Reordering the Law for a China World Order: China's Legal Warfare Strategy in Outer Space and Cyberspace

Bret Austin White*

INTRODUCTION 436
I. CHINA'S PLACE IN THE WORLD 438
A. *All Under Heaven* 438
B. *Westphalian World Order vs. Tianxia* 440
II. LEGAL WARFARE AS CHINA'S STATE POLICY 443
A. *China's Concept of Legal Warfare* 444
B. *Role of State Behavior in International Law* 447
1. The Law of Treaties 448
2. Customary International Law 449
C. *China's Legal Warfare - Testing the Waters* 450
III. CHINESE INFLUENCE ON INTERNATIONAL SPACE LAW 453
A. *The Scope of International Space Law* 455
B. *Vertical Sovereignty to the Heavens* 458
C. *Peaceful Purposes & China's Anti-Satellite Capabilities* 461
IV. DECODING THE EFFECTS OF CHINESE LEGAL WARFARE ON CYBERSPACE 466
A. *In Search of International Law of Cyberspace* 467
1. Prohibition on the Use of Force 471
2. Article 51 & Self-Defense 472
B. *The Fog of China's Cyber Legal Warfare* 475
C. *Sovereignty and Patriotic Hackers* 477
CONCLUSION 485

* Bret A. White is an active duty United States Marine Corps Judge Advocate, currently assigned as a National Security Law Attorney, United States Indo-Pacific Command. B.A., Texas A&M University (2002); J.D., Seton Hall University College of Law (2005); M.A. in Diplomacy, Norwich University (2018); LL.M in Space, Cyber, and Telecommunications Law, University of Nebraska College of Law (2019). An earlier draft of this article served as partial completion of the LL.M. requirements. The views expressed herein are solely those of the author and do not reflect the official positions of the Department of Defense, the Department of the Navy, or the United States Marine Corps.

I am exceedingly grateful for the guidance and mentorship provided by Professor Jack M. Beard of the University of Nebraska College of Law, who served as faculty thesis advisor. I also extend my sincerest gratitude to Professor Todd C. Huntley, Georgetown University Law Center, and Professor Fei-Ling Wang, Sam Nunn School of International Affairs at the Georgia Institute of Technology, both of whom were gracious with their time and provided invaluable review and commentary to further shape this article.

> Regardless of whether a war is just or not . . . the two sides in a war will both make every effort to develop 'legal warfare', and seek out means of constructing legal bases for undertaking the war, and confirm that they themselves are the reasonable and legal side. ~Fan Gaoming[†]

INTRODUCTION

From the end of World War II to the end of the Cold War, it was the United States and its Western allies who primarily shaped international law, particularly through the creation and growth in prominence of the United Nations. Following the end of the Cold War, the United States found itself in what many have labeled the "unipolar moment" where the U.S. and the West did not appear to have a direct competitor. But this period of U.S. and Western leadership may be passing in the eyes of a state like China whose history stretches back for millennia. The fact that this phase happened to coincide with China's "national humiliation," its century and a half of greatest weakness in perhaps the last two thousand years, permits China to view the Western-led world order as an aberration and not the norm.

Observers of China's rise towards great power status describe the ascent variously in aggressive and dangerous terms. Graham Allison warns that "China and the United States are currently on a collision course for war – unless both parties take difficult and painful actions to avert it."[1] Chinese political theorist Yan Xuetong also sees this friction and is a proponent of the "moral realism" school of thought.[2] This school addresses "the question of how a rising power can engage in effective competition with the dominate state in an international system . . . [and] one day overtake the dominant state."[3] Yan argues that "[i]n order to reduce the amount of friction caused by a nation's rise, moral realism posits that the rising nation should adopt the strategy of expanding its interests in emerging areas."[4] China is doing just that in the areas of outer space and cyberspace.

A recent white paper from Chinese officials states that "threats from such new security domains as outer space and cyberspace will be dealt with to maintain the common security of the world community."[5] Some strategists caution against seeing China's rise as a threat in the outer space and cyberspace domains, saying that "China's status as a rising power distorts how analysts portray Beijing's

---

† Fan Gaoming, *Public Opinion Warfare, Psychological Warfare, and Legal Warfare, the Three Major Combat Methods to Rapidly Achieving Victory in War*, GLOBAL TIMES (Mar. 8, 2005).

1. GRAHAM ALLISON, DESTINED FOR WAR: CAN AMERICA AND CHINA ESCAPE THUCYDIDES'S TRAP? vii (2017).

2. Yan Xuetong, *Strategic Challenges for China's Rise*, CARNEGIE-TSINGHUA CENTER FOR GLOBAL POLICY (Feb. 23, 2017), https://perma.cc/J8VU-5E7V.

3. *Id.*

4. *Id.*

5. STATE COUNCIL INFO. OFFICE OF THE PEOPLE'S REPUBLIC OF CHINA, CHINA'S MILITARY STRATEGY (2015), https://perma.cc/JK9A-TKUM. *See also Chinese Policy and Doctrine*, *in* GLOBAL COUNTERSPACE CAPABILITIES: AN OPEN SOURCE ASSESSMENT 1-20 (Brian Weeden, Victoria Samson, eds., 2018).

actions in cyberspace."[6] They believe that the "China threat narrative is entirely too pessimistic about future interactions with China" claiming that the source of such pessimism is "the growth of Chinese power and the fear it causes" within the defense industry.[7] Others, like renowned scholar John J. Mearsheimer, believe that China's rise will see it trying to maximize its relative power, both regionally and beyond, and will not behave in accordance with the principles of Confucian pacifism as some believe.[8]

Nor is China taking a passive approach to its growth in power and biding its time as it has seemed to do in the recent past in accordance with Deng Xiaoping's wisdom.[9] As China is on a path of returning to a position of leadership in the region and beyond, it has begun to enlist Chinese international law scholars to implement a state policy of 'legal warfare' to shape the future for a more powerful China. The application or formation of international law in areas of new and advancing technologies, such as innovations in outer space capabilities and activity in and through cyberspace, can be particularly challenging due to the lack of specific treaties and the dearth of state practice directly on point. As such, these areas – precisely the ones Yan advised China should focus its efforts – are particularly susceptible to manipulation by a determined state actor such as China.

In theory, all states that are active in international relations have a foreign policy strategy that helps that state reach its long-term goals. China's strategy is born from a deep-seated, millennia old manner in which China sees itself in relation to other states and in relation to the international order. China's political reality, for much of the last two thousand years, has been a "natural dominion over everything under heaven, a concept known in the Chinese language as *tian xia*."[10] This paper argues that China's state policy of manipulating international law in outer space and cyberspace will be informed by the *tianxia* worldview of China as benevolent leader, will increase China's relative power, and will empower its authoritarian state. Such an approach is also well in line with Yan's theory of how a rising power would act when it is replacing a dominant power.[11] He posits that during a change in global leadership, norms will change as well: "When the new international leadership is of a different type than the previous one, it will establish a new type of norms for purposes of maintaining

6. BRANDON VALERIANO, BENJAMIN JENSEN & RYAN C. MANESS, CYBER STRATEGY: THE EVOLVING CHARACTER OF POWER AND COERCION 146 (2018).

7. *Id*. at 144.

8. JOHN J. MEARSHEIMER, THE TRAGEDY OF GREAT POWER POLITICS 406-07 (Updated ed., 2014).

9. *See* HENRY KISSINGER, ON CHINA 333 (2011).

10. HOWARD W. FRENCH, EVERYTHING UNDER THE HEAVENS: HOW THE PAST HELPS SHAPE CHINA'S PUSH FOR GLOBAL POWER 4 (2017) (pointing out that translations of this term vary between "all under heaven" and "everything under the heavens", but the sense of the term is more important. It has meant 'all of the known world', from the Chinese perspective. Transliterations of the term also vary between two distinct words (*tian xia*) and a single word (*tianxia*)). When using direct quotes, I use the variation found in the original text. Otherwise, I have chosen the single word variation due to its apparent greater acceptance in the literature.

11. YAN, *supra* note 2.

its dominance of the international system."[12] China's behavior in the areas of outer space and cyberspace – seeking to take a leadership role and shape norms – is preparing the environment for when it will be one in a bipolar global order or, depending on the actions of the United States, perhaps the global leader in a shifted unipolar order.

It is important to establish the historical and conceptual foundations upon which China has built its policy of using legal warfare to achieve its strategic goals. In Part I, I will introduce the reader to the *tianxia* worldview at the core of the Chinese policies and the relationship that worldview has to the Westphalian system. China's state policy of legal warfare is a natural outgrowth of that worldview as China seeks to regain its perceived rightful place as a great power. Part II will discuss the Western concept of "lawfare" and China's related "legal warfare" policy, the manner in which China manipulates both treaty law and customary international law (CIL), and briefly examine how China has used claims and disputes in the South China Sea and East China Sea as a template for future legal warfare efforts in more complex domains.[13]

In Part III, I will consider China's efforts at legal warfare in outer space. I will first discuss the surprisingly rich body of law which governs state behavior in relation to outer space, then look more closely at specific areas wherein China may find legal warfare useful to its goals and determine whether or not China's legal warfare strategy is effective in those areas. In Part IV, I will survey the current state of international law regarding state behavior in and through cyberspace and consider how China's actions and policies demonstrate its legal warfare strategy in this domain. I will conclude by examining China's broader strategic goals, particularly considering China's rapid and continuous rise, along with what type of impact its continued use of legal warfare in expanding space and cyberspace domains is likely to have on international law in those areas. It is necessary to consider the impact of China's continuing growth in power regionally and globally and the likely subsequent impact of legal warfare strategies as China continues to adapt them to meet its broader goals.

I. CHINA'S PLACE IN THE WORLD

A. All Under Heaven

The *tianxia* system was an international order, albeit not a global order, wherein all or nearly all actors within the system operated under the dominion of China in a tributary relationship to the recognized leader in the "central kingdom".[14] The other actors in the system accepted – or feigned acceptance of – a set

12. *Id.*

13. Part II details the origin of each of these terms. Throughout this paper, I will use the term "lawfare" when referring to the US or Western conception and I will use "legal warfare" when specifically referencing the Chinese conception and implementation.

14. *See* June Teufel Dreyer, *The 'Tianxia Trope': will China change the international system?* 29 J. CONTEMP. CHINA 1015, 1020 (2015). The author focuses on the fact that some scholars, primarily Westerners, have taken to advocating for *Tianxia* as a "solution to the ills of the post-modern world", ills caused by "rampant materialism and spiritual pollution that had come in from the West as a result of

of rules governing international relations.[15] "Order is maintained under the aegis of a benign hegemonic state personified by the [Chinese] emperor as Son of Heaven, and administered for the benefit of all under heaven."[16]

Tianxia is rooted in Confucianism and other deeply held Chinese ideas and traditions over centuries.[17] By the fourteenth century, *tianxia* was accepted throughout Asia.[18] The institutions and practices embedded in *tianxia* included "periodic journeys of principals or their envoys to the Chinese capital bearing precious gifts, performing *ketou* of obeisance to the ruler of all under heaven . . . [and receiving in return] confirmation of their legitimacy as ruler of their states."[19] Ritualistic performance of acts such as these bore heavily on all political, economic, and cultural relations throughout the region.[20]

Chinese writer Zhao Tingyang finds the roots of *tianxia* in the Zhou dynasty (circa 1027 – 256 BCE) noting that the Zhou kings were the first to put the concept into practice (and in Zhao's conception the only practice worth emulating).[21] According to international law historian Stephen C. Neff, following the unification of the "Warring States" during this period, "the creative period of Chinese thought in the international relations field came largely to an end."[22] China's unification into a centralized empire meant that any consideration of foreign relations was effectively of no value.[23]

The reality of a *tianxia* world order, however, varied greatly over the centuries from this original concept. During the "Era of the Two Songs" (10th – 13th centuries), China even led a "codified Westphalia-like world order" for a time, yet only between those nearby neighbors to China within Asia.[24] Following this period, politically motivated history-writing and teaching dismissed the egalitarian concepts of the Song era.[25] Instead, the government "forcefully enshrined" the *tianxia* system as "*the* Chinese political tradition and worldview" that continued to grow until the Qing Empire (1644-1911).[26] The Qing system was perhaps an

---

Deng [Xiaoping]'s open door policy aimed at helping the PRC to industrialize." *Id.* at 1015-17. These advocates argue that "[l]acking a supreme authority, the world must perforce exist in a Hobbesian atmosphere of all against all." She concludes that, ". . . several [powerful states] claim to have superior civilizations of their own, and there are alternative organizing principles for the component parts of the totality. In this duel of competing paradigms, Westphalian sovereignty has definite advantages." *Id.* at 1027.

15. *Id.* at 1016.
16. *Id.*
17. *Id.*
18. *Id.*
19. *Id.*
20. *Id.*
21. *Id.* at 1021.
22. STEPHEN C. NEFF, JUSTICE AMONG NATIONS 39 (2014).
23. *Id.*
24. FEI-LING WANG, THE CHINA ORDER: CENTRALIA, WORLD EMPIRE, AND THE NATURE OF CHINESE POWER 57 (2017).
25. *Id.*
26. *Id.*

idyllic *tianxia* system in that it literally united and controlled the whole known world and beyond for a long time.[27]

Following the two world wars and beginning with the founding of the People's Republic of China (PRC) in 1949, *tianxia* was replaced with a "Marxist-centered universalism."[28] Under Mao Zedong's rule, however, China's role in the world left much to be desired for the ambitions of a once-powerful people.[29] In response to the failures of Marxist-Leninist theories put into practice under Mao and Deng Xiaoping, Chinese scholars began to look back to Chinese tradition "as a source of legitimacy for the Chinese state."[30] Political philosophers began to cultivate ideas of a "socialism with Chinese characteristics" turning both to the works of Confucius and mythologizing the role and success of *tianxia* in China's past.[31]

Modern *tianxia* is not only found in China; it is exported. "Beginning in 2004, a network of Confucius Institutes came into being to acquaint the world with the CCP's interpretation of ancient Chinese tradition. By the end of 2014, they numbered 433, operating in 104 countries and regions around the world."[32] These institutes are found in universities and "Confucius Classrooms" for kindergarten through middle school, "answer[ing] to the Hanban, supervised by China's Ministry of Education, with the goal of enhancing appreciation for the PRC's soft power while seeking to alleviate concerns about the country's rapid rise."[33] Writers and advocates link *tianxia* with the Confucian concept of "Great Harmony," attempting to appeal to "a world weary of war."[34] Arguing that historical acceptance of *tianxia* throughout Asia led to widespread peace under a benign hegemon, University of Southern California professor David Kang believes that "most Asian states would prefer a strong China to a weak one and do not fear its increasing power, which he credits with an important role in the past three decades of relative stability in the region."[35] The juxtaposition of *tianxia* to the current world order, often described as the Westphalian world order, yields dramatic distinctions.

B. Westphalian World Order vs. Tianxia

The Peace of Westphalia, comprised of the Treaties of Osnabrück and Münster, was concluded in 1648 and is widely credited with the establishment of the modern state system.[36]

---

27. *Id.* at 71.
28. Dreyer, *supra* note 14, at 1021.
29. *See generally* Zhao Tingyang, *A political world philosophy in terms of All-Under-Heaven (Tianxia)*, 56 DIOGENES 5, 5-18.
30. Dreyer, *supra* note 14, at 1016.
31. *Id.* at 1016-17.
32. *Id.* at 1017.
33. *Id.*
34. *Id.*
35. Dreyer, *supra* note 14, at 1017-18.
36. NEFF, JUSTICE AMONG NATIONS, *supra* note 22, at 139.

> With the passage of time, the Peace of Westphalia came to assume a sort of triple identity – first, as a settlement of immediate issues at stake in the Thirty Years War; second, and more broadly, as a basis for a longer-term European balance of power; and finally, and most expansively of all, as a model or metaphor for modern international affairs in general.[37]

While arguably not a watershed beginning of state sovereignty it is often portrayed to be, "[the Peace of Westphalia] is traditionally attributed [with] the importance and dignity of being the first of several attempts to establish something resembling world unity on the basis of states exercising untrammeled sovereignty over certain territories and subordinated to no earthly authority."[38] Neff would argue that this degree of reverence over the Peace is largely overstated in the sense that the Peace was more of a codification of practice that was already occurring in parts – that of individual German states to act independently of the Holy Roman Empire.[39] "[T]he actual terms of the settlement, interesting and novel as they may be, would hardly suffice to account for the outstanding place attributed to it in the evolution of international relations." Indeed, it is the implications of the treaties and the developments to which they provided impetus that is most notable. "[I]t has been affirmed that the Peace of Westphalia was the starting point for the development of modern international law." And, the Peace set all states on equal footing with no regard for the form of government or confessional status of their leaders.[40] Further attempts at firming up the world order and rights of separate states would travel a path through the Concert of Europe, the Paris Settlement of 1919, the League of Nations, and finally the Charter of the United Nations.[41]

For two millennia, the fundamental concepts of the Westphalian system, "a multistate system, in which the states were on . . . equal footing, was, . . . fundamentally alien to Chinese thinking."[42] Whereas the Western worldview "would ultimately become the basis of our modern international law", the Chinese worldview could claim no such credit because "it was neither international nor legal."[43] The Chinese worldview, as Neff describes it, is that of a single political community, essentially an ancient conception of a world government.[44] Furthermore, Neff explains that the Confucian view is not legal in nature, but rather moral.[45] It was based on the notion of law as "an instrument of social control, electing to rely instead on authoritarian rule by a sovereign of

37. *Id*. at 139-40.
38. Leo Gross, *The Peace of Westphalia, 1648-1948*, 42 AM. J. INT'L L. 20, 20 (1948).
39. NEFF, JUSTICE AMONG NATIONS, *supra* note 22, at 139-40.
40. Gross, *supra* note 38, at 26.
41. *Id*. at 20-24.
42. NEFF, JUSTICE AMONG NATIONS, *supra* note 22, at 39.
43. STEPHEN C. NEFF, WAR AND THE LAW OF NATIONS: A GENERAL HISTORY 33 (Paperback ed., 2008).
44. *Id*.
45. *Id*. at 33-34.

unimpeachable benevolence."[46] "According to the Confucian view, therefore, even barbarians were not utterly alien. They were merely imperfectly integrated into the great global order. The best way of dealing with them was gradually to reform them by setting a good example of what a fully civilized society was like. This normal peaceful relation with the neighboring barbarian states was symbolized by the ritualistic exchange of 'gifts' or 'tribute' between the Chinese government and envoys from the barbarian states."[47]

As China moves to regain its position as a regional hegemon and eventually the sole great power, it is faced with the decision to either integrate more fully into the current world system of co-equal states or attempt to force change to the Chinese worldview. In 2009, Zhao Tingyang argued that the world has been misled by American leadership post-World War II. Zhao "advocates creating a world government based on world theory that prioritizes the well-being of all people" as the solution for a "failed world."[48] He believes that the United Nations has demonstrated an inability to serve as such a world government.[49] The Chinese view, then, is that such leadership should naturally come from Beijing. Wang sees the strategy of the *tianxia* (or China Order) worldview as a precondition – in the eyes of the CCP-PRC hierarchy – for a "new, better, more harmonious and rational world order. . ..[which would] restore the China Order."[50] This worldview has been underlying Chinese empire, in all its forms, for centuries and is directly contrary to an egalitarian Westphalian model.

Many scholars have commented that China appears more likely to move towards a modern *tianxia* than integrate into the Westphalian model. They believe that, "when given the chance, the Chinese may wish to go back to their long-hallowed tradition of treating foreign countries as all alike but unequal and inferior to China."[51] Wang argues that the "PRC Qin-Han polity constantly and inevitably feels discontent and insecure without the China Order" and that it must "either expand to conquer or convert the whole known world, to deny the ungoverned, or to keep the ungovernable away."[52]

> Chinese dissatisfaction with an international order that it is increasingly enmeshed within, but which it did not construct, is similar to the reaction of Germany's political elites at the end of the nineteenth century. The reasoning is similar: The benefits of the extant system are dispersed asymmetrically, and most of the dividends are seen as devolving to American hegemonic power . . . the current international order does not comport with what the

46. *Id*. at 34.
47. *Id*. at 32.
48. Dreyer, *supra* note 14, at 1021.
49. *Id*. at 1022.
50. WANG, *supra* note 24, at 211.
51. FRENCH, *supra* note 10, at 266.
52. WANG, *supra* note 24, at 209.

> Chinese feel is their due . . . part of continuing injustice perpetrated by [the West].[53]

China will not take its place by use of traditional military aggression. In fact, China has determined that rather than integrate into the Westphalian system – with its egalitarian view of states operating within the bounds of international law – it will instead manipulate international law to reassert itself on the world stage.

II. LEGAL WARFARE AS CHINA'S STATE POLICY

In the West, it would be called "lawfare." The term is nearly ubiquitous in American national security and military circles, but it has a specific meaning as proposed by its initial advocate, Major General Charles J. Dunlap, Jr., United States Air Force (ret.). Since his first published conceptualization of the term in 2001, Dunlap has written and spoken at length on the topic, modifying the definition slightly in the process.[54] The final incarnation of lawfare by Dunlap's estimation is: "the strategy of using – or misusing – law as a substitute for traditional military means to achieve a warfighting objective."[55] The term "warfighting" may seem narrow to some, but if war itself is considered in the sense of an extension of politics as Clausewitz posited, then the definition holds.[56] Lawfare has since been examined and re-defined in numerous fora and for as many purposes, but they all acknowledge "that lawfare is concerned with the instrumentalization or politicization of the law to achieve a tactical, operational, or strategic effect."[57]

Dunlap remains keen to highlight that lawfare is value neutral; to be used for good or bad purposes.[58] States can, he says, "[i]deally, substitute[e] lawfare methodologies for traditional military means [to] reduce the destructiveness of war, if not its frequency."[59] He notes that, if employed intentionally, law can create the same or similar effects as traditional warfighting methodologies.[60] If designed to achieve a particular effect and employed with strategic deft, law can force an adversary to take or withhold specific action; it can build international opinion into support for a cause; it can shape the strategic environment for the state who wields it wisely. No state has created an as well-developed strategic doctrine of lawfare nor so clearly implemented its use in policy as has China.[61]

---

53. JAMES A. NATHAN, SOLDIERS, STATECRAFT, AND HISTORY: COERCIVE DIPLOMACY AND INTERNATIONAL ORDER 118 (2002).

54. Charles J. Dunlap, Jr., *Law and Military Interventions: Preserving Humanitarian Values in 21st Century Conflicts* (2001), https://perma.cc/G9YH-PUZ8.

55. Charles J. Dunlap, Jr., *Lawfare Today . . . and Tomorrow*, 87 INT'L L. STUD. 315, 315 (2011).

56. *See* KARL VON CLAUSEWITZ, ON WAR 87 (Howard & Paret trans. and eds., 1984).

57. Dale Stephens, *The Age of Lawfare*, 87 INT'L L. STUD. 327, 327 (2011).

58. Charles J. Dunlap, Jr. *Lawfare Today: A Perspective*, 3 YALE J. INT'L AFF. 146, 146-47 (2008).

59. *Id*. at 147.

60. Charles J. Dunlap, Jr., *Does Lawfare Need An Apologia?*, 43 CASE W. RES. J. INT'L. L. 121, 122 (2010).

61. *See generally* ORDE F. KITTRIE, LAWFARE: LAW AS A WEAPON OF WAR 8, 161 (2016).

A. China's Concept of Legal Warfare

In 1864, an American missionary, William A. P. Martin, translated into Chinese the first systematic treatise on international law in the English language, Henry Wheaton's *Elements of International Law* (1836).[62] French and American diplomats alike observed this development with some concern noting that, coming as it did just over two decades after the Opium War, this treatise was "legal ammunition" which could enable the Chinese to cause "endless trouble" for the West.[63] Fears that the Chinese "might start looking for legal grounds to contest" matters of unequal treatment were well-founded.[64] In the same year China received the translation, Chinese officials used Wheaton's text to resolve a dispute that arose between Prussia and Denmark over the capture of a Danish ship within Chinese territorial waters.[65] This capture violated China's rights as a neutral and China ably advocated for such rights using Wheaton's treatise as her guide.[66] The dispute was resolved in China's favor with Prussia forced to release the ship and pay $1,500 in compensation.[67]

Stymied by numerous wars and the National Humiliation, China did not institutionalize its use of lawfare until the beginning of the 21st century. This policy is one supporting effort of a broader policy that grew out of China's observations of the magnificent speed at which information in all forms became key to societies and integral to national infrastructure and power.[68] Chinese political analysts defined what they called "informationization" (*xinxihua*) as:

> [A] comprehensive system of systems, where the broad use of information technology is the guide, where information resources are the core, where information networks are the foundation, where information industry is the support, where information talent is a key factor, where laws, policies, and standards are the safeguard.[69]

In so doing, the Chinese Communist Party (CCP) was following through on Chinese President Jiang Zemin's guidance to a group of Chinese international law experts in 1996: "we must be adept at using international law as a weapon."[70] The resulting product was the conception of *falu zhan*, or "legal warfare," as one of the "Three Warfares" approved by the CCP and the Chinese Central Military Commission in 2003 as non-kinetic weapons of war:

---

62. NEFF, JUSTICE AMONG NATIONS, *supra* note 22, at 228, 313.
63. *Id.*
64. *Id.*
65. *Id.*
66. *Id.*
67. *Id.*
68. DEAN CHENG, CYBER DRAGON: INSIDE CHINA'S INFORMATION WARFARE AND CYBER OPERATIONS 1 (2017).
69. *Id.*
70. KITTRIE, *supra* note 61, at 161.

> 1) *Psychological Warfare*: the use of propaganda, deception, threats, and coercion to affect the enemy's ability to understand and make decisions; 2) *Media Warfare*: the dissemination of information to influence public opinion and gain support from domestic and international audiences for China's military actions; and 3) *Legal Warfare*: the use of international and domestic law to gain international support and manage possible political repercussions of China's military actions.[71]

Several additional publications in China have elaborated on legal warfare since the announcement of the Three Warfares in 2003[72]. The descriptions of the usages and methods of legal warfare by these authors prove instructive for how China views law in this context.

One exhaustive treatment of historical cases of legal warfare, *Analysis of 100 Cases of Legal Warfare* (2004) published by the People's Liberation Army (PLA), speaks of legal warfare in strong terms as a tool to control the enemy with the law or constrain the enemy.[73] Chinese officials using international law can "find a lot of room for manipulation in the respects of the content, timing, and extent of application [of the law of war]."[74] The PLA is implored to "enhance the art and level in the application of the law of war so as to attain the best effect."[75] Published in 2005, *Legal Warfare in Modern War*, explains that the Law of Armed Conflict (LOAC) should be viewed as a "weapon to achieve such objectives as manipulating the perception of the international community."[76] And, the quite broad conception in one of the PLA's military texts for a general military audience, not just international lawyers: "war is not only a military struggle, but also a comprehensive contest on fronts of politics, economy, diplomacy, and law."[77]

In his study of China's information operations and cyber operations capabilities, force structure, and strategy, Dean Cheng said of the legal warfare strategy:

> In peacetime, legal warfare influences domestic and foreign populations and leaders, weakening opposing coalitions while building support for one's own side. In wartime, it manipulates the rule of law in order to 'destroy the will to fight by undermining the public support that is indispensable' for successful warfighting.[78]

The peacetime role is particularly noteworthy. The strategy attempts to influence target populations worldwide as a sort of "political preparation of the

71. *Id.* at 162.
72. *Id.* at 161-65.
73. *Id.* at 162.
74. *Id.*
75. *Id.*
76. *Id.*
77. *Id.*
78. CHENG, *supra* note 68, at 49.

battlefield" and employs legal scholars and other voices on China's behalf to "propagate Chinese legal positions and perspectives" in order to gain support for their positions in advance of needing to rely on that support.[79]

It is important to note, however, that China does not view its own employment of legal warfare as unique – Chinese officials believe that other states in the West, particularly the United States, are already adept at employing legal warfare.[80] "According to the PLA analyses of recent conflicts, including the two Gulf Wars, the United States is one of the leading practitioners of legal warfare."[81] In the cyberspace context, Chinese academics believe the U.S. is engaging in a legal warfare strategy by pushing behind the scenes for the development of *Tallinn Manual 2.0: On The International Law Applicable to Cyber Operations*.[82] One Chinese media commentator described the U.S. as attempting to "spur the international community into drawing up rules for cyberwarfare in order to put a cloak of legality on its 'preemptive strike' strategy in cyberwarfare."[83] Chinese commentators specifically state that *Tallinn Manual 2.0* would serve only to legitimize U.S. "abuses."[84] When assessing these comments, it is important to note that, while they are not accurate assessments of the U.S. role in *Tallin Manual 2.0*, they likely present an accurate portrayal of how China views the utility of legal warfare.

China's policy of employing legal warfare to achieve its strategic goals is not merely because the United States does so. There are two reasons, as articulated by Peter Mattis: 1) China's view of an expansive array of threats to the CCP, and 2) China's assessment that the PLA could not win a force-on-force, kinetic conflict with the United States.[85] Mattis describes China's assessment of the national security threats as "nearly unlimited" in the context of China's National Security Law of 2015:

> National security refers to the relative absence of international or domestic threats to the state's power to govern, sovereignty, unity and territorial integrity, the welfare of the people, sustainable economic and social development, and other major national interests, and the ability to ensure a continued state of security.[86]

79. *Id*. at 48.

80. Dean Cheng, *Winning Without Fighting: Chinese Legal Warfare*, THE HERITAGE FOUNDATION (May 21, 2012), at 3.

81. *Id*. at 4.

82. Julian Ku, *How China's Views On the Law of Jus ad Bellum Will Shape Its Legal Approach to Cyberwarfare*, Aegis Series Paper No. 1707 HOOVER INSTITUTION, Aug. 17, 2017, at 16.

83. *Id*. at 16-17.

84. *Id*. at 19.

85. Peter Mattis, *China's 'Three Warfares' In Perspective*, WAR ON THE ROCKS (Jan. 30, 2018), Peter Mattis, *China's 'Three Warfares' In Perspective*, WAR ON THE ROCKS (Jan. 30, 2018), https://perma.cc/W6MT-YPZT (describing the PLA as the military arm of the CCP, explaining that "the Chinese military's purpose is to create political power for the party").

86. *Id*. (citing Article II of the 2015 National Security Law of China).

Mattis' study of official CCP documents further reveal its assessment that the PLA's capabilities against its likely adversaries in the West are no match and are particularly incompatible with winning wars conducted in the high-tech manner that the United States and its closest allies would conduct.[87] Particularly damning is the assessment by the CCP that "there are big gaps between the level of our military modernization compared to the requirements for national security."[88]

Considering the breadth of China's national security needs and the comparative weakness of the PLA to its most likely adversaries, it is certainly to China's strategic benefit to use legal warfare to at least the same degree as it perceives the United States doing so. And, as Dunlap emphasized, lawfare is ideologically neutral. Any state can employ it to achieve their objectives. We turn next to a discussion of how international law avails itself to manipulation by state actors, particularly powerful states.

B. Role of State Behavior in International Law

Since international law has, throughout history, lacked the triad of bodies found in typical Western national legal systems – legislative, executive, and judicial bodies – international law can be more difficult to define and interpret than national law.[89] It is critical, then, that in modern international law, Article 38(1) of the Statute of the International Court of Justice (ICJ) is accepted as the first place to determine both the sources and the precedence of international law:

> . . . [The ICJ], whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply: (a) international conventions, whether general or particular, establishing rules expressly recognized by the contesting states; (b) international custom, as evidence of a general practice accepted as law; (c) the general principles of law recognized by civilized nations; (d) subject to the provisions of Article 59, judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for determination of rules of law.[90]

There is no serious disagreement that Art. 38(1) "expresses the universal perception as to the enumeration of sources of international law."[91] As the primary actors and subjects of international law, the behavior of states is of utmost consideration. A single state, particularly a powerful and influential state, can have the most intentional impact on international law in the contexts of treaties (or international conventions) and CIL.

87. *Id.*
88. *Id.*
89. MALCOLM N. SHAW, INTERNATIONAL LAW 49 (7th ed., 2014).
90. Statute of the International Court of Justice art. 38, ¶ 1.
91. SHAW, *supra* note 89, at 50.

1. The Law of Treaties

A treaty is defined broadly in Article 2(1)(a) of the Vienna Convention on the Law of Treaties (VCLT) as "an international agreement concluded between states in written form and governed by international law, whether embodied in a single instrument or in two or more related instruments and whatever its particular designation", be it an agreement, convention, pact, treaty, covenant, declaration, or otherwise.[92] Thus, the principal manner in which a state can impact international law in the treaty context is by participating in the drafting of such an agreement. Once a state has entered into a treaty and formalized its consent to be bound, perhaps the oldest principle of international law governs: *pacta sunt servanda*.[93] This rule simply means that agreements are binding to parties of an agreement. Powerful states certainly impact international law in the treaty context by influencing the language of the treaty, encouraging other states to participate in the treaty, and negotiating compromises to ensure that a treaty is actually concluded.

The general rule for interpretation of treaties, found at Article 31 of the VCLT provides that treaties shall first be "interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in light of its object and purpose."[94] States may also influence the way in which treaties are applied or its terms are interpreted subsequent to the conclusion of the treaty in two particular ways of note: "(a) any subsequent agreement between the parties regarding the interpretation of the treaty or the application of its provisions; (b) any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation."[95]

States can also have a role in shaping international law in a treaty context by declining to participate in the treaty at all; and for some states, this may have a significant impact on which other states and how many ultimately join in the treaty. Frequently and for various reasons, states participate in treaties but derogate from them in writing through means of a reservation.[96] In effect, a state may reject or modify certain limited language in a treaty while agreeing to the remainder. This could be done in order to modify language to comport with that state's national requirements and have the treaty fall in line with their own laws to avoid conflicting obligations. Not all treaties allow reservations. But, the utility of doing so in many cases is that reticent states may consent to a treaty which they would otherwise reject in its entirety without the reservation. "This may have beneficial

92. Vienna Convention on the Law of Treaties art. 2(1)(a), May 23, 1969, 1155 U.N.T.S 331 [hereinafter VCLT].

93. SHAW, *supra* note 89, at 655.

94. VCLT art. 31(1).

95. VCLT art. 31(3)(a)–(b).

96. VCLT art. 2(1)d. A reservation is "a unilateral statement, however phrased or named, made by a state, when signing, ratifying, accepting, approving or acceding to a treaty, whereby it purports to exclude or to modify the legal effect of certain provisions of the treaty in their application to that state." The relevance of the "however phrased or named" term is that various parties may use different naming conventions for reservations, e.g., understandings, declarations, etc.

results in the cases of multilateral conventions, by inducing as many states as possible to adhere to the proposed treaty."[97]

2. Customary International Law

In contrast to the definitive nature of treaties, CIL is far more nebulous and is often not written down, especially in the formative stages. Shaw describes this type of law as "a dynamic source of law in the light of the nature of the international system and its lack of centralized government organs", particularly in light of a comparison both to international treaty law and to custom in the national legal context.[98] The definition provides two parts to custom, the generalized practice of states and acceptance of such a practice as law.[99] CIL forms over an unspecified duration of time that may be long, as in the law of the sea;[100] or may be exceptionally short, as in areas of rapidly developing technology like outer space and cyberspace.

State practice is not the practice of individual states on their own. It is found in the "extensive and virtually uniform" practice of states, particularly "that of states whose interests are specially affected."[101] The ICJ clarified the uniformity aspect of state practice:

> [T]he Court deems it sufficient that the conduct of states should, in general, be consistent with such rules, and that instances of state conduct inconsistent with a given rule should generally have been treated as breaches of that rule, not as indications of the recognition of a new rule.[102]

Furthermore, specially affected states are those such as seafaring states in a law of the sea dispute, spaceflight capable states in an outer space issue, or technologically advanced states in a cyberspace concern.

The second aspect of the ICJ's definition of CIL is the condition that the behavior is conducted out of a sense of legal obligation – *opinio juris* – and not merely out of convenience, nor threat or other coercion.[103] It is the "presence or absence (as the case may be) of a general or collective consensus on the part of states as to the existence of a law."[104] This factor can be far more difficult to identify in conjunction with an observed state behavior because it is the 'why' aspect of state action or inaction. In modern usage, states assist legal scholars (and other states)

---

97. SHAW, *supra* note 89, at 663.

98. *Id*. at 52.

99. Statute of the International Court of Justice art. 2, ¶ 1(a).

100. Notably, the law of the sea was largely formed as a set of CIL rules and later codified in the form of a treaty in the United Nations Convention on the Law of the Sea. China's use of legal warfare in this arena is discussed below.

101. North Sea Continental Shelf, Judgement, 1969 I.C.J. 3, 29 (Feb. 20).

102. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, 98 (June 27).

103. SHAW, *supra* note 89, at 60.

104. NEFF, JUSTICE AMONG NATIONS, *supra* note 22, at 418.

in identifying the motivating force behind an action by their public official statements or national policies related to an undefined area of CIL.

State behavior during the formation or modification of CIL taken in *response* by other states is of great importance, as well. In the *Gulf of Maine* case, the ICJ defined 'acquiescence' as "equivalent to tacit recognition manifested by unilateral conduct which the other party may interpret as consent."[105] As such, when a state takes a particular action with an accompanying official statement that the action is legal under international law, other states must protest or their acquiescence will be seen as consent. An additional consideration during the formation or modification of a rule of CIL is the role of the 'persistent objector.' This rule provides that a "state opposing the existence of a custom from its inception" will not be bound by such a rule.[106] The combination of state behavior inconsistent with custom and acquiescence by other states may be the beginning of a new customary rule or, at minimum, an exception to an old rule.

The nature of CIL can be described as "democratic in that all states may share in the formulation of new rules, though the precept that some are more equal than others in this process is not without its grain of truth."[107] Thus state behavior in CIL is of great significance, as is the identity of a state who seeks to form a new rule or exception. Powerful and influential states may gather others to their cause in supporting statements of *opinio juris* or find that its allies acquiesce to an action and statement while testing the receptivity of the behavior on the international stage.

C. China's Legal Warfare - Testing the Waters

It is instructive to consider China's application of legal warfare in the law of the sea context to better identify legal warfare methods and objectives in other domains. The law of the sea is comprised of CIL and the convention law found within the United Nations Convention on the Law of the Sea (UNCLOS).[108] China is a signatory to UNCLOS and has ratified it, and although the U.S. is not a party to UNCLOS it has asserted that the navigation provisions within UNCLOS are representative of CIL.[109] In the law of the sea, it is the "fundamental principle . . . that the land territorial situation constitutes the starting point for the determination of the maritime rights of a coastal state."[110]

China has undertaken extensive efforts in shaping the international law of the sea to suit its strategic goals. Geopolitical analyst Robert D. Kaplan describes the South China Sea as to China as the Caribbean Sea was to the United States in

105. Delimitation of the Maritime Boundary in the Gulf of Maine Area (Can. v. U.S.), 1984 I.C.J. 246, 305 (Oct. 12).

106. SHAW, *supra* note 89, at 64.

107. *Id.* at 52.

108. United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 397 [hereinafter UNCLOS].

109. John W. Bellflower, *The Influence of Law on Command of Space*, 65 A.F. L. REV. 107, 135 (2010).

110. SHAW, *supra* note 89, at 401.

the nineteenth and early twentieth centuries.[111] "The United States recognized the presence and claims of European powers in the Caribbean, but sought to dominate the region, nevertheless."[112] And for China, all of the states surrounding the South China Sea were once either part of China or subject to its suzerainty.[113] For China, that difference in station is still the case. This historically based thought process feeds into China's possessory interest in the South China Sea.

Professor Kittrie warns that "[b]y changing international law today, so as to push U.S. and other ships and aircraft farther away from China's coastline, China is providing its military more breathing room tomorrow."[114] China uses its claims of historical legitimacy as a basis to prepare the environment for future conflict, or to gain a strategic advantage to prevent a conflict occurring at all. In building its "great wall at sea," China has methodically taken measures in the South China Sea, East China Sea, and Yellow Sea in an attempt "to assert sovereignty over disputed islands and vast maritime resources, to protect and expand its southern and eastern maritime boundaries, and to enhance its naval capabilities to counter U.S. Navy dominance in the Pacific."[115] China seeks to accomplish this by way of its famous "Nine-Dash Line" map: a document China submitted to the UN in May 2009 with a dashed line and the claim that "China has indisputable sovereignty over the islands in the South China Sea and the adjacent waters as well as the seabed and subsoil thereof."[116]

Successfully contesting her rights in the Exclusive Economic Zone (EEZ) contrary to UNCLOS would give China the greatest strategic gain. As such, China has claimed that it can regulate passage through its EEZ, by requiring prior consent. UNCLOS clearly provides that a state cannot regulate passage in its EEZ and a majority of states, including the US, view China's claims as inconsistent with international law.[117] In this manner, China is essentially attempting to establish a custom of international law in its claim by reliance on the persistent objector rule in CIL wherein "a state opposing the existence of a custom from its inception would not be bound by it."[118] In fact, China persists in its assertion that all the waters within the nine-dash line have been Chinese territory since "time immemorial."[119] Although, this is certainly a fair amount of Chinese revisionism.[120] The U.S. demonstrates its protestations against these claims both in public international fora and by conducting Freedom of Navigation Operations

111. ROBERT D. KAPLAN, ASIA'S CAULDRON: THE SOUTH CHINA SEA AND THE END OF A STABLE PACIFIC 13 (2014).

112. *Id.*

113. FRENCH, *supra* note 10, at 266.

114. KITTRIE, *supra* note 61, at 166.

115. Raul (Pete) Pedrozo, *The Building of China's Great Wall at Sea*, 17 OCEAN & COASTAL L.J. 253, 254 (2012).

116. KITTRIE, *supra* note 61, at 167.

117. *Id.* at 166.

118. SHAW, *supra* note 89, at 64.

119. FRENCH, *supra* note 10.

120. *Id.*

(FONOPS) through the EEZ consistent with U.S. and UNCLOS interpretations of the law of the sea.[121]

Perhaps China's most ambitious efforts in the law of the sea revolve around island building. The law of the sea grants control over the sea surrounding islands to the state which has sovereignty over that island and specifically defines an island as "a naturally formed area of land, surrounded by water, which is above water at high tide."[122] China has engaged in extensive construction efforts to turn rocks and reefs into islands capable of supporting buildings.[123] For example, China completed construction efforts on Johnson South Reef which morphed a once-submerged reef into a 100,000 square meter island.[124] These efforts will certainly "make it 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."[125]

China remains undeterred in its use of legal warfare in the law of the sea context. Successes, regardless of degree, mean that China is resolved to use legal warfare in other areas. It has proven effective to the degree that China still makes its assertions and other states are still forced to rebut and respond to them in order to keep their objections alive. China's use of legal warfare in outer space and cyberspace is perhaps more dangerous because the law in those domains is not as fully formed in both custom and treaty as is the Law of the Sea. This means that China can potentially have more of an influence – whether positive or negative – on the formation and crystallization of the law in outer space and the law governing state action in cyberspace.

Professor Kittrie assesses that the "PRC is waging lawfare today in an effort to tilt to its advantage future kinetic battlegrounds" in the arenas of sea, space, and cyberspace.[126] In the maritime and outer space arenas, China's objective appears to be to "create and promote international legitimacy for expanding [its] sovereignty rights as part of its access control strategy."[127] China's use of legal warfare in cyberspace, however, is to allow itself the greatest freedom of action in the cyber domain, while limiting the ways in which international law applies to China's detriment.[128] It is to these areas of new and rapidly advancing technologies where we turn next and where China may have the greatest ability to shape international law.

---

121. Pedrozo, *supra* note 115.

122. UNCLOS, *supra* note 108, art. 121.

123. KITTRIE, *supra* note 61, at 167.

124. *Id.*

125. *Id.*

126. KITTRIE, *supra* note 61, at 165. Kittrie's list also includes aviation. However, his use of the air domain in this context is largely air flight over Chinese waters, not as a distinct area of international law in aviation. *Id.*

127. *Id.*

128. In the domestic law arena, China also asserts a degree of sovereignty that enables it to claim ownership over all information within its cyber domain and, in effect, to provide legal justification for its control of information on the internet accessible by the Chinese people. CHENG, *supra* note 68, at 60.

III. CHINESE INFLUENCE ON INTERNATIONAL SPACE LAW

With over 1,800 active satellites on orbit owned and operated by over 50 countries and multinational organizations, activity in outer space continues to grow at a blinding pace as does the reliance upon the benefits such activity provides to global commerce and everyday human activity.[129] "Nine countries", each of which are important players in global politics and international law, "and one international organization can independently launch spacecraft: China, India, Iran, Israel, Japan, Russia, North Korea, South Korea, the United States, and the European Space Agency (from French Guiana)."[130] Much of this activity serves purposes that are of a general civilian use and a broader national security purpose. While not overtly aggressive in nature, space power can serve the important functions of enabling self-defense and technical means of verification in arms control treaty contexts. Furthermore, "[s]pace power can also improve the overall capabilities of a military and serve as a deterrent force not just against the use of specific types of weapons, but also as a general capability that can deter a country from even becoming involved in a conflict."[131] The very nature of space power and space activity is that behavior in space is observable by adversaries, making it particularly useful for deterrence.

Space capabilities also aid militaries in increasing their effectiveness, precision, and lethality in the event of an armed conflict. Space is critical for targeting, intelligence, and communication. These strengths and benefits of space-based capabilities are viewed as vulnerabilities by an adversary. As China observed the United States use of space in recent decades, its "analysts assess that the U.S. military relies upon space for 70–90 percent of its intelligence and 80 percent of its communications. . . Chinese military analysts have noted the dependence of the U.S. military on space and have concluded that the loss of the use of space for the U.S. military may cause it to lose the conflict."[132] Both China and Russia "are developing a variety of means to exploit perceived U.S. reliance on space-based systems and challenge the U.S. position in space."[133] The U.S. relies heavily on its space capabilities to project military power across the globe. It comes as no surprise then, that the ability to "counter U.S. space capabilities is a key element of China's ability to assure its freedom of action and deter potential U.S. military operations in its sphere of influence."[134]

Although U.S. reliance on space power has been evident since the first Gulf War, recent indications are that the U.S. intends to place an even greater emphasis on space power and achieving dominance in space. U.S. military leaders have

129. DEF. INTELLIGENCE AGENCY, CHALLENGES TO SECURITY IN SPACE 7 (2019) [hereinafter *DIA Report*].

130. *Id.*

131. *Chinese Policy and Doctrine*, *supra* note 5, 1-21.

132. *Id.*

133. *DIA Report*, *supra* note 129.

134. *Chinese Policy and Doctrine*, *supra* note 5, at 1-1.

identified the "need for the military to prepare to defend itself in space."[135] This emphasis is largely informed by potential adversary activity in the same domain. The U.S. Department of Defense (DoD) has declared a "need to identify threats in space, be able to withstand aggressive counterspace programs, and counter adversary space capabilities."[136] U.S. presidents of late have also highlighted the importance of U.S. space power. The 2010 National Space Policy declares that the U.S. "will employ a variety of measures to help assure the use of space for all responsible parties, and consistent with the inherent right of self-defense, deter others from interference and attack, defend our space systems and contribute to the defense of allied space systems, and, if deterrence fails, defeat efforts to attack them."[137] And current U.S. President Donald Trump has placed great emphasis on space policy, as well. Such a focus suggests a realization within the highest levels of the U.S. government that its dominance in space is at risk of eroding in relation to other states.

China surely represents the greatest threat to that power. Its space program began in 1958, shortly after the Soviet Union's launch of Sputnik-1.[138] Despite delays and stagnation due to larger problems in China during The Great Leap Forward and the Cultural Revolution, China's program has recovered significant lost territory and is now growing rapidly.[139] "China is second only to the United States in the number of operational satellites" with over 120 ISR and remote sensing satellites on orbit.[140] As important as the raw numbers is the political and cultural value that this increase in space power provides to China. The program is a significant source of national pride and part of President Xi Jinping's "China Dream to establish a powerful and prosperous China."[141]

China has developed a complex structure for its space capabilities which "comprises organizations in the military, political, defense-industrial, and commercial sectors."[142] Recent policies, particularly its 2015 defense white paper, China's Military Strategy, highlight the importance of space power wherein China "for the first-time designated outer space as a military domain and linked developments in the international security situation to defending China's interests in space."[143] China has further declared its intent to "keep abreast of the dynamics of outer space, deal with security threats and challenges in that domain, and secure its space assets to serve its national economic and social development, and maintain outer space security."[144] And, in 2015, China's National Security Law

135. *Id.*
136. *Id.*
137. *Id.* at 3-16.
138. *DIA Report*, *supra* note 129, at 13.
139. *Id.*
140. *Id.* at 20.
141. *Id.* at 13.
142. *Id.* at 14.
143. *Chinese Policy and Doctrine*, *supra* note 5.
144. *Id.*

made the defense of China's interest in space a legally binding requirement on the PRC.[145]

A. The Scope of International Space Law

In contrast to the law of the sea, the LOAC, and many other areas of international law, "[s]pace law . . . is a relatively novel concept that rapidly emerged within a few years of the opening of the space age and thereafter greatly slowed."[146] Space law consists principally of five major treaties, but also includes CIL as applied to outer space.[147] In fact, Art. III of the Outer Space Treaty (OST) requires us to look further than these five treaties alone: "States Parties to the Treaty shall carry on activities in the exploration and use of outer space, including the Moon and other celestial bodies, in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international co-operation and understanding."[148] It would be a mistake, then to only rely on the five core outer space treaties for the legal regime in outer space.

The OST, ringing with ideals of peace, cooperation, and mutual benefit for all mankind, was developed "against a background of evident optimism regarding humanity's ventures into outer space."[149] The preamble sets forth the authors' lofty goals that "the exploration and use of outer space should be carried on for the benefit of all peoples" and that the "common interest of all mankind" is in the "exploration and use of outer space for peaceful purposes."[150] Key provisions within the substantive articles include that "exploration and use of outer space, including the Moon and other celestial bodies. . . shall be the province of all mankind" (Art. I); the Moon, other celestial bodies, and outer space itself are "not subject to national appropriation by claim of sovereignty" (Art. II); the prohibition of placing nuclear weapons or other weapons of mass destruction in orbit or on celestial bodies (Art. IV); and "the Moon and other celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful purposes" further

145. *Id.*

146. Peter L. Hays, *Space Law and the Advancement of Spacepower*, *in* TOWARD A STRATEGY FOR SPACEPOWER: SELECTED ESSAYS 299 (Charles D. Lutes et al. eds., 2011).

147. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies [hereinafter the OST], pmbl., Dec. 19, 1966, 18 U.S.T. 2410, 610 U.N.T.S. 205, 6 I.L.M. 386; Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space, Apr. 22, 1968, 19 U.S.T. 7570, 672 .N.T.S. 119; Convention on International Liability for Damage Caused by Space Objects, Mar. 29, 1972, 24 U.S.T. 2389, 961 U.N.T.S. 187; Convention on Registration of Objects Launched into Outer Space, Jan. 14, 1975, 28 U.S.T.695, 1023 U.N.T.S. 15; Agreement Governing the Activities of States on the Moon & Other Celestial Bodies, Dec. 18, 1979, 1363 U.N.T.S. 3, 18 I.L.M. 1434.

148. OST, *supra* note 147, art. III.

149. Dale Stephens, *The International Legal Implications of Military Space Operations: Examining the Interplay between International Humanitarian Law and the Outer Space Legal Regime*, 94 INT'L L. STUD. 75, 80 (2018).

150. OST, *supra* note 147, at pmbl.

prohibiting the construction of military bases or other structures on the Moon (Art. IV).[151]

Peter Hays argues that "[a]lthough there is some substance to arguments that the OST only precludes those military activities that were of little interest to the superpowers and does not bring much clarity or direction to many of the most important potential space activities, the treaty nonetheless provides a solid and comprehensive foundation upon which to build additional legal structures needed to advance spacepower."[152] Indeed, the inclusive provision of Art. III provides the entire corpus of international law as the legal foundation for national activity in outer space. Professor David Koplow describes CIL as "a prominent, dynamic component of international jurisprudence, regularly applied and enforced in other contexts, and perhaps having some novel, salutary effects in the realm of outer space as well."[153]

CIL brings to bear a unique "jurisprudential power" that treaty law does not: "once a norm is established as CIL, it becomes binding on all states, even those that did not participate in the evolving pattern, that may not be fully aware of its occurrence and that might not be entirely supportive of the norm, if they thought more deeply about it."[154] This factor is key because states which are not now spacefaring or not now great powers are still bound by CIL as applied to outer space unless they have preserved their dissent as a persistent objector.[155] Indeed, Koplow points out that CIL will have developed at a rapid pace once the first spacefaring nations ventured into the heavens.[156] "The early activities of the first spacefaring nations, eliciting near-uniform endorsement from other countries, initiated a remarkably rapid period of CIL generation in the new realm of outer space."[157]

A matter of great urgency in the space law community at present is the interplay between existing International Humanitarian Law (IHL, synonymous with LOAC) and the treaty regime of outer space law. Armed conflict in space includes "both the use of force in outer space itself and the use of space assets to achieve military effect in the air, land, and sea environments."[158] Professor Dale Stephens warns of "the potential for unanticipated outcomes arising from a collision of these [legal] regimes" without the proper dedicated analysis of how the two regimes interact in practical effect.[159] For instance, despite the "peaceful purposes" provisions in the OST, he notes that the inherent right of self-defense and

151. OST, *supra* note 147, at *passim*.

152. Hays, *supra* note 146.

153. David Koplow, *International Legal Standards and the Weaponization of Outer Space*, *in* SECURITY IN SPACE: THE NEXT GENERATION 159-73 (U.N. Inst. for Disarmament Research ed., 2008).

154. *Id.* at 161.

155. *Id.*

156. *Id.* at 163.

157. *Id.* (Such speed is only rivaled by the application of CIL to activities in cyberspace, discussed further below.)

158. Stephens, *supra* note 149, at 77.

159. *Id.* at 78.

the body of IHL will take priority over the OST regime in the event of an armed conflict.[160] In one sense, the urgency in clarifying this dynamic appears to be on the rise partially because of the potential practical need for clarification and codification of the existing law as China and others seek to grow their space power and militarization of outer space shows no signs of slowing.

Professor Stephens is part of the team working on one of two efforts seeking to articulate the applicable law: *The Woomera Manual on the International Law of Military Space Operations* (The Woomera Manual).[161] The Woomera Manual's stated mission, simply put, is "to develop a Manual that objectively articulates and clarifies existing international law applicable to military space operations."[162] Importantly, the Woomera Manual "also seeks to create a normative feedback loop, whereby the legal norms articulated are accepted or rejected (which is equally useful), thus contributing to a better understanding of the legal rules within the field."[163] The urgent need for clarification of the law is underscored by the fact that an additional manual is in progress as well, led by McGill University (Canada): the *Manual on the International Law Applicable to Military uses of Outer Space* (MILAMOS).[164] The MILAMOS group aims to create "a manual that objectively articulates and clarifies existing international law applicable to military uses of outer space in time of peace, including in situations posing threats to the peace."[165] Upon the conclusion of both manuals, the reception and subsequent state practice will be invaluable in determining what the law really is in this field.[166]

The convergence of the OST regime, CIL, and existing IHL along with various other treaties, means that the international law governing outer space may be more robust than a rising space power would be able to influence. China, however, finding itself as an emerging space power, has taken measures to push the legal regime of outer space in order to serve its own purposes, in accordance with its state policy of legal warfare. We will examine three specific areas where China's behavior in relation to outer space exhibits legal warfare tactics: China's claims of "vertical sovereignty," China's recent landing of a rover on the dark side of the Moon, and China's growing counterspace capabilities. We will further consider the successes or futility of such practices and attempts to manipulate international law governing outer space.

---

160. *Id.*

161. Stephens, *supra* note 149, at 99. (describing the Woomera Manual as a "collaborative effort led by The University of Adelaide (Australia), Exeter University (United Kingdom), the University of Nebraska (United States), and The University of New South Wales (Australia)").

162. *The Woomera Manual*, THE UNIVERSITY OF ADELAIDE, (last visited May 1, 2019), https://perma.cc/V7KF-6FZP

163. Stephens, *supra* note 149, at 99.

164. *Manual on International Law Applicable to Military Uses of Outer Space*, MCGILL CENTRE FOR RESEARCH IN AIR & SPACE LAW (May 1, 2019), https://perma.cc/XG5C-FGTY.

165. *Id.*

166. See *infra* Part IV for a discussion of the *Tallinn Manual 2.0* which did not have the same benefit of a competing statement of the law which could create a greater dialogue on the state of international law in that domain.

B. Vertical Sovereignty to the Heavens

As in the law of the sea context, Chinese legal warfare is at work in outer space law seeking to maximize sovereignty. Professor Kittrie has identified potential legal warfare tactics in an "increasing number of scholarly articles published by Chinese authors claiming that China's terrestrial borders extend indefinitely upward through outer space and that all the space within those perimeters is China's sovereign territory."[167] As we will see, however, China's position on this has changed in the last decade as another opportunity for legal warfare appeared in this same issue. In initially arguing for vertical sovereignty, China may be seen as attempting to "claim sovereignty over national space above the usual heights at which such satellites orbit so as to subject them to [China's] consent and control", thereby limiting the freedom of movement of other states for both satellites and, potentially, for manned spacecraft.[168]

Such an assertion of infinite vertical sovereignty, however, is contrary to the OST (and the Convention on Civil Aviation) to which China is a party, and how this issue is generally understood.[169] The OST certainly fails to define the delimitation of "outer space," but it clearly suggests that there is a distinction between national air space and outer space.[170] The question of a boundary between the underlying national air space and outer space is not resolved, but as Professor Frans von der Dunk describes it, "outer space is a global commons, where freedom to operate is the baseline rule and restrictions to that freedom can only arise under *jus cogens*, international treaties or [CIL]."[171] Disputes, therefore, regarding this matter are largely related to where the boundary should be drawn, not whether there is or is not a boundary. National sovereignty stops at any such boundary, beyond which is outer space "not subject to national appropriation by claim of sovereignty[.]"[172]

The boundary question first came to the fore in relation to the geostationary orbit (GEO) which has the unique characteristics of being directly above the equator and, due to being 'geostationary', meant that "equatorial states were faced with (the prospect of) satellites being more or less permanently stationed above their territory – even if at an altitude of about 35,786 km."[173] The equatorial states claimed sovereignty to the heavens at that time, but geopolitics being what they are and equatorial states being a small minority of states with a vested interest in the GEO, their claim did not carry the day at the Legal Sub-Committee

167. KITTRIE, *supra* note 61, at 168.

168. *Id*. For a detailed analysis of the competing functionalism and spatialism theories for delimiting airspace and outer space, see Paul Stephen Dempsey & Maria Manoli, *Suborbital Flights and the Delimitation of Air Space vis-à-vis Outer Space: Functionalism, Spatialism, and State Sovereignty*, 92 ANNALS AIR & SP. L. 197, 197-238 (2017).

169. *Id.*

170. OST, *supra* note 147.

171. THE HANDBOOK OF SPACE LAW 60 (Frans von der Dunk & Fabio Tronchetti, eds., 2015).

172. OST, *supra* note 147, art. II.

173. THE HANDBOOK OF SPACE LAW, *supra* note 171, at 61.

of the Committee on the Peaceful Uses of Outer Space.[174] States were granted an "equitable use" of the GEO rather than a vertical sovereignty.[175] Of the equatorial states, only Colombia retains its claim of sovereignty over that portion of the GEO that is over its terrestrial territory, and that appears to only be the case because its Constitution mandates it.[176]

Outside of the now-resolved matter of the equatorial states' vertical sovereignty claims, other debates of the boundary between air space and outer space have been largely theoretical.[177] The so-called "Kármán line," named after Theodore von Kármán whose work demonstrated that at roughly 100 km, Earth's atmosphere becomes too thin for practical utility in aviation, is a common reference point in this debate.[178] So much so is this the case, that despite lacking any particular agreement delimiting outer space at 100 km, "considerable state practice and *opinio juris* has developed assuming, firstly, a boundary would indeed be necessary, and secondly, that a 100 km altitude . . . would make most sense."[179] The United States, a hold-out on the specifics of where the line should be, primarily arguing that it is too early to draw such a line, has asserted a right of innocent passage for satellites stating that all states "have the rights of passage through and operations in space without interference."[180]

Chinese assertions of an absolute vertical sovereignty attempted to take advantage of the lack of a definition of "outer space" in the OST.[181] Chinese authors have argued that "there is no clear standard in international law as to the altitude to which territorial space extends" and China therefore can fill the perceived gap in the law by claiming sovereignty up to altitudes well beyond any accepted norms.[182] These "[e]fforts to construct legal justifications of China's sovereignty claims are intended to engender international support while also justifying the preparation of China's military forces to engage in military conflict in the event that its claims are challenged by force."[183] The 2006 U.S. National Space Policy rebuts these claims outright: "[the United States] rejects any claims to sovereignty by any nation over outer space . . . or any portion thereof, and rejects any limitations on the fundamental rights of the United States to operate in and acquire data from outer space."[184]

Had China's justification gained support from other states, it may have had far-reaching consequences on other states and persons around the world. China could

174. *Id*. at 62. *See also* Historical summary on the consideration of the question on the definition and delimitation of outer space, U.N. Doc. A/AC.105/769, Sect. 23, at 6 (Jan. 18, 2002).

175. THE HANDBOOK OF SPACE LAW, *supra* note 171, at 62.

176. *Id*.

177. *Id*. at 65.

178. *Id*.

179. *Id*. at 69.

180. *Id*. *See also* KITTRIE, *supra* note 61, at 168.

181. U.S.- China Economic and Security Review Commission, *2008 Annual Report To Congress* (Nov. 20, 2008) at 152.

182. *Id*. at 157.

183. *Id*. at 152.

184. KITTRIE, *supra* note 61, at 168.

have argued that their vertical sovereignty meant they set the rules for any passage through its space, which could range from limiting signal transmission during transit to imposition of fees. Importantly for international relations, China's theory of vertical sovereignty would "effectively vitiate national means of verification of compliance regarding any existing or new arms control treaties[] and would render meaningless any proposal to ban or limit weapons in space."[185]

When considering the impact of China's claim, we look to the text of the OST and subsequent practice of states. The OST clearly contemplates a difference between national airspace and outer space and "states have generally come to accept that there is a fundamental difference between the two and behave in a way that tacitly acknowledges that there is some kind of demarcation line."[186] China's assertion was well beyond the state practice of any other state. The effectiveness of China's assertions in this context was negligible because no other states have recognized an absolute vertical sovereignty.[187] China itself has apparently abandoned its claim of vertical sovereignty for another opportunity for legal warfare in its joint proposals with the Russian Federation on the "Treaty on the Prevention of the Placement of Weapons in Outer Space, and the Threat or Use of Force against Outer Space Objects" (PPWT) in 2008 and updated in 2014.[188] In the 2008 proposal, China aimed to establish a delimitation between national airspace and outer space at the 100km mark above sea level.[189] The present variant of the PPWT, currently tabled at the Conference on Disarmament, has removed this specific delimitation and captured a potential definition in this manner: "A device is considered to have been 'placed in outer space' if it orbits the Earth at least once, or follows a section of such an orbit before leaving that orbit, or is permanently located in outer space or on any celestial bodies other than the Earth."[190]

This shift in tactics by the Chinese is legal warfare. In this case, rather than seek to shape the specific law of sovereignty over airspace and where outer space begins, China has sought to be seen as a leader in developing a new and broad treaty covering many aspects of outer space law.[191] Wang asserts that the use of ruses to game the system is part of the China Order mindset, avoiding change and adaptation in favor of reordering the surrounding environment.[192] As such, China

185. Bellflower, *supra* note 109, at 141.

186. *Id*. at 147.

187. *Id*. at 140.

188. Report of the Conference on Disarmament to the General Assembly of the United Nations, U.N. Doc CD/1879 (Feb. 29, 2008); Letter dated 10 June 2014 from the Permanent Representative of the Russian Federation and the Permanent Representative of China to the Conference on Disarmament addressed to the Acting Secretary-General of the Conference transmitting the updated Russian and Chinese texts of the draft treaty on prevention of the placement of weapons in outer space and of the threat or use of force against outer space objects (PPWT) introduced by the Russian Federation and China, U.N. Doc. CD/1985 (June 12, 2014) [collectively "PPWT"].

189. *Id*.

190. *Id*.

191. Other aspects of the PPWT proposals are further covered *infra*, conclusion of Part III.

192. WANG, *supra* note 24, at 213.

has identified greater benefits in seeming to be a global leader in this context than to be persistent in its vertical sovereignty claim.

C. Peaceful Purposes & China's Anti-Satellite Capabilities

Perhaps the most ambiguous, yet hope-filled, concept enshrined in the OST regime is the objective of all states using outer space exclusively for "peaceful purposes."[193] "[T]his ambiguous phrase has historically been subject to competing interpretations. The prevailing interpretation, which allows the use of space 'for military purposes as long as they are not aggressive in character,' has left space open to diverse and expanding military activities."[194] States drew a line in their subsequent practice between militarization of space and weaponization of space. State practice supports the interpretation that the OST permits the use of space capabilities in support of military operations and functions on the Earth.[195] This is the widely accepted interpretation of "militarization" of space.[196] On the other hand, "weaponization" of space is the "deployment of weapons of an offensive nature in space or on the ground with their intended target located in space."[197] Due in large part to the era in which the OST was drafted and the fear surrounding nuclear war, the state parties to the OST agreed "not to place in orbit around the Earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapons in outer space in any other manner."[198]

The interplay of other legal regimes with the OST regime and the application in outer space comes into focus again in this aspect. The militarization of space has meant that space-based assets are in use for positioning, navigation, and timing (PNT); intelligence collection; communications; and more. In invoking the inherent right of self-defense articulated in the U.N. Charter, Article 51, a state may rightfully argue that disruption, denial, or destruction of an adversary satellite would be a permissible use of force in response to an armed attack.[199] Considering the potential need to disable enemy satellites in a future conflict,

193. *See* discussion *supra* Part III.A (introducing this topic).

194. Jack M. Beard, *Soft Law's Failure on the Horizon: The International Code of Conduct for Outer Space Activities*, 38 U. PA. J. INT'L L. 335 (2017) (citing P.K. MENON, THE UNITED NATIONS' EFFORTS TO OUTLAW THE ARMS RACE IN OUTER SPACE: A BRIEF HISTORY WITH KEY DOCUMENTS 29, 34 (1988)) (noting that interpretation of the phrase "peaceful purposes" has been a highly controversial problem since the beginning of the space age – with one principal school of thought holding that the phrase refers to "nonmilitary use" and the other holding that it refers to "nonaggressive use.").

195. THE HANDBOOK OF SPACE LAW, *supra* note 171, at 333.

196. *Id*. at 333-34.

197. *Id*.

198. OST, *supra* note 147, art. IV. (This provision continues in full as follows: "The Moon and other celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful purposes. The establishment of military bases, installations and fortifications, the testing of any type of weapons and the conduct of military maneuvers on celestial bodies shall be forbidden. The use of military personnel for scientific research or for any other peaceful purposes shall not be prohibited. The use of any equipment or facility necessary for peaceful exploration of the Moon and other celestial bodies shall also not be prohibited.")

199. U.N. Charter art. 2(4).

states are well within their rights to build and test anti-satellite (ASAT) systems. These capabilities come in two general categories: co-orbital ASATs and Direct Ascent ASATs (DA-ASAT). Co-orbital ASATs are "weapons that are placed into orbit and then maneuver to approach the target" and DA-ASATs are "weapons that use ground, air-, or sea-launched missiles with interceptors that are used to kinetically destroy satellites through force of impact, but are not placed into orbit themselves."[200]

Following the opening of the space age, the Soviet Union and the United States both pursued ASAT development well into the 1980s by which time each had developed an operational ASAT capability.[201] Perhaps seeing no need for further development into a greater arms race, "a remarkable hiatus then followed, as both countries refrained from further overt ASAT-test operations."[202] It would be short-sighted to consider this period of inactivity as a development of state practice supporting a prohibition on further ASAT development principally because the halt in activity did not have the associated *opinio juris* required to develop into CIL. Rather, the two states simply saw it not in their interests to pursue the matter further having effectively demonstrated to the other that they could target each other's space-based satellites.[203] But, this "complacency", as Professor Koplow puts it, "was rudely shattered in 2007, when China dramatically entered the ASAT testing business" by launching an ASAT which destroyed a defunct Chinese satellite at an altitude of 865 km.[204]

The 2007 Chinese ASAT test resulted in the largest amount of space debris from a single event – over 3,000 pieces of debris large enough to be a hazard to other space objects.[205] And space debris is a considerable problem for the future of space activity:

> Approximately 21,000 large objects – which are at least 10 cm in size – are tracked and catalogued in Earth's orbit, and only about 1,800 of them are active satellites. The remaining objects are debris, which includes derelict spacecraft, upper stages of SLVs, and remnants from explosions or collisions. The length of time debris remains in orbit depends on the altitude, ranging from a few years for objects below 600 kilometers to over a century for objects at higher orbits. The vast majority of debris harmlessly burns up in the atmosphere upon reentry.[206]

200. *Chinese Policy and Doctrine*, *supra* note 5, at xviii.

201. David Koplow, *The Fault Is Not in Our Stars: Avoiding an Arms Race in Outer Space*, 59 HARV. INT'L L.J. 331, 339-40 (2018).

202. *Id.* at 340.

203. *Id.*

204. *Id.* at 340-41.

205. *Id.* at 341. *See DIA Report*, *supra* note 129, at 35 ("Today, more than one third of all catalogued debris is from two major events: China's destruction of a defunct satellite in 2007 and the accidental collision between a U.S. communications satellite and a defunct Russian satellite in 2009.")

206. *DIA Report*, *supra* note 129, at 35.

The quandary of space debris is insidiously problematic: all activity in space leaves some amount of space debris; that which remains in orbit for any considerable length of time adds to the circling cloud of projectiles serving as a potential hazard to satellites and spacecraft; this cloud of debris in orbit will eventually need to be removed; and any debris removal technology is potentially dual-purpose, capable of serving the civilian utility of clearing out debris or satellite maintenance, or the military utility of damaging or destroying adversary satellites.

The fact of this problem is not lost on the U.S. Defense Intelligence Agency whose 2018 report, *Challenges to Security in Space*, makes the same observation: The increase in number of objects on orbit has implications for policymakers worldwide and is encouraging the development of space debris removal technology [which] is dual-use because it could be used to damage another satellite."[207] China's integration of civilian and military activity in space serves to blur the lines even more when other states attempt to assess China's actions objectively. China lauds the "civil-military integration" of its space industry as an advantage for greater and more rapid achievement, but it also uses the phrase partly "to refer to the leveraging of dual-use technologies, policies, and organizations for military benefit."[208] "The PLA also sees counterspace operations as a means to deter and counter a possible U.S. intervention during a regional military conflict."[209]

Since the 2007 test, China has continued to grow its ASAT program. Publicly available reporting on China's co-orbital ASAT capabilities reveals that China is dedicating significant resources to testing ASAT technologies. According to The Secure World Foundation's 2018 report, *Global Counterspace Capabilities: An Open Source Assessment*, "China has conducted multiple tests of technologies for close approach and rendezvous in both low-earth orbit (LEO) and [GEO] that could lead to a co-orbital ASAT capability. However, as of yet, the public evidence indicates they have not conducted an actual destructive intercept of a target, and there is no proof that these technologies are definitively being developed for counterspace use as opposed to intelligence gathering or other purposes."[210] Similarly, China's DA-ASAT programs are fully active: "China has at least one, and possibly as many as three, programs underway to develop DA-ASAT capabilities, either as dedicated counterspace systems or as midcourse missile defense systems that could provide counterspace capabilities. China has engaged in multiple, progressive tests of these capabilities since 2005, indicating a serious organizational effort. Chinese DA-ASAT capability against LEO targets is likely mature and may be operationally fielded on mobile launchers within the next few years."[211]

China's capabilities are sure to grow in the coming years as the PRC continues to place heavy emphasis on space innovation for both its national security

207. *Id.*
208. *Id.* at 15.
209. *Id.*
210. *Chinese Policy and Doctrine*, *supra* note 5, at 1-2.
211. *Id.* at 1-11.

purposes and national pride. Doctrinal integration of space capabilities is also more developed for China compared to the recent past: "China continues to improve its counterspace weapons capabilities and has enacted military reforms to better integrate cyberspace, space, and EW into joint military operations."[212] And any state who sees itself as a space power or who has assets to protect in space is essentially forced to keep pace with China's ASAT innovations. The U.S. has certainly revived and updated programs that had slowed since the end of the Cold War.[213] And India declared itself a part of this exclusive club on March 27, 2019, when it conducted a successful ASAT test with the "Mission Shakti" launch.[214]

Professor Kittrie cautions that "[t]he PRC seems to be deploying an asymmetric strategy to deny U.S. use of space as much as possible, including through lawfare justifying the development and deployment of capabilities to damage and interfere with American satellite systems so as to blind the U.S. military in the event of conflict."[215] Yet, China's actions are no different in quality than what the U.S. and Soviet Union did during the earlier days of ASAT development. The difference is more in quantity in the sense that China's 2007 ASAT launch created such a historically large debris field compared to the U.S. and Soviet ASAT launches. In fact, this is not asymmetric at all, as Professor Kittrie suggests, because the U.S. and Soviet Union had developed the same capabilities, refraining from further launches not out of a sense of *opinio juris*, but more likely simply because they had no reason to conduct further launches. It is the same as the other states' interpretation of the "peaceful purposes" of space, by the OST, and subsequent state practice. But, China's legal warfare in this context took advantage of a gap in the existing law left open by the drafters of the OST and by the U.S. and Soviet Union when they simply stopped the ASAT race of their own accord rather than formalize an agreement that could foreclose a reckless arms race in space in the future. The complacency Professor Koplow described following the U.S. and Soviet ASAT development in the 1980s left the door open for a waking China to follow suit decades later.

China's legal warfare strategy applied to outer space is yielding mixed results, but it appears to be paving the way for better successes in the future. The vertical sovereignty claims were certainly the weakest and have been discarded. Further, it would be fair for China to assert that it did not start a new arms race in ASAT capabilities and that it is "merely attempting belatedly to follow the space weaponization lead pioneered by the United States."[216] Answering the call for new

212. *DIA Report*, *supra* note 129, at 13.

213. *Chinese Policy and Doctrine*, *supra* note 5, at 3-1–3-15.

214. Doris Elin Urrutia, *India's Anti-Satellite Missile Test is a Big Deal. Here's Why*, SPACE.COM (Mar. 30, 2019), https://perma.cc/PUQ8-RESS; *US tracking 250-270 objects from Indian ASAT test debris; ISS not at risk: Pentagon*, THE NEW INDIAN EXPRESS (Mar. 30, 2019), https://perma.cc/manage/create?folder=7199.

215. KITTRIE, *supra* note 61, at 170.

216. Koplow, *supra* note 201, at 344.

agreements to limit space militarization, two proposals merit our brief attention: the joint proposal of the Russian Federation and the PRC, the PPWT; and the proposal by the European Union (EU), the International Code of Conduct for Outer Space Activities (ICOC).[217]

The PPWT, however, contains no means for verification of compliance and was met with significant criticism by the United States.[218] The scope of the criticism extends to vagaries in the PPWT surrounding employment of space-based weapons versus research and development of such weapons; the failure to cover terrestrial-based weapons; implicit prohibition of temporary and reversible electronic jamming; and more.[219] The U.S. criticisms conclude broadly that the PPWT would (a) place prohibitions on military and intelligence uses of space, to include impinging on the lawful use in armed conflict and (b) "fail to preserve the rights of the United States to conduct research, development, testing, and operations in space for military, intelligence, civil, or commercial purposes."[220] The combined criticisms of the U.S. find that the proposal as a whole can easily be read to allow a state to develop a "breakout capability" of co-orbital ASAT capabilities or space-based weapons.[221] China's efforts with the PPWT stand out in one sense, though, despite failure to gain U.S. agreement to even *negotiate* it further: China is taking action on these issues whereas the United States took the position in the Obama Administration of "listen[ing] to proposals and concepts for new measures of space arms control ... [but declining to] exercise any forward-leaning leadership on point or sponsor any overtures of their own."[222]

In a similar vein, the ICOC is a non-binding code of conduct which Professor Jack Beard describes as "a case study in the limitations of soft law" which, while aimed at "the critical problem of orbital space debris and the challenge of preventing an arms race in space ... fails in its attempts to achieve progress in either of these areas and instead undermines such efforts."[223] Neither the ICOC or the PPWT have gained significant traction globally, but for China that appears not to be immediately critical to the success of this tactic. China's legal warfare strategy in this context then, is taking steps to influence international treaty law by taking a leadership role not against the United States, but *in its place*. As there is no real risk of the U.S. joining in on the ICOC because of its non-binding nature, China is standing alone with the Russian Federation with the PPWT as the only

217. *Id.* at 351-52. *See also DIA Report*, *supra* note 129, at 7 ("While China and Russia are developing counterspace weapons systems, they are promoting agreements at the United Nations that limit weaponization of space. Their proposals do not address many space warfare capabilities, and they lack verification mechanisms, which provides room for China and Russia to continue to develop counterspace weapons.")

218. Koplow, *supra* note 201, at 352. *See* U.S. comments to the 2008 PPWT, U.N. Doc. CD/1847 (Aug. 26, 2008); Chinese/Russian response, U.N. Doc. CD/1872 (Aug. 18, 2009).

219. U.N. Doc. CD/1847 (Aug. 26, 2008).

220. *Id.*

221. *Id.*

222. Koplow, *supra* note 201 at 353.

223. Beard, *supra* note 194, at 344.

significant effort for real disarmament in outer space and improvement of the gaps left by the OST regime.

The future of legal warfare in space is bright for China, particularly considering the expanding possibilities in non-military applications. In 2017, the China National Space Administration (CNSA) announced plans to land a rover on the far side of the Moon in 2018.[224] China had already landed rovers on the near side of the Moon, only the third state to do so.[225] The challenge of a far side landing is one of communication, an issue which China resolved in May 2018 by placing on orbit a lunar relay satellite to enable communication between the lunar rover and the Earth."[226] Then, in early January 2019, China performed the first-ever lunar far side landing with its Chang'e-4 rover, named after a moon goddess of Chinese folklore.[227] The mission is widely lauded as impressive and Chinese spokespersons only discussed the mutually beneficial purposes of research and exploration in connection with the mission.[228] The PRC echoed its earlier announcement from March 2018 of plans "to assemble a robotic research station on the Moon by 2025 and has started establishing the foundation for a human lunar exploration program to put astronauts on the Moon in the mid-2030s."[229] With such an active Moon research and exploration program, China will be placing itself at the forefront of one of the next great questions in international space law: space resource utilization.[230] As with development of ASAT capabilities, the first in the field has the opportunity to shape CIL in that field.

IV. DECODING THE EFFECTS OF CHINESE LEGAL WARFARE ON CYBERSPACE

Chinese political strategists believe that their strategies, including legal warfare, are "different due to the legitimacy of their interests and as a response to historical aggression by the West."[231] In the law of the sea, China seeks to increase

224. Marina Koren, *China's Growing Ambitions in Space*, THE ATLANTIC (Jan. 23, 2017), https://perma.cc/29RR-GEE6; Matt Rivers, Helen Regan & Steven Jiang, *China lunar rover touches down on far side of the moon, state media announce*, CNN (Jan. 4, 2019), https://perma.cc/YEU4-5ZLT (The far side of the moon is the hemisphere that never faces Earth, due to the moon's rotation. It is sometimes mistakenly referred to as the "dark side of the moon," even though it receives just as much sunlight as its Earth-facing side.).

225. *DIA Report*, *supra* note 129, at 18.

226. *Id.*

227. *Id.*

228. *See, e.g.*, Leroy Chiao, *Astronaut: What China's moon landing means for US*, CNN (Jan. 8, 2019), https://perma.cc/CS4G-TLDK; Mike Wall, *China makes historic 1st Landing on Mysterious Far Side of the Moon,* SPACE.COM (Jan. 3, 2019), https://perma.cc/4SAR-24WQ; Wendy Wittman Cobb, *Will China's Moon Landing Launch a New Space Race?*, THECONVERSATION.COM (Jan. 4, 2019), https://perma.cc/E4UP-QLMS; Marcia Smith, *China Lands Probe on Far Side of Moon for the First Time*, SPACEPOLICYONLINE.COM (Jan. 2, 2019), https://perma.cc/RQ69-AFWQ; Marina Koren, *Why the Far Side of the Moon Matters so Much,* THE ATLANTIC (Jan. 3, 2019), https://perma.cc/9kza-m43z.

229. *DIA Report*, *supra* note 129, at 18.

230. On March 11, 2019, the Secure World Foundation, in partnership with the SDA Bocconi School of Management-Space Economy Evolution (SEE) Lab, and the George Washington University Space Policy Institute held a one-day workshop entitled "Mining the Moon for Profit: A Case Study in Space Utilization," https://perma.cc/F68Q-YCCK.

231. VALERIANO, *supra* note 6, at 152.

its military and economic power by growing its EEZ and expanding its definition of sovereignty. In space, China's advances take advantage of gaps in law to assert itself as a growing military power and will make it a leader in areas of new technology that will enable it to define the rules of the road. As China's legal warfare is applied to cyberspace, it will further seek to grow its military and economic power while protecting and expanding its own sovereignty.

Western strategists note that "[i]f China is to become an active hegemon with global interests it will need to assert itself in the cyber domain."[232] And so China has done and continues to do. Inkster notes that "the cyber domain has been a powerful enabler of China's rise."[233] For China, "the risk posed by the cyber domain has deepened an ingrained sense of insecurity – a sense that to outside observers seems at odds with the country's economic power, growing military capacity and general aura of stability."[234] But, it seems to be the nature of authoritarian powers to always be insecure of their future and jealously seek more power. This has been indoctrinated in China's 2016 Chinese National Cyberspace Security Strategy which is "organized around three 'grave threats': political stability, economic progress, and culture solidarity. The strategy mentions that competition is expanding online, and that a small number of nations are aggravating a cyber arms race."[235] China has proven itself a willing and able participant in that cyber arms race.

Furthermore, the drive has been to recover from the period of National Humiliation and gain the preeminent position China believes it lost in the last century and a half due to the West. "China's rise is predicated on catching up to the United States in economic and military domains, and it sees the theft of Western technologies and intellectual property as a shortcut to this goal."[236] Cyber espionage and theft of intellectual property are China's due, in this sense. Below we will explore the international law governing cyberspace and the manner in which China can and has taken advantage of the relative lack of clarity in that domain. China has continued its legal warfare in this domain in advantaging its military power by embracing the lack of clarity and consensus in cyberspace giving adversaries uncertainty over how China may act in that domain. We explore how China's legal warfare seeks to strengthen its sovereignty by enabling control over the Internet at the national level, in attempts to both keep international actors out and contain threats from within.

A. In Search of International Law of Cyberspace

Despite the lack of a specific treaty for cyberspace, "[i]nternational law provides a framework for cooperation that is foundational to the successful

232. *Id.* at 148.

233. *Id.* ("[C]yberspace is an enabler of China's emergence as a great power in the twenty-first century.")

234. *Id.*

235. *Id.* at 149.

236. *Id.* at 159. *See also id.* at 139 ("Combining subjective and objective factors, psychological warfare, and cyber intrusions gives China a unique perspective as a cyber actor due to its targeted focus on seeking an information advantage after falling behind.").

preservation of international peace and security", and state practice will continue to inform how that framework can provide more substance for states operating in cyberspace.[237] The LOAC, as found in the U.N. Charter and CIL, as well as the fundamental norms of international law, such as sovereignty and non-intervention, make up this framework. But, the vagaries of cyberspace make it challenging to simply overlay cyberspace concepts and activity onto the framework to reveal a refined set of rules and laws for interaction among states.

Most legal scholars tend to use the term "cyber operations" only in conjunction with military operations or operations which may be attributed to a state as military action.[238] Other bodies of law, such as domestic criminal law, govern activities in and through cyberspace that would not qualify as military operations, such as theft or espionage.[239] However, with that in mind, it is important to recognize that traditional theft and espionage activities are conducted on the territory of state who could obtain personal jurisdiction over a thief or spy if caught. In the case of cyberspace operations akin to theft or espionage, it may be premature to remove theft and espionage from the discussion because of a lack of consensus on what is permissible or impermissible in cyberspace as either a use or threat of force, an armed attack, or otherwise.

A great deal of the dialog at present centers around the idea of a "cyber weapon" and a "cyber-attack" or even "cyber war."[240] Professor Yoram Dinstein, in relation to cyber-attacks, provided the reassuring comment that "[t]he novelty of a weapon – any weapon – always baffles statesmen and lawyers, many of whom are perplexed by technological innovation. . . [A]fter a period of gestation, it usually dawns on belligerent parties that there is no insuperable difficulty in applying the general principles of international law to the novel weapon[.]"[241] This period of gestation is still ongoing particularly because of the secretive nature of state practice in cyberspace, both on the part of the attacker and the defender.

The secretive nature of cyber means of warfare does not equate to a lawless battlefield. Additional Protocol I (AP I) to the Geneva Conventions clearly contemplates application of existing IHL to new weapons in Art. 36:

> In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be

237. Gary P. Corn & Robert Taylor, *Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0 Sovereignty in the Age of Cyber*, 111 AJIL UNBOUND 207, 208 (2017).

238. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 564 (Michael N. Schmitt ed. 2017) [hereinafter TALLINN MANUAL 2.0] ("Cyber operations" can be defined as "[t]he employment of cyber capabilities to achieve objectives in or through cyberspace . . .").

239. International Committee of the Red Cross, *International Humanitarian Law and The Challenges of Contemporary Armed Conflicts*, ICRC Doc 321C/15/11 (Oct. 2015), 41-42.

240. *See, e.g.*, THOMAS RID, CYBER WAR WILL NOT TAKE PLACE (2013).

241. Yoram Dinstein, *Computer Network Attacks and Self-Defense*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 114 (Michael N. Schmitt & Brian T. O'Donnell, eds., 2002).

> prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.[242]

More broadly speaking, Art. 1(2) of AP I gives assurances of the enduring nature of the principles found in the treaty in the Martens Clause:

> In cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience.[243]

Furthermore, the ICJ's 1995 Advisory Opinion, *Legality of the Threat or Use of Nuclear Weapons*, affirmed that IHL applies to "any use of force, regardless of the weapons employed."[244] Gary Solis argues that state practice applying norms to new weapons, such as cyber weapons, can be slow to evolve.[245] The slow evolution of state practice may particularly be the case with cyber warfare, at least in terms of the actual employment of cyber capabilities, because states will naturally want to keep such capabilities close-hold.

Without significant state practice to inform how states apply existing international law to cyberspace – both in terms of treaty law and CIL – we find ourselves focusing on public statements which may or may not take the form of *opinio juris*. For example, the Obama Administration, in 2011, articulated its views on the application of existing norms: "The development of norms for state conduct in cyberspace does not require a reinvention of CIL, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace."[246] Military manuals and public statements or policies are also relevant for analysis of state practice, although only the UK and the U.S. have unclassified military manuals which reference cyberspace operations.[247] Professor Matthew Waxman highlights the value of these sources in noting that "legal evolution is likely to occur in significant part through defensive planning doctrine and declaratory policies issued in advance of actual

242. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 36, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I].

243. AP I art. 1(2).

244. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 39 (July 8).

245. GARY D. SOLIS, THE LAW OF ARMED CONFLICT: INTERNATIONAL HUMANITARIAN LAW IN WAR 673-74 (2nd ed. 2016).

246. THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 9 (2011).

247. MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 27 (2014).

cyber-attack crises."[248] States may also value the benefit of the ambiguity in the current state of IHL in cyber operations, thereby allowing them to act or respond with more leeway than if the law were memorialized in a treaty.[249] Furthermore, states such as the U.S. may be conflicted on where exactly they should fall in establishing their state practice, especially because the U.S. is both extremely vulnerable and exceptionally powerful in the cyberspace domain.[250]

The rapid emergence of the cyberspace domain – a concern not relevant during the formation of treaty or customary IHL – presents a time when scholars are grasping for the rare statement of public officials: "[e]xpressions of *opinio juris* are especially meaningful with respect to emerging domains of State interaction not anticipated when the present law emerged in the form of either treaty or customary law."[251] And, as yet, there appears to be "no political stomach" for a treaty specifically for interstate cyberspace activities.[252] This forces the focus of energy into interpreting existing IHL and applying it to cyberspace activities.[253] Legal scholars have taken the silence of states – both in terms of publicizing their practice and statements of *opinio juris* – as an opportunity to hold an active dialog about what the law is (or should be). According to the ICJ, however, "the teachings of the most highly qualified publicists of the various nations [may *only* be considered] as subsidiary means for the determination of rules of law."[254] Yet, many hold such publications, chief among them *Tallinn Manual 2.0*, to be an authoritative statement of the law; whether due to the simplicity they provide of a relatively clear statement for purposes of discussion or from mistakenly placing undue authority in such publications. Neither the first iteration nor *Tallinn Manual 2.0* have had the benefit of competing volumes to draw out dialog from actual state actors. More to the point, such a volume suffers from the same lack of state practice for analysis as does the overall discussion of international law for cyber operations.

Into this fog of law steps China, a once great regional power rising to compete for global power again. The PRC's position on the governing law is difficult to pin down and has certainly evolved. As its power evolves, so too does China's implementation of its legal warfare strategy with respect to cyberspace. However, unlike its strategy for legal warfare in outer space, we have significantly less state practice to consider in the analysis. Official statements of government officials are similarly uncommon. But, public statements or writings of legal scholars are worthy of consideration, in part because it is part of China's overall legal warfare strategy to inject its views of the law into the legal debates

248. Matthew C. Waxman, *Self-Defensive Force against Cyber Attacks: Legal, Strategic, and Political Dimensions*, 89 INT'L L. STUD. 109, 116 (2013).

249. Michael N. Schmitt & Sean Watts, *The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare*, 50 TEX INT'L. L.J. 189, 223 (2014).

250. *Id.*

251. *Id.* at 194.

252. *Id.* at 222.

253. *Id.*

254. Statute of the International Court of Justice art. 38.

through its academic community. China uses this community to to gain legitimacy for its views and stimulate a growing popularity over time. Specifically, we will examine China's legal warfare strategy with respect to IHL and the use of force construct as well as China's views of sovereignty and how the interplay of these two positions aver to China's benefit.

1. Prohibition on the Use of Force

In conducting any legal analysis of interstate cyber operations, the first stop is the U.N. Charter and its key articles. Specifically, they focus on the general prohibition on the threat or use of force, found in Art. 2(4), and the inherent right of self-defense to an "armed attack," found in Art. 51. The nuanced language in the Charter is important and the fact that there is potential for a gap between what is considered "force" and what is an "armed attack" presents itself immediately. Simply put, "all armed attacks are uses of force, but not all uses of force qualify as armed attacks."[255] Views among specially affected states, such as the U.S., are certainly divergent on this matter, particularly as it relates to the complexities of the cyber context. Article 2(4)'s statement of the general prohibition of the use of force clearly sets out the norm that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[256]

Many cyber operations may not reach the use of force threshold at all, even if they are violations of other rules of international law.[257] There must be a minimum level of intensity or gravity surpassed to be considered "force."[258] The ICJ addressed the use of force threshold in the *Nicaragua* case in 1986.[259] The Court determined that U.S. assistance in the form of arming and training of the *Contras* while they were engaged in hostilities against Nicaragua constituted a use of force.[260] Reconciling a principle of force to the cyberspace arena has certainly proven unwieldy to many, yet many also make strong statements about what this *so clearly* means. Two U.S. DoD officials wrote that "[d]espite the lack of complete clarity, it is generally accepted that at a minimum, cyber activities that proximately result in death, injury, or significant destruction, or that represent an

255. Michael N. Schmitt, *Cyber Operations and the Jus Ad Bellum Revisited*, 56 VILLANOVA L. REV. 569, 587 (2011).

256. U.N. Charter art. 2(4); Reese Nguyen, *Navigating "Jus Ad Bellum" in the Age of Cyber Warfare*, 101 CALIF. L. REV. 1079, 1114 (2013) (explaining that force does not include political pressure, economic coercion, unfavorable trade treatment, or changes in diplomatic or economic relations. States have also widely accepted that some forms of intelligence surveillance and espionage do not equate to force.).

257. OLIVER CORTEN, THE LAW AGAINST WAR: THE PROHIBITION ON THE USE OF FORCE IN CONTEMPORARY INTERNATIONAL LAW 77 (2010).

258. Thomas Ruys, *The Meaning of Force and the Boundaries of the Jus Ad Bellum: Are Minimal Uses of Force Excluded from UN Charter Article 2(4)?*, 108 AM. J. INT'L L. 159 (2014).

259. Nicar. v. U.S., *supra* note 102, at 14.

260. Michael N. Schmitt, *The Law of Cyber Warfare: Quo Vadis?*, 25 STAN. L. & POL'Y REV. 269, 279 (2014).

imminent threat thereof, constitute a use of force."[261] And as extreme as that analysis is, Professor Schmitt (a DoD academic) argues that, as applied in a cyberspace context, this use of force decision by the ICJ means that "non-destructive cyber operations" can amount to a use of force under the right circumstances.[262]

2. Article 51 & Self-Defense

Although a use of force analysis is useful for determining if a state has violated the norm of international law with its cyber operations, the victim state may only use force in response to cyber operations if the self-defense exception is triggered or upon UN Security Council sanction. The self-defense exception in response to an "armed attack" is provided for in the U.N. Charter, Art. 51:

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.[263]

In *Nicaragua*, the ICJ asserted the 'gap' between Art. 2(4) and Art. 51 of the U.N. Charter, declaring that we must "distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms" and asserting that the proper differentiating factors would be "scale and effects".[264] The *Nicaragua* Court also decided that "a mere frontier incident," a concept which the ICJ declined to clarify, would not equate to an armed attack, albeit not without severe criticism.[265] Later, in the *Oil Platforms* case, the ICJ affirmed that a single incident, could give rise to the inherent right of self-defense.[266] Rather than a clear rule, however, international law tends to leave scholars and states alike with "only a handful of examples showing what *is* and what *is not* armed attack."[267]

While the ICJ and the prevailing view among states is that not all uses of force will equate to an armed attack, the U.S. has denied the existence of a gap between Art. 2(4) and Art. 51 of the U.N. Charter. The U.S. has disagreed with limiting armed attacks to those which cause injury or damage, asserting to the U.N. that, "under some circumstances, a disruptive activity in cyberspace could constitute an armed attack."[268] Such a statement would seem surprising for the global leader in both cyber capabilities and vulnerabilities while also running contrary to the notion of a gap between use of force and armed attack as first articulated in the

261. Corn & Taylor, *supra* note 237.
262. Schmitt, *supra* note 260, at 280.
263. U.N. Charter art. 51.
264. Ruys, *supra* note 258, at 165.
265. Schmitt, *supra* note 260, at 282.
266. Ruys, *supra* note 258, at 165.
267. Nguyen, *supra* note 256, at 1115.
268. U.N. Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security 18-19, U.N. Doc. A/66/152 (July 15, 2011).

Nicaragua case.[269] In 2012, Harold Koh, then State Department Legal Advisor, said of the U.S. position in an address to USCYBERCOM that "the inherent right of self-defense potentially applies against *any* illegal use of force. In our view, there is no threshold for a use of deadly force to qualify as an 'armed attack' that may warrant a forcible response."[270]

This denial of a gap can be rather problematic for several reasons. In fact, Professor Schmitt believes the U.S.'s minority position is likely to weaken over time.[271] He argues that "[i]n the kinetic context, the approach made sense for states that wielded significant military power[,]" whereas in the cyberspace context, "militarily weak states may nevertheless enjoy the ability to inflict significant damage by cyber means." [272] Furthermore, Professor Jack Goldsmith notes that, unlike with kinetic weapons, cyber operations may take place gradually over time and many of the effects are reversible.[273] States will see a cyber operation differently if, for instance, an operation shuts down the computer systems of a military unit for two days compared to two weeks.[274] He poses the question of whether destruction of "critical economic or military data, without any physical consequences, is a use of force" amounting to an armed attack.[275]

Similarly, consider that Professor Schmitt argued in 2011 that if any state conducts cyber operations which "result in damage to or destruction of objects or injury to or death of individuals of another [s]tate", such actions would be armed attacks justifying self-defense.[276] Later, in 2014, he argued that further state practice should be observed before the law can be settled on this topic.[277] This is a sound approach, because the full scope of cyberspace capabilities is not yet known. As such, it is likely that without actual state practice to observe, scholars will be unable to opine whether non-destructive cyber-attacks could breach the armed attack threshold. The complexity of the question combined with the desire to not wait for CIL to be more clearly defined over time has led scholars to attempt to create principles upon which the international community may rely in determining whether a cyberspace operation is an armed attack, or a mere use of force.

There are at least four approaches among academics to analyzing what constitutes an armed attack: the instrument-based approach, which focuses on the

269. Schmitt, *supra* note 260, at 284.
270. *Id*.
271. Schmitt, *supra* note 260.
272. *Id*. at 284-85.
273. Jack Goldsmith, *How Cyber Changes the Laws of War*, 24 EUR. J. INT'L L. 129, 133-34 (2013).
274. *Id*. at 134
275. *Id*.
276. Michael N. Schmitt, *Cyber Operations and the Jus in Bello: Key Issues*, 87 INT'L LAW STUD. 89, 94 (2011).
277. Schmitt, *supra* note 260, at 283.

characteristics of the weapon employed;[278] the target-based approach, which primarily considers damage to national critical infrastructure in a strict liability construct;[279] the effects-based approach, a very subjective approach weighing factors which, in themselves leave significant room for variance from case to case;[280] and an integrated approach called the cyber-physical systems approach, which proposes that a cyber-attack is an armed attack if it is "intended to cause irreversible disruption or physical damage" to a computer system with a physical component.[281]

---

278. Under the instrument-based approach, the focus is on the weapon used to conduct an attack. *See* Nguyen, *supra* note 256, at 1118-19 (asserting that the instrument-based approach forces the international community to be tied to 1945 ideas of weaponry until a specific treaty is developed to address new technology). *See also* ROSCINI, *supra* note 247, at 46-47 (noting that he instrument-based approach, then, is weakened by its link to the physical characteristics of a weapon). Some have argued that if the instrument-based approach were applied in its traditional usage to digital codes, the logical conclusion would be that cyber operations could never amount to an armed attack. This approach, therefore, is too limiting and would potentially lead to the need for a cyberspace treaty before states had clear norms of behavior.

279. Nguyen, *supra* note 256, at 1119-20 ("By categorizing all cyber intrusions into critical infrastructure as acts of war, the target-based approach puts the United States at war with China, Russia, and a number of other countries that have already penetrated U.S. infrastructure systems for unknown purposes."). The target-based approach suffers from the opposite problem in that it is overbroad. This approach hinges on the status of the target of an attack, typically national critical infrastructure (NCI). It is a type of strict liability test that highlights the importance of NCI to state function and national security. *See also* ROSCINI, *supra* note 247, at 47 (suggesting that any cyber operation that affects NCI – even a mere intrusion or minor disruption – would be an armed attack, regardless of the effects of such an operation). Clearly the practice of those states demonstrates that they did not view those actions as armed attacks, nor did the US view them as such, as the US lack of a response (or limited complaint) demonstrates. The target-based approach simply casts too broad a net and is clearly not accepted by the international community.

280. Primarily endorsed by TALLINN MANUAL 2.0, *supra* note 238. The most widely discussed approach is the effects-based approach. *See* Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 847 (2012) (suggesting that there is difficulty in articulating what type of effects are grave enough to thereby provide sufficient behavioral guidance for states which focuses on the severity of the effects of a cyber attack to identify an armed attack). This approach is subject to criticism for the potential to miss cumulative damage. *See* Todd C. Huntley, *Controlling the Use of Force in Cyber Space: The Application of the Law of Armed Conflict during a Time of Fundamental Change in the Nature of Warfare*, 60 NAVAL L. REV. 1, 34-35 (2010) (describing the "potential for cumulative damage caused by a series of lower-level cyber-attacks"). Several prominent scholars have argued that these factors are so subjective that application will almost always enable an analyst to find in favor of an armed attack, and therefore an armed response. *See, e.g.*, Nguyen, *supra* note 256, at 1123-24 (offering specific examples of how Schmitt's own application finds an armed attack where most scholars find only a use of force, or less). *See also* Hathaway et al., *supra* note 280, at 847. A subjective test as malleable as Schmitt's would not allow the requisite amount of predictability for states to determine their behavior. Despite the mass appeal, it is likely that the acceptance is based on the fact it simply has fewer issues than the instrument-based or target-based approaches and potentially represents a starting point for further discourse.

281. Nguyen, *supra* note 256, at 1125-29, (attempting to resolve the subjectivity problems in Schmitt's effects-based approach and asserting that the cyber-physical systems (CPS) approach resolves many of the issues of the earlier approaches and gives credit to the uniqueness of cyber warfare). Important here is the intent aspect; intent is built into the payload of a cyber-attack. This suggests that an exploitation that is stopped before its payload can execute, but whose payload upon examination reveals the requisite intended outcome under this method, could be viewed as an armed attack.

B. The Fog of China's Cyber Legal Warfare

China's views on this use of force and self-defense issue are difficult to define, in part because they may be evolving over time as China's primacy evolves. While China "has repeatedly refused to recognize that international law, including the LOAC, applies in cyberspace[,]" the U.S., NATO, and the EU concur that cyberspace activities *are* governed by international law including LOAC. [282] China's actions at the U.N., in particular, give good indication of their views on the application of LOAC to cyberspace. After first submitting a draft voluntary "code of conduct for information security" in January 2015, which suggested that "China continues to resist applying existing international law to cyberspace", it later took the opportunity in April of that same year to more firmly assert this position.[283] In a meeting of the "UN Group of Governmental Experts on cyberspace security, the PRC reportedly aggressively asserted that international law does not apply in cyberspace, with PRC delegates going so far as to propose to 'delete all the sections having to do with international law'".[284]

Legal scholars and observers of China propose various reasons for why China might take such a strong position. Considering the relative unity of message and depth of strategy that appears to go into China's decision-making in this sphere, legal warfare is certainly being applied to China's benefit. Professor Kittrie believes that this refusal to apply LOAC to cyberspace activities is a type of "lawfare [that] could tilt to China's advantage a future kinetic battleground between it and the United States."[285] He points to the Deputy Chief of the General Staff of the Chinese military, Lieutenant-General Qi Jianguo, who said, "in the information era, seizing and maintaining superiority in cyberspace is more important than seizing command of the sea and command of the air were in World War II" in homing in on why China would desire as much freedom of action as possible in cyberspace.[286] Professor Kittrie explains further:

> In light of cyberspace's key role in Chinese military strategy, continued Chinese insistence that LOAC does not apply in cyberspace would provide China with a considerable advantage, especially if the United States continues to insist that its own cyberspace activities are constrained by LOAC. Given the centrality of LOAC to U.S. warfighting today, and the U.S. domestic pressures promoting increasingly strict interpretations of LOAC, it would be nearly impossible for the United States to reverse its current position and decide that its cyberspace activities would not be governed by LOAC.

---

282. KITTRIE, *supra* note 61, at 169 ("While the PRC joined in a 2013 U.N. Group of Governmental Experts report which stated that international law is applicable to the cyber arena, that step appears to be an outlier, as the PRC in 2015 returned to its pre-2013 position that international law does not apply in cyberspace.").

283. *Id.* at 170.

284. *Id.* (quoting Joseph Marks, *U.S. makes new push for global rules in cyberspace*, POLITICO (May 5, 2015, 10:16 AM), https://perma.cc/8V2G-9YGV).

285. *Id.*

286. *Id.*

While this is a fair comment to make, it misses the fact that public statements by U.S. officials in this context that the U.S. reserves the right to respond to cyber-attacks with a kinetic use of force can certainly serve as a deterrent factor. In fact, the more one claims adherence to the LOAC in general, the greater justification a state would have for retaliatory action after being subject to an armed attack. Thus, it is not likely that China intends to use this strategy to avoid the application of LOAC during a future armed conflict, but more that China intends to create an element of unpredictability around its behavior in cyberspace and some freedom to operate unhindered while arguing that it is permissible.

Professor Kittrie further raises the issues of proportionality and distinction as important principles which apply under the LOAC that China would apparently be unencumbered by in a conflict, with particular focus on statements by Shi Haiming, a researcher at China's National University of Defense Technology. In this regard, we look to Article 57 of AP I, which embodies the proportionality requirement that the civilian harm expected to be caused by an attack not be "excessive in relation to the concrete and direct military advantage anticipated."[287] The principle of distinction, as laid out in Article 48 of AP I states as follows: "In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives."

Shi Haiming posits that "the proportionality requirement is much more difficult in cyberspace because of the expanse and penetration of the Internet and the difficulty in containing unintended effects of attacks," and that such a requirement should therefore not apply in cyberspace.[288] He also suggested that LOAC should not apply because "it is impossible to distinguish between civilian and military assets" in cyberspace.[289] While both of these requirements are challenging in cyberspace, for certain, Shi Haiming's statements are not necessarily evidence of Chinese state practice or *opinio juris*. They could just as easily be an opportunity for deception to adversaries or they may serve as a deterrent for an adversary unsure of how China may respond in cyberspace. Any amount of time and space bought by this type of statement may be all China needs as it prepares the legal battlefield along with the rest of the environment.

Professor Kittrie summarizes his concerns of China's refusal to concede that LOAC applies to cyberspace by posing this scenario: "the LOAC requirements of proportionality and distinction could severely constrain PLA cyberattacks against key U.S. transportation hubs and civilian communications networks used by the military, including with cyber viruses, which do not discriminate between military and civilian objectives and thus may threaten computer-controlled hospitals,

287. AP I, *supra* note 242, art. 57.
288. KITTRIE, *supra* note 61, at 171.
289. *Id.*

dams, civilian airliners, and other forbidden targets."[290] He also raises the concern that indiscriminate PLA cyber-attacks could cause "hundreds of deaths of U.S. civilians through collateral malfunctions or shutdowns of critical infrastructure, hospitals, and the like in the United States."[291] But, this is quite hyperbolic for a type of capability that has not been publicly linked to a single death, let alone hundreds. It is commentary like this that demonstrates that China's legal warfare strategy is serving its purpose.

It may not always be that the strategy is to convince others of China's view of the law. In a case like this, it is equally valuable to serve as a deterrent or fear-inducing factor. China gains more in this area by creating uncertainty around the law and how it will apply the law to cyberspace. Recall that China uses legal warfare in peacetime to influence foreign populations and weaken support for action. How better to weaken support for action against China than to stoke fear of China's employment of cyber capabilities. Chinese statements of the law must always be measured against their likely long-term purpose. And that purpose may not always be to provide a firm interpretation of the law.

C. Sovereignty and Patriotic Hackers

As it is the case with the sea, outer space, and all of China's foreign policy behavior, sovereignty is a key factor for China in respect to cyberspace.[292] "Beijing is both the target of rival cyberattacks and the originator of the majority of espionage operations. It is also a leading digital authoritarian for activists who see the Great Firewall of China as the future of digital oppression."[293] China's legal warfare focused on cyber sovereignty serves the purposes of keeping adversaries out – both in terms of attacks and in terms of attributing actions originating from inside China – and stabilizing threats from within.

The head of the China Cyberspace Administration, also known as the State Internet Information Office (SIIO), is a man named Lu Wei, appointed directly by Xi Jinping.[294] At the World Economic Forum in Davos in 2014, Lu commented that "we must have a public [international] order. And this public order cannot impact any particular local order."[295] These comments are taken to support the PRC's calls for national sovereignty over the internet.[296] Chinese actors have argued for some time that states alone should have a governance role over the Internet.[297] The present model is of the nonprofit NGO, the Internet Corporation for Assigned Names and Numbers (ICANN) that administers the domain name system (DNS) and which links to Internet Protocol (IP) addresses.[298]

290. *Id.*
291. *Id.*
292. VALERIANO, *supra* note 6, at 143.
293. *Id.* at 146.
294. CHENG, *supra* note 68, at 59.
295. *Id.* at 60.
296. *Id.*
297. *Id.* at 61.
298. *Id.*

ICANN has operated in a "multi-stakeholder" model, giving states and NGOs equal voices, which sustains the Internet "as a borderless realm, where information flows freely."[299]

China, Russia, and other authoritarian states have made moves to attempt to reduce the role of ICANN to enable greater control for states over the Internet.[300] For instance, they proposed transferring Internet governance to the International Telecommunications Union (ITU), a subordinate organization of the UN, in a move which would give China and Russia greater control over the Internet.[301] In one of these proposals, China included language that would "reaffirm all the rights and responsibilities of States to protect, in accordance with relevant laws and regulations, their information space and critical information infrastructure from threats, disturbance, attack, and sabotage."[302] This is only one way in which China has sought to increase the legal justification for its authoritarian control over the Internet leading to greater control over its people. "China seeks to maintain control over the population through the subtle accumulation of control over their digital systems" and methods like these slowly increase that control over time.[303]

Legal warfare in this context is not just conducted through international bodies, but also in the domestic system. China has been "steadily creating a domestic legal and regulatory framework that firmly extends the state's grip over all parts of China's internal cyber community.[304] Over time, the international and domestic efforts China has undertaken would theoretically reinforce each other, as their holistic legal warfare strategy would require. China's laws now clearly link domestic cybersecurity to national security, as in Article 25 of the 2015 Chinese National Security Law which lists among the state's national security responsibilities: "maintaining national network and information security, stopping unlawful and criminal activity, including dissemination of unlawful and harmful information, as well as maintaining cyberspace sovereignty, security, and development interests."[305]

These domestic legal measures, including incredible limits to speech on the Internet, have culminated in what is commonly known as the Great Firewall of China (GFWC). In this case, the legal measures justify the technical measure of the GFWC which aims to protect China from "internal destabilizing threats."[306] According to Dean Cheng, the GFWC not only has the ability to censor website, pages, or images, it can theoretically "shut down connectivity between China and the rest of the global Internet entirely, if necessary."[307] China's vision of

299. *Id.*
300. *Id.* at 62.
301. *Id.*
302. *Id.*
303. VALERIANO, *supra* note 6, at 166.
304. CHENG, *supra* note 68, at 63
305. *Id.* at 66.
306. VALERIANO, *supra* note 6, at 167.
307. CHENG, *supra* note 68, at 67.

state-level control over the Internet leads directly to a more authoritarian state and, the more this view is perpetuated, it will justify like measures in other authoritarian states.

China has also found the threats from outside the state to be extremely active in cyber intrusions against China, inspiring the PRC to grow its own cyber-attack capabilities. "Beijing . . . is often on the receiving end of cyber degradation operations originating in the United States[.]"[308] Some Western strategists describe cyberspace as "inherently lawless" where "liberties are taken by the Chinese state, but when called out by the opposition, the state backs down and tries again later [indicating] tacit bargaining even in the ambiguity of cyberspace."[309] This strategy in cyberspace allows China to cause friction between other states while remaining below any arguable threshold of armed attack or use of force.[310] Largely, China is not conducting what many would consider offensive cyber-attacks, any type of operation with a digital payload to degrade an adversary system; rather, China prefers to "conduct covert operations to leverage sufficient deniability."[311] If China were able to gain greater support for its view of national sovereignty over the Internet, such a development would enable China's goal of deniability because states would find it more difficult to track back Chinese cyber intrusions to their source.

China has significantly preferred to conduct intellectual property theft or hacking into governmental nonmilitary entities or tangential nongovernmental entities for intelligence purposes rather than hacking adversary military targets directly.[312] "China by far account[s] for most of the attacks on governmental nonmilitary targets when compared to Russia and the United States."[313] Western strategists have mapped China's behavior and responses from adversaries and identified a pattern: "China usually casts out global espionage campaigns in search of intellectual property, and the United States will counter with a sophisticated degradation action to persuade the PLA hackers or other Chinese entities and proxies into ceasing operations, regrouping, and beginning another espionage campaign until the United States shuts that campaign down as well."[314] In this way, China tests the limits of what it can do and what its adversaries will tolerate and continues to be successful at reaching its strategic goals while remaining in the range of acceptable retaliation. While this is not an escalatory approach, China is taking advantage of the lack of consensus on where force and coercion lie within cyberspace.

To this end, China has "employ[ed] thousands of cyber hackers to defend the digital domain and state interests, target internal actors, and catch up in

308. VALERIANO, *supra* note 6, at 147
309. *Id.*
310. *Id.* at 148.
311. *Id.* at 147.
312. *Id.* at 158-59.
313. *Id.*
314. VALERIANO, *supra* note 6, at 155.

technological sectors where the state is not permitted [to] acquire technology legally."[315] On top of those directly employed by the state, China has co-opted and nurtured a network of patriotic cyber militias estimated by some to have a membership between 8-10 million hackers.[316] China must keep its hacker base occupied, however, because after helping to build this many-headed beast, it has perhaps inadvertently built the potential for an internal threat. The state's relationship with hackers has evolved since the 1990s to the present, over the course of three leaders who have each taken a progressively more proactive approach to controlling these groups.[317] Tim Maurer has studied state relationships with proxy hacker groups in several states and found "China [to be] an excellent case study to trace how a state moved from permitting the malicious behavior of hackers, to creating institutions and structures to orchestrate private actors, and eventually to tightening the leash even further and moving from orchestration to delegation."[318]

Founded in 1997, the Green Army was China's first known hacker group, and a surge of other patriotic hackers followed.[319] During the presidency of Jiang Zemin (1994-2003), this growing number of hackers were able to conduct actions the government was not able to do yet and were supporting the state's purposes.[320] They were "defacing foreign websites and launching DDoS attacks against them while also targeting domestic critics of the state."[321] As these groups grew in size and number, the state realized that it could gain great benefit from them: "[In] the early 2000s it was becoming increasingly clear that there was an active group of private citizens ready and willing to serve as proxies, who enjoyed support from the Chinese population and were even revered in some circles as patriotic heroes."[322] In 1999, the *PLA Daily* signaled this more proactive approach in an article reporting on government plans for "developing a computer network warfare capability, training a large number of network fighters in PLA academies, strengthening network defenses in China, and *absorbing a number of civilian computer masters* to take part in future network wars."[323] By the end of Zemin's presidency, militia units were established through local "telecommunications and cybersecurity companies in the city of Guangzhou, a technology hub in China's south."[324]

The state of the proxy relationship that Hu Jintao inherited as president (2003-2013) is widely agreed to have been a mix of militia groups and

315. *Id.* at 147.
316. *Id.* at 154.
317. TIM MAURER, CYBER MERCENARIES: THE STATE, HACKERS, AND POWER 107 (2018).
318. *Id.*
319. *Id.* at 108.
320. *Id.* at 109.
321. *Id.*
322. *Id.* at 110.
323. *Id.*
324. *Id.* at 111.

independent actors who were "state tolerated" or "state encouraged."[325] The PLA began to incorporate hackers into their major exercises around 2006 using hacker competitions and job postings.[326] Although the Chinese government consistently denied any type of sponsorship of these hacker groups, below the surface it was clear that the state was steadily increasing its control.[327] "[A]s the militia system matured and was further institutionalized in the mid-2000s, the government was increasing its domestic control over the Internet by requiring Chinese users to use their actual names and IDs online and cracking down on cybercriminals that did not play by the (implicit) rules."[328] This is also the timeframe when reporting on hacking by Chinese actors was first made public.[329]

The present-day proxy system for China coincides with President Xi Jinping's (2013-present) and the PRC's first public acknowledgment of PLA information operations and cyber operations capabilities found in the 2013 Science of Military Strategy Report.[330] Beijing began exerting further control and institutionalizing civilian hacker groups and militias as well as professionalizing hackers within the military.[331] MIT analyst Eric Heginbotham described Chinese network operations forces as divided into (1) professional network warfare forces, (2) authorized forces, and (3) civilian forces:

> Professional network warfare forces are armed forces operational units specially employed for carrying out network attack and defense; authorized forces are organized local forces authorized by the armed forces to engage in network warfare, mainly built within the associated government departments, including the Ministry of State Security and the Ministry of Public Security; and the civilian forces are nongovernmental forces which spontaneously carry out network attack and defense and which can be employed for network operations after mobilization.[332]

China's hacker collective pressed the limits, as per their strategy, and were on the agenda for discussion between President Xi and President Obama when the former visited the White House in September 2015. "A few weeks prior to President Xi's visit . . . the Chinese government responded at last to years of sustained international pressure and arrested several hackers after "US intelligence and law enforcement agencies drew up a list of the hackers the United States wanted arrested."[333] Maurer observes that the political purpose was served, but it is unclear whether justice was served in the process.[334]

---

325. *Id.* at 113.
326. *Id.*
327. *Id.*
328. *Id.* at 114-15.
329. *Id.* at 114.
330. *Id.* at 115.
331. *Id.*
332. *Id.* at 115-16, 118 ("Like private cybersecurity contractors, China's militias carry out activities that are mostly defensive in nature.").
333. *Id.* at 116.
334. *Id.* at 117.

During the meeting in Washington, DC, "President Xi and President Obama had made an explicit agreement committing both countries not to conduct cyber-enabled theft of intellectual property for competitive advantage."[335] Following their meeting, the Chinese theft of IP for competitive advantage came to a near stand-still in a dramatic, noticeable fashion.[336] For observers, this demonstrated a level of control over these hackers that had not been present in China in the past. "China's actions in the coming years will therefore help clarify to what extent China's officials at the top have effective control over the various intelligence agencies, units of the PLA, and the networked system of militias across the country."[337]

"The government essentially tries to walk a fine line between leveraging actors and capabilities detached from the state and keeping those actors' patriotism in check to avoid unintended escalation."[338] That escalation could be in the form of external action that could get China into a conflict not of its choosing, or internal action that increases instability within the state.[339] Chinese military strategic documents state that "since 'military and civilian attacks are hard to distinguish,' the PLA should 'persist in the integration of peace and war [and] the integration of the military and civilians.' Such that 'in peacetime, civilians hide the military, [while] in wartime, the military and the people, hands joined, attack together."[340]

China's capabilities and desire to control hackers and its focus on a strict view of sovereignty are mutually reinforcing. This helps China to avoid attribution or responsibility for cyber actions when it is politically beneficial and take action to reduce or control it when that supports the regime's goals. China has found the value of trying to catch up to its rivals using patriotic hackers, but now with the state making its own technological advances and as China attempts to be a bigger, more responsible player internationally, China is tightening its control and turning them more towards network defensive responsibilities.[341]

The lack of consensus and a clear set of rules has led some scholars to call for a treaty specific to cyberspace. In 2010, Rex Hughes proposed basic principles for such a treaty, noting, however, that IHL certainly already applies.[342] He conceded that serious analytical rigor would be required to know exactly how those IHL principles should apply.[343] Hathaway, et al, concur, finding that the lack of a treaty leaves states wanting for the clarity that a "codified definition of cyber-attack or written guidelines on how states should respond" would surely

335. *Id.*
336. *Id.* at 119.
337. *Id.* at 117.
338. *Id.* at 119.
339. VALERIANO, *supra* note 6, at 154.
340. MAURER, *supra* note 317, at 108.
341. VALERIANO, *supra* note 6, at 143 ("the shift from a state seeking to use cyber espionage to catch up to its adversaries to a state focused on maintaining dominance in the Asia Pacific region and within China itself.").
342. Rex Hughes, *A Treaty for Cyberspace*, 86 INT'L AFF. 523, 534 (2010).
343. *Id.*

provide.[344] They argue that without such a treaty, states are more likely to respond to cyber attacks with kinetic force, believing that invoking self-defense is legitimate.[345] Robin Geiß notes that the continued innovation in cyberspace and expanding capabilities may make a treaty even more necessary.[346] As discussed above, the opposite could also result, with states comfortable with the ambiguity that a lack of a specific treaty provides.

Schmitt and Vihul have discussed the nature of international norms in a cyberspace context and argue that treaty law tends to emerge slowly, as exemplified in the law of the sea context, which took until 1958 to crystallize into a treaty after centuries of naval warfare; and air warfare, which has no treaty governing such conduct after a century of application of existing principles.[347] They present the case convincingly that it is far too soon for a treaty governing state activities in cyberspace in highlighting the United Kingdom's submission to the U.N. in 2013:

> Experience in concluding these agreements on other subjects shows that they can be meaningful and effective only as the culmination of diplomatic attempts to develop shared understandings and approaches, not as their starting point. The United Kingdom believes that the efforts of the international community should be focused on developing common understandings on international law and norms rather than negotiating binding instruments that would only lead to the partial and premature imposition of an approach to a domain that is currently too immature to support it.[348]

It is critical to note that at this early stage of testing the limits of application of existing law to cyberspace activities, attempts to conclude a multilateral treaty means the final product "would likely be perforated with individual reservations, thereby degrading its practical effect."[349]

Cyberspace operations lend themselves to testing boundaries, since the prospect of battlefield casualties for the attacker is so low.[350] Therefore, we may yet see a day when, due to the unpredictability of cyberspace capabilities, a state finds itself a victim of a type of attack not contemplated before, that state responds (or desires to respond) with force, and justifies itself on the world stage. This would be the clearest form of state practice; not mere words, but actions, consequences,

344. Hathaway, *supra* note 280, at 880.

345. *Id*. at 840.

346. Robin Geitß, *The Conduct of Hostilities in and via Cyberspace, American Society of International Law*, 93 AM. J. INT'L L. 322, 372 (2017).

347. Michael N. Schmitt & Liis Vihul, *The Nature of International Law Cyber Norms,* Tallinn Papers No. 5 at 19 (2014), https://perma.cc/VDP7-48CG.

348. *Id*. at 19 (quoting U.N. Secretary-General, *Developments in the field of information and telecommunications in the context of international security*, 19, UN Doc. A/68/156 (July 16, 2013) https://perma.cc/FYV5-GKP5).

349. *Id*. at 20-21.

350. Louise Doswald-Beck, *Confronting Complexity and New Technologies: A Need to Return to First Principles of International Law*, 106 AM. J. INT'L L. 109 (2012).

and acceptance or rejection by the world community. Such an event would likely either lead to a global call for a cyberspace treaty or serve to solidify the interpretation of norms applied to cyberspace.

China, too, has proposed a voluntary code of conduct for information security in the form of a proposed U.N. General Assembly Resolution on 14 September 2011.[351] The proposal, co-sponsored by the Russian Federation, Tajikistan, and Uzbekistan, is completely voluntary, meaning that there is no binding nature to it whatsoever. It also promotes some of the same themes discussed above regarding China's focus on national control and sovereignty over the Internet and establishment of a "multilateral, transparent and democratic international Internet management system" which falls in line with China's previous proposal to reduce the authority of the ICANN and move Internet responsibilities to the ITU.

China has begun to at least outwardly evidence changes in attitude regarding economic espionage for competitive advantage. "A leading source of cyber security news recently declared that China is now the active source for cyber security norms after they followed up the [Xi-Obama] agreement with similar agreements with Canada, the UK, and Europe."[352] After the past three decades of using proxies to gain an advantage in cyberspace, "China might have concluded that a more stable cyberspace [is in] the interest of all, especially with a violent domestic population and criminal actors . . . [and] China is now seeking to be the leader in cyber security norms for the international system."[353] Valeriano, et al, expect China to "focus on maintaining domestic control and shaping Internet governance in an image that supports control over actions within its borders."[354]

A strong view of sovereignty and a firmer definition of norms in cyberspace internationally are certainly to China's advantage as its strategic needs have changed. "This shift likely demonstrates China's interest in shaping the normative system in cyberspace, directing allowed action away from commercial espionage because it achieves no clear gain for China, and focusing instead on allowing for the continuation of hacking activities to achieve a military advantage in case of future conflict."[355] Growing a norm of national sovereignty over the Internet enables China to limit talk of democracy within its country, thereby ensuring the continuity of the CCP at the head of the PRC.[356] The *New York*

351. Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, UN Doc A/66/359 (Sept. 14, 2011), https://perma.cc/7HK9-WHPJ.

352. VALERIANO, *supra* note 6, at 169.

353. *Id*. at 170.

354. VALERIANO, *supra* note 6, at 169-70 ("How China operates in cyberspace is also influenced by their views of how the domain should be governed. They advocate a multilateral model where each state makes the rules for their territory based on the principle of sovereignty, differing from the multi-stakeholder model typically advocated by Western actors [i.e, the Westphalian order]. This view would suggest a limited utility of attacking externally but does not preclude the utility of espionage in order to protect sovereign interests.").

355. *Id*. at 167.

356. Editorial Board, Opinion, *There May Soon Be Three Internets. America's Won't Necessarily be the Best*, N.Y. TIMES (Oct 15, 2018), https://perma.cc/KE2Z-XT4X.

Times also argues that an "increasingly sophisticated system of digital surveillance plays a major role in human rights abuses, such as the persecution of the Uighurs."[357] As its power has grown, China has seen the benefit to limit external cyber actions to espionage along with its peers and rivals, while maintaining focus on national sovereignty over the Internet to hold onto control of its population through censorship and digital surveillance.

CONCLUSION

At the outset of this inquiry, we discussed that Yan Xuetong proposes a philosophy for China that, as the "rising nation [it] should adopt the strategy of expanding its interests in emerging areas."[358] As China has done that, it has used legal warfare to prepare the environment of those domains for China's continuing advance. Yan continued his recommendations advising that "[t]he rising nation should also make timely adjustments to its external strategy in accordance with its own capabilities in each area."[359] China has taken this advice on with vigor, advancing into a STEM (science, technology, engineering, and mathematics) revolution in education:

- In 2015, Tsinghua University passed MIT in the *U.S. News & World Report* rankings to become the number-one university in the world for engineering;
- China annually graduated four times as many students as the U.S. (1.3 million vs. 300,000) [in STEM fields];
- In every year of the Obama administration, Chinese universities awarded more PhDs in STEM fields than American Universities.[360]

With the advances in education, China is focusing on the next areas of emerging technology and will be ready to use legal warfare to set the international norms for those domains as is being done in outer space and cyberspace. Those changes, thus far, have been in areas to strengthen China's military and economic power and to increase its own sense of sovereignty – a brand of sovereignty that could eventually lead to China's dream of operating as a benign hegemon in a new unipolar system. The PRC's foreign policy runs against the current world order, "especially the post-World War II norms of national autonomy, sovereign equality, universal human rights, and political democracy.[361] As China moves into the fore in areas such as machine learning, artificial intelligence, 5G technology, and more, China will set the norms and the legal rules of the road. That is

357. *Id.*
358. Yan, *supra* note 2.
359. *Id.*
360. ALLISON, *supra* note 1, at 16-19 (Bullets excerpted are only a sampling of the research showing China's acceleration into STEM primacy over the United States).
361. WANG, supra note 24, at 197.

their legal warfare strategy at work. "The PRC was thus born to be a rebel and has remained always an insurgent, seeking no less than a revolutionary change of the current world's political order in its own image whenever and wherever possible, so as to ensure the security and power of the ruling CCP leadership."[362]

China attempts to shape international law in these areas of emerging technology to suit its goals of creating a 21st century *tianxia* world order. Fei-Ling Wang's deep study of *tianxia* world order indicates that Beijing "constantly and inevitably feels discontent and insecure without the [*tianxia*] China Order."[363] Xi Jinping said in his 2017 New Year's Message "Chinese people have always wanted to have a great harmony for the whole world as one family."[364] Wang finds this tone strikingly similar to Mao's concept of a "grand solidarity of the world's people" and sees Xi's idea as a "restoration of the China Order at new scale that tantalizingly suggests a fundamental challenge to the four-century-old Westphalia System."[365]

Those such as Valeriano, Jensen, and Maness consider China's behavior almost benign or at least no cause for concern: "Beijing's actions [in the digital domains] tend to be predictable and restrained. They operate in cyberspace to seek economic and research advantages, maintain a position of control over their population, promote regime stability, and sometimes activate national sentiment over common issues such as rights to shipping lanes and the treatment of North Korea."[366] They call others, such as Mearsheimer, Allison, and Cheng, "pessimists [who] see a cyber dragon, characterizing Chinese strategic moves in the digital domain as destabilizing."[367] And, their conclusions about the state of the relationship between the U.S. and China is that it is a "competitive but stable great power relationship" rather than an "unstable US-China competition shap[ing] the international order."[368]

Yan presents a theory of leadership change that convincingly argues that the U.S. is unlikely to prevent at least a bipolar world order in the coming decades. He explains that the position of a dominant state leads it to become comfortable and less motivated to make reforms that would maintain or grow its relative advantage.[369] The position of the U.S., he argues, is declining even faster than it might otherwise due to the leadership within the U.S. "At times when the government of a rising state has a greater sense of responsibility than the dominant state does, such disparity is manifest in the former's implementation of more reforms than the latter, which will gradually reduce the capability disparity between them.

362. *Id*.
363. *Id*. at 209.
364. *Id*. at 212.
365. *Id*.
366. VALERIANO, *supra* note 6, at 145.
367. *Id*.
368. *Id*.
369. Yan, *supra* note 2, at 192.

If this situation lasts for a number of decades, the rising state's comprehensive capability will catch up with or even surpass that of the dominant state."[370]

According to Yan, power redistribution results in transformation in the international system.[371] He finds that this transformation more often occurs between two states of differing norms than two of the same.[372] As Yan has argued, a new great power at the top of an international order will naturally change the norms to enable that power to maintain its position at the top.[373] It stands to reason that as long as China is on the rise, it will plan to change the norms of international law through its doctrinal legal warfare strategy and the domains that will see it first and most dramatic are in outer space, cyberspace, and other areas of advanced technological innovation. Doing so prepares the environment for when China is one of a bipolar order and then sole power at the top of a new unipolar order under a China Order. Many PRC scholars and PLA leaders believe and have openly argued that the U.S. decline is the opportunity for China to take its alleged rightful place, under the Mandate of Heaven, as world leader.[374]

370. *Id*. at 193.
371. *Id*. at 196-97.
372. *Id*.
373. *Id*.
374. WANG, *supra* note 24, at 211.

***