trevor Thrall, Brian M. Mazanec (eds) *Information Warfare in the Age of Cyber Conflict* (Routledge, 2020), 186

Siegel, Alexandra, and Joshua Tucker, 'The Islamic State's information warfare: Measuring the success of ISIS's online strategy' (2018) 17(2) *Journal of language and politic*s 258

Taddeo, Mariarosaria, 'Information warfare: A philosophical perspective' (2012) 25 *Philosophy & Technology*, 112

Terranova, Tiziana, ‘Futurepublic: On information warfare, bio-racism and hegemony as noopolitics’ (2007) 24(3) *Theory, Culture & Society*, 125

Theohary, Catherine, ‘Information warfare: Issues for congress’ (2018) *Congressional Research Service*, 1

van Bentham, Tsvetelina, Talita Dias and Duncan B Hollis ‘Information Operations under International Law’ (2023) 55.5 *Vanderbilt Journal of Transnational Law* 1217

Ventre, Daniel, *Information Warfare* (John Wiley & Sons, 2016)

Whyte, Christopher et al (eds), *Information Warfare in the Age of Cyber Conflict* (Routledge, 2021)

Zannettou, Savvas, et al, ‘Characterizing the use of images in state-sponsored information warfare operations by Russian trolls on twitter’ (2020) 40 in *Proceedings of the International AAAI Conference on Web and Social Media* 774

B Cases

Australian Competition and Consumer Commission v Meta Platforms, Inc. [2022] FCA 1062

Island of Palmas (United States v Netherlands) (1928) 2 RIAA 829

Military and Para-military Activities in and against Nicaragua (Nicaragua v United States) (Judgment) [1986] ICR Rep 14

SS ‘Lotus’ (France v Turkey) (Judgment) [1927] PCIJ (ser A) No 9

C Legislation

Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023 (Cth)

Competition and Consumer Act 2010 (Cth)

Criminal Code Act 1995 (Cth)

Foreign Influence Transparency Scheme Act 2018 (Cth)

Security of Critical Infrastructure Act 2018 (Cth)

Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023

Privacy Act 1988 (Cth)

Rome Statute of the International Criminal Court, opened for signature 17 July 1998, 2187 UNTS 90 (entered into force 1 July 2002)

Statute of the International Court of Justice

D Treaties

Charter of the United Nations, opened for signature 26 June 1045, 1 UNTS XVI (entered into force 24 October 1945)

International Covenant on Civil and Political Rights, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976)

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, opened for signature 8 June 1977, 1125 UNTS 3 (entered into force 7 December 1978)

E Other

Australian Competition and Consumer Commission, 'ACCC takes action over allegedly misleading conduct by meta for publishing scam celebrity crypto ads on Facebook' (Media release, 18 March 2022) https://www.accc.gov.au/media-release/accc-takes-action-over-alleged-misleading-conduct-by-meta-for-publishing-scam-celebrity-crypto-ads-on-facebook

Australia Department of Defence, (2006), *Law of Armed Conflict*, ADDP 06.4, https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/AUS-Manual-Law-of-Armed-Conflict.pdf

Australian Government, *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023 – Fact Sheet* Department of Infrastructure, Transport, Regional Development, Communications and the Arts

Australian Government, *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023 – Guidance Note*, Department of Infrastructure, Transport, Regional Development, Communications and the Arts

Australian Government, "National Defence: Defence Strategic Review" <https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review> (2023) 51

Australian Human Rights Commission 'Finding balance: combatting misinformation and disinformation without threatening free expression' Submission to the Department of

Infrastructure, Transport, Regional Development, Communications and the Arts, 18 August 2023, <https://humanrights.gov.au/our-work/legal/submission/finding-balance-fighting-disinformation-without-threatening-free>

Canada, (2001), *Law of Armed Conflict at the Operational and Tactical Level*, para 602 (land), para 705 (air), para 856 (sea), https://usnwc.libguides.com/ld.php?content_id=2998098

Cullen, Simon and Jade Macmillan, 'US Government Urges Court not to Drop Charges Against Donald Day, the Extremist Linked to the Wieambilla Shooting' *ABC News* (online, 10 January 2024) <https://www.abc.net.au/news/2024-01-10/qld-donald-day-wieambilla-stacey-train-gareth-nathan-police/103306006>

Explanatory Memorandum, Foreign Influence Transparency Scheme Bill 2017 (Cth)

Explanatory Memorandum, Security of Critical Infrastructure Bill 2017 (Cth)

Explanatory Memorandum, National Security Legislation Amendments (Espionage and Foreign Interference) Bill 2017 (Cth)

Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States, GA Res 36/103, UN GAOR, 36th sess, 91st plen mtg, UN Doc A/RES/36/103 (9 December 1981)

Department of Defence. Information Warfare Division. <https://defence.gov.au/jcg/iwd.asp>

Department of Defence. Information Warfare Division – Joint Capabilities Group. https://defence.gov.au/jcg/iwd.asp

Digital Industry Group Inc, *Australian Code of Practice on Disinformation and Misinformation* (22 December 2022)

Digital Industry Group Inc, *2022 Review of The Australian Code of Practice on Disinformation and Misinformation: Response to submissions* (22 December 2022)
German Ministry of Defence, *Law of Armed Conflict: Manual, Joint Service Regulation (ZDv) 15/2*, May 2013, para 487 (original emphasis), https://www.bmvg.de/resource/blob/93610/ae27428ce99dfa6bbd8897c269e7d214/b-02-02-10-download-manual-law-of-armed-conflict-data.pdf

Government Communication Service UK, *RESIST 2: Counter-Disinformation Toolkit*, available at: <https://gcs.civilservice.gov.uk/wp-content/uploads/2021/11/RESIST-2-counter-disinformation-toolkit.pdf>

Helsinki Final Act of the Conference on Security and Co-operation in Europe, 1 August 1975, 14 ILM 1292, Principle VI: Declaration on Principles Guiding Relations between Participating States

Iorio, Kelsie and Jessica Black 'Man arrested in Arizona over religiously motivated terror attack at Wieambilla sent shooters 'end of days' ideological messages' *ABC News* (online, 6 December 2023) <https://www.abc.net.au/news/2023-12-06/qld-wieambilla-shooting-arrest-arizona-queensland-police/103196120>

Keast, Jacinta, 'Shadow Play – A pro-China technology and anti-US influence operation thrives on YouTube' *Australian Strategic Policy Institute* (online, 14 December 2023) <https://www.aspi.org.au/report/shadow-play

Maher, Charlotte, Separating Fact from Fiction on Social Media in Times of Conflict, Bellingcat,
October 26, 2023, https://www.bellingcat.com/resources/how-tos/2023/10/26/separating-fact-from-fiction-on-social-media-in-times-of-conflict/.

Major General Susan Coyle, Head of Information Warfare, Department of Defence, *Committee Hansard*, 25 June 2021, p. 9, cited in Inquiry into the Department of Defence Annual Report 2019-20, November 2021, Commonwealth of Australia 2021, 3.2

Mikhaeil, Christine, 'Conspiracy theories: how social media can help them spread and even spark violence' *The Conversation* (online, 2 August 2023) <https://theconversation.com/conspiracy-theories-how-social-media-can-help-them-spread-and-even-spark-violence-209413>

Morgan, Edward, and Marcus Thompson 'Building Allied Interoperability in the Indo-Pacific Region' Discussion Paper 3, Information Warfare: An Emergent Australian Defence Force Capability, Center for Strategic and International Studies, October 2018.

NATO, 'Media - (Dis)Information – Security' available at: <https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf>

New Zealand Defence Force, (2019), *Manual of Armed Forces Law: Law of Armed Conflict*, https://usnwc.libguides.com/ld.php?content_id=47364407.

Nguyen, Kevin, et al, 'Inside the God-fearing and Conspiratorial Worldviews of Donald Day Jr' *ABC News* (Online, 8 December 2023) < https://www.abc.net.au/news/2023-12-08/inside-god-fearing-conspiratorial-worldviews-of-donald-day-jr/103204360>.

Nguyen, Kevin, and Emilie Gramenz, 'Donald Day Jr, US sovereign citizen linked to Wieambilla murders, was prepared for deadly 'last stand' with police, court hears' *ABC News*

(online, 29 December 2023) <https://www.abc.net.au/news/2023-12-29/donald-day-jr-wieambilla-shootings-court-transcript/103271920>

Non-interference in the internal affairs of states, GA Res 31/91, UN GAOR, 31st sess, 98th plen mtg, Supp No 39, UN Doc A/RES/31/39 (14 December 1976)

Rapid7, *Common Types of Cybersecurity Attacks* (online, 2023) available at <https://www.rapid7.com/fundamentals/types-of-attacks/>

Tuffley, David, 'An AI-driven influence operation is spreading pro-China propaganda across YouTube' *The Conversation* (online, 19 December 2023) https://theconversation.com/an-ai-driven-influence-operation-is-spreading-pro-china-propaganda-across-youtube-219962?utm_medium=email&utmcampaign=Latest%20from%20The%20Conversation%20for%20December%2020%202023%20-%202831928692&utmcontent=Latest%20from%20The%20Conversation%20for%20December%2020%202023%20-%202831928692+CID_c2d51a9e64c9ba21ee1a53889fd881c7&utm_source=campaign_monitor&utm_term=An%20AI-driven%20influence%20operation%20is%20spreading%20pro-China%20propaganda%20across%20YouTube

UK Ministry of Defence, (2004), *The Joint Service Manual of the Law of Armed Conflict*, JSP 383, para 5.15.1, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/27874/JSP3832004Edition.pdf

United Nations Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, GA Res 2131 (XX), UN GAOR, 20th sess, 1408th plen. mtg, UN Doc A/Res/20/2131 (21 December 1965)

United Nations Declaration on the Principles of International Law concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, GA Res 2625 (XXV), UN GAOR, 6th Comm, 25th sess, 1883rd plen mtg, Agenda Item 85, UN Doc A/RES/2625 (XXV), annex (24 October 1970)

US Department of Defense, (2016), *Law of War Manual*, https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190.