Flinders UNIVERSITY

Jeff Bleich Centre
for the US Alliance
in Digital Technology,
Security & Governance

JBC
Flinders University
Bedford Park SA 5042
https://www.flinders.edu.au/jeff-bleich-centre

Department of Foreign Affairs and Trade
R. G. Casey Building
John McEwen Crescent
Barton ACT 0221 Australia

Responsible state behaviour in cyberspace in the context of international security at the United Nations

This submission is from the Jeff Bleich Centre for the US Alliance in Digital Technology, Security, and Governance. Our research in this space leads us to caution that cyber security should not only be understood as a technological issue, but also as a social issue. This submission will focus on the importance of placing cyber security within its human and social context to understand the challenges of *social* cyber security, and how these issues should shape Australia's engagement with UN processes relating to responsible state behaviour in cyberspace in the context of international security.

1. What existing and emerging threats should inform Australia's approach to discussions on the Framework for Responsible State Behaviour in Cyberspace (international law, norms, confidence building measures and capacity building) in the OEWG and GGE?

A key emerging threat which should inform Australia's approach to discussions on the Framework for Responsible State Behaviour in Cyberspace is the social and democratic implications of the breadth of misinformation and disinformation which now exists as part of our information society. This is an issue which must be tackled across all four pillars of the Framework: international law, norms, confidence building measures, and capacity building. The three reports from the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security which form the basis of the Framework focus heavily on issues such as cybercrime and critical infrastructure attacks, however it is also clear that 'malicious use of ICT by State and non-State actors' exists in a broader spectrum of concern.[1] More clearly defining some of the threats which exist in this broader spectrum of concern is an important starting point.

[1] United Nations General Assembly, *A/65/201: Group of Governmental Experts on Developments in the Field of Information and Telecommunication sin the Context of International Security,* 2010; United Nations General Assembly, *A/68/98: Group of Governmental Experts on Developments in the Field of Information and Telecommunication sin the Context of International Security,* 2013; United Nations General Assembly, *A/70/174: Group of Governmental Experts on Developments in the Field of Information and Telecommunication sin the Context of International Security,* 2015.

The foreword by the Secretary-General in the 2015 report highlighted that 'cyberspace touches every aspect of our lives'.[2] It is important that the four pillars are responsive to this reality, particularly given that the changing nature of warfare means that 'every aspect of our lives' matters a great deal when it comes to international security. To understand the ways in which this is the case, Australia's strategic environment can be understood in terms of society-centric warfare.[3] Emerging trends in warfare have blurred the lines between peace and war and between civilian and military domains as persistent conflict and competition take place below the traditional threshold of conventional conflict.[4] This has led to the whole of society being involved in competition and conflict. While traditional cyber attacks have used information networks to target critical infrastructure, and traditional misuse of information has sought to alter beliefs through propaganda, the current environment has seen a third kind of threat emerge: 'efforts to manipulate or disrupt the information *foundations* of the effective functioning of economic and social systems'.[5] This can take place as part of a malicious external act, but it can also take place from within, with misinformation and disinformation a persistent and significant feature of the infospheres of states.[6]

The threat of misinformation and disinformation to democracy is vast, both for established and less-established democracies. The Philippines, for example, has been referred to as 'patient zero' of the 'global disinformation epidemic'.[7] The centrality of Facebook in particular to Filipino life meant it played a prominent role in the 2016 election, and became yet 'more central and entrenched' in the 2019 midterms.[8] The

[2] United Nations General Assembly, *A/70/174: Group of Governmental Experts on Developments in the Field of Information and Telecommunication sin the Context of International Security,* 2015, p. 4.

[3] Ariel E. Levite and Jonathan (Yoni) Shimshoni, "The Strategic Challenge of Society-Centric Warfare," *Survival* 60, no. 6 (2018): 91–118; Rand Waltzman, "The Weaponization of Information: The Need for Cognitive Security," § Senate Armed Services Committee, Subcommittee on Cybersecurity (2017), https://www.rand.org/pubs/testimonies/CT473.html; Maryanne Kelton et al., "Australia, The Utility of Force and the Society-Centric Battlespace," *International Affairs* 95, no. 4 (2019): 859–76; Emily Bienvenue and Zac Rogers, "Strategic Army: Developing Trust in the Shifting Strategic Landscape," *Joint Force Quarterly* 95, no. 4 (2019): 4–13.

[4] Bienvenue and Rogers, "Strategic Army: Developing Trust in the Shifting Strategic Landscape"; Kelton et al., "Australia, The Utility of Force and the Society-Centric Battlespace"; Michael J. Mazarr et al., "The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment" (RAND Corporation, 2019); Levite and Shimshoni, "The Strategic Challenge of Society-Centric Warfare"; Waltzman, The Weaponization of Information: The Need for Cognitive Security.

[5] Michael J. Mazarr et al., "The Emerging Risk of Virtual Societal Warfare", *RAND Corporation,* 2019, p. xii, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2714/RAND_RR2714.pdf

[6] Infosphere is a term taken from Mazarr et al., "The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment."

[7] Jonathan Corpus Ong, Ross Tapsell, and Nicole Curato, "Tracking Digital Disinformation in the 2019 Philippine Midterm Election" (New Mandala, August 2019), 7.

[8] Ong, Tapsell, and Curato, 7–8.

Cambridge Analytica scandal and the role of disinformation in the 2016 U.S. election captured international attention. Closer to home, disinformation and misinformation throughout the 2019-2020 bushfire crisis has played a significant role in discourse and response to events.[9] These are issues which have variously been captured under the terms of post-truth, truth decay,[10] information crisis,[11] and information disorder.[12] Both the global nature of these challenges, and the role they play within the changing nature of warfare, makes the UN processes relating to responsible state behaviour in cyberspace in the context of international security appropriate fora in which to pursue global cooperation on these matters.

Such cooperation would be in line with the existing Human Rights Council resolutions 20/8 and 26/13 on 'the promotion, protection and enjoyment of human rights on the Internet',[13] and the General Assembly resolution 68/127 and 69/166 on 'the right to privacy in the digital age'.[14] Human rights were discussed in the 2015 report which contributes to the basis of the Framework, with respect of these resolutions pointed to as an important norm to maintain 'in ensuring the secure use of ICTs'.[15] Respect for human rights was also mentioned as a key consideration in the application of international law to the use of ICTs by states.[16] Another useful source of guiding ideas is the Christchurch Principles. The Principles were set out in a report by the Helen Clark Foundation which

[9] Christopher Knaus, "Bots and Trolls Spread False Arson Claims in Australian Fires 'Disinformation Campaign,'" *The Guardian*, January 7, 2020, https://www.theguardian.com/australia-news/2020/jan/08/twitter-bots-trolls-australian-bushfires-social-media-disinformation-campaign-false-claims; Elise Thomas, "Bushfires, Bots and the Spread of Disinformation," The Strategist, January 14, 2020, https://www.aspistrategist.org.au/bushfires-bots-and-the-spread-of-disinformation/.

[10] Jennifer Kavanagh and Michael D. Rich, "Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life" (RAND Corporation, 2018).

[11] The LSE Commission on Truth Trust and Technology, "Tackling the Information Crisis: A Policy Framework for Media System Resilience" (London: The London School of Economics and Political Science, 2018), http://www.lse.ac.uk/media-and-communications/assets/documents/research/T3-Report-Tackling-the-Information-Crisis-v6.pdf.

[12] Clair Wardle and Hossein Derakhshan, "Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making" (Council of Europe Report DGI(2017)09, 2017).

[13] United Nations Human Rights Council, *Resolution A/HRC/RES/20/8: The promotion, protection and enjoyment of human rights on the Internet*, 16 July 2012; United Nations Human Rights Council, *Resolution A/HRC/RES/26/13: The promotion, protection and enjoyment of human rights on the Internet*, 14 July 2014.

[14] United Nations General Assembly, *Resolution A/RES/68/167: The right to privacy in the digital age*, adopted 18 December 2013; United Nations General Assembly, *Resolution A/RES/69/166: The right to privacy in the digital age*, adopted 18 December 2014.

[15] United Nations General Assembly, *A/70/174: Group of Governmental Experts on Developments in the Field of Information and Telecommunication sin the Context of International Security,* 2015, p. 8.

[16] United Nations General Assembly, *A/70/174: Group of Governmental Experts on Developments in the Field of Information and Telecommunication sin the Context of International Security,* 2015, p. 12.

aimed to provide a complementary set of principles to the Christchurch Call. Whereas the Christchurch Call focuses specifically on violent and extremist content online, the Principles aim 'to be more ambitious and applicable to the broader concept of harmful content', incorporating the broad suite of challenges associated with 'new technologies and an increasingly interconnected world'.[17] The Principles are:

1. The principle of equal participation
2. The duty to protect
3. The responsibility to respect
4. The responsibility to remedy
5. The principle of structural change
6. The duty of care
7. The principle of democratic means
8. The principle of decentralisation
9. The principle of inclusivity
10. The principle of communicative action

Alongside the UN resolutions, the Christchurch Principles are useful in guiding a response to the challenges of promoting responsible state behaviour in cyberspace in the context of international security which is grounded in democratic means.

Engaging with the OEWG and the GGE in a way which incorporates the broad suite of challenges associated with the way in which 'cyberspace touches every aspect of our lives' can take place within the existing four pillars of the Framework. International law, norms, confidence building measures, and capacity building will all be key to promoting international cooperation to ensure responsible state behaviour in cyberspace, when the context of international security is understood in a way which appreciates the changing nature of warfare. International law will continue to require adaptation to cyberspace, from digital governance to human rights and beyond. New norms will need to be imagined and enacted which respond to the ways in which digital platforms are used to undermine democratic processes, harm human rights, and imperil human and state security. Confidence building measures will be necessary in promoting trust and cooperation on these new challenging areas of security concern. Capacity building will aid in ensuring states have the capacity to cooperate and to respond to these challenges.

[17] "The Christchurch Principles" (Helen Clark Foundation, The Workshop, and Auckland University of Technology, 2019).