10
Lawfare, China, and the Grey Zone

Orde F. Kittrie

1. Introduction

Sun Tzu, the preeminent ancient Chinese military strategist and author of *The Art of War*, wrote that 'defeating the enemy without fighting is the pinnacle of excellence'.[1] Consistent with his adage, the People's Republic of China (PRC) today is waging sophisticated and systematic lawfare, deftly using law as a weapon to achieve warfighting objectives without needing to fire a shot.

The stakes are high. For example, as this chapter will describe, the PRC is currently using grey zone lawfare in the maritime and aviation domains to take control of the South China Sea.

In addition, the PRC and the West are using lawfare in a struggle to predetermine which side would dominate the information technology domain during, or on the brink of, a future kinetic conflict. The chapter will delineate both this struggle and its enormous stakes. For example, if the United States and its allies fail now to stop the PRC from dominating their telecommunications networks, China could someday be in position to shut down the West's critical electrical and other infrastructure without bombing a single power plant. In addition, the PRC is developing the means to revolutionize the brink and conduct of any future kinetic conflict through the hyper-personalization of war, in which it would deploy financial, health, and other personalized data about Western troops to blackmail, distract, and demoralize individual Western warfighters and their families.

This examination of PRC grey zone lawfare comes at a time of increasing tension between the PRC on the one hand and its Asian neighbours, the United States, and the NATO alliance on the other. In February 2022, days before Russia invaded Ukraine, Chinese leader Xi Jinping and Russian President Vladimir Putin declared that their partnership now had 'no limits' and committed to cooperate in opposing 'certain States' attempts to impose their own 'democratic standards' on other countries' and in shaping a new international order more

[1] Sun Tzu, *The Art of War* (J. J. L. Duyvendak tr, Wordsworth 1998).

Orde F. Kittrie, *Lawfare, China, and the Grey Zone* In: *Hybrid Threats and Grey Zone Conflict*. Edited by: Mitt Regan and Aurel Sari, Oxford University Press. © Oxford University Press 2024. DOI: 10.1093/oso/9780197744772.003.0010

conducive to their own authoritarian regimes.[2] Since the war began, China has undercut Western sanctions by increasing its own trade with Russia, including the export of semiconductors Moscow desperately needs to resupply its military.[3]

Over the course of 2022, the PRC escalated its rhetoric and menacing military actions towards Taiwan.[4] This included massive military exercises practicing a blockade of the island.[5] President Joe Biden responded by declaring on four separate occasions that the United States will defend Taiwan militarily in the event it is attacked by China.[6] This represents a change to the traditional US policy of ambiguity as to how it would respond to such an attack.[7] It comes at a time when US officials reportedly fear that an attack by the PRC is becoming more likely.[8]

In response to the PRC's escalating rhetoric and actions, the North Atlantic Treaty Organization (NATO), the preeminent military alliance of liberal democracies, has for the first time developed a comprehensive China strategy. In its new 'Strategic Concept', issued in June 2022, NATO declared that the PRC 'strives to subvert the rules-based international order' and asserted that the PRC's 'stated ambitions and coercive policies challenge our interests, security and values'.[9]

NATO heads of State and government committed to work together 'to address the systemic challenges posed by the PRC to Euro-Atlantic security'.[10] As if to underscore these concerns, the June 2022 NATO summit included, for the first time, the leaders of four Asia-Pacific countries: Australia, Japan, New Zealand, and South Korea.[11] NATO has, at the same time, developed a sophisticated initiative to address lawfare (which NATO refers to as 'legal operations').[12]

The PRC's current lawfare reflects both Sun Tzu's famous adage and also the assertion of a modern Chinese military text, the *Science of Military Strategy*, that 'war is not only a military struggle, but also a comprehensive contest on

[2] US-China Economic Security and Review Commission, '2022 Report to Congress' (November 2022) <https://www.uscc.gov/sites/default/files/2022-11/2022_Annual_Report_to_Congress.pdf> accessed 5 March 2023.

[3] Ibid.

[4] Ibid.

[5] Ibid.

[6] Kevin Liptak, 'Biden's Past Promises for US to Defend Taiwan under Microscope in Meeting with China's Xi' (*CNN*, 14 November 2022) <https://www.cnn.com/2022/11/13/politics/joe-biden-taiwan/index.html> accessed 5 March 2023

[7] Ibid.

[8] Ibid.

[9] North Atlantic Treaty Organization, 'Strategic Concept' (29 June 2022) <https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf> accessed 5 March 2023.

[10] Ibid.

[11] Amy Qin and Austin Ramzy, 'Labeled a "Challenge" by NATO, China Signals Its Own Hard-Line Worldview', New York Times (New York, 1 July 2022), <https://www.nytimes.com/2022/07/01/world/asia/china-nato.html> accessed 5 March 2023

[12] See, e.g., Rodrigo Vazquez Benitez, Kristian W. Murray, and Pavel Kriz, 'Legal Operations: The Use of Law as an Instrument of Power in the Context of Hybrid Threats and Strategic Competition' [2021] Army Lawyer, Issue 5, 51.

fronts of politics, economy, diplomacy, and law'.[13] Meanwhile, the PRC's evident willingness to challenge the current rules-based international order reflects the words of Wang Xiangsui, a People's Liberation Army (PLA) colonel and co-author of the influential book *Unrestricted Warfare*, who wrote, 'War has rules, but those rules are set by the West . . . so do we need to fight according to your rules? No'.[14]

The PRC is the world's current preeminent practitioner of sophisticated and systematic lawfare in the grey zone. The PRC's embrace of lawfare is particularly notable—and worrying—because the PRC is the leading rival of the United States for global dominance and will continue to be so for the foreseeable future. Since the United States is a far more law-oriented society, with a higher proportion of its best minds entering the legal field, and has pre-eminently shaped the current rules-based international order, one might expect it to be the world's dominant lawfare power. But its lawfare efforts tend to be far less diligent and systematic than those of the PRC. Unlike the PRC, and now NATO, the United States has no lawfare strategy or doctrine.

The second section of this chapter will provide some context, including an overview of why law is becoming an increasingly powerful weapon of war.[15] The third section will provide an overview of China's lawfare doctrine. The fourth section will address China's long-standing use of maritime and other access-denial lawfare against the United States and its allies. The fifth section will address both sides' efforts to use lawfare to shape the future of information technologies. In doing so, the fifth section will describe the critical role that civilian information technologies are likely to play during a period of heightened tensions just short of, or in, any future kinetic conflict between China and the West. The sixth section will address the PRC's grey zone use of its trade regulatory authorities to pursue military policy objectives.

2. Lawfare's increase in power and prevalence

The term 'lawfare' was introduced into the legal and international relations literature by Charles J. Dunlap, Jr. in 2001, when he was a colonel in the US Air

[13] US Department of Defense, 'Annual Report to Congress: Military Power of the People's Republic of China 2007' (2007) 13 <https://apps.dtic.mil/sti/pdfs/ADA528060.pdf> accessed 5 March 2023.

[14] John Pomfret, 'China Ponders New Rules of "Unrestricted War"' Washington Post (Washington, DC, 8 August 1999) <https://www.washingtonpost.com/archive/politics/1999/08/08/china-ponders-new-rules-of-unrestricted-war/ad255e11-9670-4580-a0ff-7f7befb76f3e/> accessed 5 March 2023.

[15] In addressing these topics, this chapter draws heavily on several previous works by the author, including Orde F. Kittrie, *Lawfare: Law as a Weapon of War* (OUP 2016) and Orde F. Kittrie, 'Lawfare and US National Security' (2011) 43 Case Western Reserve Journal of International Law 393.

Force Judge Advocate General's Corps.[16] Dunlap ultimately defined 'lawfare' as 'the strategy of using—or misusing—law as a substitute for traditional military means to achieve a warfighting objective'.[17]

In my 2016 book *Lawfare: Law as a Weapon of War*, I refined Dunlap's definition to focus on both effect and intention. I suggested that in order to qualify as lawfare, an action must meet the following two tests:

(1) the actor uses law to create the same or similar effects as those traditionally sought from conventional kinetic military action—including impacting the key armed force decision-making and capabilities of the target; and
(2) one of the actor's motivations is to weaken or destroy an adversary against which the lawfare is being deployed.[18]

I suggested in my book that the increasing power and prevalence of law as a weapon of war is largely the result of four factors. These factors, which have retained their pre-eminence, include the increased number and reach of international laws and tribunals, the rise of influential non-governmental organizations focused on law of armed conflict and related issues, the information technology revolution, and the advance of globalization and thus economic interdependence. These factors provide important context for the rise and power of PRC lawfare.

2.1 Increased number and reach of international laws and tribunals

Governments worldwide have entered into more than forty-five thousand bilateral treaties and eight thousand multilateral treaties since World War II.[19] In addition, several globally focused tribunals applying international law have been created in recent decades, including the World Trade Organization (WTO) dispute settlement provisions (1995), the International Tribunal for the Law of the Sea (1996), and the International Criminal Court (2002). The maritime lawfare

[16] Charles J. Dunlap, Jr., 'Law and Military Interventions: Preserving Humanitarian Values in 21st Conflicts' (Humanitarian Challenges in Military Intervention Conference, Carr Center for Human Rights Policy, 29 November 2001) <http://people.duke.edu/~pfeaver/dunlap.pdf> accessed 5 March 2023.

[17] Charles J. Dunlap, Jr., 'Lawfare Today . . . and Tomorrow' (2011) 87 International Law Studies 315.

[18] Kittrie, *Lawfare: Law as a Weapon of War* (n 15).

[19] Thomas J. Miles and Eric A. Posner, 'Which States Enter into Treaties, and Why?' (John M. Olin Program in Law and Economics Working Paper No. 420, 2008) <https://chicagounbound.uchicago.edu/law_and_economics/623/> accessed 5 March 2023.

discussed later in this chapter centres on disputes related to the UN Convention on the Law of the Sea (UNCLOS), which entered into force in 1994.

2.1.1 The rise of NGOs focused on law of armed conflict and human rights law

Human rights non-governmental organizations (NGOs) such as Amnesty International (AI) and Human Rights Watch play a key role in documenting, and drawing Western attention to, alleged violations of human rights law and the law of armed conflict. Their reports and accusations have come to carry considerable weight with countries that are responsive to public opinion and care about their international image.

Human rights NGOs have far less impact on autocratic countries like China and Russia, and on terrorist groups such as Hamas and Hezbollah, that place relatively low priority on their publics' opinions and on how their law of armed conflict and human rights compliance records are perceived internationally. This contributes to such autocratic countries and terrorist groups engaging in 'compliance-leverage disparity lawfare', a type of lawfare which is designed to gain advantage from the greater leverage that international law and its processes exert over the United States and other democracies.

This chapter will describe how the PRC regularly engages in compliance-leverage disparity lawfare against the United States and its allies. Such behaviour is consistent with the PRC military's *Basics of International Law for Modern Soldiers*, which states: 'We should not feel completely bound by specific articles and stipulations detrimental to the defence of our national interests. We should therefore always apply international laws flexibly in the defence of our national interests and dignity, appealing to those aspects beneficial to our country while evading those detrimental to our interests'.[20]

2.1.2 The information technology revolution

The vast increase in online data availability has enabled governmental and even non-governmental lawfare practitioners located anywhere on earth to quickly find and deploy many types of information at the level of detail and timeliness necessary to wage lawfare. These include commercial satellite imagery, ship-tracking websites, corporate annual reports, trade press articles, foreign press articles, international agreements, local laws, and national laws from around the world.

[20] Zhao Peiying (ed), *Basics of International Law for Modern Soldiers* (1996) 3, quoted in Jonathan G. Odom, 'A China in the Bull Shop? Comparing the Rhetoric of a Rising China with the Reality of the International Law of the Sea' (2012) 17 Ocean and Coastal Law Journal 201, 222.

At the same time, personal and other digital communications technology and the proliferation of online media outlets have enabled governments, NGOs, and even individuals to in some cases record and disseminate remarkable evidence of war crimes and other violations of international law. For example, researchers collecting evidence in Bucha and other war crimes scenes which Ukraine recaptured from Russia produced detailed dossiers linking particular perpetrators to specific crimes.[21]

However, the information technology revolution has, with limited exceptions,[22] been less useful thus far in identifying perpetrators in areas such as Xinjiang to which access has been closed off by authoritarian regimes. Indeed, information technology has in the case of the PRC thus far played a greater role in perpetrating oppression than in documenting human rights abuses.[23]

Both China and the United States recognize that control over information technology services, and the data that they generate, would likely be an important weapon on the brink of or in a future hot conflict between them. As a result, a struggle over such control is a major aspect of the current grey zone lawfare between them.

2.1.3 Globalization and economic interdependence

The final major reason for the increasing power and prevalence of lawfare is the advance of globalization, which has vastly increased governments' non-kinetic leverage over other countries and their companies by intensifying international economic interdependence. Since 1970, national economies have become much more dependent on trade, with the share of trade as a percentage of worldwide gross domestic product (GDP) increasing from 25 per cent in 1970 to 57 per cent in 2021.[24] The share of trade as a percentage of China's GDP has increased particularly sharply, from 5 per cent in 1970 to 37 per cent in 2021.[25] Meanwhile, the share of trade as a percentage of US GDP has increased from 11 per cent in 1970 to 25 per cent in 2021.[26]

[21] Yousur Al-Hlou et al, 'Caught on Camera, Traced by Phone: The Russian Military Unit that Killed Dozens in Bucha', *The New York Times* (New York, 22 December 2022) <https://www.nytimes.com/2022/12/22/video/russia-ukraine-bucha-massacre-takeaways.html> accessed 5 March 2023.

[22] See e.g. Scilla Alecci, 'UK, US and Germany say Xinjiang Police Files Offer "Shocking" New Evidence of China's Human Rights Abuses' (*International Consortium of Investigative Journalists*, 24 May 2022) <https://www.icij.org/investigations/china-cables/uk-us-and-germany-say-xinjiang-police-files-offer-shocking-new-evidence-of-chinas-human-rights-abuses/> accessed 5 March 2023.

[23] See e.g. Steven Feldstein, 'China's High-Tech Surveillance Drives Oppression of Uyghurs' (*Bulletin of the Atomic Scientists*, 27 October 2022) <https://thebulletin.org/2022/10/chinas-high-tech-surveillance-drives-oppression-of-uyghurs/> accessed 5 March 2023

[24] World Bank, 'Trade (% of GDP)' <https://data.worldbank.org/indicator/NE.TRD.GNFS.ZS> accessed 5 March 2023.

[25] World Bank, 'Trade (% of GDP)—China' <https://data.worldbank.org/indicator/NE.TRD.GNFS.ZS?locations=CN> accessed 5 March 2023

[26] World Bank, 'Trade (% of GDP)—United States <https://data.worldbank.org/indicator/NE.TRD.GNFS.ZS?locations=US> accessed 5 March 2023

As a result of the rise in trade, many nations (including China and the United States) have an increased reliance on international commerce, and many companies are subject to significant leverage in jurisdictions beyond where they are headquartered. For example, the PRC owned some $934 billion in US Treasury securities as of September 2022[27] and also had vast leverage over many major US companies, including those with investments in China and those that are heavily dependent on the Chinese market. At the same time, the US government has regulatory leverage over, for example, the many major Chinese companies that have come to be listed on US stock exchanges (there were 262 Chinese companies listed on the three largest US exchanges as of September 2022).[28] None of this existed in Mao's day.

US grey zone lawfare has regularly leveraged transnational economic interdependence, especially since the US Treasury Department first began its sophisticated use of international economic lawfare about fifteen years ago.[29] During 2022, the United States used economic lawfare as a remarkably effective grey zone tool to degrade Russia's ability to resupply its kinetic invasion of Ukraine. In a report issued in October 2022, the US State Department detailed how the use of export controls and sanctions to restrict Russia's access to advanced technology had 'degraded the Russian weapons industry's ability to produce and stockpile weapons to replace those that have been destroyed in the war'.[30]

For example, US-led financial sanctions 'immobilized about $300 billion worth of Russian Central Bank assets, limiting the central bank's ability to aid the war effort and mitigate sanctions impacts'.[31] In addition, US-led restrictions on the export to Russia of various foreign components, including especially semiconductors, 'nearly ceased' the production of 'Russian hypersonic ballistic missile[s];' 'stalled' production of Russia's 'next-generation airborne early warning and control military aircraft'; and 'shut down' Russian plants 'producing surface-to-air missiles'.[32]

While this and other recent lawfare initiatives of the US Treasury and Commerce departments have been remarkably impactful, the United States—unlike the PRC, NATO, and Israel[33]—has yet to adopt a comprehensive and

[27] 'Foreign Holdings of Treasuries Drop to Lowest Since May 2021' (*Reuters*, 16 November 2022) <https://www.reuters.com/business/finance/update-foreign-holdings-treasuries-drop-lowest-since-may-2021-data-2022-11-16/> accessed 5 March 2023.

[28] US-China Economic Security and Review Commission, 'Chinese Companies Listed on Major US Stock Exchanges' (30 September 2022) <https://www.uscc.gov/sites/default/files/2022-09/Chinese_Companies_Listed_on_US_Stock_Exchanges.pdf> accessed 5 March 2023.

[29] See e.g. Kittrie (n 15) 311–28.

[30] 'The Impact of Sanctions and Export Controls on the Russian Federation', US Department of State, 20 October 2022, <https://www.state.gov/the-impact-of-sanctions-and-export-controls-on-the-russian-federation/> accessed 5 March 2023.

[31] Ibid.

[32] Ibid.

[33] See e.g. Kittrie, *Lawfare: Law as a Weapon of War*(n 15).

coordinated lawfare strategy, doctrine, or mechanism. Such a strategy, doctrine, and mechanism would enable the United States to make even more effective use of lawfare.

3. China's lawfare doctrine

Unlike the US government, the PRC has explicitly adopted lawfare (the synonymous term in Chinese is '*falu zhan*' or 'legal warfare') as a key element of its strategic doctrine. In 2003, the Chinese Communist Party Central Committee and the Chinese Central Military Commission approved the concept of 'Three Warfares', highlighting in their doctrine the following non-kinetic tools:

> *Psychological Warfare:* the use of propaganda, deception, threats, and coercion to affect the enemy's ability to understand and make decisions
> *Media Warfare:* the dissemination of information to influence public opinion and gain support from domestic and international audiences for China's military actions
> *Legal Warfare:* the use of international and domestic laws to gain international support and manage possible political repercussions of China's military actions.[34]

Since this decision, several PRC military texts have been dedicated entirely to *falu zhan*.[35] In addition, important conceptual context for the PRC's use of legal warfare is provided by a treatise titled *Unrestricted Warfare*, which was written by two PLA colonels, Qiao Liang and Wang Xiangsui, and published by the PLA in 1999. The treatise suggests various tactics—including legal warfare—that developing States, China in particular, might use to offset their military inferiority vis-à-vis the United States.[36] Liang was subsequently promoted to major general and rose to deputy secretary of the PRC's National Security Policy Committee.[37]

[34] US Department of Defense, 'Annual Report to Congress: Military Power of the People's Republic of China 2008' (2008) 19; Central Military Commission, 'People's Liberation Army of China Regulation on Political Work', Article 14(18) (December 2003), cited in Paul A. Stempel, 'Reading Lawfare in Chinese: The Meaning of the Term 'Falu Zhan ("Lawfare") in Chinese Military Literature' (July 2011) (unpublished article).

[35] Stempel (n 34). Stempel notes that when the Chinese government printed a translated version of an article titled 'Lawfare: A Decisive Element of 21st-Century Conflicts?' by Major General Charles Dunlap, the former Deputy Judge Advocate General of the US Air Force who coined the term 'lawfare', the PRC's translators used the term *falu zhan* where Dunlap used the term 'lawfare'.

[36] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Pan American 2002).

[37] See e.g. US-China Perception Monitor, 'The Inaugural Carter Center—Global Times Foundation Forum for Young Chinese and American Scholars' (2014), Qiao Liang biographical paragraph <http://www.uscnpm.org/papers> accessed 5 March 2023.

In 2008, the US State Department's International Security Advisory Board noted that China was engaged in the previously referenced, non-kinetic 'Three Warfares' even as the United States and the PRC existed nominally in a state of peace:

> It is essential that the United States better understand and effectively respond to China's comprehensive approach to strategic rivalry, as reflected in its official concept of 'Three Warfares'. If not actively countered, Beijing's ongoing combination of Psychological Warfare (propaganda, deception, and coercion), Media Warfare (manipulation of public opinion domestically and internationally), and Legal Warfare (use of 'legal regimes' to handicap the opponent in fields favorable to him) can precondition key areas of strategic competition in its favor.[38]

The PRC's use of lawfare is consistent with the doctrines of the Chinese Communist Party Chairman Mao Zedong, as well as those of Sun Tzu. Unlike many Western strategists, Mao also tended to think of the clash of arms as just one element, and not necessarily the most important element, of conflict.

China's vigorous use of lawfare is rooted in the uniquely instrumental role law has played, and continues to play, in historical and contemporary Chinese culture.[39] In pre-Communist imperial China, law served as a tool of authority, not a constraint upon it.[40] Following the Communist revolution of 1949, China adopted the Marxist view that law serves as an instrument of politics (rather than, for example, a check on politics and an autonomous, objective arbiter of justice).[41]

Consistent with Sun Tzu's emphasis on winning without fighting, PRC strategists have emphasized that legal warfare should begin, and is exceptionally valuable, 'before the outbreak of physical hostilities'.[42] Today, China is actively engaged in lawfare in the maritime, aviation, space, information technology, and trade domains.

PRC lawfare today is aimed at both gaining current advantage and tilting future kinetic battlegrounds to China's benefit. This chapter's next section will illustrate this by describing how the PRC deploys lawfare arguments, in the maritime

[38] International Security Advisory Board, 'China's Strategic Modernization: Report from the ISAB Task Force' (US Department of State 2008) <https://nuke.fas.org/guide/china/ISAB2008.pdf> accessed 5 March 2023.

[39] Robert Strausz-Hupé et al, *Protracted Conflict: A Challenging Study of Communist Strategy* (Harper 1959).

[40] See e.g. Dean Cheng, 'Winning without Fighting: Chinese Legal Warfare' (Heritage Foundation, 18 May 2012) <https://www.heritage.org/asia/report/winning-without-fighting-chinese-legal-warfare> accessed 5 March 2023.

[41] Eric W. Orts, 'The Rule of Law in China' (2001) 34 Vanderbilt Journal of Transnational Law 43.

[42] Cheng (n 40).

and aviation domains, in order to promote Beijing's access control strategy both by creating current facts on the ground (e.g., turning disputed reefs into airbases) and by promoting future international legitimacy for China's expanding claims of sovereignty rights.

4. PRC grey zone lawfare in the maritime and aviation domains

The PRC has been engaged in a sophisticated maritime and aviation lawfare strategy for over a dozen years. In 2009, James Kraska and Brian Wilson, two senior US Navy attorneys, warned that 'China has begun to engage in a resourceful legal warfare, or "lawfare" strategy to deny access to its coastal seas to warships and aircraft of the United States, Japan, and other countries in the region.'[43] In Kraska and Wilson's description, the PRC was endeavouring to use 'international law as an instrument to deter adversaries prior to combat . . . [including by shifting the law of the sea] away from long-accepted norms of freedom of navigation and toward interpretations of increased coastal State sovereign authority.'[44]

In the years since, the PRC has continued to work to change international law, so as to push US and other ships and aircraft farther away from China's coastline, in order to provide its military more breathing room in a potential future kinetic conflict. This lawfare has focused in large part on the South China Sea.

The South China Sea encompasses an area of around 1.4 million square miles[45] (1.5 times larger than the Mediterranean Sea).[46] According to various estimates, some $3 to $5 trillion per year in trade, more than one fifth of the world's total, transits through the South China Sea.[47] The Sea also reportedly contains approximately 11 billion barrels of oil and 190 trillion cubic feet of natural gas in proved and probable reserves.[48] That equals approximately 3 per cent

[43] James Kraska and Brian Wilson, 'China Wages Maritime Lawfare' (*Foreign Policy*, 12 March 2009) <http://foreignpolicy.com/2009/03/12/china-wages-maritime-lawfare/> accessed 5 March 2023.

[44] Ibid.

[45] 'South China Sea', Encyclopedia Britannica <https://www.britannica.com/place/South-China-Sea/Economic-aspects> accessed 5 March 2023

[46] 'Mediterranean Sea', Encyclopedia Britannica, https://www.britannica.com/place/Mediterranean-Sea> accessed 5 March 2023.

[47] Jim Gomez and Aaron Favila, 'US Admiral Says China Fully Militarized Isles' (*Associated Press*, 21 March 2022) <https://apnews.com/article/business-china-beijing-xi-jinping-south-china-sea-d229070bc2373be1ca515390960a6e6c> accessed 5 March 2023; Sean M. Holt, 'Five Countries, Other than China, Most Dependent on the South China Sea' (*CNBC*, 17 November 2022) <https://www.cnbc.com/2022/11/18/five-countries-other-than-china-most-dependent-on-the-south-china-sea.html> accessed 5 March 2023.

[48] US Energy Information Administration, 'South China Sea' <https://www.eia.gov/international/analysis/regions-of-interest/South_China_Sea> accessed 5 March 2023.

of global proven natural gas reserves.[49] The Sea is surrounded by Brunei, China, Indonesia, Malaysia, the Philippines, Singapore, Taiwan, and Vietnam.[50]

The PRC has for decades claimed sovereignty or some form of exclusive jurisdiction over most of the South China Sea.[51] It has done so by asserting a variety of claims which have long been rejected—as inconsistent with international law—by the United States, numerous States, and an arbitral tribunal.[52]

The PRC's claims were for many years expressed through its circulation of maps featuring a 'nine-dashed-line' asserting control over the vast majority of the South China Sea. In a 2009 submission to the UN Secretary General, the PRC stated 'China has indisputable sovereignty over the islands in the South China Sea and the adjacent waters, and enjoys sovereign rights and jurisdiction over the relevant waters as well as the seabed and subsoil thereof (see attached map)'.[53]

The most authoritative refutation of these PRC claims was issued in 2016, by an arbitral tribunal convened in accordance with UNCLOS, the multilateral treaty governing maritime sovereignty.[54] The PRC is a party to UNCLOS.[55] Ruling on a claim brought against the PRC by the Philippines, the tribunal issued a unanimous decision ruling in favour of the Philippines on nearly every count.[56] Under the terms of UNCLOS, the tribunal decision is final and binding on the PRC.[57] Yet the PRC has refused to abide by the arbitral decision, declaring it 'null and void'.[58]

Since 2016, the PRC has shifted to making claims based on its purported sovereignty over four 'island groups' in the South China Sea.[59] This includes claims not only to the actual islands but also to ostensibly related maritime features that are either fully submerged or below water at high tide.[60] The four-island group

[49] British Petroleum, 'Statistical Review of World Energy: 2021' <https://www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/energy-economics/statistical-review/bp-stats-review-2021-natural-gas.pdf> accessed 5 March 2023

[50] US Department of State, 'People's Republic of China: Maritime Claims in the South China Sea' (January 2022) 3 <https://www.state.gov/wp-content/uploads/2022/01/LIS150-SCS.pdf> accessed 5 March 2023.

[51] Ibid. 1.

[52] *South China Sea Arbitration (The Republic of Philippines v. The People's Republic of China)*, Award, PCA Case No. 2013-19 (July 12, 2016).

[53] US Department of State, 'China: Maritime Claims in the South China Sea' (5 December 2014) <https://www.state.gov/wp-content/uploads/2019/10/LIS-143.pdf> accessed 5 March 2023.

[54] *South China Sea Arbitration* (n 52).

[55] Ibid.

[56] Ibid.

[57] Permanent Court of Arbitration, 'South China Sea Arbitration (*The Republic of Philippines v. The People's Republic of China*)', Press Release (12 July 2016) <https://pcacases.com/web/sendAttach/1801> accessed 5 March 2023. While the United States is not a party to UNCLOS, it considers the relevant provisions of UNCLOS to 'reflect customary international law binding on all states. See US Department of State (n 53) 5.

[58] Congressional Research Service, 'China Primer: South Sea Disputes' (19 December 2022) <https://crsreports.congress.gov/product/pdf/IF/IF10607> accessed 5 March 2023.

[59] US Department of State (n 50) 2, 5.

[60] Ibid.

claim depends on many of the same mischaracterizations of the law of the sea, and has much the same practical effect of vastly expanding China's purported maritime seas, as did the nine-dash-line.

UNCLOS provides that each State is entitled to a 12-nautical-mile territorial sea over which it enjoys sovereignty, as well as a 200-nautical-mile exclusive economic zone (EEZ) in which it enjoys the sole right to exploitation of natural resources.[61] UNCLOS specifies that foreign States have freedom of navigation and overflight within EEZs.[62]

The 12- and 200-nautical-mile lines are measured not just from a State's mainland but also from any islands which are part of the State. For these purposes, UNCLOS defines an island as 'a naturally formed area of land, surrounded by water, which is above water at high tide', excluding '[r]ocks which cannot sustain human habitation or economic life of their own'.[63] Each such island generates its own 12-nautical mile-territorial sea and 200-nautical-mile EEZ.[64] A rock which is above water at high tide but not capable of sustaining habitation or economic life generates only a territorial sea.[65]

Whether a feature meets the criteria of being above water at high tide, or sustaining human habitation or economic life of its own, must be assessed based on its natural state.[66] Human activity cannot transform a low-tide or submerged feature or a rock into an island that is fully entitled to maritime zones.[67] UNCLOS specifically provides that '[a]rtificial islands, installations and structures do not possess the status of islands'.[68]

Beijing has continued to both express, and act pursuant to, its alternative interpretation of these and other provisions of the law of the sea. For example, the PRC falsely claims 'sovereignty' over more than one hundred features in the South China Sea that are submerged below the surface at high tide.[69] The PRC uses such claims to extend its territorial sea and EEZ claims.[70]

The PRC is also engaged in construction designed to turn some submerged reefs and mere rocks into inhabited islands. For example, the PRC occupies and has built artificial islands on Mischief Reef and Subi Reef, which it appeared to use as a basis for its maritime sovereignty claims. The 2016 tribunal confirmed that both reefs are submerged at high tide in their natural conditions, which

[61] UN Convention on the Law of the Sea (10 December 1982) 1833 UNTS 3 (UNCLOS).
[62] UNCLOS, Arts. 58 and 87.
[63] Ibid. Art. 121.
[64] Ibid.
[65] Congressional Research Service (n 58).
[66] US Department of State (n 50) 6.
[67] Ibid. 6–7.
[68] UNCLOS, Art. 60.
[69] US Department of State (n 50) 1.
[70] Ibid.

means they are not entitled to territorial seas.[71] 'As time goes on', said Professor Ingrid Wuerth, 'it may become harder and harder to document which features were 'rocks', which were 'islands' and which were neither prior to construction—and these determinations may be essential to resolving contested maritime claims in the region'.[72]

As of spring 2022, the PRC had not only turned both Mischief Reef and Subi Reef into artificial islands but also placed on them multi-story buildings, airstrips, fighter jets, seaports, and missile systems.[73] PRC military officials were also repeatedly (and contrary to international law) ordering US Navy planes flying nearby to exit what the PRC officials claimed was China's territory.[74]

In addition to claiming (and seeking to enforce) 12-nautical-mile territorial seas around artificial islands, the PRC also falsely asserted that it can regulate passage on the seas, and also overflight within the airspace, in its EEZ. For example, PRC officials have repeatedly complained about foreign military vessels transiting the Taiwan Strait even though the strait, 70 miles wide at its narrowest, goes well beyond China's 12-nautical-mile territorial sea.[75]

Raul Pedrozo, a professor of military law at the US Naval War College, referred to China's 'untenable position that foreign military activities in the EEZ are subject to coastal notice and consent' as part of 'China's ongoing lawfare strategy to misstate or misapply international legal norms to accommodate its anti-access strategy'.[76] China has used this inaccurate interpretation of EEZ law to justify the interception and harassment of US and other nations' ships operating within its EEZ, and of US and other nations' aircraft flying above its EEZ.[77]

Nor is China's maritime coercion exclusive to its regular armed forces. The People's Armed Forces Maritime Militia (PAFMM) is a naval militia force organized at the local level which, according to a US Defense Department report, 'plays a major role in coercive activities to achieve China's political goals without fighting, part of broader PRC military doctrine stating confrontational operations short of war can be an effective means of accomplishing political objectives'.[78] PAFMM includes nearly two hundred thousand fishing

[71] *South China Sea Arbitration* (n 52) 174.

[72] Ingrid Wuerth, 'US Policy on the South China Sea' (*Lawfare*, 26 March 2015) <https://www.lawfareblog.com/us-policy-south-china-sea> accessed 5 March 2023

[73] Gomez and Favila (n 47).

[74] Ibid.

[75] Lynn Kuok, 'Narrowing the Differences between China and the US Over the Taiwan Strait' (*International Institute for Strategic Studies*, 13 July 2022) <https://www.iiss.org/blogs/analysis/2022/07/narrowing-the-differences-between-china-and-the-us-over-the-taiwan-strait> accessed 5 March 2023.

[76] Raul Pedrozo, 'The Building of China's Great Wall at Sea' (2012) 17 Ocean and Coastal Law Journal 253, 284.

[77] M. Taylor Fravel and Charles L. Glaser, 'How Much Risk Should the United States Run in the South China Sea?' (2022) 47 International Security 88.

[78] US Department of Defense, 'Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2018' (16 May 2018) 72 <https://media.defense.gov/

vessels,[79] often indistinguishable from regular fishing vessels,[80] which train with the PRC Navy and Coast Guard and take direction from PRC authorities.[81]

Ostensibly private Chinese 'cargo ships and fishing vessels are used as government proxies to interfere with US ships'.[82] On occasion they are dispatched en masse to 'intimidate and ram fishing or law enforcement boats from other countries'.[83] Using fishing vessels in this manner 'provides the Chinese government with some level of plausible deniability', making it more challenging to hold the PRC accountable, although from a practical perspective 'the pattern of behavior is easily ascribable to the Chinese government'.[84]

China's continued actions pursuant to its inaccurate interpretations of the law of the sea appear to be aimed at changing customary international law. Customary international law can be nullified or even changed through State practice undertaken in conjunction with an assertion that such practice is consistent with international law.[85]

In the law of the sea context, customary international law can, over time, be affected by maritime operations, diplomatic statements, domestic implementing legislation, and the writings of legal scholars, as well as statements and judgements from international organizations and tribunals.[86] Supplementing its maritime operations, China's EEZ lawfare strategy includes 'declaratory statements incorporated into China's UNCLOS ratification depositary instrument', domestic legislation formally claiming security interests in its EEZ, development of supportive legal scholarship, and a strategic communications campaign.[87]

For the PRC, however, such lawfare activities as turning reefs into islands are not necessarily designed to create an argument that would win before the International Court of Justice the next year. Sometimes, the activity is apparently designed in part to create a legal or legal-sounding argument that can create a narrative today that will 'persuade the Chinese people that their government's

2018/Aug/16/2001955282/-1/-1/1/2018-CHINA-MILITARY-POWER-REPORT.PDF> accessed 5 March 2023

[79] James Kraska and Michael Monti, 'The Law of Naval Warfare and China's Maritime Militia' (2015) 91 International Law Studies 450, 452.

[80] Ibid.

[81] US Department of Defense (n 78.

[82] Pedrozo (n 76) 284.

[83] Ian Urbina, 'How China's Massive Fishing Fleet Is Transforming the World's Oceans' (*Slate*, 2 September 2020) <https://slate.com/news-and-politics/2020/09/beijing-fishing-fleet-subsidies-north-korea.html> accessed 5 March 2023.

[84] Robert T. Kline, 'The Pen and the Sword: The People's Republic of China's Effort to Redefine the Exclusive Economic Zone through Maritime Lawfare and Military Enforcement' (2013) 216 Military Law Review 122.

[85] See e.g. Statute of the International Court of Justice (26 June 1945), 33 UNTS 933, Art. 38.

[86] Robert C. De Tolve, 'At What Cost? America's UNCLOS Allergy in the Time of "Lawfare"' (2012) 61 Naval Law Review 1.

[87] Ibid.

actions are justified'.[88] The activity may also, or instead, be designed to plant the seed of arguments that will grow in strength as the PRC causes customary international law to evolve and/or as neighbours, intimidated by the PRC's military might, acquiesce to its claims. Thus, from the perspective of the United States, Australia, and their allies, it is essential to contest such claims early and forcefully lest they gain momentum and set the stage for a future fait accompli.

Demonstrating continuing control over a specific body of water or island is 'vitally important to claims of sovereignty' over it under theories of historic title, customary international law, and UNCLOS.[89] The extent to which other States accept or contest a historic claim is a key criteria for establishing the claim.[90] Since inaction may be viewed as acquiescence to the claim, China benefits legally from creating or bolstering a claim by creating a new island or other facts, and then militarily dissuading other States from contesting the claim.[91]

This strategy for obtaining sovereignty over South China Sea islands and waters is, as one US Navy legal expert put it, 'slowly proving effective . . . if successful, China will have achieved through the use of lawfare what it traditionally would have had to achieve almost solely through military force'.[92] As Professor Douglas Guilfoyle, a leading Australian maritime law expert put it in October 2022, China is successfully 'advancing a series of legal, historical, and security arguments in favor of what seems to be a new regional maritime order, one centred on rules generated in Beijing'.[93]

5. US-China grey zone lawfare in the information technology domain

Both China and the United States recognize that control over information technology services, and the data they generate, is currently a principal cold war battlefield and would likely be an important weapon on the brink of or in a future hot conflict between them. As a result, a struggle over such control is a major aspect of the current grey zone lawfare between Beijing and Washington. The information technology battle is being fought in lawfare domains including the following: theft of intellectual property, the content of international law in

[88] Peter Dutton, 'China's Maritime Disputes in the East and South China Seas, Testimony of Peter Dutton' (2014) 67 Naval War College Review 7.
[89] Kline (n 84).
[90] Ibid.
[91] Ibid.
[92] Ibid.
[93] Douglas Guilfoyle, 'AUKUS and the International Rules-Based Order in the Maritime Domain' (*Security and Defense Plus*, 25 October 2022) <https://www.unsw.adfa.edu.au/security-defence-plus-aukus-and-international-rules-based-order-maritime-domain> accessed 5 March 2023.

the cyber arena, control over Americans' private information, and whose telecommunications pipelines supply the world.

5.1 Theft of intellectual property

The stakes of this battle are extremely high. Even now, in peacetime, '[t]he theft of intellectual property by the People's Republic of China costs America as much as $500 billion per year', according to William Evanina, director of the US government's National Counterintelligence and Security Center.[94]

The PRC's intellectual property theft is aimed in part at strengthening its weapons systems. According to a US Defense Department report, the PRC leverages 'State-sponsored industrial and technical espionage' in part to 'increase the level of technologies and expertise available to support military research, development, and acquisition'.[95] According to Daniel Coats (when he was US Director of National Intelligence) and numerous press reports,[96] the PRC has stolen designs and other data for the US Air Force's F-35 and F-22 aircraft programs.[97] In 2019, Secretary of Defense Mark Esper warned that China is perpetrating 'the greatest intellectual property theft in human history'.[98]

The other principal aim of the PRC's theft of intellectual property is to bolster its commercial enterprises. FBI director Christopher Wray and MI5 Director General Ken McCallum addressed this issue in a July 2022 joint address to business leaders in London. McCallum noted that the event was the first time the heads of the FBI and MI5 had ever shared a public platform, and explained that they were 'doing so to send the clearest signal we can on a massive shared challenge: China'.[99]

[94] Naveed Jamali and Tom O'Connor, 'US, China's Cold War is Raging in Cyberspace, Where Intellectual Property is a Costly Front' (*Newsweek*, 16 September 2020) <https://www.newsweek.com/us-chinas-cold-war-raging-cyberspace-where-intellectual-property-costly-front-1532133> accessed 5 March 2023.

[95] US Department of Defense, 'Military and Security Developments Involving the People's Republic of China, Annual Report to Congress 2020' (2020) xi <https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF> accessed 5 March 2023.

[96] See e.g. Eli Fuhrman, 'How China Stole the Designs for the F-35 Stealth Fighter' (*1945*, 15 July 2021) <https://www.19fortyfive.com/2021/07/how-china-stole-the-designs-for-the-f-35-stealth-fighter/> accessed 5 March 2023.

[97] Daniel R. Coats, 'Worldwide Threat Assessment of the US Intelligence Community' (11 May 2017) <https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf> accessed 5 March 2023.

[98] Ellen Ioanes, 'China Steals US Designs for New Weapons, and It's Getting Away with 'The Greatest Intellectual Property Theft in Human History' (*Business Insider*, 24 September 2019) https://www.businessinsider.com/esper-warning-china-intellectual-property-theft-greatest-in-history-2019-9> accessed 5 March 2023.

[99] MI5, 'Joint Adress by MI5 and FBI Heads' (6 July 2022) <https://www.mi5.gov.uk/news/speech-by-mi5-and-fbi> accessed 5 March 2023.

In his speech at the event, FBI director Christopher Wray described the PRC's motivation as follows: 'The Chinese government is set on stealing your technology—whatever it is that makes your industry tick—and using it to undercut your business and dominate your market. And they're set on using every tool at their disposal to do it'.[100]

Wray described one such tool as the PRC's 'lavishly resourced hacking program that's bigger than that of every other major country combined'.[101] Wray explained that '[t]he Chinese Government sees cyber as the pathway to cheat and steal on a massive scale'.[102]

But Wray emphasized that 'in addition to traditional and cyber-enabled thievery, there are even more insidious tactics they'll use to essentially walk through your front door—and then rob you'.[103] The PRC does this, he said, 'by making investments and creating partnerships that position their proxies to steal valuable technology'.[104]

Wray described how the PRC frequently does this by evading Western laws and leveraging PRC laws. He explained that the PRC 'uses elaborate shell games to disguise its efforts' from Western governments' investment-screening programs like the Committee on Foreign Investment in the United States.[105] Wray also noted the PRC's efforts to change US laws, including 'when the Chinese Embassy warned US companies that, if they want to keep doing business in China, they need to fight bills in our Congress that China doesn't like'.[106]

The PRC leverages its own laws in several ways, explained Wray. For example, the PRC requires that Western companies doing business in China 'partner with Chinese businesses, partners that often turn into competitors'.[107]

In addition, Wray warned his audience of Western businesses that the PRC is 'legislating and regulating their way into your IP and your data'.[108] For example, a 2017 Chinese law requires particular Western companies to store their data in China, where the PRC government 'has easier access to it'.[109] The PRC's access is eased by another 2017 law that forces Chinese organizations and individuals 'to assist in Chinese intelligence operations' and a series of 2021 laws that gives the PRC 'access to and control of' data collected in China.[110]

[100] Federal Bureau of Investigation, 'Director's Remarks to Business Leaders in London' (6 July 2022) <https://www.fbi.gov/news/speeches/directors-remarks-to-business-leaders-in-london-070622> accessed 5 March 2023.
[101] Ibid.
[102] Ibid.
[103] Ibid.
[104] Ibid.
[105] Ibid.
[106] Ibid.
[107] Ibid.
[108] Ibid.
[109] Ibid.
[110] Ibid.

Wray hinted at the difficulty that the United States and its allies have in fighting back against the PRC's no-holds-barred tactics, stating that in 'targeting countries around the world that value the rule of law . . . Beijing may think our adherence to the rule of law is a weakness'.[111] While he insisted 'they're wrong', he did not explain in what way they're wrong or provide an explanation as to how the US government can turn the tables on the PRC.[112]

5.2 Battle over the content of international law in the cyber arena

In its 2022 annual report to Congress, the US-China Economic Security Review Commission declared that 'China enjoys an asymmetric advantage over the United States in cyberspace due to the CCP's unwillingness to play by the same rules'.[113] The Commission explained that the two countries 'diverge sharply on the norms that should guide responsible State behavior in cyberspace during peacetime'.[114]

One example the Commission provided was 'China's perpetration of cyberespionage for illegitimate economic advantage'.[115] While such cyberespionage is apparently not prohibited by international law,[116] the United States has declared that it will 'help build an international environment that recognizes such acts as unlawful and impermissible',[117] a stance supported by the G-20.[118] The PRC's persistence in undertaking such espionage violates the 2015 political agreement of President Barack Obama and President Xi Jinping that 'neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors'.[119]

[111] Ibid.
[112] Ibid.
[113] US-China Economic Security and Review Commission (n 2) 418.
[114] Ibid.
[115] Ibid.
[116] NATO Cooperative Cyber Defence Centre of Excellence, 'Cyber Law Toolkit: Economic cyber espionage' <https://cyberlaw.ccdcoe.org/wiki/Scenario_09:_Economic_cyber_espionage#cite_note-66> accessed 5 March 2023.
[117] The White House, 'International Strategy for Cyberspace' (May 2011) <https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf> accessed 5 March 2023.
[118] G20 Leaders' Communique, Antalya Summit (2015) <https://www.consilium.europa.eu/media/23729/g20-antalya-leaders-summit-communique.pdf> accessed 5 March 2023.
[119] The White House, 'Fact Sheet: President Xi Jinping's State Visit to the United States' (25 September 2015) <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states> accessed 5 March 2023.

The Commission also described how the United States and China 'differ substantially in their interpretations of certain provisions [of international law] that would be relevant to cyber operations in a military context'.[120] For example, China disagrees with the US view that malicious cyber activities may constitute a use of force that triggers the target country's right under international law to 'defend itself through proportionate offensive operations, cyber or otherwise'.[121]

5.3 Battle over control of Americans' private information

The hyper-personalization of war, in which militaries collect and deploy electronic dossiers on individual members of their opponents' militaries, has been predicted by experts including Maj. Gen. Charles J. Dunlap, Jr., USAF (Ret)., who separately introduced the term 'lawfare' into the legal and international relations literature.[122] Both the collection and the deployment of such dossiers could leverage other developing technologies including drones and facial recognition software.[123] Swarms of drones equipped with facial recognition software could 'roam battlefields looking for very specific members of an enemy's force', with the goal of either killing or communicating with them.[124]

It would not be surprising to see the PRC use such dossiers to wage lawfare against, or otherwise threaten, particular US or allied commanders. PRC analysis of the second Iraq War noted with great interest that the US-led coalition contacted Iraqi generals directly to warn them of prosecution if they followed any orders by Saddam Hussein to use weapons of mass destruction.[125]

Personal information could also be used to wreak havoc on the home front of targeted warfighters. An adversary could distract and demoralize the warfighter by emptying their bank accounts, hacking and publishing their medical records or messaging accounts, or sending them false messages from their families.[126] An adversary could also hack into the bank, medical, school, social media, or other accounts of the warfighters' spouses, children, or other relatives and issue very precise threats to them.[127] Something similar has already occurred,

[120] US-China Economic Security and Review Commission (n 2) 461.
[121] Ibid.
[122] Charles J. Dunlap Jr., 'The Hyper-Personalization of War: Cyber, Big Data, and the Changing Face of Conflict' (2014) 15 Georgetown Journal of International Affairs 108–18 <https://scholarship.law.duke.edu/faculty_scholarship/3381/> accessed 5 March 2023.
[123] Ibid. 110–11.
[124] Ibid. 111.
[125] Dean Cheng, 'Winning without Fighting: Chinese Legal Warfare' (*Heritage Foundation*, 18 May 2012) <http://www.heritage.org/research/reports/2012/05/winning-without-fighting-chinese-legal-warfare> accessed 5 March 2023.
[126] Dunlap (n 122).
[127] Ibid. 112, 115.

when Muslim extremists in Denmark 'tried to intimidate families of Danish soldiers in Afghanistan' by contacting them directly, hacking email accounts, and 'intercepting cell phone calls between soldiers in Afghanistan and their families'.[128]

Such hyper-personalized warfare could cause the warfighter to become anxious about the safety of their loved ones and make it extremely difficult for them to focus on their warfighting duties.[129] As such, it would be consistent with 'psychological warfare', which the PRC adopted alongside 'legal warfare' as a key element of its strategic doctrine.

The strong possibility that hyper-personalization will drastically change future armed conflicts underscores the importance of control over Americans' private information. One example of the battle over such control is the US government effort to restrict access to TikTok.[130] TikTok has approximately one hundred million monthly active users in the United States, fifty million of whom use it daily.[131] FBI Director Wray warned in December 2022 that control over TikTok provides the PRC with the ability to collect user data which 'can be used for traditional espionage operations' and with the ability to conduct 'malicious cyber activity' through 'access to the software' on millions of Americans' devices.[132]

In contrast, the Chinese internet is far more restricted, by what is sometimes dubbed 'the Great Firewall of China'. The PRC blocks foreign social media platforms including Facebook, Instagram, and Twitter; leading Western news sources including the *New York Times* and *Wall Street Journal*; entertainment and media sites including Netflix and YouTube; search engines including Google; and messaging apps including Signal and WhatsApp.[133] The PRC also rigorously censors communications on domestic social media.[134]

The PRC has already acquired massive amounts of Americans' personal information by hacking into databases. Attorney General William Barr attributed

[128] Ibid. 113.
[129] Ibid. 115.
[130] David Ingram, 'Biden Signs Tik Tok Ban for Government Devices' (*NBC News*, 30 December 2022) <https://www.nbcnews.com/tech/tech-news/tiktok-ban-biden-government-college-state-federal-security-privacy-rcna63724> accessed 5 March 2023.
[131] Alex Sherman, 'TikTok reveals detailed user numbers for the first time' (*CNBC*, 24 August 2020) <https://www.cnbc.com/2020/08/24/tiktok-reveals-us-global-user-growth-numbers-for-first-time.html> accessed 5 March 2023.
[132] Christopher Wray, '2022 Josh Rosenblatt Memorial Talk' (2 December 2022, University of Michigan) <https://fordschool.umich.edu/sites/default/files/2022-12/2022-12-02%20Christopher%20Wray_%202022%20Josh%20Rosenthal%20Memorial%20talk%20%28Audio%20ENG%29.txt> accessed 5 March 2023.
[133] See e.g. Junaid Ahmed, 'The Complete List of Blocked Websites in China' (*Security Gladiators*, 8 November 2022) <https://securitygladiators.com/censorship/blocked-websites-china/> accessed 5 March 2023.
[134] Gu Ting, 'China Steps Up Social Media Censorship, 'Upgrades' Great Firewall Ahead of Congress' (*Radio Free Asia*, 7 October 2022) <https://www.rfa.org/english/news/china/ccp-censorship-10072022135730.html> accessed 5 March 2023.

to the PRC the 2015 hack of the US Office of Personnel Management which stole the personnel records of practically every US federal civilian employee, including not just Social Security numbers but also the security clearance forms known as SF-86s, which contain very detailed and sensitive information.[135] Barr also attributed to the PRC the 2017 hack of Equifax which stole the personal credit and other information of 147 million people, roughly the entire adult population of the United States.[136] In addition, he attributed to the PRC the 2015 hack of Anthem, which stole the insurance information of nearly eighty million Americans.[137]

As a result of such hacks, Chinese intelligence has amassed a 'database more detailed than any nation has ever possessed about one of its adversaries'.[138] The value of this database includes 'identif[ying] potential weaknesses—through background checks, credit scores, and health records—of intelligence targets China may someday hope to recruit' or otherwise influence.[139]

A third method by which the PRC has attempted to acquire Americans' personal data has been through the purchase of US companies. For example, in 2020 the US government's Committee on Foreign Investment in the United States blocked a Chinese entity from buying a fertility clinic in San Diego, which contains the home port of the US Pacific Fleet.[140]

John Demers, head of the Justice Department's National Security Division, expressed concern that fertility clinic data, 'among the most intimate information about you', could be used by the PRC to coerce Americans.[141] He also speculated that such data could be used to develop 'some kind of biological weapon', noting that 'if you had all of the data of a population you might be able to see what the population is most vulnerable to and then develop something that's taking advantage of that vulnerability'.[142]

Notwithstanding these concerns, at least one other US fertility clinic has reportedly already been successfully purchased by entities connected to the Chinese Communist Party.[143] If Washington is going to more successfully counter the PRC's efforts to collect and deploy electronic dossiers of individual

[135] Garrett M. Graff, 'China's Hacking Spree Will Have a Decades-Long Fallout' (*Wired*, 11 February 2020) <https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/> accessed 5 March 2023.
[136] Ibid.
[137] Ibid.
[138] Ibid.
[139] Ibid.
[140] Eamon Javers, 'US Blocked Chinese Purchase of San Diego Fertility Clinic Over Medical Data Security Concerns' (*CNBC*, 16 October 2020) https://www.cnbc.com/2020/10/16/trump-administration-blocked-chinese-purchase-of-us-fertility-clinic.html> accessed 5 March 2023.
[141] Ibid.
[142] Ibid.
[143] Ibid.

Americans, the United States must strengthen both the content and the enforcement of its laws designed to protect Americans' private information.

5.4 Battle over whose telecommunications pipelines supply the world

The high value of personal information makes it essential to control the major telecommunications pipelines that transmit it. The grey zone lawfare battle over control of such pipelines includes efforts to set the technical standards which govern such pipelines. It also includes efforts to promote or retard the use of Huawei and other Chinese-made telecommunications equipment.

Technical standards are essential to the interoperability of telecommunications platforms. In 2021, the PRC released a fifteen-year plan, sometimes referred to as China Standards 2035, laying out China's strategy for setting the global standards for the next generation of technologies in fields including telecommunications and artificial intelligence.[144] China's technical advantage over other countries in 5G reportedly gives the PRC important leverage in standards discussions.[145]

The PRC's technical standards strategy is working to 'stack the digital deck in China's favor', according to a 2021 report by Daniel Russel, who previously served as President Obama's National Security Council Senior Director for Asian Affairs.[146] Russel's report outlines how the PRC has been achieving this objective.

For example, the PRC is working diligently to increase its influence within international standards development organizations (ISDOs), including by vigorously lobbying for key positions in these organizations.[147] The PRC's 'top-down, State-centric approach towards technical standards setting' contrasts sharply with the US government's 'longstanding hands-off approach, [which leaves] standard setting to the private sector and experts'.[148]

[144] Xinhua News Agency, 'The Chinese Communist Party Central Committee and the State Council Publish the 'National Standardization Development Outline' (Georgetown University Center for Security and Emerging Technology, 19 November 2021) <https://cset.georgetown.edu/publication/the-chinese-communist-party-central-committee-and-the-state-council-publish-the-national-standardization-development-outline/> accessed 5 March 2023.

[145] Helen Toner, 'Will China Set Global Tech Standards?' (*ChinaFile*, 22 March 2022) <https://www.chinafile.com/conversation/will-china-set-global-tech-standards> accessed 5 March 2023

[146] Daniel R. Russel and Blake H. Berger, 'Stacking the Deck: China's Influence in International Technology Standards Setting' (*Asia Society Policy Institute*, 2021) <https://asiasociety.org/sites/default/files/2021-11/ASPI_StacktheDeckreport_final.pdf> accessed 5 March 2023.

[147] Ibid. 18.

[148] Daniel R. Russel and Blake Berger, 'Will China Set Global Tech Standards?' (*ChinaFile*, 22 March 2022) <https://www.chinafile.com/conversation/will-china-set-global-tech-standards> accessed 5 March 2023

Beijing's involvement raises concerns that it will advocate for standards that 'ease greater surveillance or censorship through network infrastructure or protocols', no matter where the equipment is manufactured.[149] US Secretary of Commerce Gina Raimondo warned in November 2022 that China often 'packs' important international standard-setting bodies with 'government and business representatives who work together to push the country's authoritarian standards and values'.[150]

In addition, once Chinese standards are adopted, that 'creates a path dependency that locks other countries into using Chinese vendors'.[151] The use of Chinese vendors then provides 'access to immense quantities of data that are useful to both Chinese companies and government agencies'.[152] As a result, '[n]umerous US government officials have raised concerns about how the adoption of Chinese standards could cause potential compromises to national and personal security'.[153]

In addition to the grey zone lawfare battle over international telecommunications standards, the United States is also using lawfare to attempt to prevent Chinese companies, namely, Huawei and ZTE, from dominating the world's telecommunications network equipment. Huawei and ZTE are among the world's four largest makers of such equipment, along with the Finnish firm Nokia and the Swedish firm Ericsson.[154] Huawei is estimated to have the largest share of the global market, with about 30 per cent.[155]

The US government has repeatedly used law as a weapon to restrict Huawei's presence in the United States and limit its presence in global networks. For example, in 2017 and 2018, Congress prohibited various US government agencies from using or obtaining Huawei equipment or services.[156] In November 2021, the Federal Communications Commission effectively barred both Huawei and ZTE from selling new equipment in the United States.[157] In 2020, the Commerce

[149] Graham Webster, 'Will China Set Global Tech Standards?' (*ChinaFile*, 22 March 2022) <https://www.chinafile.com/conversation/will-china-set-global-tech-standards> accessed 5 March 2023.

[150] US Department of Commerce, 'Remarks by US Secretary of Commerce Gina Raimondo on the US Competitiveness and the China Challenge' (30 November 2022) <https://www.commerce.gov/news/speeches/2022/11/remarks-us-secretary-commerce-gina-raimondo-us-competitiveness-and-china> accessed 5 March 2023.

[151] Russel and Berger (n 146) 7.

[152] Ibid. 7.

[153] Russel and Berger (n 148).

[154] Jill C. Gallagher, 'US Restrictions on Huawei Technologies: National Security, Foreign Policy, and Economic Interests', Congressional Research Service (5 January 2022), 5, <https://crsreports.congress.gov/product/pdf/R/R47012> accessed 5 March 2023.

[155] Ibid.

[156] Ibid. 12–15.

[157] Reuters, 'US Bans Huawei, ZTE Equipment Sales Amid Chinese Spying Fears' (*CNN*, 26 November 2022) <https://www.cnn.com/2022/11/26/us/us-washington-huawei-zte-ban-security-risk-intl-hnk/index.html> accessed 5 March 2023.

Department limited Huawei's access to foreign-produced semiconductors made with US technologies.[158] In 2019 and 2020, the Justice Department charged Huawei with financial fraud, sanctions violations, racketeering, and conspiracy to steal trade secrets.[159]

Meanwhile, the US government has also been pressuring its allies to ban Huawei. For example, the UK[160] and Canadian[161] governments reportedly banned Huawei from their 5G telecoms network at least partly in response to US pressure. The UK's official reason for the ban was reportedly that US sanctions on Huawei would render the Chinese company's technology unreliable.[162]

Australia was the first country to ban Huawei products from its 5G network. It did so in 2018, after Mike Burgess, director-general of the Australian government's Signals Directorate, determined that Huawei products would not only risk PRC 'interception of telephone calls'.[163] Burgess identified an even greater risk: that much of Australia's critical infrastructure would come to be dependent on 5G and Beijing would be able to order Huawei to shut it off.[164]

Huawei has insisted that it would not comply with an order from the PRC government. The Australian prime minister who decided to bar Huawei, Malcolm Turnbull, did not believe the company. 'Huawei says, 'Oh no, we would refuse'. That's laughable', said Turnbull, asserting Huawei 'would have no option but to comply',[165] including because of the PRC's 2017 law that requires all Chinese persons and companies to cooperate with the government on any national security matter.[166]

Such a shutdown, Burgess concluded, would mean, 'The sewerage pump stops working. Clean water doesn't come to you . . . the public transport network doesn't work'.[167] In other words, the PRC would be able to bring Australia to its knees without firing a shot.

[158] Gallagher (n 154) 27.
[159] Ibid. 1–2.
[160] Alexander Smith, 'After Months of US Pressure, U.K. Bans China's Huawei from Its 5G Network' (*NBC News*, 14 July 2020) <https://www.nbcnews.com/news/world/after-months-u-s-pressure-u-k-bans-china-s-n1233752> accessed 5 March 2023.
[161] Andy Blatchford, 'Canada Joins Five Eyes in Ban on Huawei and ZTE' (*Politico*, 19 May 2022) <https://www.politico.com/news/2022/05/19/canada-five-eyes-ban-huawei-zte-00033920> accessed 5 March 2023.
[162] Smith (n 160).
[163] Peter Hartcher, 'Huawei? No Way! Why Australia Banned the World's Biggest Telecoms Firm', Sydney Morning Herald (Syndey, 11 May 2021) <https://www.smh.com.au/national/huawei-no-way-why-australia-banned-the-world-s-biggest-telecoms-firm-20210503-p57oc9.html> accessed 5 March 2023.
[164] Ibid.
[165] Ibid.
[166] Ibid.
[167] Ibid.

6. PRC grey zone lawfare using its trade authorities

In recent years, the PRC has accelerated deployment of its trade authorities to pursue military policy objectives. In contrast with the United States, China's coercive measures have typically not been formally announced (presumably in part as a way to circumvent potential WTO objections).

One such incident occurred in September 2010, after a Chinese boat, fishing in waters controlled by Japan but claimed by the PRC, collided with two Japanese Coast Guard ships.[168] Japan detained the Chinese boat's captain and refused at first to release him, saying his case was being handled by Japan's courts.[169] The PRC government then blocked exports to Japan of rare earth minerals, which are critical to Japan's manufacturing sector and largely supplied by China.[170] The PRC reportedly did so by quietly advising Chinese companies to halt rare earth exports and quietly ordering PRC customs officials to discretely block any such exports.[171] Publicly, PRC officials denied having imposed an embargo, while asserting that all of China's rare earth exporters 'simultaneously decided to halt shipments because of their personal feelings towards Japan'.[172]

Had there been a public announcement of a government-mandated export ban, Japan could have filed an immediate complaint with the WTO, alleging a violation of free trade laws.[173] However, the PRC's quiet blocking of such exports, combined with a public denial that it was taking such a step, put pressure on Japan without incurring legal consequences. A few days later, Japan released the Chinese captain.[174] When China lost a WTO ruling in 2014 in relation to its formal restrictions on rare earth exports, the ruling did not address the PRC's informal embargo on Japan, nor prevent a future such informal embargo.[175]

The PRC took a similar WTO-evading approach to South Korea in 2017. Following Seoul's installation of a US Terminal High Altitude Area Defense (THAAD) battery, China imposed unannounced economic sanctions on South

[168] Keith Bradsher, 'Amid Tension, China Blocks Vital Exports to Japan', *The New York Times* (New York, 22 September 2010) <http://www.nytimes.com/2010/09/23/business/global/23rare.html?pagewanted=all> accessed 5 March 2023.

[169] Bloomberg News, 'China Denies Japan Rare-Earth Ban Amid Diplomatic Row' (*Bloomberg*, 23 September 2010) <https://www.bloomberg.com/news/articles/2010-09-23/china-denies-japan-rare-earth-ban-amid-diplomatic-row-update1-> accessed 5 March 2023.

[170] Bradsher (n 168).

[171] Ibid.

[172] Paul Krugman, 'Rare and Foolish', *The New York Times* (New York, 17 October 2010) <http://www.nytimes.com/2010/10/18/opinion/18krugman.html> accessed 5 March 2023.

[173] Bradsher (n 168).

[174] AFP, 'China Blocked Exports of Rare Earth Metals to Japan, Traders Claim' (*The Telegraph*, 24 September 2010) <http://www.telegraph.co.uk/finance/china-business/8022484/China-blocked-exports-of-rare-earth-metals-to-Japan-traders-claim.html> accessed 5 March 2023.

[175] WTO Dispute Settlement, *China—Measures Related to the Exportation of Rare Earths, Tungsten and Molybdenum*, Dispute DS431 (29 August 2014).

Korean tourism, retail, and entertainment firms.[176] While the PRC never specifically linked the sanctions to the THAAD deployment, the message was clearly and painfully received.[177] A drastic decrease in Chinese tourism to South Korea cost the latter's economy an estimated $6.5 billion in lost revenue.[178] The billions in lost revenue contrast notably with the smaller ($800 million) cost of the THAAD battery.[179]

Such measures posed a greater economic risk to South Korea than to China; 26 per cent of South Korea's exports go to China,[180] and China provides 24 per cent of South Korea's imports.[181] In contrast, South Korea receives 4.5 per cent of China's exports,[182] and provides 8.8 per cent of China's imports.[183]

During the 2022 South Korean election, when one leading presidential candidate proposed that South Korea field a second THAAD battery to protect against North Korean missiles, the other responded by warning that doing so was a 'really dangerous act' that would 'ruin our economy' by provoking China.[184]

The PRC's use of its trade authorities to achieve military objectives has not been limited to its Asian neighbours. For example, in 2021, the PRC used these authorities in response to Lithuania's invitation to Taiwan to open a 'Taiwan Representative Office' in Vilnius.[185] Lithuania's invitation ran counter to the PRC's efforts to isolate Taiwan, potentially in preparation for kinetic action against the island.

Chinese customs responded by simply (and without a formal announcement) deleting Lithuania from its list of origin countries, making it impossible to file customs forms for cargoes to or from Lithuania.[186] When this failed to alter Lithuania's behaviour, the PRC first warned multinationals that they would be

[176] Christine Kim and Ben Blanchard, 'China, South Korea Agree to Mend Ties After THAAD Standoff' (*Reuters*, 30 October 2017) <https://www.reuters.com/article/us-northkorea-missiles/china-south-korea-agree-to-mend-ties-after-thaad-standoff-idUSKBN1D003G> accessed 5 March 2023.

[177] Ibid.

[178] Ibid.

[179] David Choi, 'South Korean Presidential Candidates Spar Over Need for More THAAD Missile Defense' (*Stars and Stripes*, 4 February 2022) <https://www.stripes.com/theaters/asia_pacific/2022-02-04/south-korea-thaad-missile-defense-battery-presidential-candidates-4623125.html> accessed 5 March 2023.

[180] Trading Economics, 'South Korea Exports by Country' <https://tradingeconomics.com/south-korea/exports-by-country> accessed 5 March 2023.

[181] Trading Economics, 'South Korea Imports by Country' <https://tradingeconomics.com/south-korea/imports-by-country> accessed 5 March 2023.

[182] Trading Economics, 'China Exports by Country' <https://tradingeconomics.com/china/exports-by-country> accessed 5 March 2023.

[183] Trading Economics, 'China Imports by Country' <https://tradingeconomics.com/china/imports-by-country> accessed 5 March 2023.

[184] Choi (n 179).

[185] Andrius Sytas, 'Lithuania Says Chinese Customs Is Blocking Its Exports' (*Reuters*, 3 December 2021) <https://www.reuters.com/article/china-lithuania-trade/lithuania-says-chinese-customs-is-blocking-its-exports-idUSKBN2II0Y7> accessed 5 March 2023

[186] Ibid.

subjected to secondary sanctions if they did not sever their ties with Lithuania, and then blocked from clearing PRC customs the cargoes of at least one German firm that sources from Lithuania.[187]

The PRC's coercive use of its trade authorities has also included Australia. In October and November 2020, the PRC took an unannounced series of purportedly technical actions restricting its trade with Australia.[188] This included delaying shipments of perishables such as fruit and live lobster, and verbally telling importers to avoid the import of several other Australian products due to possible delays clearing customs.[189] As a result of China's unofficial ban of Australian coal, several vessels laden with that product remained stuck off the coast of China for some six months.[190] The PRC reportedly issued no formal notice of the bans.[191]

Such measures pose a greater economic risk to Australia than China; 42 per cent of Australia's exports go to China,[192] making it Australia's largest market by far, and 29 per cent of Australia's imports come from China, making it Australia's largest source by far.[193] In contrast, 2 per cent of China's exports go to Australia, ranking it fourteenth,[194] and 6.7 per cent of China's imports come from Australia, ranking it fourth.[195]

That November, the PRC issued a public list of fourteen complaints about Australian government security policy, which Beijing said had 'poisoned' bilateral relations.[196] Many of the grievances were essentially complaints about Australian lawfare or interference with PRC lawfare. They included Australia: rejecting

[187] Matthew Reynolds and Matthew P. Goodman, 'China's Economic Coercion: Lessons from Lithuania' (*CSIS*, 6 May 2022) <https://www.csis.org/analysis/chinas-economic-coercion-lessons-lithuania> accessed 5 March 2023.

[188] Su-Lin Tan, 'China-Australia Relations: What's Happened Over the Past Year, and What's the Outlook?', South China Morning Post (20 April 2021) <https://www.scmp.com/economy/china-economy/article/3130109/china-australia-relations-whats-happened-over-past-year-and?module=inlineandpgtype=article> accessed 5 March 2023.

[189] Su-Lin Tan, 'What Happened Over the First Year of the China-Australia Trade Dispute?', South China Morning Post (28 October 2020) <https://www.scmp.com/economy/china-economy/article/3107228/china-australia-relations-what-has-happened-over-last-six?module=inlineandpgtype=article> accessed 5 March 2023.

[190] Su-Lin Tan (n 188).

[191] Su-Lin Tan (n 189).

[192] Trading Economics, 'Australia Exports by Country' <https://tradingeconomics.com/australia/exports-by-country> accessed 5 March 2023.

[193] Trading Economics, 'Australia Imports by Country' <https://tradingeconomics.com/australia/imports-by-country> accessed 5 March 2023.

[194] Trading Economics, 'China Exports by Country' <https://tradingeconomics.com/china/exports-by-country> accessed 5 March 2023.

[195] Trading Economics, 'China Imports by Country' <https://tradingeconomics.com/china/imports-by-country> accessed 5 March 2023.

[196] Jonathan Kearsley, Eryk Bagshaw, and Anthony Galloway, 'If You Make China the Enemy, China Will Be the Enemy': Beijing's Fresh Threat to Australia', Sydney Morning Herald (Sydney, 18 November 2020) <https://www.smh.com.au/world/asia/if-you-make-china-the-enemy-china-will-be-the-enemy-beijing-s-fresh-threat-to-australia-20201118-p56fqs.html> accessed 5 March 2023.

several Chinese investments on national security grounds; banning Huawei and ZTE from its 5G network; making a 'statement on the South China Sea to the United Nations;' and 'interfer[ing] in China's Xinjiang, Hong Kong and Taiwan affairs'.[197]

7. Conclusion

The PRC's grey zone lawfare has thus far been remarkably successful in achieving its objectives without firing a shot. Beijing's successes have leveraged several differences between the PRC on the one hand and the United States and its liberal democratic allies on the other hand. While it may not be possible to mitigate the PRC's leveraging of all of the differences, others could be more effectively managed by the West.

One difference is the greater leverage that law and its processes exert over the United States and its liberal democratic allies. This leverage results from a difference in ideology (with the PRC taking an exceptionally instrumental view of law), the lack of judicial or other independent checks and balances within the PRC government, and the relatively minimal influence over the PRC of NGOs, independent media, and other private-sector actors.

A second difference is the PRC's greater ability (including pursuant to its 2017 law) and willingness to use purportedly private-sector Chinese companies, individuals, and boats as proxies. This includes large companies such as Huawei as well as individual fishing vessels in the South China Sea. The West can, and should, respond by developing more effective means of countering the PRC's use of proxies to advance lawfare and other national policies behind a veil of 'plausible deniability'.

A third, somewhat related, difference is the PRC's particular ability, as an authoritarian regime, to take government actions without transparency. As a result, the PRC, unlike liberal democracies, can readily benefit from particular grey zone lawfare steps (such as blocking trade) without being held accountable for them under international law.

A fourth difference is the West's general hesitancy to regulate the internet and other telecommunications platforms that are available to Western audiences (especially compared with the 'great firewall of China' which strictly controls the Chinese internet). A fifth difference is that many of China's neighbours are more reliant on trade with the PRC than vice versa.

A sixth difference, which would be the easiest to remedy, is the US lack of a sophisticated and systematic, whole-of-government lawfare strategy and

[197] Ibid.

mechanism. If the United States is to win its current grey zone struggle against the PRC, and be fully prepared for a future kinetic war against China, it must promptly both adopt a comprehensive and coordinated lawfare strategy and create an interagency team to implement it.

The objectives should include both enhancing the US lawfare arsenal in general and better understanding and more effectively countering PRC lawfare. Implementation could enhance US lawfare by collecting and drawing lessons from case studies of US and allied lawfare successes and failures; by systematically identifying or developing US and allied points of lawfare leverage over the PRC; and by enhancing coordination and synergies amongst lawfare practitioners in the US government, allied governments, and the private sector. The initiative could more effectively counter PRC lawfare by improving the US's currently non-systematic monitoring of PRC lawfare; identifying and preparing for PRC next steps in current lawfare arenas; and identifying and preparing for PRC lawfare in new arenas.