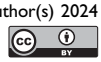
Article

Alternative Law Journal
2024, Vol. 49(2) 142–148



DOI: 10.1177/1037969X241253472
journals.sagepub.com/home/alj


Virus, weapon, litter, industry: Generative metaphors that shape policy around emerging threats

Samuel White
Adelaide Law School, The University of Adelaide, Australia

Abstract
This article examines the use of generative metaphors in the context of interference operations, particularly focusing on trolling and disinformation. It begins by emphasising the crucial role of metaphors in shaping perceptions of cybersecurity issues and subsequent government policies. To demonstrate this, the study delves into two case studies – the Philippines and Australia – analysing how their historical and political contexts have shaped the metaphors they employ to address trolling and disinformation. The article evaluates the effectiveness of these metaphors in both cases, considering their impact on policy formulation. It employs Allan McConnell's methodology to assess process and program success, ultimately concluding that, while the virus metaphor conveys urgency, it falls short in addressing the root causes of trolling. Conversely, the industry metaphor, as exemplified in the Philippines, promotes accountability and regulation.

Keywords
Comparative law, competition policy and law, public law, regulatory theory and practice

Choice of language (and metaphors) within government documents are often deliberate to the policy end being sought. Policies always have advocates prior to their adoption and justifications are made about them afterwards which may differ from the original problem frames in an effort to adapt to the politics of the moment. The actions taken and the political situation are often factors that influence language choices rather than the other way around. John Kingdon's multi-stream framework argues that policy solutions often float around waiting for the convergence of a policy problem and appropriate political license.[1] This convergence can occur, sometimes, through the analogies and metaphors used. These are often called generative metaphors – those which 'generate mental models that carry over associations from one domain to another'[2] – to explore the policy and legal implications for emerging technology. This is particularly so in areas of emerging technologies and threats.

There is a widespread adoption of metaphors by national governments, international legal bodies, and private companies to describe cybersecurity issues and activities.[3] Examples within the domain of cyber include: 'cyber *weapons*, bot *armies*, and virtual *arsenals*.'[4] Underpinning these are a wider metaphor of 'war' that applies to cyberspace; it just as readily could be constructed as an 'information environment' where cyber weapons are pollution.

Such metaphors play a crucial role in shaping stakeholders' reactions to current cybersecurity conditions and problems, influencing their perceptions of responsibility

[1]John W Kingdon, *Agendas, Alternatives, and Public Policies* (Pearson, 2nd ed, 2003). Kingdon's multiple stream framework constitutes a powerful tool to understand the policy process through three streams: problems, policies and politics. However, it is not without its critiques: see Daniel Beland and Michael Howlett, 'The role and impact of the multiple-streams approach in comparative policy analysis' (2016) 18(3) *Journal of Comparative Policy Analysis* 221–7.
[2]Julia Slupska, 'War, Health and Ecosystem: Generative Metaphors in Cybersecurity Governance' (2021) 34(3) *Philosophy & Technology* 469.
[3]Ibid 467.
[4]Ibid (emphasis added).

Corresponding author:
Dr Samuel White, Adelaide Law School, The University of Adelaide, Adelaide, SA 5005, Australia.

Email: samuel.white@adelaide.edu.au

and liability in the face of threats and breaches.[5] A critical argument is that the language used often creates limits and blind spots in policy, limiting its effectiveness. This article seeks to question the efficacy of these metaphors, through looking at how they've impacted Filipino and Australian approaches to trolling / disinformation. The history of democracy in these two case studies has informed the metaphors they used to address the novelty of trolling, which in turn informs policies against disinformation depend on their perception of democracy and the generative metaphors they use. This article questions the generative metaphors currently used in the trolling debate and asks whether the policy frameworks should shift.

Interference operations and trolling

To accurately assess the generative metaphors used by the governments of Australia and the Philippines (through their government documents and statements by government officials) trolling as a tool needs to be critically assessed. Trolling has led to what Hannan calls 'post-truth politics' wherein public discourse is now driven by lies, inappropriate behaviour, and deeper polarisation.[6] Scholars, military professionals, reporters and politicians have used a host of terms to describe the threat: fake news;[7] computational propaganda;[8] information warfare;[9] influence operations;[10] strategic communications;[11] active measures;[12] hostile social manipulation;[13] hashtag warfare;[14] unrestricted warfare;[15] malign cyber operations;[16] psychological operations.[17] Some of these are military metaphors; others are not. For the most part, these terms focus on specific and visible techniques, tools or modes of military action while ignoring the larger and more opaque manipulation of civilian populations. The exception, of course, is espionage – a distinct threat separate to that covered in this article. At the core of espionage are acts related to the theft of information – from industrial and trade through to official, classified government secrets.[18] The focus of this work is actions taken to achieve mass influence on opinions and/or actions of individuals, governments and/or publics.[19]

The conflation of terms is understandable: the use of information as a resource, environment and weapon within the 21st century is an emergent capability, 'still seeking both language and concepts to become normative for discussions of warfare'.[20] But it does have some consequences – such as a set metaphor that has been adopted by States or regional blocs. As Antulio J Echevarria argues:

> While the original aim of such labelling, or re-labelling, may have been to draw the attention of busy policymakers to rapidly emerging security issues, it has evolved into something of a culture of replication in which the labels are repeated more out of habit than conscious reflection. This habit has led to a wealth of confusion that has clouded the thinking of policymakers and impaired the development of sound counter-strategies.[21]

The naming also risks conflating two broad forms of strategy: 'an all-encompassing effort to use all measures short of war; and the more targeted and specific approach of employing information to achieve disruptive effects'.[22] Part of the difficulty, therefore, is the lack of a set definition.[23] It fails to have an accepted policy response as well, even down to the metaphors used.

This study adopts Slupska's argument wherein she evaluates the effectiveness of prevailing metaphors in guiding policy formulation. Slupska argues that current metaphors that relate cybersecurity to 'war' do not capture the fullness of issues that governments experience.[24] She advocates for governments' heightened awareness of the

[5]Ibid.
[6]Jason Hannan, 'Trolling ourselves to death? Social Media and Post-Truth Politics' (2018) 33(2) *European Journal of Communication* 214–226, 214.
[7]Peter Roudik et al, *Initiatives to Counter Fake News in Selected Countries* (Library of Congress, 2019).
[8]See, eg, Oxford Internet Institute, 'Computational Propaganda', *University of Oxford* (Web Page) https://www.oii.ox.ac.uk/research/projects/computational-propaganda/.
[9]Michael Schmitt, 'Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law' in Christopher Whyte, A Trevor Thrall and Brian M Mazanec (eds), *Information Warfare in the Age of Cyber Conflict* (Routledge, 2020) 186; Duncan Hollis, 'The Influence of War: The War for Influence' (2018) 32(1) *Temple International and Comparative Law Journal* 31.
[10]Dale Stephens, 'Influence Operations and International Law' (2020) 19(4) *Journal of Information Warfare* 1.
[11]Mohammad Ali, 'Fake-News Network Model: A Conceptual Framework for Strategic Communication to Deal With Fake News' (2022) 16(1) *International Journal of Strategic Communications* 1.
[12]Thomas Rid, *Active Measures* (Macmillan, 2020).
[13]Michael Mazarr et al, *Hostile Social Manipulation* (RAND, 2019).
[14]Tom Sear and Michael Jensen, 'Hashtag War: Russian Trolls and the Project to Undermine Australian Democracy' (2018) 64 *Griffith Review* 29.
[15]Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (People's Liberation Army, 1992).
[16]Jeff Kosseff, 'Retorsion as a Response to Ongoing Malign Cyber Operations' (Conference Paper, 12th Conference 20/20 Vision, 2020) 9–25.
[17]Tim Hwang and Lea Rosen, 'Harder, Better, Faster, Stronger: International Law and the Future of Online PsyOps' (ComProp Working Paper No 1, Oxford Internet Institute, 2017) 2.
[18]Gary Corn and Robert Taylor, 'Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0: Sovereignty in the Age of Cyber' (2017) 111 *American Journal of International Law* 207; Brian Egan, 'International Law and Stability in Cyberspace' (Speech, University of California, Berkeley School of Law, 10 November 2016).
[19]US Department of State, *Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986–87* (Report, Bureau of Public Affairs, 1987) viii.
[20]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) 6.
[21]Antulio J Echevarria II, *Operating in the Gray Zone: An Alternative Paradigm for US Military Strategy* (Strategic Studies Institute, US Army War College Press, 2016) 1.
[22]Mazarr (n 13) 11.
[23]See Samuel White and Morgan Thomas, 'Closing the (National Security) Gap' (2023) 22(2) *Journal of Information Warfare* 16–30.
[24]Slupska (n 2) 474–82.

metaphors they use and recommends for them to adopt those which foster accountabilities for all stakeholders involved.[25] These include alternate metaphors such as an information ecosystem (where misinformation is the equivalent of littering); data as a valuable goldmine to be explored (or data as uranium which can be powerful or radioactive); an industry to be regulated (such as the Philippines); or a virus to be disinfected (such as Australia). These metaphors will be explored below.

Case study: Philippines

Philippine politics has a 'patron–client factional framework',[26] also called 'mutual aid relationships', or a bond of exchange between wealthy providers and supporters who pledge their loyalty and support to particular political parties.[27] This results in political parties that 'continue to be candidate-centred coalitions of provincial bosses, political machines, and local clans, anchored on clientelistic, parochial, and personal inducements rather than on issues, ideologies, and party platforms'.[28]

A 2010 study found that Philippine trust and governance levels were low due to 'political instability, the failure of the political leaders to deliver the goods and combat corruption effectively, and its unfavorable policy context'.[29] Philippine democratic processes are claimed to be neither 'participative nor equitable'.[30] However, disenchanted Filipino voters have developed subversive tendencies against the educated elites – feeling disrespected as it presumes their lack of agency.[31] Rather, the poor tend to vote on a 'moral economy' – who will offer the most benefit to their local community?[32] Thus, politicians appropriated this in their empathetic campaigns, pitting a fight against the elite.[33]

In 2016, former president Rodrigo Duterte introduced a revolutionary campaign strategy by hiring social media advertising coordinators.[34] This produced an unprecedented surge in pro-Duterte social media interactions.[35] It sprang from a mechanised online network: individuals took on multiple user accounts to spread pro-Duterte information and exponentially multiply its exposure, in a move described through the generative metaphor of 'troll farms'.[36] Duterte admitted to engaging these services,[37] highlighting the growing industry.[38] Pro-Duterte sentiments grew widespread; his presidential statements had corresponding positive reception and anti-Duterte statements were condemned.[39]

Incumbent president Ferdinand Marcos Jr is alleged to have applied the same tactics, but he denies it.[40] Soon after his victory in the 2022 Philippine presidential elections, an anonymous individual called a national radio station, claiming to be a member of a trolling think tank that contributed to Marcos' winning social media campaign.[41] He said he was paid ₱2.5 million (around AUD $67,987) for trolling work that year.[42] Many workers were from top Philippine universities.[43] The caller felt guilty for contributing to the victory of a former dictator's son and wanted to come clean.[44] He claimed to know the troll farm operators' relevant names and office addresses. He said Marcos was their biggest client among their other politicians. Before elections, they bought Facebook accounts and pages having around 300,000 followers that shared trivial content.[45] Each account or page ranged in cost from ₱2500 (around AUD68) to ₱1 million (AUD27,193).[46] After buying these accounts, trolls shared funny, shocking and entertaining memes for re-sharing and attracting new followers.[47] Come election period, trivial content was replaced by material

[25]Ibid.
[26]Carl Herman Landè, *Leaders, and Parties, Factions: The Structure of Philippine Politics* (Southeast Asia Studies, Yale University, 1965) quoted in Julio Cabral Teehankee, 'Factional Dynamics in Philippine Party Politics, 1900–2019' (2020) 39(1) *Journal of Current Southeast Asian Affairs* 98, 101–2.
[27]Ibid.
[28]Julio C Teehankee, 'The Philippines' in Takashi Inoguchi and Jean Blondel (eds), *Political Parties and Democracy: Contemporary Western Europe and Asia* (Palgrave Macmillan, 2012) 187–205.
[29]John ST Quah, 'Trust and Governance in the Philippines and Singapore: A Comparative Analysis' (2010) 11(2) *International Public Management Review* 4.
[30]Mark R Thompson, 'Review Essay: Philippine Politics and Governance' (2008) 29(52) *Philippine Political Science Journal* 117–124, 117.
[31]Mark R Thompson, 'Southeast Asia's Subversive Voters: A Philippine Perspective' (2016) 64(2) *Philippine Studies: Historical and Ethnographic Viewpoints* 265, 266–8.
[32]Ibid 276–81.
[33]Ibid 281.
[34]'Trolls and Triumph: A Digital Battle in the Philippines', *BBC Trending* (Blog Post, 7 December 2016) https://www.bbc.com/news/blogs-trending-38173842.
[35]Ibid.
[36]Maria A Ressa, 'Propaganda War: Weaponizing the Internet', *rappler.com* (online, 3 October 2016) https://www.rappler.com/nation/148007-propaganda-war-weaponizing-internet/.
[37]Catherine S Valente, 'Duterte on use of "troll" army: I have followers', *Manila Times* (online, 25 July 2017) https://www.manilatimes.net/2017/07/25/latest-stories/breakingnews/duterte-on-use-of-troll-army-i-have-followers/340560.
[38]Jonathan Corpus Ong and Jason Vincent A Cabañes, *Architects of Networked Disinformation: Behind the Scenes of Troll Accounts and Fake News Production in the Philippines* (2018) 1–3 https://scholarworks.umass.edu/communication_faculty_pubs/74/.
[39]Ibid.
[40]Neil Arwin Mercado, 'Trolls? "Show me One, They Don't Exist" – Marcos Jr', *Inquirer.net* (online, 27 April 2022) https://newsinfo.inquirer.net/1588374/marcos-camp-has-online-trolls-show-me-one-they-dont-exist-says-bongbong.
[41]Catalina Ricci S Madarang, 'Troll Farm Workers Speak Out, Bare System, Earnings as Part of Campaign Ops', *PhilStar Interaksyon* (online, 11 May 2022) https://interaksyon.philstar.com/trends-spotlights/2022/05/11/217024/troll-farm-workers-radio-caller-salary-campaign/.
[42]Ibid.
[43]Ibid.
[44]Ibid.
[45]Ibid.
[46]Ibid.
[47]Ibid.

promoting candidates.[48] The revelation brought with it cries for regulation – underpinned by the generative metaphor of trolling as an industry, reflecting the multiple supply chains and stakeholders[49] including social media influencers, bloggers and digital freelancers.[50]

Case study: Australia

By comparison, the Australian democratic experience and construct has shaped the metaphors it uses. The Australian *Constitution* supports an active exchange of 'political communication' between the people and the members of government.[51] This is a recognised, but constitutionally implied, freedom of political communication and has been subject to recent judicial skepticism as to its existence.[52] Perhaps, because such a freedom is undefined and unclear (and indeed is not a personal right), metaphors around regulation have been overtaken by metaphors around trolling and disinformation as a virus.

The desire to protect the information 'environment', specifically with respect to elections, is not new. In the 1912 case of *Smith v Oldham*,[53] the validity of legislation prohibiting newspapers and other publishers from publishing anonymously written articles on matters of the election was questioned. Isaacs J scathingly remarked that

> the public injury, so far as political results are concerned, is as great when the opinion of the electorate is warped by reckless, or even careless, misstatements, as when they are knowingly untrue; in each case the result is falsified[54]

The recent High Court case of *Libertyworks v Commonwealth* (*Libertyworks*) confirms this.[55] In *Libertyworks*, the compulsive provisions within the new *Foreign Influence Transparency Scheme Act 2018* (Cth) ('the FITS Act') as a precondition to engaging in political communication with the public, or a section of the public were challenged as unduly restricting the implied freedom of political communication. The Australian government's intent was for the 'sunlight' of truth[56] to act as a 'disinfectant' to disinformation[57] alongside other lines of effort. This strategic framework mirrors that of the United States (US) in the late 1930s and can be titled *illumination*.[58] A majority of the Court found in favour of the provisions and their constitutionality.

This generative metaphor of a 'sickness' that must be 'disinfected' has permeated through government rhetoric in Australia. Northern Territory former Chief Minister, Michael Gunner decried international trolling activity originating from the US, United Kingdom and Canada that spread fake news, claiming that Aboriginal people had been captured by the army and forcibly jabbed with the COVID vaccine.[59] Former Australian Prime Minister Scott Morrison, responding to the 2019 cyber interference in the Australian Parliament House computer network (although unconfirmed whether it was from foreign entities), reassured that the government would take on a serious fight against cyber-attacks, noting that 'malicious actors are constantly evolving', and that his government would take a 'proactive and coordinated approach to protecting Australia's sovereignty, economy and national security',[60] by investing and strengthening its cybersecurity agency.

COVID-19 clearly enhanced the attractiveness of the metaphor. The Australian Communications and Media Authority also adopted the World Health Organization's coined term 'infodemic', as they studied misinformation origins and activity in their June 2020 position paper, *Misinformation and News Quality on Digital Platforms in Australia*, stating in their conclusion:

> The COVID-19 infodemic has also brought home that combating malicious behaviour from state actors and scammers is only one facet of misinformation, which is a far broader issue requiring a multi-pronged response.[61]

The metaphor makes sense, particularly against the backdrop of increased global health awareness. Yet, it is not new. The origin of 'infodemic' traces back to 2003 and was published in a *Washington Post* column by David Rothkopf, in which he was discussing the Severe Acute Respiratory Syndrome (SARS) outbreak and combined the terms 'information' and 'epidemic'. He wrote:

> What exactly do I mean by 'infodemic'? A few facts, mixed with fear, speculation and rumor, amplified and relayed swiftly worldwide by modern information technologies, have affected

[48]Ibid.
[49]Ong and Cabañes (n 38) 25.
[50]Ibid 29–30.
[51]*Nationwide News Pty Ltd v Wills* (1992) 177 CLR 1; *Australian Capital Television Pty Ltd v The Commonwealth* (1992) 177 CLR 106; *Unions NSW v New South Wales* [2013] HCA 58.
[52]*Libertyworks v Commonwealth* (2021) 274 CLR 1.
[53](1912) 15 CLR 355 (*Smith v Oldham*).
[54]Ibid 362–3 (emphasis added).
[55]*Libertyworks v Commonwealth* (2021) 274 CLR 1.
[56]Ibid 19 [57] (Kiefel CJ, Keane and Gleeson JJ); 35 [104] (Gageler J); 43 [122] (Gordon J); 79 [206] (Edleman J).
[57]Commonwealth, *Parliamentary Debates*, House of Representatives, 7 December 2017, 13145 (Malcolm Turnbull, Prime Minister).
[58]The use of this metaphor derives from an essay written by Louis D Brandeis, 'What Publicity Can Do', *Harper's Weekly* (20 December 1913) 10. See also Louis D Brandeis, *Other People's Money and How the Bankers Use It* (Frederick A Stokes Publishing, 1932) 92. The metaphor was adopted by the Committee on the Judiciary of the House of Representatives of the United States in explaining the *Foreign Agents Registration Act 1938* (US). See 1381 *Congressional Record* 2 (1937, House of Representatives).
[59]'NT Chief Minister Attacks "International Trolls" for Spreading Covid Misinformation', *The Guardian* (online, 25 November 2021) https://www.theguardian.com/australia-news/video/2021/nov/25/nt-chief-minister-attacks-international-trolls-for-spreading-covid-misinformation-video.
[60]Commonwealth, *Parliamentary Debates*, House of Representatives, 18 February 2019, 673 (Scott Morrison, Prime Minister).
[61]Australian Communications and Media Authority, *Misinformation and News Quality on Digital Platforms in Australia: A Position Paper to Guide Code Development* (June 2020) 47.

> national and international economies, politics and even security in ways that are utterly disproportionate with the root realities. It is a phenomenon we have seen with greater frequency in recent years – not only in our reaction to SARS, for example, but also in our response to terrorism and even relatively to minor occurrences such as shark sightings.[62]

But long before the COVID-19 pandemic occurred, disinformation spread real-life harm on an impactful scale – deeper hate and polarisation of citizens, persecution of public officials, and even homicide.[63] Massachusetts Institute of Technology (MIT) data scientists discovered that fake news spreads 'faster, deeper, and more broadly' than true news.[64] The swiftness is attributed to 'novelty', wherein creators make fake news items that shock, surprise, and thus become more shareable.[65] Underpinning this is an economy; there is money to be made in shocking news stories (hence, clickbait). What, then, should be done about the metaphors being used?

Evaluating the metaphors

This article has sought to outline what generative metaphors are, and how they have potentially shaped (or been shaped by) policy outcomes. It is, of course, near impossible to measure how these metaphors have impacted on the legal frameworks of the two countries in any definitive way. The closest criteria that could be relied upon are found within the methodology of political scientist, Professor Emeritus Allan McConnell.[66] McConnell defines success when policy 'achieves the goals that proponents set out to achieve and attracts no criticism of any significance, or support is virtually universal.'[67] McConnell then breaks 'success' into three categories:

- process (where government identifies a problem, considers potential solutions, consults with stakeholders, and makes a policy decision);
- program (how government implements its statement of intent); and
- political (what the consequences of the policy are on the government's reputation, and how their electoral chances affect the policy's funding and programs).

Ultimately, the metaphors arise from a desire for political success – but seem to impact on process and program success. Rather than working through McConnell's criteria, this article seeks to look at which metaphor (virus or industry) might be preferable within an Australian policy context – chosen because this article is written for an Australian journal, and an Australian audience. The same analysis could occur in reverse, to see which metaphor is best placed for a Filipino audience. By asking these questions, this article seeks to expose not only how the mental shortcuts inherent in metaphors may illuminate a society, but also expose aspects of a society that are omitted through a metaphor.

The value of industry

The industry metaphor holds actors accountable for their contributed actions. It goes to the heart of a nation-State's role – to regulate for the good of the people – and seeks to protect those in the industry. Knowing the production levels and relationship networks can give insight on penalisation and its severity. Public officials may receive heavier penalties for undesirable or unsafe behaviour than the general public, as they hold positions of public trust and confidence.

This was the focus of the Senate Select Committee on Foreign Interference through Social Media. Dr Andrew Dowse, Director of RAND Australia, submitted to the Select Committee that regulation was key to achieve

> a series of interventions, ranging from addressing the motivation of actors to addressing structural issues in social media networks, to various ways of reducing the likelihood of the audience believing or amplifying force content. In my view such interventions should be priorities for our government, as otherwise the risks and potential consequences of interference through social media will just continue to get worse.[68]

The Committee agreed, pushing away from a 'whack-a-mole' regulatory approach in favour of a more comprehensive regulation of the industry.[69] It is not clear however that such industry regulation is well placed in Australia. Since 1788, Australian society has been particularly against government intervention in industrial matters. The storming of the Eureka Stockade has captured and divided public opinion within Australia for over 160 years. Generally, government intervention in industrial action (or industry more generally) is characterised by 'deeply held, even if imperfectly understood, reservations.'[70] While government intervention in industrial action is neither

[62]David Rothkopf, 'When the Buzz Bites Back', *The Washington Post* (online, 11 May 2003) https://www.washingtonpost.com/archive/opinions/2003/05/11/when-the-buzz-bites-back/bc8cd84f-cab6-4648-bf58-0277261af6cd/.

[63]Elyse Samuels, 'How Misinformation on WhatsApp Led to a Mob Killing in India', *The Washington Post* (online, 21 February 2020) https://www.washingtonpost.com/politics/2020/02/21/how-misinformation-whatsapp-led-deathly-mob-lynching-india/; Shruti Menon, 'Coronavirus: The Human Cost of Fake News in India', *BBC Reality Check* (BBC News, 1 July 2020) https://www.bbc.com/news/world-asia-india-53165436; The Australia Institute, 'Trolls and Polls: The Economic Cost of Online Harassment and Cyberhate' (Research Report, January 2019) 6–10 https://australiainstitute.org.au/wp-content/uploads/2020/12/P530-Trolls-and-polls-surveying-economic-costs-of-cyberhate-5bWEB5d_0.pdf.

[64]Soroush Vosoughi, Deb Roy and Sinan Aral, 'The spread of true and false news online' (2018) 359(6380) *Science* 1146–51, 1146 https://www.science.org/doi/10.1126/science.aap9559.

[65]Ibid 1149.

[66]Allan McConnell, 'Policy success, policy failure and grey areas in-between' (2010) 30(3) *Journal of Public Policy* 345–62

[67]Ibid 351.

[68]Dr Andrew Dowse, *Submission 11 to the Senate Select Committee on Foreign Interference through Social Media, Parliament of Australia*.

[69]Senate Select Committee on Foreign Interference through Social Media, Parliament of Australia, *Foreign Interference through Social Media* (Report, August 2023) 71 – 72.

[70]Margaret White, 'The Executive and the Military' (2005) 28(2) *UNSW Law Journal* 438.

novel nor unique,[71] it remains an understudied area of the law in Australia and this historical aversion perhaps has prohibited the use of an industry metaphor within Australian policy responses to trolling. Since the advent of national, collective bargaining, the role of the military in assisting the civil authority has become increasingly controversial 'in a democracy committed to solving labour-management disputes through collective bargaining mechanisms.'[72] This is all to say that Australia has had historically high levels of union membership, and the use of the industrial relations and corporations powers under our *Constitution* might lead to a different expectation of what industry regulation looks like in Australia.[73]

The value of a virus

The virus metaphor is particularly compelling, as it encapsulates the risk of disinformation and bids to try to contain it. Clinically, trolling is propagated by users with higher trait psychopathy and lower affective empathy – they can predict their victim's potential emotional suffering.[74] Making offensive comments is also contagious.[75] Stanford University cyber-risk researchers studied how disinformation proliferation by Russia during the 2016 US elections mimicked a virus' spread, modelled under Ebola.[76] They aimed to 'find the most effective way to cut transmission chains, correct the information if possible and educate the most vulnerable targets'.[77]

A virus metaphor reduces the government's liability to efficiently stop disinformation from spreading and providing user rehabilitation for those who have suffered from trolling. However, from a process perspective, a virus metaphor fails to engage with the notion that disinformation propagation stems not from digital organisms like bots, but from genuine individuals who must be held accountable. The metaphor is only limited to reactive methods: diligent fact-checking, reacting to fake news, using social media's artificial intelligence systems to sort fake from real news, and reporting disinformation occurrences. Unfortunately, the source of the 'virus' still seems unknown to law enforcement officers when, in fact, such networks are traceable (with effort).[78]

The suite of legislation to respond to the 'virus' of misinformation has been built around a pillar of 'sunlight' concept – a disinformation 'disinfectant' that aims to 'ensure activities are exposed'.[79] As noted above, this is based around the idea of illumination. The importance of illumination as a central tenet of countering Information Operations (IOs) was reinforced in 2018 with Australia's Counter Foreign Interference Strategy, operationalised by the National Counter Foreign Interference Coordinator within the Department of Home Affairs.[80] The strategy, in acknowledging the need for 'convincing foreign interference actors that their actions will have costs',[81] clarified that this would occur by 'showing foreign interference actors that their actions can and will be revealed'.[82]

Illumination would appear to be founded on the doctrine of the 'marketplace of ideas' or 'counterspeech'.[83] These concepts denote the philosophical rationale for freedom of expression, using an analogy of the economic concept of a free market, where ideas can be traded and accepted. It is the underlying concept of Australia's implied freedom of political communication.[84] The marketplace of ideas, and thus illumination, is premised on a rational audience where individuals exposed to the same information, who are able to distinguish between true and false information, will place more value on the truth. John Milton, arguing against British censorship laws, stated in 1644:

> And though all the winds of doctrine were let loose to play upon the earth, so Truth be in the field, we do injuriously by licensing and prohibiting to misdoubt her strength. Let her and Falsehood grapple; who ever knew Truth put to the worse in a free and open encounter?[85]

It is important to note that this rational audience, also known as the 'wisdom of crowds' or 'wealth of networks',

[71] See KGJ Knowles, 'Strikes: A Study in Industrial Conflicts' (1953) 290(1) *American Academy of Political and Social Sciences* 330–45; Sidney Webb and Beatrice Webb, *The History of Trade Unionism* (Passfield Publishing, 1920).
[72] James B Jacobs, 'The Role of Military Forces in Public Sector Labor Relations' (1982) 35(2) *Industrial and Labour Relations Review,* 163–180.
[73] Samuel White, 'Military Intervention in Australian Industrial Action' (2020) 31(4) *Public Law Review* 423–443.
[74] Natalie Sest and Evita March, 'Constructing the Cyber-troll: Psychopathy, Sadism, and Empathy' (2017) 119 *Personality and Individual Differences* 69 https://www.sciencedirect.com/science/article/pii/S0191886917304270?via%3Dihub.
[75] K Hazel Kwon and Anatoliy Gruzd, 'Is Offensive Commenting Contagious Online? Examining Public vs Interpersonal Swearing in Response to Donald Trump's YouTube Campaign Videos' (2017) 27(4) *Internet Research* 991, 994.
[76] Edmund L Andrews, 'How Fake News Spreads Like a Real Virus', *Stanford Engineering* (online, 9 October 2019) https://engineering.stanford.edu/magazine/article/how-fake-news-spreads-real-virus.
[77] Ibid.
[78] See, eg, the excellent open-source journalism by Bellingcat at https://www.bellingcat.com/.
[79] *Parliamentary Debates* (n 60).
[80] Department of Foreign Affairs and Trade, Submission No 10 to Senate Select Committee on Foreign Interference through Social Media, Parliament of Australia, *Inquiry into Foreign Interference through Social Media* (13 March 2020) 3. For further information, see Department of Home Affairs, 'Countering foreign interference' (Web Page, 31 January 2024) https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/overview.
[81] Department of Foreign Affairs and Trade (n 80).
[82] Ibid.
[83] Bill Swannie, 'Speaking Back: Does counterspeech provide adequate redress for racial vilification?' (2021) 42(2) *Adelaide Law Review* 39.
[84] *Libertyworks v Commonwealth of Australia* [2021] HCA 18.
[85] John Milton, *Areopagitica*, with a Commentary by Sir Richard C Jebb and with Supplementary Material (Cambridge at the University Press, 1918) 58.

has been subject to sustained criticism starting from at least the advent of a broadcast-era model of information distribution.[86] One critique aptly notes that as a model it is 'undeniably elegant and compelling, an Enlightenment-era cocktail of Bayesian opinion formation, free speech, and capitalism. Unfortunately, its most foundational premise is false.'[87] This fatal flaw has crystallised in an algorithmic marketplace of ideas, and the efficacy of counter-speech has been questioned by former Prime Minister Kevin Rudd.[88] It seems then that the virus metaphor has been built around an even more-outdated metaphor of free trade ('the marketplace'). Is it fit for purpose?

Within the limited scope available, this article suggests it is. It is interesting to note that the rise of the virus metaphor has resulted from a shift in global events and changing expectations around how governments *can* respond to a virus. It is important, then, in that the meaning of the virus metaphor has unexpectedly shifted – and the Australian government has sought to embrace both the old and new meanings of the metaphor.

It is suggested that since the Australian federal government's response to COVID-19 and mass vaccination highlighted that global pandemics *can* be controlled and responded to, there has there been a shift in the idea that a government has little role in stopping a virus spreading. This is a marked change from the intent of federal government – as AV Dicey once noted, 'federal government means weak government.'[89] There are very limited options for Australia to take steps domestically, outside of funding state and territory responses or utilising the 'nuclear option' (another generative metaphor) of calling in the Australian Defence Force to enforce Commonwealth laws.[90] Yet the experiences of COVID-19 highlighted that co-operative federalism can and does work. As such, within the emerging technology space, digital 'hygiene' can be comprehended and sold in policy responses; individual resilience to a wider 'virus' can be requested by a government; and responsibility can be devolved from government to individuals, organisations and states and territories (in a federal construct).

Conclusion

Although an industry metaphor allows for accountability in all levels of disinformation production and dissemination, the virus metaphor allows governments and people to understand its urgency and its ability to damage an interconnected population. This article suggests that, although the virus metaphor was inappropriate prior to COVID-19, collective experiences of a federated system responding to a national emergency have now changed to the extent that the virus metaphor can catalyse private and public action. This is to be compared to adopting an industry perspective – which, against the backdrop of Australian historical experiences of industry regulation, might not be appropriate.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Samuel White https://orcid.org/0000-0003-0838-5649

Samuel White is the inaugural Cybersecurity Postdoctoral Research Fellow at Adelaide Law School, a Visiting Fellow at UNSW Canberra and an Adjunct Associate Professor at the University of New England. The opinions and errors herein are his alone.

[86]Darren Bush, '"The Marketplace of Ideas": Is Judge Posner Chasing Don Quixote's Windmills' (2000) 32 *Arizona State Law Journal* 1107, 1146; Stanley Ingber, 'The Marketplace of Ideas: A Legitimizing Myth' (1984) 1 *Duke Law Journal* 1; Daniel E Ho and Frederick Schauer, 'Testing the Marketplace of Ideas' (2015) 90 *New York University Law Review* 1160, 1167.

[87]A Trevor Thrall and Andrew Armstrong, 'Bear Market? Grizzly Steppe and the American Marketplace of Ideas' in Christopher Whyte, A Trevor Thrall and Brian M Mazanec (eds), *Information Warfare in the Age of Cyber Conflict* (Routledge, 2020) 73, 78.

[88]Kevin Rudd, *The Case for Courage* (Monash University Publishing, 2021); Kevin Rudd, Submission No 52 to Senate Standing Committees on Environment and Communications, Parliament of Australia, *Inquiry into Media Diversity in Australia* (undated) 2 [4], 3 [7].

[89]AV Dicey, *Introduction to the Study of the Law of the Constitution* (Macmillan, 8th ed, 1915) 167.

[90]Samuel White, *Keeping the Peace of the Realm* (LexisNexis, 2021).