Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches

Zhixiong Huang* and Kubo Mačák**

Abstract

China and Western countries have repeatedly portrayed each other as potential or actual adversaries in cyberspace. Yet, both sides ostensibly subscribe to an international consensus that cyber operations must be subjected to the rule of law. Against this background, the article examines five key aspects of the rule of law in cyberspace, which are ordinarily understood as areas of contention: (1) preferred method of identification and development of international law; (2) competing models of cyberspace governance; (3) application of sovereignty to cyberspace; (4) question of militarization of cyberspace; and (5) legality of cyber espionage. Our analysis demonstrates that it is inaccurate to view China and the West as sharply divided and competing camps. Rather, the emerging picture reveals a web of relationships and views that reflect an overall trajectory of convergence, even if modest in scope and velocity.

I. Introduction

1. Within the time-span of one generation, cyberspace has become an environment where human relationships are forged and broken, where economic deals are struck and subverted, and where States engage in open

* Luojia Chair Professor, Wuhan University Institute of International Law, China, fxyhzx@whu.edu.cn. His research on this topic was supported by the Major Projects of National Social Science Fund of China (Grant No.: 16ZDA074).

** Senior Lecturer in Law, University of Exeter, United Kingdom, k.macak@exeter.ac.uk. The authors are grateful to Ana Beduschi, Duncan Hollis, Agnieszka Jachec-Neale, Eric Jensen, Andrea Lista, and Michael N. Schmitt for their helpful comments on earlier drafts of this article. We gratefully acknowledge the research assistance of Xiaoqi Chen. The research collaboration at the heart of this project was made possible by the support of the University of Exeter Visiting International Academic Fellowships and the Outward Mobility Academic Fellowships programmes. The article was finalised on 14 May 2017 and the websites cited were current as of that date.

diplomacy as well as covert espionage. Its importance for economic growth and human progress cannot be underestimated. In 2014 alone, the Internet sector contributed 6 percent of real gross domestic product (GDP) in the United States and 7 percent in China.[1] As of March 2017, nearly half of the world's population was online[2] and this figure is expected to grow to almost 60 percent by the end of this decade.[3]

2. In parallel with the growing importance of cyberspace for virtually every aspect of human interaction, States have recognized the potential strengths and vulnerabilities of this new domain. Real and perceived threats range from cybercrime and cyber espionage[4] to rather less realistic concerns about an impending "cyber Pearl Harbor".[5] They have rattled the imagination and the composure of State and non-State actors alike. Meanwhile, cyberspace has proven a crucial "enabler" of China's emergence as a great power on the world stage.[6] Rightly or wrongly, China and Western countries have repeatedly portrayed each other as potential or actual adversaries in cyberspace.

3. Many incidents could be emphasised in the chequered history of the relationship between these two sides. Already in 1997, the US military was

---

1 Internet Association, New Report Calculates the Size of the Internet Economy (10 Dec. 2015), (internetassociation.org/121015econreport); Kou Jie, Internet economy 7% of China's GDP, Global Times (30 Oct. 2015), (www.globaltimes.cn/content/949867.shtml).

2 Internet World Stats: Usage and Population Statistics (25 Mar. 2017), (www.internetworldstats.com/stats.htm).

3 Forrester, Forrester Research World Online Population Forecast, 2015 to 2020 (Global) (7 Oct. 2015), (www.forrester.com/go?objectid=RES127940).

4 For a recent example of the destructive potential of both, particularly in combination, see, e.g., Sam Jones, Timeline of cyber attack: How WannaCry's secret weapon spread, Financial Times (14 May 2017), (https://www.ft.com/content/82b01aca-38b7-11e7-821a-6027b8a20f23) (reporting on the spread of the ransomware program WannaCry, which was allegedly based on a repurposed cyber espionage tool stolen from the US National Security Agency and which had, by the time of writing, infected and disabled over 200,000 computers around the world, including many that were vital to the national critical infrastructure of various countries).

5 Sean Lawson, Does 2016 Mark the End of Cyber Pearl Harbor Hysteria? (7 Dec. 2016), (www.forbes.com/sites/seanlawson/2016/12/07/does-2016-mark-the-end-of-cyber-pearl-harbor-hysteria).

6 Jon R. Lindsay, Introduction: China and Cybersecurity: Controversy and Context, in: Jon R. Lindsay, Tai Ming Cheung and Derek S. Reveron (eds.), China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain (2015), 2.

reportedly preparing for high-tech contingency operations involving China.[7] In 2010, the relationship came under strain following Google's very public decision to withdraw from the Chinese market, which it justified in part as a response to alleged sophisticated cyber intrusions originating from China.[8] Since then, the two sides have traded multiple accusations of cyber attacks. For instance, China claimed the US "was behind" cyber operations against the Chinese search engine Baidu,[9] and the US issued an indictment against five members of the Chinese military for alleged acts of economic cyber espionage.[10] There is little sign that this latent conflict, a "Cyber Cold War" perhaps, will be abating any time in the near future.[11]

4. Although the two sides disagree on the factual circumstances underpinning these confrontations, they are in agreement on the general need to subject operations in cyberspace to the rule of law. This is not in doubt; after all, like any other human activity, conduct in cyberspace is not beyond the regulatory reach of States. Moreover, the borderless nature of cyberspace and its impact on key State interests necessitate a normative response at the level of international law. This is consonant with the approach of the International Court of Justice (ICJ), which has emphasized the international dimension of the principle of the rule of law in several of its rulings.[12]

---

7 Thomas Rid, Rise of the Machines: A Cybernetic History (2016), 311.

8 Google, A New Approach to China (12 Jan. 2010), (googleblog.blogspot.co.uk/2010/01/new-approach-to-china.html).

9 Bill Gertz, Beijing accuses U.S. of cyberwarfare, Washington Times (26 Jan. 2010), (www.washingtontimes.com/news/2010/jan/26/beijing-accuses-us-of-cyberwarfare).

10 US Department of Justice, Attorney General Eric Holder Speaks at the Press Conference Announcing U.S. Charges Against Five Chinese Military Hackers for Cyber Espionage (19 May 2014), (www.justice.gov/iso/opa/ag/speeches/2014/ag-speech-140519.html).

11 See, e.g., US DoD, Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2016 (26 Apr. 2016), (www.defense.gov/Portals/1/Documents/pubs/2016%20China%20Military%20Power%20Report.pdf), 64 (noting that computer systems owned by the US government continued to be targeted for intrusions in 2015, some of which appeared to be attributable to China's government and military); Chen Weihua, China, US talk cyber standards, China Daily (12 May 2016), (www.chinadaily.com.cn/world/2016-05/12/content_25240074.htm) (reporting that attacks originating from the US had not decreased following the US-China summit in Sept. 2015).

12 See, e.g., Asylum Case (Colombia v. Peru), Judgment, ICJ Reports 1950, 266, 284 (contrasting "arbitrary action" with the rule of law); Case

Furthermore, as Brian Tamanaha observed in *On the Rule of Law*, "[i]f there is to be an enduring international rule of law, it must be seen to reflect the interests of the entire international community". [13] Understanding the differences between the Chinese and Western approaches to the international rule of law in cyberspace accordingly takes on urgent importance.

5. This article argues that the shared general commitment of both sides to the rule of law acts as a powerful force of convergence that will lead to gradually overcoming, or at least narrowing, key points of contention. This is a dramatically different picture than that painted by numerous scholars, who typically speak of competing "camps" of countries holding fundamentally dissimilar views on matters of cyberspace.[14] We challenge this view and argue that, upon close inspection, China and the West are slowly coming together on many central issues, including Internet governance or sovereignty in cyberspace.

6. The article counterposes Chinese views, approaches and positions with those held by Western countries. Two notes of caution are in order. First, although the US is the most prominent and the most powerful of the category of countries referred to herein as "the West" and for this reason it receives the lion's share of attention in this article, it bears noting that the US views are naturally not always identical or even similar to those of other Western countries. Therefore, we have attempted to highlight such "internal" discrepancies.

7. Second, although by any account Russia is—next to the US and China—the third major cyber power in the world, we do not analyse its positions in detail in this article. While it would certainly be interesting to triangulate the Russian views vis-à-vis its Chinese and Western counterparts, doing so would take us outside of the scope of the article and as such it has to

---

Concerning Elettronica Sicula S.p.A. (ELSI) (USA v. Italy), Judgment, ICJ Reports 1989, 15, 76, para. 128 ("Arbitrariness is not so much something opposed to a rule of law, as something opposed to the rule of law.").

13 Brian Tamanaha, On the Rule of Law: History, Politics, Theory (2004), 136. For a theoretical discussion of the notion of international rule of law, see further, e.g., Sir Arthur Watts, The International Rule of Law, 36 German YIL (1992), 5; James Crawford, International Law and the Rule of Law, Adelaide LR (2003), 3; Simon Chesterman, An International Rule of Law?, 56 American JCL (2008), 331; Robert McCorquodale, Defining the International Rule of Law: Defying Gravity?, 65 ICLQ (2016), 277.

14 See, e.g., Scott Shackleford and Amanda Craig, Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity, 50 Stanford JIL (2014), 119, 135; Kristen E. Eichensehr, The Cyber-Law of Nations, 103 Georgetown LJ (2015), 317, 333; Nigel Inkster, China's Cyber Power (2015), 9.

remain a possible subject of future research. Nonetheless, we do refer to the Russian views on occasion in order to cast a clearer light on the Chinese position on issues where the two might be or have been conflated.

8. The structure of the article is as follows. In the next section, we examine the extent of the commitment of States on both sides of the supposed East-West divide to the international rule of law in cyberspace and consider the probable reasons for their shared understanding. We then analyse five specific aspects of the rule of law in cyberspace on which China and Western countries are ordinarily understood as taking fundamentally incompatible views. These perceived areas of contention include the preferred method of identification and development of international law (section III); the supposed clash between the "multilateral" and "multi-stakeholder" models of Internet governance (section IV); the application of the concept of sovereignty to cyberspace (section V); the allegations of militarization of cyberspace levelled against the West (section VI); and cyber espionage under international law (section VII). The final section of the article summarizes our argument and offers some concluding observations.

II. International rule of law in cyberspace: Shared concept, diverse conceptions

9. In the "path-breaking"[15] 2011 *International Strategy for Cyberspace*, the Obama Administration declared for the first time that it "support[s] the rule of law in cyberspace", and that "[l]ong-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace".[16] Expressions of commitment to the rule of international law by other Western States soon followed. For example, the European Union's 2013 *Cybersecurity Strategy* stated that "[i]n its international cyberspace policy, the EU will seek to promote openness and freedom of the Internet, encourage efforts to develop norms of behaviour and apply existing international laws in cyberspace".[17]

---

15 Paul Meyer, Outer Space and Cyberspace: A Tale of Two Security Realms, in: Anna-Maria Osula and Henry Rõigas (eds), International Cyber Norms: Legal, Policy & Industry Perspectives (2016), 164.

16 The White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (2011), (www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf), 9 (hereinafter "US International Strategy").

17 EU, European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1

10. China has likewise clearly declared full support for the rule of law approach to the governance of cyberspace. As early as 2010, in response to criticism levied by Western countries against Internet regulation in China,[18] the Chinese government stated that "China abides by the general obligations and any specific commitment as a WTO member, [… and] guarantees the citizens' freedom of speech on the Internet as well as the public's right to know, to participate, to be heard and to oversee in accordance with the law."[19] This policy statement marked the first expression of China's view on the rule of law in cyberspace. At the 2012 Budapest International Conference on Cyberspace, Huang Huikang, the Head of the Chinese Delegation, reaffirmed this commitment when he noted, "[a]s an old Chinese saying goes, nothing can be accomplished without rules. […] Although cyberspace is virtual, it needs rules and norms to follow."[20] And at the 6th China-US Internet Industry Forum held in Beijing in 2013, the Chinese representative observed, "[w]e need a cyberspace with international rule of law […] The rule of law is the best approach to Internet governance because it is in parallel with the development of human civilization today which seeks to operate in a rule-based environment".[21]

11. Since these first proclamations by the US and China, an international consensus on the importance of a rule-of-law approach to

---

final (7 Feb. 2013), 2 (hereinafter "EU Cybersecurity Strategy").

18 In particular, it has been claimed that China's Internet regulations violated China's obligations under various agreements of the World Trade Organization, as well as its international human rights obligations on freedom of speech (although China has yet to accede to the 1966 International Covenant on Civil and Political Rights). See, e.g., David Coursey, US May Use WTO to Resolve Google-China Dispute (4 Mar. 2010), (news.techworld.com/networking/3214222/us-may-use-wto-to-resolve-google-china-dispute) (stating that the Obama Administration is reportedly considering using the World Trade Organisation to help Google in its censorship battle with China).

19 China, White Paper on the Internet in China (8 June 2010), (www.china.org.cn/government/whitepaper/2010-06/08/content_20207975.htm).

20 Huang Huikang, Statement at Budapest Conference on Cyber Issues (4 Oct. 2012), (www.chinesemission-vienna.at/eng/zgbd/t977627.htm).

21 Ma Xinmin, What Kind of Cyberspace We Need?, 3 Contemporary International Relations (2015), 102–107. In early 2017, the aim to "enhance international rule of law in cyberspace" was named as one of China's strategic goals. See International Strategy of Cooperation on Cyberspace. Xinhuanet (1 Mar. 2017), (http://news.xinhuanet.com/english/china/2017-03/01/c_136094371.htm).

cyberspace governance has been achieved. An early indication of this consensus came in the form of a "landmark"[22] report of the United Nations (UN) Group of Governmental Experts (GGE) adopted in June 2013.[23] The report, agreed to by representatives of fifteen cyber-active nations selected on the basis of equitable geographic distribution, confirmed that "[i]nternational law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT [information and communication technology] environment".[24] In another consensus report adopted by the UN GGE (albeit one of slightly differently composition) in July 2015, further progress was achieved as to how international norms, rules and principles apply to State-conducted ICT-related activities.[25] The consensus of the UN GGE was widely acknowledged within and outside the UN at, *inter alia*, the Seoul Conference on Cyberspace 2013[26] and at the Antalya Summit of G20 Leaders in 2015.[27]

12. Therefore, the premise that international rule of law is indispensable for the future order of cyberspace has now become universally accepted. For instance, during President Xi Jinping's State visit to the US in September 2015, China and the US issued a statement to the effect that:

> Both sides are committed to making common effort to further identify and promote appropriate norms of state behavior in cyberspace within the international community. The United States and China welcome the July 2015 report of the UN Group of Governmental Experts in the Field

---

22 United States, Department of State, Statement on Consensus Achieved by the UN Group of Governmental Experts On Cyber Issues (7 June 2013), (www.state.gov/r/pa/prs/ps/2013/06/210418.htm).

23 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98, 24 June 2013 (hereinafter "UN GGE 2013").

24 Ibid., para.19.

25 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174, 22 July 2015 (hereinafter "UN GGE 2015").

26 Seoul Framework for and Commitment to Open and Secure Cyberspace, (www.mofat.go.kr/english/visa/images/res/SeoulFramework.pdf).

27 G20 Leaders' Communiqué at Antalya Summit, (www.cfr.org/economics/g20-leaders-communique-antalya-summit/p37362).

> of Information and Telecommunications in the Context of International security, which addresses norms of behavior and other crucial issues for international security in cyberspace.[28]

13. It is true that States have different interests and divergent perceptions of the international order in cyberspace. Yet, their readiness to embrace the rule of law in cyberspace can be seen as a rational choice based on their common interest and inter-dependence in cyberspace. As Malcolm Shaw put it, "[i]n the long march of mankind from the cave to the computer a central role has always been played by the idea of law—the idea that order is necessary and chaos inimical to a just and stable existence".[29] Here, just as on the high seas, in the airspace, in the outer space and in other international domains, the rule of law offers stability and predictability which allows members of the international community, including China and Western countries, to pursue their common interests while accommodating their differences. This is all the more so due to the fact that both sides share a similar mix of strengths and vulnerabilities, very well expressed by a high-ranking Chinese military officer at a meeting with US representatives in this vivid metaphor: "The United States has big stones in its hands but also has a plate-glass window. China has big stones in its hands but also a plate-glass window. Perhaps because of this, there are things we can agree on".[30]

III. Identification and development of international cyberspace law

14. While a general consensus may be and—it is submitted—has been reached in the international community on the level of general principles, States remain divided on many key issues regarding the rule of law in cyberspace. The reasons for these divergences are varied. They include mankind's limited knowledge and practice regarding cyberspace and different, sometimes even opposing, ideologies, values and national interests. Compared to most other fields of international law, the rule of law in cyberspace is still in a nascent stage.

15. The first area where Western and Chinese views appear to diverge relates to the preferred method of development and interpretation of

---

28 The White House, FACT SHEET: President Xi Jinping's State Visit to the United States, (www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states).

29 Malcolm N. Shaw, International Law (7th edn., 2014), 1.

30 Joseph Menn, Agreement on cybersecurity "badly needed", Financial Times (12 Oct. 2011), (www.ft.com/cms/s/0/e595e568-f4dc-11e0-ba2d-00144feab49a.html).

international legal rules for State conduct in cyberspace. This issue is closely related to the preferred mode of Internet governance, discussed later in this article.[31] In principle, the key difference relates to the question whether there is a need for new rules of international law governing cyber operations or whether the existing body of law is satisfactory.

16. On the one hand, the US has argued that the existing international law framework is adequate. In its view, the novel nature of cyber operations may necessitate the reinterpretation of some of the applicable rules, but by and large, the pre-Internet rules should suffice for the online era. This was clearly outlined already in the White House's 2011 *International Strategy for Cyberspace*:

> The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, 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.[32]

17. US endorsement of the existing legal framework implied two logical consequences. First, it translated into an invitation—or even soft pressure—for other States to issue similar acknowledgments. That they would do so had not always been foreordained. In the mid-1990s, Internet activists were attempting to keep cyberspace free of any government regulation, whether pre-existing or new, an approach epitomised by John Perry Barlow's 1996 *Declaration of the Independence of Cyberspace*.[33] Twenty years later, the document, which describes governments as "weary giants of flesh and steel" and their

---

31 See section IV below.

32 US International Strategy, above n.16, 9. This appears to have remained the US view until the present day. In his speech delivered at Berkeley Law School on 10 Nov. 2016, Brian J. Egan, Legal Adviser of the US Department of State, reiterated that "[e]xisting principles of international law form a cornerstone of the United States' strategic framework of international cyber stability during peacetime and during armed conflict". See Brian J. Egan, International Law and Stability in Cyberspace (www.justsecurity.org/wp-content/uploads/2016/11/Brian-J.-Egan-International-Law-and-Stability-in-Cyberspace-Berkeley-Nov-2016.pdf), 2. No change in this respect has been discernible between the inauguration of President Donald Trump in Jan. 2017 and the completion of this article in May 2017.

33 John P. Barlow, A Declaration of the Independence of Cyberspace (1995), (projects.eff.org/~barlow/Declaration-Final.html).

laws as "hostile and colonial measures",[34] may sound oddly antiquated. But at that time it was conceivable (and seriously argued) that the rules designed for the "offline world" would not, and should not, reach into cyberspace.[35]

18. Nonetheless, calls for cyberspace as a sovereignty-free zone remained fantasies. Gradually, other States from all geographical regions issued statements affirming that they too considered international law applicable to conduct in cyberspace.[36] This viewpoint was cemented in the 2013 UN GGE report mentioned above,[37] which was later endorsed by a resolution of the UN General Assembly.[38] Therefore, today the international community shares the originally predominantly US position that international law is applicable to the cyber domain.

19. Secondly, acceptance *that* international law applies in general begs the question of *how* precisely it does so in specific circumstances. In other words, the US position implies the need for States to interpret the existing rules in the context of novel situations that arise in connection with States' and other actors' conduct in cyberspace.

20. This is equally relevant to both principal sources of international law. With respect to treaties, the agreement of State parties to a treaty on a specific interpretation of a provision is considered "authentic interpretation"[39] or "authoritative interpretation"[40] and carries greater weight in the interpretive process, a point that is confirmed by the Vienna Convention on the Law of Treaties.[41] Interpretation of customary rules by States may likewise contribute

---

34 Ibid.

35 See, e.g., David R. Johnson and David Post, Law and Borders: The Rise of Law in Cyberspace, 48 Stanford LR (1996), 1367.

36 See, e.g., UN Doc A/65/154 (2010), 15 (United Kingdom); UN Doc A/68/156/Add.1, 4 (Canada); ibid., 12 (Iran); ibid., 15 (Japan); ibid., 16–17 (Netherlands); UN Doc A/66/152 (2011), 6 (Australia); ibid., 18 (US); UN Doc A/68/156 (2013), 18 (United Kingdom); UN Doc A/69/112 (2014), 16 (Switzerland).

37 UN GGE 2013, above n.23, para.19.

38 GA Res 68/243 (9 Jan. 2014), preambular para.18.

39 ILC, Summary record of the 765th meeting, UN Doc A/CN.4/SR.765 (1964), 277 para.34 (Ruda) ("as between States the only legally valid interpretation of a treaty was the *authentic interpretation* by the parties to the treaty") (emphasis added).

40 Delimitation of the Polish-Czechoslovakian frontier (question of Jaworzina), advisory opinion, PCIJ Reports, Series B, No. 8 (1923), 37 ("it is an established principle that the right of giving an *authoritative interpretation* of a legal rule belongs solely to the person or body who has power to modify or suppress it") (emphasis added).

41 Vienna Convention on the Law of Treaties (VCLT), 1155 UNTS 331, art. 31(3)(a) (requiring to take into account, together with the context, "any

towards the clarification of their content or development, as the line between interpretation and creation of customary international law is notoriously indistinct.[42] Therefore, whatever the source in question, official statements of States concerning existing rules of international law are of crucial importance. Regrettably, such statements have been infrequent in the area of cyber security.[43]

21. On the other hand, the Chinese position on this issue differs in crucial aspects from that of the US. Although China, as one of the States continuously represented in the UN GGE, accepts the general applicability of international law to cyberspace, it differs substantially with regard to the need for new rules. Its representatives emphasize that novel "unique problems without ready solutions" emerge from cyberspace and "it is necessary to formulate new legal rules to solve them".[44] This approach is also reflected in the new Chinese 2016–2020 five-year plan, which for the first time expressly suggests that China should "[a]ctively participate in the making of international rules on the Internet".[45] In support of this view, Chinese

---

subsequent agreement between the parties regarding the interpretation of the treaty or the application of its provisions").

42 Cf. Reparation for Injuries Suffered in the Service of the United Nations, Advisory Opinion, ICJ Reports 1949, 174, 190 (ind. op. Alvarez) ("[I]n many cases it is quite impossible to say where the development of law ends and where its creation begins").

43 See further Michael N. Schmitt and Sean Watts, The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare, 50 Texas ILJ (2015), 189 (on State silence concerning IHL and cyberspace); Kubo Mačák, From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers, 30 Leiden JIL (2017) (forthcoming) (on States' general reluctance to engage in international law-making in the area of cyber security). For two notable exceptions to this trend, see Harold H. Koh, International Law in Cyberspace, 54 Harvard ILJ Online (2012), 1 (outlining the US position on a number of issues concerning the application of international law to cyber operations); Egan, above n.32, 8–22 (outlining the US views on how certain rules of international law apply to States' behaviour in cyberspace).

44 Ma Xinmin, Letter to the Editors: What Kind of Internet Order Do We Need?, 14 Chinese JIL (2015), 399, 401.

45 Goals, missions of China's new five-year plan, Xinhuanet (5 Mar. 2016), (news.xinhuanet.com/english/2016-03/05/c_135158252.htm). See also International Strategy of Cooperation on Cyberspace. Xinhuanet (1 Mar. 2017), (http://news.xinhuanet.com/english/china/2017-03/01/c_136094371.htm) ("China supports formulating universally accepted international rules and norms of state behavior in cyberspace").

representatives have repeatedly invoked the metaphor of cyberspace as a road system with heavy traffic, but no comprehensive "traffic rules".[46]

22. The first significant attempt to draw up such "traffic rules" with global reach is the joint Sino-Russian proposal for an *International Code of Conduct for Information Security*.[47] This document was drafted in the form of a proposed UN General Assembly resolution and contains thirteen numbered "pledges", with content varying from the reaffirmation of existing international legal rules[48] to the taking a stand on contested issues like Internet governance.[49] In addition to Russia and China, the initiative is presently supported by the other members of the Shanghai Co-operation

---

46 See, e.g., China, Speech by H.E. Ambassador Wang Qun at the First Committee of the 66th Session of the GA on Information and Cyberspace Security (20 Nov. 2011), (www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t869580.shtml) ("In this information age, information 'highway' has reached almost all corners of our planet. It is worrisome, however, that in this virtual space where traffic is very heavy, there is, hitherto, no comprehensive 'traffic rules'. As a result, 'traffic accidents' in information and cyber space constantly occur with ever increasing damage and impact."); Shen Jian, An International Code of Conduct for Information Security: China's perspective on building a peaceful, secure, open and cooperative cyberspace (Geneva, 10 Feb. 2014), (www.unidir.ch/files/conferences/pdfs/a-cyber-code-of-conduct-the-best-vehicle-for-progress-en-1-963.pdf) ("Nowadays, the information 'highway' has reached almost every corner in the world. It is of great concern, however, that in this virtual space where traffic is very heavy, there is still no comprehensive 'traffic rules'. As a result, 'traffic accidents' in information and cyber space constantly occur with ever increasing damage and impact.").

47 Letter dated 12 Sept. 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, 14 Sept. 2011, 3–5 (hereinafter "Code of Conduct 2011"); Letter dated 9 Jan. 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, UN Doc 69/723, 13 Jan. 2015, 3–6 (hereinafter "Code of Conduct 2015").

48 See, e.g., Code of Conduct 2015, above n.47, para.1 (mandating compliance with the UN Charter and other "universally recognized norms governing international relations").

49 Ibid., para.8 ("All States must play the same role in, and carry equal responsibility for, international governance of the Internet […] in a way which promotes the establishment of multilateral, transparent and democratic international Internet governance mechanisms").

Organization (SCO)—Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan.[50]

23. China also has demonstrated its preference for the development of new legal norms in its regional and bilateral norm-making initiatives. The Code of Conduct itself reflects many concepts contained in the SCO's binding 2009 Information Security Agreement (Yekaterinburg Agreement).[51] Further, in 2015, China entered into a bilateral agreement with Russia aimed at the enhancement of co-operation between the two countries on information security issues.[52] Both of these agreements contain specific binding commitments to co-operate in ensuring "international information security" in multiple areas.[53] Together, these initiatives confirm China's desire to expand its role in global governance on the basis of a conviction that it should transform itself from a "rule taker" to a "rule maker".[54]

24. What remains to be seen is, despite the potential flaws of the "law-by-analogy approach" of applying existing law in cyberspace,[55] whether other States will accept the need for the development of new international legal norms for the cyber domain. For now, the probability of other States joining

---

50 Code of Conduct 2015, above n.47, 1.

51 Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security (signed 16 June 2009, entered into force 5 Jan. 2012) (hereinafter "Yekaterinburg Agreement").

52 Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on Cooperation to Ensure International Information Security [*Соглашение между Правительством Российской Федерацией и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности*] (signed 8 May 2015), (government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf) (in Russian) (hereinafter "Russia-China Agreement"). On 25 June 2016, the presidents of the two countries signed a further joint declaration on promoting the development of information and cyber space. See Xinhua News Agency, China, Russia sign joint statement on strengthening global strategic stability, (news.xinhuanet.com/english/2016-06/26/c_135466187.htm).

53 See, e.g., Yekaterinburg Agreement, above n.51, art. 3; Russia-China Agreement, above n.52, art. 3.

54 See further Scott Kennedy and Shuaihua Cheng (eds.), From Rule Takers to Rule Makers: The Growing Role of Chinese in Global Governance (2012).

55 See Duncan Hollis, Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?, in: Jens David Ohlin et al. (eds.), Cyberwar: Law and Ethics for Virtual Conflicts (2015), 148–155 (discussing the inaccuracies, ineffectiveness and incompleteness of the law-by-analogy approach).

the Yekaterinburg Agreement is low, although this might change following the expected accession of India and Pakistan to the SCO in June 2017.[56] Similarly, the Sino-Russian Code of Conduct has achieved little traction beyond the six sponsoring States. Western States in particular have been said to view the initiative with suspicion and as "aimed at establishing a strict national sovereignty model over content flow over the Internet and potentially a tool of oppressive regimes".[57] Moreover, it has been suggested that even China may be sceptical with respect to multilateral binding commitments of this kind out of concern that "Russia would play the spoiler in any multilateral negotiation".[58]

25. Nevertheless, identification of norms through the UN GGE process is a strong indication of a convergence between the two "camps". As was mentioned, in 2013 the UN GGE adopted a "landmark consensus"[59] on the applicability of international law in cyberspace.[60] While the actual import of the consensus is controversial, as it was expressed in the form of a non-binding report, such non-binding documents may effectively lead to binding rules over time.[61] Also, the symbolic value of the GGE as a norm-making process should not be underestimated. Composed of representatives of 15 UN member states, including the three "cyber superpowers" (China, Russia, and the United States), the GGE's position can be taken as confirming a shared understanding in the international community. [62] In 2015, the

56 See India, Pakistan edge closer to joining SCO security bloc, The Express Tribune (24 June 2016), (tribune.com.pk/story/1129533/india-pakistan-edge-closer-joining-sco-security-bloc); Liu Caiyu, India, Pakistan to become full SCO members, Global Times (9 Mar. 2017), (http://www.globaltimes.cn/content/1036971.shtml).

57 Theresa Hitchens, Cybersecurity: Global Responses to a Global Challenge (21 Mar. 2014), (textlab.io/doc/953515/madrid--21-march-2014).

58 Scott Warren Harold, Martin C. Libicki and Astrid Stuth Cevallos, Getting to Yes With China in Cyberspace (2015), 64 (attributing this view to an unnamed high-level Chinese respondent).

59 United States, Department of State, Statement on Consensus Achieved by the UN Group of Governmental Experts On Cyber Issues (7 June 2013), (www.state.gov/r/pa/prs/ps/2013/06/210418.htm).

60 UN GGE 2013, above n.23.

61 See further Alan Boyle and Christine Chinkin, The Making of International Law (2007), 211–229 (exploring the significance of soft law for international law-making in general); Mačák, above n.43, section 5.1 (examining the consolidation of non-binding norms into binding rules in the legal regimes for Antarctica and nuclear safety, from the perspective of the emerging body of international cyber security law).

62 The UN General Assembly subsequently "[w]elcom[ed]" the GGE report in a unanimously adopted resolution without, however, discussing the details

reconstituted UN GGE adopted a new consensus document, which proposed 11 voluntary, non-binding norms, rules or principles of responsible State behaviour, as well as six views on how international law applies to the use of ICTs by States.[63] The unique role played by the UN GGE as a norm-making process was again confirmed by the acknowledgement it received at the G20 summit in 2015,[64] the G7 summit in 2016,[65] and a number of other international forums. Additionally, a new GGE was established again by the UN Secretary-General in 2016 and is expected to report to the UN General Assembly in 2017.[66]

26. The norms, rules and principles adopted by the UN GGE thus far largely reflect the extent of the current compromise between Western countries and emerging economies, including China. To be sure, China has contributed significantly to the GGE process. This can be seen, *inter alia*, from the GGE's emphasis on sovereignty and other principles enshrined in the UN Charter[67]; and the attention it paid to the unique attributes of cyberspace and the resulting need for developing additional norms beyond

---

of its contents. See GA Res 68/243 (9 Jan. 2014), preambular para.11. In 2014/15, the membership of the GGE expanded to 20 States and subsequently to the current number of 25 participating States.

63 UN GGE 2015, above n.25. Among others, the norms, rules or principles of responsible behaviour of States provide that states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs; states, in ensuring the secure use of ICTs, should guarantee full respect for human rights, including the right to freedom of expression; a state should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure. The 6 views on the application of international law suggest that states have jurisdiction over the ICT infrastructure located within their territory; states may exercise the inherent right to take measures consistent with international law and as recognized in the Charter; states must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts; states must meet their international obligations regarding internationally wrongful acts attributable to them under international law.

64 G20 Leaders' Communiqué at Antalya Summit, see above n.27.

65 G7 Ise-Shima Leaders' Declaration (G7 Ise-Shima Summit, 26–27 May 2016), (www.whitehouse.gov/the-press-office/2016/05/27/g7-ise-shima-leaders-declaration).

66 GA Res 70/237 (30 Dec. 2015), para.5.

67 UN GGE 2013, above n.23, paras.19–20; UN GGE 2015, above n.25, para.25.

existing international law.[68] In the meantime, China's acceptance of norms, rules, and principles advocated by Western countries, including the rules on state responsibility,[69] and the reference to due diligence,[70] also serves as a strong signal that countries with different interests and values can work together to pursue effective cooperation.

27. Ongoing bilateral negotiations transcending the usual East-West divide also suggest that more progress might be made in the future. For instance, in June 2015, the US Secretary of State John Kerry announced that the US and China "agreed that we must work together to complete a code of conduct regarding cyber activities".[71] A few months later, the two countries reportedly held talks to discuss a bilateral cyber arms control treaty.[72] Other Western States have concluded non-binding political agreements on cybersecurity with China since then.[73] These developments may gradually pave the way towards the adoption of legally binding cyber treaties,[74] thus

---

68 UN GGE 2013, above n.23, para.16 ("Given the unique attributes of ICTs, additional norms could be developed over time"); UN GGE 2015, above n.25, para.15.

69 UN GGE 2013, above n.23, para.23 ("States must meet their international obligations regarding internationally wrongful acts attributable to them. States must not use proxies to commit internationally wrongful acts. States should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs."); UN GGE 2015, above n.25, para.13 ("States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs").

70 UN GGE 2015, above n.25, para.28 ("States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts").

71 US, John Kerry, The Strategic & Economic Dialogue / Consultation on People-to-People Exchange: Closing Statements, (24 June 2015), (www.state.gov/secretary/remarks/2015/06/244208.htm).

72 David E. Sanger, U.S. and China Seek Arms Deal for Cyberspace, New York Times, (19 Sept. 2015), (www.nytimes.com/2015/09/20/world/asia/us-and-china-seek-arms-deal-for-cyberspace.html?_r=0).

73 See, e.g., UK, UK-China Joint Statement 2015 (22 Oct. 2015), (www.gov.uk/government/news/uk-china-joint-statement-2015) (agreement not to conduct or support cyber-enabled theft of intellectual property); China, Germany agree deeper cooperation, Xinhuanet (29 Oct. 2015), (news.xinhuanet.com/english/2015-10/29/c_134763586.htm) (agreement to launch bilateral consultations on cyber affairs).

74 Cf. Dinah Shelton, International Law and "Relative Normativity", in: Malcolm D. Evans (ed.), International Law (4th edn., 2014), 162 ("process of negotiating and drafting non-binding instruments can greatly facilitate the

continuing to bring the two camps closer together.[75]

IV. Internet governance and international law

28. A closely connected potential area of divergence concerns the preferred method of Internet governance (also referred to as "cyberspace governance"). While in the previous section we focussed on debates about the need for new norms and their claim to authority under the existing legal frameworks, we now turn to the related question of the preferred frameworks and processes of governance.

29. Historically, the Internet has evolved in a diffuse and decentralized way. Military researchers in the US laid the network's fundaments in the 1960s. Since then it has grown organically as universities, research institutions, and private entities from around the world have gradually joined in. Throughout this period, the governance of the growing network, and matters related to its governance, have evolved in an equally haphazard, organic, and decentralized manner. This is the main reason why today the process of cyberspace governance consists of a technical ecosystem of thousands of "stakeholders" dispersed globally.

30. Originally, the role of States in Internet governance was very limited. As late as 1992, David Clark, a computer science professor at MIT, expressed the ethos of the prevailing government-free governance model in a memorable phrase: "We reject: kings, presidents and voting. We believe in: rough consensus and running code."[76] Nonetheless, States have gradually inched their way into governance. Governments now belong among the relevant "stakeholders", in addition to civil society organizations, semi-public standards organizations, network operators, Internet service providers, individuals, and other actors.

31. Two bodies stand out in this complex web of relationships. The first is the Internet Corporation for Assigned Names and Numbers (ICANN), a private entity based in the US. ICANN manages the global Domain Name System, which is a vast distributed database that translates domain names (such as chinesejil.oxfordjournals.org) to their corresponding IP addresses (such as 209.135.222.209). In this way, the DNS—sometimes referred to as the Internet's phone book—enables the users to communicate

---

achievement of the consensus necessary to produce a binding multilateral agreement").

75 Mačák, above n.43, section 5.3.

76 David D. Clark, A Cloudy Crystal Ball: Visions of the Future (IETF, July 1992), (groups.csail.mit.edu/ana/People/DDC/future_ietf_92.pdf).

and as such is a key component of the functionality of the Internet. ICANN had been under the oversight of the US Department of Commerce for nearly two decades since its establishment in 1998. In June 2016, the US agreed to relinquish control over ICANN and pass it to the global Internet community.[77] The transition officially took place on 1 October 2016,[78] following the rejection by a US federal court of a request for injunction brought by several US states that sought to prolong US oversight.[79]

32. The second key entity is the Internet Governance Forum (IGF), a platform for the representatives of States, private industry, civil society, and intergovernmental organizations to discuss public policy issues relating to the Internet. Although it lacks formal decision-making powers (or even members *stricto sensu*), the IGF allows participating stakeholders to discuss their views on contentious matters and share best practices. Created in 2006 at the UN-sponsored World Summit on the Information Society in Geneva,[80] the IGF retains a close link with the UN.[81] In December 2015, the UN General Assembly acknowledged the role of the IGF as "a multi-stakeholder platform for discussion of Internet governance issues" and decided to extend its mandate for another ten years.[82]

33. This governance model is best described as "multi-stakeholder" due to its inclusion of a plethora of non-State actors alongside governments. In other words, the status quo is "organic, open, yet non-representative".[83] Most Western countries endorse this approach to cyber governance. For example, the US co-ordinator for cyber issues, Christopher Painter, stated in 2013 that

---

77 US, Letter to ICANN Chairman Crocker Transmitting Assessment of IANA Transition Proposal (9 June 2016) (www.ntia.doc.gov/files/ntia/publications/crocker_transmittal_letter_20160609.pdf).

78 ICANN, Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends (1 Oct. 2016), (www.icann.org/news/announcement-2016-10-01-en).

79 US, District Court-Southern District of Texas, State of Arizona et al v. National Telecommunications and Information Administration (NTIA) et al, Civil Action No 3:16-CV-274, Order (3 Oct. 2016), (domainnamewire.com/wp-content/hanks-iana.pdf) (confirming the order made orally on 30 Sept. 2016, which had denied the plaintiffs' motion for a temporary restraining order and a preliminary injunction).

80 GA Res 60/252 (27 Mar. 2006), para.9.

81 See further IGF, About the IGF (undated), (www.intgovforum.org/cms/aboutigf). The IGF formally belongs under the UN Department of Economic and Social Affairs (DESA).

82 GA Res 70/125 (16 Dec. 2015), para.63.

83 Peter W. Singer and Allan Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know (2014), 29.

the US "is committed […] to a multistakeholder model that gives all appropriate stakeholders in the Internet the ability to participate in its evolution". [84] Similarly, clear statements have recently been issued by representatives of various other Western countries, including the United Kingdom,[85] Germany,[86] and Canada,[87] as well as by the European Union.[88]

34. In contrast, China has expressly endorsed the competing "multilateral" conception of cyberspace governance. As Lu Wei, the head of the Cyberspace Administration of China, succinctly put it in 2014, "with regard to the cyberspace governance, the U.S. advocates 'multi-stakeholders' while China believes in 'multilateral'".[89] Domestically, the same goal occupied a prominent place in the new five-year plan for 2016–2020, which called on China to "[p]ush forward the establishment of a *multilateral*, democratic and transparent international Internet governance system".[90]

---

84 US, Statement for the Record by Christopher Painter, Coordinator for Cyber Issues, Cyber Attacks: An Unprecedented Threat to U.S. National Security (21 Mar. 2013), (docs.house.gov/meetings/FA/FA14/20130321/100547/HHRG-113-FA14-Wstate-PainterC-20130321.pdf), 2.

85 UK, Sajid Javid's [then Cultural Secretary] speech at the CyFy 2014 Conference, India (16 Oct. 2014), (www.gov.uk/government/speeches/sajid-javids-speech-at-the-cyfy-2014-conference-india) ("Internet governance should be built on a fully inclusive, multi-stakeholder process.").

86 Federal Republic of Germany, Statement of Dr. Norbert Riedel, Ambassador, Commissioner for International Cyber Policy (22 Oct. 2014), (www.itu.int/en/plenipotentiary/2014/statements/file/Pages/germany.aspx) ("For further developing internet governance, Germany will […] stick to the multi-stakeholder model[.]").

87 Canada, Address by Minister Baird on Importance of Internet Freedom and Governance (25 Nov. 2014), (news.gc.ca/web/article-en.do?nid=909199) ("I like plain speaking, so let's be honest: 'multi-stakeholder Internet governance' is not the snappiest or sexiest phrase. But it's exactly what we need to preserve, if we are going to ensure that the Internet remains innovative, free and open to benefit all users.").

88 EU Cybersecurity Strategy, above n.17, 4 ("The EU reaffirms the importance of all stakeholders in the current Internet governance model and supports this multi-stakeholder governance approach[.]").

89 Lu Wei, Cyber Sovereignty Must Rule Global Internet, World Post (15 Dec. 2014), (www.huffingtonpost.com/lu-wei/china-cyber-sovereignty_b_6324060.html).

90 Goals, missions of China's new five-year plan, Xinhuanet (5 Mar. 2016), (news.xinhuanet.com/english/2016-03/05/c_135158252.htm) (emphasis

35. From the Chinese perspective, the existing multi-stakeholder platforms are "fragmented and divided with limited function and authorization, and confined to specific areas, regions or interests", with the overall framework lacking in "design and coordination".[91] Instead, China prefers the multilateral model, which is top-down, State-centric, and co-ordinated in nature. As it ascribes a decisive role to national governments,[92] the primary forum for this governance model is, quite logically, the UN.[93]

36. It is in the UN context that the moment of greatest discord on matters of cyberspace governance arguably occurred. In 2012, countries led by Russia and China made an important push for the multilateral approach at a conference of the International Telecommunication Union (ITU) in Dubai, in the context of the revision of the International Telecommunication Regulations (ITRs). These States submitted several proposals aimed at the strengthening of the position of governments in Internet governance.[94] Some

---

added); see also International Strategy of Cooperation on Cyberspace. Xinhuanet (1 Mar. 2017), (http://news.xinhuanet.com/english/china/2017-03/01/c_136094371.htm) ("International cyberspace governance should follow a multilateral approach.").

91 Ma Xinmin, above n.44, 400.

92 See Shen Jian, An International Code of Conduct for Information Security: China's Perspective on Building a Peaceful, Secure, Open and Cooperative Cyberspace (Geneva, 10 Feb. 2014), (www.unidir.ch/files/conferences/pdfs/a-cyber-code-of-conduct-the-best-vehicle-for-progress-en-1-963.pdf) ("we should give full play to the leading role of the governments").

93 White Paper on the Internet in China, above n.19, section VI ("China holds that the role of the UN should be given full scope in international Internet administration."); International Strategy of Cooperation on Cyberspace. Xinhuanet (1 Mar. 2017), (http://news.xinhuanet.com/english/china/2017-03/01/c_136094371.htm) ("The United Nations, as an important channel, should play a leading role in coordinating positions of various parties and building international consensus."). See also Jon R. Lindsay and Derek S. Reveron, Conclusion: The Rise of China and the Future of Cybersecurity, in: Jon R. Lindsay, Tai Ming Cheung and Derek S. Reveron (eds.), China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain (2015), 346; Nigel Inkster, above n.14, 147.

94 See, e.g., ITU, WCIT-12, Proposals Received from ITU Member States for the Work of the Conference, Doc DT/1-E (30 Nov. 2012), (www.soumu.go.jp/main_content/000188223.pdf), 98–99 (proposed Article 3A); ITU, WCIT-12, Algeria, Saudi Arabia, Bahrain, China, United Arab Emirates, Russian Federation, Iraq, Sudan: Proposals for the Work of the Conference, Doc 47-E (11 Dec. 2012), (files.wcitleaks.org/public/S12-WCIT12-C-0047!!MSW-E.pdf), 7–8 (endorsing and expanding the Russian

of the language from the proposals was eventually included in a non-binding resolution [95] adopted amidst much controversy on the final day of the conference.[96] Although the ITU Secretary General later emphasised that the revised ITRs did not even mention the Internet,[97] the "negotiating schism" at the conference [98] resulted in the refusal of more than a third of the participating countries (including virtually all Western countries) to sign the amended treaty.[99]

37. Whilst the developments in Dubai cemented China and Russia as allies on matters of cyber governance, it should be noted that the two countries' positions are not identical.[100] It is true that both China and Russia generally support the multilateral model. For instance, they presented a united front at the UN's World Summit on Information Society in 2015, pushing for the inclusion of the term "multilateral" in the event's outcome document.[101] This effort was ultimately successful and the outcome document was modified to include compromise wording to the effect that "the management of the Internet as a global facility includes *multilateral*, transparent, democratic *and multi-stakeholder* processes".[102]

---

proposal).

95 ITU, WCIT-12, Final Acts of the World Conference on International Telecommunications (2012), (www.itu.int/en/wcit-12/documents/final-acts-wcit-12.pdf), 20 (Resolution PLEN/3).

96 See, e.g., Richard Hill, The New International Telecommunication Regulations and the Internet: A Commentary and Legislative History (2014), 60–63.

97 Monika Ermert and Jimm Phillips, 89 Nations Sign Revised ITRs at WCIT, 55 Opposed or "May Sign Later", Communications Daily (17 Dec. 2012), (reporting that the ITU Secretary-General Hamadoun Touré said that "[t]he treaty text does not include the Internet, it does not include content").

98 David Fidler, Internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations, 17(6) ASIL Insights (2013), 1, 2.

99 ITU, WCIT 2012: Signatories of the Final Acts (14 Dec. 2012), (www.itu.int/osg/wcit-12/highlights/signatories.html).

100 But see, e.g., Inkster, above n.14, 10 (describing Russia and China as leaders of the "camp [of] authoritarian states" on matters of cyber security and Internet governance).

101 Dan Levin, At U.N., China Tries to Influence Fight Over Internet Control, The New York Times (16 Dec. 2015), (www.nytimes.com/2015/12/17/technology/china-wins-battle-with-un-over-word-in-internet-control-document.html?_r=2).

102 UN GA, Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of

38. However, China's position is more moderate than that espoused by Russia. This could be seen in the landmark NETmundial meeting held in Brazil in 2014, at the end of which a non-binding *Multistakeholder Statement* was agreed to by participants ranging from governments and industry to civil society and academia.[103] The document stated that "Internet governance should be built on democratic, *multistakeholder* processes".[104] As such, it was repudiated by the Russian representative in an unusual strongly worded statement delivered during the event's closing session.[105] Conversely, China agreed to the document, likely to demonstrate its willingness to reach a compromise solution in view of its long-term goals. These goals may have included the building of a broader coalition of States in order to gradually disrupt the US monopoly over the control of Internet resources and its aforementioned control of ICANN.[106]

39. Therefore, there certainly seems to be space for future convergence between the extreme poles of multi-stakeholderism and multilateralism. As we have seen, even the supposed proponents of these archetypal positions are not doctrinal purists in the sense of rejecting every aspect of the alternative view. In fact, various modalities of combination and/or alignment of the two positions are imaginable. To some extent, they may already be emerging now.

40. Importantly, representatives of both supposed opposing camps have sowed the seeds of convergence. In the same article in which he contrasted China's multilateral model with the US multi-stakeholder approach (discussed above), Lu Wei noted that the "two alternatives are not intrinsically contradictory. […] Without 'multilateral,' there would be no 'multi-stakeholders'."[107] In a similar vein, Ma Xinmin, a senior Chinese diplomat and international lawyer, recently proposed "the option of establishing a special

---

the World Summit on the Information Society, UN Doc A/70/L.33 (13 Dec. 2015), para. 57 (emphases added).

103 NETmundial, NETmundial Multistakeholder Statement (24 Apr. 2014), (netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf).

104 Ibid., 6 (emphasis added).

105 NETmundial, NETmundial Closing Session (24 Apr. 2014), (netmundial.br/wp-content/uploads/2014/04/NETMundial-23April2014-Closing-Session-en.pdf), 21–22.

106 Cf. Zhong Sheng, Norms and Standards are Key in Internet Governance, Renmin Ribao [People's Daily] (28 Apr. 2014), (opinion.people.com.cn/n/2014/0428/c1003-24947988.html) (describing the transition of ICANN's functions as a "positive signal for global Internet governance").

107 Lu Wei, Cyber Sovereignty Must Rule Global Internet, World Post (15 Dec. 2014), (www.huffingtonpost.com/lu-wei/china-cyber-sovereignty_b_6324060.html).

committee on Internet governance under the UN General Assembly, which will take into account interests of multi-stakeholders […] so as to build a harmonious, rule-based order for cyberspace".[108]

41. US representatives have also recently made conciliatory remarks. For instance, Julie Zoller, the US State Department official responsible for communications and information policy relative to multilateral organizations, publicly extolled the IGF's potential to bring the two camps together:

> The connection to the United Nations provides the IGF legitimacy in the eyes of many participants from the developing world, and the multistakeholder nature of the IGF gives it the expertise and vibrancy to address the critical issues of the day.[109]

42. Additionally, the UN GGE appears to be taking "interests of multi-stakeholders" into account. It is true that neither of its consensus documents, adopted in 2013 and 2015 respectively, made direct reference to the term "multi-stakeholders". Yet, on a number of occasions, the role of the private sector and civil society organizations was cited. For example, the 2015 document emphasized that:

> While States have a primary responsibility for maintaining a secure and peaceful ICT environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organizations.[110]

43. What these statements share is a willingness to bring the seemingly irreconcilable positions together. Rather than forcing a choice between the two options,[111] which seems exceedingly unlikely to be accepted by the key players, it may be more productive to allow the different understandings to coexist and continue the dialogue between the parties in order to enable the

---

108 Ma Xinmin, above n.44, 400.

109 US, Julie Zoller, Advancing the Multistakeholder Approach in the Multilateral Context (16 July 2015), (www.state.gov/e/eb/rls/rm/2015/245157.htm).

110 UN GGE 2015, above n.25, para. 31.

111 Cf. Alexander Klimburg, The Internet Yalta (5 Feb. 2013), (www.cnas.org/publications/reports/the-internet-yalta), 7 ("The only hope for liberal democracies may well be to go on the offensive: Rather than allow the multistakeholder approach to be increasingly squeezed into the field of Internet governance alone, the principle should be extended to other fields and not only limited to cyberspace.").

gradual creation of global governance of cyberspace.[112]

V. Sovereignty in cyberspace

44. Long before the emergence of the Internet, sovereignty had been firmly established as a fundamental principle of international law, one that, in the words of James Crawford, constitutes "the standard operating assumption of a decentralized international system".[113] However, in the virtual world of cyberspace, the notion of sovereignty is controversial, for it may be questioned whether and to what degree sovereignty exists in this borderless, interconnected domain.[114] Although the general applicability of sovereignty in cyberspace has by now become part of the international consensus described above,[115] China and Western countries nevertheless take divergent views regarding its nature in the cyberspace context.

45. China is one of the first countries that actively advocated the concept of "cyber sovereignty".[116] As an illustration, consider the Chinese reaction to Google's decision to withdraw from China in early 2010 due to its dissatisfaction with China's Internet regulatory measures.[117] In response, the Chinese government argued that "the Internet is an important infrastructure facility for the nation. Within Chinese territory, the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China should be respected and protected".[118] Similarly, the *International Code of Conduct on Information Security* proposed by China, Russia and other members of the SCO in September 2011 stated that "policy authority for Internet-related public issues is the sovereign right of States, which have rights and responsibilities

---

112 See also Paul Cornish, Governing Cyberspace through Constructive Ambiguity, 57(3) Survival (2015), 153, 173 (arguing that the application of the classical Westphalian conception of sovereignty allows for different understandings of cyber governance to coexist rather than conflict with one another).

113 See James Crawford, Sovereignty as a Legal Value, in: James Crawford and Martti Koskenniemi (eds.), The Cambridge Companion to International Law (2012), 132.

114 See e.g. Barlow, above n.33 (claiming that governments of the industrial world "have no sovereignty where we gather").

115 See paras.11 and 25 above.

116 In the Chinese context, "cyber sovereignty" is often used interchangeably with "Internet sovereignty".

117 Google, A New Approach to China (www.google.com/press/new-approach-to-china).

118 White Paper on the Internet in China, above n.19.

for international Internet-related public policy issues".[119] Following the proposal, China continued to promote the idea of "cyber sovereignty".[120] This effort culminated in the keynote speech delivered by President Xi Jinping at the World Internet Conference in 2015, in which he stressed the importance of respecting Internet sovereignty as one of the principles that should be adhered to in order to promote global Internet governance system reform. According to the president of China,

> [w]e should respect the right of each and every country to independently choose its internet development path, internet management system, internet public policy and to equally participate in governance of international cyberspace. We shall not seek internet hegemony, not interfere in other's internal affairs, and not participate in or provide any form of support or even encouragement for any internet activities that will undermine other's national security.[121]

46. The importance placed by China on cyber sovereignty can be explained by two separate but related factors. On the one hand, China relies heavily on Internet censorship, and in particular its "great firewall", to block and filter online information which it considers harmful to social stability and national security. As in the case of Google's withdrawal from China in 2010, when faced with accusation by Western countries that such policies constitute a threat to Internet freedom,[122] China justifies them on the basis of cyber

---

119 Code of Conduct 2011, above n.47.

120 For example, in his remarks at the Seoul Conference on Cyberspace held in Seoul on 17 Oct. 2013, Dr. Huang Huikang, Legal Adviser of the Ministry of Foreign Affairs of the People's Republic of China, argued that cyber sovereignty is the natural extension of state sovereignty into cyberspace and should be respected and upheld; every country is entitled to formulate its policies and laws in light of its history, traditions, culture, language and customs, and manage the Internet accordingly. Huang Huikang, Working Together to Build a Harmonious and Progressive International Cyberspace Order (www.fmprc.gov.cn/ce/cgmb/chn/wjbxw/P020131021538048406901.doc). See also International Strategy of Cooperation on Cyberspace. Xinhuanet (1 Mar. 2017), (http://news.xinhuanet.com/english/china/2017-03/01/c_136094371.htm) ("As a basic norm in contemporary international relations, the principle of sovereignty enshrined in the UN Charter covers all aspects of state-to-state relations, which also includes cyberspace.").

121 Keynote speech delivered by President Xi Jinping at World Internet Conference (28 Dec. 2015), (en.chinaapw.com/newsitem/277219397).

122 Hillary Rodham Clinton, Remarks on Internet Freedom

sovereignty. For instance, a semi-official piece in the Chinese media observed that Western countries resort to similar practices to "censor" Internet content.[123] In this connection, the proposal of a "Great British Firewall" by the UK surveillance agency GCHQ in September 2016 will likely only strengthen such *tu quoque* arguments.[124]

47. On the other hand, in view of the technical advantages and capacities of major Western countries like the US, China increasingly resorts to cyber sovereignty as a protection from perceived threats. This is so especially after the Snowden revelations in 2013, in the context of which it was reported that the US National Security Agency (NSA) had monitored the communications of top Chinese leaders for years.[125] Thus, in a speech delivered at the National Congress of Brazil in 2014, President Xi Jinping stressed that "[n]o matter how developed a country's Internet technology is, it just cannot violate the information sovereignty of other countries".[126] He described a scenario in which some countries enjoy a secure Internet, while others do not, as unacceptable. He added that a State cannot pursue its own Internet security at the price of threatening the security of other countries: "there are no double standards in the information sector and every country has the right to preserve its own information security".[127]

48. However, the gap between Chinese and Western understandings of cyber sovereignty may be narrower than it would appear at first glance. It is true that seemingly radical views, including those calling for the establishment

---

(www.state.gov/secretary/rm/2010/01/135519.htm); Hillary Rodham Clinton, Internet Rights and Wrongs: Choices & Challenges in a Networked World (www.state.gov/secretary/rm/2011/02/156619.htm).

123 See, e.g., Xinhua, China Voice: Don't be prejudiced against China's Internet regulation (5 Feb. 2015), (news.xinhuanet.com/english/china/2015-02/05/c_133972903.htm) ("Internet content is censored not only in China, but also in other countries including the United States. Although freedom of speech is strictly protected by the First Amendment, the United States has enacted federal laws to provide exceptions to free speech.").

124 Ewen MacAskill, GCHQ's "Great British Firewall" raises serious concern – privacy groups, The Guardian (14 Sept. 2016), (www.theguardian.com/uk-news/2016/sep/14/gchqs-great-british-firewall-raises-serious-concern-privacy-groups).

125 See, e.g., NSA Spied on Chinese Government and Networking Firm, Der Spiegel (22 Mar. 2014), (www.spiegel.de/international/world/nsa-spied-on-chinese-government-and-networking-firm-huawei-a-960199.html).

126 Xi Jinping, Carry Forward Traditional Friendship and Jointly Open up New Chapter of Cooperation (http://gb.cri.cn/other/chinanews/eng140901.pdf).

127 Wu Jiao and Zhao Shengnan, Xi: Respect cyber sovereignty, China Daily USA (usa.chinadaily.com.cn/epaper/2014-07/17/content_17818027.htm).

of "Internet borders" and the emergence of a "territorial cyberspace", may be found, especially in opinion pieces published in the Chinese state-run media.[128] Yet, the official proclamations referred to above do not appear to be irreconcilable with the views of Western countries. After all, governments have always tried to maintain at least some degree of control over information disseminated in their territories.

49. In this connection, it should be noted that already the 1865 International Telegraph Convention contained a clause that States "reserved the right to stop any transmission that they considered dangerous for state security, or in violation of national laws, public order or morals".[129] Thus, it is hardly surprising that the UN GGE's 2013 consensus report confirmed that "State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory".[130] The *Tallinn Manual on International Law Applicable to Cyber Warfare*,[131] prepared by a group of experts from Western countries in 2013,[132] also acknowledges in its very

128 For example, a China Youth Daily editorial called for the establishment of "Internet border" in China. See Ye Zheng & Zhao Baoxian, How to fight cyberwarfare?, Zhongguo Qingnian Bao [China Youth Daily] (2011), (zqb.cyol.com/html/2011-06/03/nw.D110000zgqnb_20110603_1-09.htm) (arguing that China needs to "express to the world its principled stance of maintaining an 'Internet border' and protecting its 'Internet sovereignty,' unite all advanced forces to dive into the raging torrent of the age of peaceful use of the Internet, and return to the Internet world a healthy, orderly environment"). Some scholars also proposed the idea of "territorial cyberspace". See Fang Binxing, It's Time to Pay Attention to Cyber Sovereignty, Renmin Zhengxie Bao [Chinese People's Political Consultative Conference Daily] (2016), (epaper.rmzxb.com.cn/detail.aspx?id=381711) (arguing that cyber sovereignty should be exercised in a country's "territorial cyberspace" within its "Internet border").

129 Convention télégraphique internationale de Paris [International Telegraph Convention of Paris] 1865, art. 19 ("Les Hautes Parties contractantes se réservent la faculté d'arrêter la transmission de toute dépêche privée qui paraîtrait dangereuse pour la sécurité de l'Etat, ou qui serait contraire aux lois du pays, à l'ordre public ou aux bonnes mœurs, à charge d'en avertir immédiatement l'expéditeur.").

130 UN GGE 2013, above n.23, para.20; see also UN GGE 2015, above n.25, para.27.

131 Michael N. Schmitt (ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare (2013).

132 In 2017, the Manual was thoroughly revised, extended to cover aspects of peacetime international law, and published as Michael N. Schmitt (ed.),

first rule that "[a] State may exercise control over cyber infrastructure and activities within its sovereign territory".[133] Finally, in a recently issued strategic document, "Joint Operating Environment 2035",[134] the United States designated the protection of "its sovereign cyberspace" as a long-term goal for its military.[135]

50. Accordingly, it can be argued that the issue of the application of sovereignty in cyberspace has now been settled, although China and Western countries still have rather different understandings about its precise meaning and parameters.[136] Western counties, especially the US, have described the Chinese emphasis on cyber sovereignty as a threat to Internet freedom that could lead to the division of global Internet. In the 2011 *International Strategy for Cyberspace*, the US asserted that free speech and association, privacy, and the free flow of information are core principles that should be preserved when confronting online challenges.[137] For instance, although favoring certain "dynamic and adaptable" cybersecurity solutions that "secure systems without crippling innovation, suppressing freedom of expression or association, or impeding global interoperability", the document noted that "other approaches—such as national-level filters and firewalls—[provide] only an illusion of security while hampering the effectiveness and growth of the Internet as an open, interoperable, secure, and reliable medium of exchange".[138] The EU appears to share this view.[139] For these Western

---

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2017). The first and the second author of this article acted in the Tallinn 2.0 process respectively as a member of the international group of experts and a peer reviewer.

133 Tallinn Manual, above n.131, 15. See also Tallinn Manual 2.0, above n.132, 11 (declaring in Rule 1 expressly that "[t]he principle of State sovereignty applies in cyberspace"). The revised Manual dedicates its first five rules to issues of State sovereignty: ibid., 11–29.

134 US, Joint Operating Environment 2035 (14 July 2016), (www.dtic.mil/doctrine/concepts/joe/joe_2035_july16.pdf).

135 Ibid., 33 ("In 2035, the United States will need to defend its sovereign cyberspace, protect the use of non-sovereign cyber commons, and control key parts of cyberspace (both sovereign and nonsovereign).").

136 For a representative view of "cyber sovereignty" among Western scholars, see, e.g., Eric T. Jensen, Cyber Sovereignty: The Way Ahead, 50 Texas ILJ (2015), 275–304.

137 US International Strategy, above n.16, 5.

138 Ibid.

139 EU Cybersecurity Strategy, above n.17, 2 (claiming that "[a]n open and free cyberspace has promoted political and social inclusion worldwide; it has broken down barriers between countries, communities and citizens,

countries, China's advocacy of cyber sovereignty, particularly its attempts to strengthen online content control, constitutes a threat to the openness and freedom of cyberspace.[140]

51. In short, with the "return of States"[141] in cyberspace comes the "return of sovereignty". Sovereignty will play an increasingly prominent role in the debate over the future international order in cyberspace. In the meantime, and although they have accepted the application of sovereignty in cyberspace, China and Western countries will continue to express different views as to the meaning of sovereignty, and how it should be applied in cyberspace.

VI. International law and the militarization of cyberspace

52. There is no doubt that in addition to its many social and economic benefits, the the cyber domain has also resulted in unprecedented vulnerabilities. Today, cyber attacks may threaten States' critical infrastructure,[142] compromise and disrupt financial flows,[143] and even interfere with the provision of medical services.[144] Malicious cyber operations may thus

---

allowing interaction and sharing of information and ideas across the globe; it has provided a forum for freedom of expression and exercise of fundamental rights, and empowered people in their quest for democratic and more just societies").

140 See, e.g., Egan, above n.32, 15 (criticizing "some States" for "invok[ing] the concept of State sovereignty as a justification for excessive regulation of online content, including censorship and access restrictions [… and] in an attempt to shield themselves from outside criticism").

141 Ralf Bendrath, The Return of the State in Cyberspace: the Hybrid Regulation of Global Data Protection, in: Myriam Dunn, Sai Felicia Krishna-Hensel and Victor Mauer (eds.), Resurgence of the State: Trends and Processes in Cyberspace Governance (2007), 111.

142 See, e.g., Daniel Wagner and Bailey Schweitzer, The Growing Threat of Cyber-Attacks on Critical Infrastructure, Huffington Post (24 May 2016), (www.huffingtonpost.com/daniel-wagner/the-growing-threat-of-cyb_b_10114374.html).

143 See, e.g., Michael Corkery, Once Again, Thieves Enter Swift Financial Network and Steal, The New York Times (12 May 2016), (www.nytimes.com/2016/05/13/business/dealbook/swift-global-bank-network-attack.html).

144 See, e.g., Kim Zetter, Hacker Can Send Fatal Dose to Hospital Drug Pumps, Wired (6 Aug. 2015), (www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps).

wreak considerable havoc on entire communities or even States and have rightly become the source of concern for top-level policymakers in every country.

53. The fourth area of apparent divergence relates to the paradigm within which such cyber threats should be seen and analysed. Perhaps on account of their national security implications, the first significant responses to these threats from Western States and scholars were firmly based on a military paradigm. This was strongly opposed by others, including prominent Chinese State representatives as well as academics. But, as discussed below, there are positive signs that suggest this divergence is not irreversible.

54. To begin with, perhaps the first comprehensive public pronouncement by a State on the framework of responding to malicious cyber operations was issued by the US in its 2011 *International Strategy for Cyberspace*:[145]

> When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests.[146]

55. This was soon complemented by the US State Department Legal Advisor Harold Koh's detailed speech entitled "International Law in Cyberspace".[147] In it, Koh reiterated the US view that a State may respond in self-defence to "computer network activities that amount to an armed attack or imminent threat thereof".[148] Additionally, he discussed how various law of armed conflict (LOAC) rules and principles would apply to inter-State cyber operations.[149] Strikingly, with the exception of a very minor digression into the law of human rights,[150] the text's substantive focus was solely on the law on the use of force (*jus ad bellum*) and LOAC (*jus in bello*).[151]

---

145 US International Strategy, above n.16.

146 Ibid., 14**.**

147 Koh, above n.43.

148 Ibid. 4.

149 Ibid. 4–8.

150 Ibid. 9–10.

151 Ibid. (passim). Even though, as will be argued below, the US approach has developed and become more nuanced since 2012, it is worth noting that the

56. Western scholarly discussion of the international law dimension of cybersecurity had by that time also treated this domain through the military prism. Most of the relevant publications considered whether and under what circumstances cyber attacks could be seen as amounting to an armed attack triggering the States' right to resort to self defence[152] and examined the related question of LOAC's applicability to cyber operations.[153] This trend of associating cyber security with cyber warfare culminated with the publication of the highly influential *Tallinn Manual on International Law Applicable to Cyber Warfare* in 2013.[154]

57. The Manual was an effort to identify rules of customary international law applicable to cyber warfare undertaken by an international group of experts led by Professor Michael Schmitt. As apparent from its title, the Manual was firmly based on the military paradigm and focussed almost exclusively on the *jus ad bellum* and the *jus in bello*. Apart from nine general rules added in the final stages of the project (rules 1–9), the remaining 86 rules related solely to activities occurring at or above the level of the use of

---

armed conflict perspective remains dominant in the US legal thinking about this area. Hence, when Koh's successor Brian Egan delivered a similar speech on the relationship between international law and cyber activities in Nov. 2016, he similarly treated the issue of cyber operations in the context of armed conflict as the starting point of his analysis. See Egan, above n.32, 8–10.

152 See, e.g., Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, 37(3) Columbia JTL (1999), 914; Yoram Dinstein, Computer Network Attacks and Self-Defense, 76 International Law Studies (1999), 99; Horace B. Robertson, Self-Defense against Computer Network Attack under International Law, 76 International Law Studies (1999), 121; Eric Jensen, Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense, 38 Stanford JIL (2002), 207.

153 See, e.g., Louise Doswald-Beck, Some Thoughts on Computer Network Attack and the International Law of Armed Conflict, 76 International Law Studies (2002), 172; Michael N. Schmitt, Wired Warfare: Computer Network Attack and Jus in Bello, 84 International Review of the Red Cross (2002), 396; Cordula Droege, Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians, 94 International Review of the Red Cross (2012), 533; Heather Harrison Dinniss, Cyber Warfare and the Laws of War (2012).

154 Tallinn Manual, above n.131; see also ibid., 13 (stating that "international cyber security law" as understood by the Manual includes aspects of the *jus ad bellum* as well as general international law concepts related to the operation of the *jus ad bellum* and the *jus in bello*).

force (rules 10–95). Although the experts were acting in their personal capacity, the Manual project was sponsored by a centre of excellence established in Tallinn by NATO, a military alliance.[155]

58. This predominantly Western approach was met with fierce criticism from Chinese press, officials, and academics. The US declaration that it will respond to hostile acts in cyberspace as to national security threats[156] was described as amounting to an unwarranted militarization of cyberspace.[157] Similarly, an early Chinese reaction to the Tallinn Manual accused it of "obviously want[ing] to put a cloak of legality on US cyber warfare".[158] A particularly significant characterization of the Manual was offered by Ma Xinmin, a senior Chinese diplomat and international lawyer. In his view, the Manual reflected the view of "[s]ome States" that cyber attacks should be analysed through the prism of the military paradigm.[159] He continued in a highly critical vein: "Yet this 'military paradigm' of response to cyberattacks disregards the principle of non-use of force in international law and over-emphasizes such exceptions as the right to self-defense, *thus aggravating cyberspace militarization and arms race*."[160]

59. In public statements, Chinese officials have repeatedly condemned the purported militarization of cyberspace undertaken by the US and other Western States.[161] They have insisted that any development of China's military capabilities is only a defensive response to the efforts of other countries to militarize cyberspace with their offensive capabilities.[162] The credibility of such assertions has been questioned by Western analysists. For instance, Michael Swaine noted that the distinction between offensive and defensive systems is often very difficult to make as "in most cases, 'offensive' capabilities are developed as an effective and necessary means of defense and deterrence".[163]

---

155 Ibid., 1–11.

156 US International Strategy, above n.16, 9.

157 LU Desheng, US Military Look for New Excuse to use Force Abroad: Pentagon to Announce First Cyber Strategy, PLA Daily (8 June 2011).

158 Zhong Sheng, Blackening China Can Hardly Conceal the Evil Behavior of the "Hackers" Empire, People's Daily (8 May 2013).

159 Ma Xinmin, above n.44, 402.

160 Ibid., (emphasis added).

161 Nigel Inkster, above n.14, 98.

162 Kimberly Hsu and Craig Murray, China and International Law in Cyberspace (6 May 2014), (origin.www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf), 1–2.

163 Michael D. Swaine, Chinese Views on Cybersecurity in Foreign Relations, 42 China Leadership Monitor (2013), 1, 14–15.

60. Be that as it may, the fact remains that most cyber operations to date do not clear the threshold of the use of armed force between States. This observation holds even for the most prominent inter-State cyber incidents. The series of cyber attacks against Estonia in 2007 caused very little damage in the physical world and despite some initial statements to the contrary,[164] even the Estonian government had to eventually admit that it did not have sufficient evidence to link the attacks to another State.[165] Similarly, although the cyber operations against Georgia in 2008 occurred in the context of an international armed conflict with Russia, their effect was limited, making the application of LOAC to them "highly problematic".[166] Even the (in)famous Stuxnet virus, which reportedly destroyed about 20% of Iran's nuclear centrifuges,[167] left scholars divided with respect to its legal qualification.[168]

---

164 Eesti Päevaleht, Statement by the Foreign Minister Urmas Paet (1 May 2007), (epl.delfi.ee/news/eesti/statement-by-the-foreign-minister-urmas-paet?id=51085399) ("The European Union is under attack, because *Russia is attacking Estonia*.") (emphasis added).

165 Estonia Says Cyber-Assault May Involve the Kremlin, The New York Times (17 May 2007), (nyti.ms/1M7k8eD); see also "Estonia Has No Evidence of Kremlin Involvement in Cyber Attacks" RIA Novosti (6 Sept. 2007), (sptnkne.ws/2QP).

166 Eneken Tikk, Kadri Kaska and Liis Vihul, International Cyber Incidents: Legal Considerations (2010), 90 ("it is highly problematic to apply Law of Armed Conflict to the Georgian cyber attacks—the objective evidence of the case is too vague to meet the necessary criteria of both state involvement and gravity of effect.").

167 Michael B. Kelley, The Stuxnet Attack on Iran's Nuclear Plant Was "Far More Dangerous" Than Previously Thought, Business Insider (20 Nov. 2013), (www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11).

168 See, e.g., Tallinn Manual, above n.131, 45 (concluding that Stuxnet amounted to a use of force), 58 (noting disagreement among the experts whether it amounted to an armed attack); Tallinn Manual 2.0, above n.132, 342 (noting that all experts considered Stuxnet as amounting to a use of force, but that only some of them took the view that it had also reached the armed attack threshold); Andrew Moore, Stuxnet and Article 2(4)'s Prohibition Against the Use of Force: Customary Law and Potential Models, 64 Naval LR (2015), 1, 26–27 (arguing that Stuxnet amounted to a use of force and possibly to an armed attack); but see, e.g., Mary Ellen O'Connell, Cyber Security without Cyber War, 17 Journal of Conflict and Security Law (2012), 187, 202 ("The Stuxnet attack while unlawful was not the equivalent of an Article 51 armed attack."); Marco Roscini, Cyber Operations and the Use of Force in International Law (2014), 76 (doubting

Significantly, the victim State never qualified it as an armed attack or even a use of force.[169]

61. Therefore, most (if not all) malicious cyber operations must be assessed through the lens of peacetime international law. That being so, some of the Chinese criticism seems on point, in particular insofar as it was directed at statements by Western States and academics that were based on the military paradigm. However, there are a number of indications that the contrast between the two positions is not as stark as it might appear.

62. Firstly, the focus on the military paradigm has received a fair dose of criticism from some Western scholars, as well. Already in 2012, Mary Ellen O'Connell excoriated advocates of the positions described above for being "trapped by an ideology of militarism" and argued for a de-militarization of legal approaches to cyber security.[170] Robin Geiss and Henning Lahmann also argued that we need to look beyond the military paradigm to identify feasible solutions to the problem of cyber security. [171] On their analysis, countermeasures and the state of necessity provide more viable international law alternatives of responding to cyber incidents.[172]

63. Secondly, there is evidence that the tide may be turning even among those who might once have been seen as proponents of the supposed military paradigm. Professor Schmitt, the chairman of the Tallinn Manual project, has since acknowledged that "preoccupation with cyber armed attacks is counter-

---

that "Stuxnet had scale and effects significant enough to qualify as an armed attack"); contrast further with, e.g., David Fidler, Was Stuxnet an Act of War? Decoding a Cyberattack, 9(4) IEEE Security & Privacy (2011), 56, 59 (arguing that as "covert cyberaction", Stuxnet "didn't cross the threshold into a use of force"); Katharina Ziolkowski, Stuxnet: Legal Considerations, 25 Journal of International Law of Peace and Armed Conflict (2012), 139, 147 (suggesting that as a "legal masterpiece", this operation did not breach any rules of international law).

169 See Iran, Statement by H.E. Dr. Ali Akbar Salehi Minister of Foreign Affairs of the Islamic Republic of Iran (28 Sept. 2012), (iran-un.org/en/2012/09/28/28-september-2012-2) (describing cyber attacks against Iran's nuclear facilities as "a manifestation of nuclear terrorism and consequently a grave violation of the principles of UN Charter and international law" but stopping short from using the language of the *jus ad bellum*).

170 O'Connell, above n.168, 191.

171 Robin Geiss and Henning Lahmann, Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention, in: Katharina Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy (2013), 621.

172 Ibid., 628–652.

experiential".[173] Moreover, the recently published second edition of the Manual (Tallinn Manual 2.0), treats "below-the-threshold" cyber operations by addressing many areas of peacetime international law, including State responsibility, the law of the sea, international telecommunications law, diplomatic law, and even human rights law.[174] This strengthens the project's overall relevance and serves to dispel some of the criticism cited above.[175]

64. Thirdly, States seem to be coming closer to one another with respect to this issue. On the one hand, China has started to move away from its pointed language denouncing the alleged militarization of cyberspace. Indeed, in its most recent Defence White Paper, China expressly recognized that cyberspace had become "a new domain of national security" and committed itself to the expedited development of its cyber military capabilities.[176] On the other hand, Western States have come to accept that the military prism is too limited to effectively meet the diverse challenges posed by cyberspace. For instance, a recent statement by the US Director of National Intelligence indicates a move away from fanciful concerns about cyber warfare to more realistic considerations of cyber security:

> Rather than a "Cyber Armageddon" scenario that debilitates the entire US infrastructure, we envision something different. We foresee an ongoing series of low-to-moderate level cyber attacks from a variety of

---

173 Michael N. Schmitt, "Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law, 54(3) Virginia JIL (2014), 697, 698.

174 See Tallinn Manual, above n.131.

175 It deserves mentioning that compared with the Tallinn Manual in 2013, the Tallinn 2.0 process has been more internationalized and inclusive. Besides the inclusion of representatives of more than 50 governments from different part of the world, including China, in the two governmental consultative meetings held in the Hague in 2014 and 2015, the composition of the Tallinn 2.0 International Group of Experts has also, for the first time, included three non-Western experts (from Thailand, Belarus and China respectively), which allowed the voices and perspectives of the non-Western world to be reflected in the process. See further Tallinn Manual 2.0, above n.132, 2–6.

176 Xinhua, full text: China's Military Strategy (26 May 2015), (www.chinadaily.com.cn/china/2015-05/26/content_20820628.htm); see also International Strategy of Cooperation on Cyberspace. Xinhuanet (1 Mar. 2017), (http://news.xinhuanet.com/english/china/2017-03/01/c_136094371.htm) ("China will give play to the important role of the military in safeguarding the country's sovereignty, security and development interests in cyberspace.").

sources over time, which will impose cumulative costs on US economic competitiveness and national security.[177]

65. Crucially in this regard, representatives of over 50 States met in early 2016 in the context of the so-called Hague Process sponsored by the Dutch Ministry of Foreign Affairs to discuss the draft text of the second edition of the Tallinn Manual.[178] Participating States notably included both the United States and China, as well as a host of other key cyber powers.[179] Although the content of the consultations remains confidential,[180] the fact of such broad participation suggests that the Manual (at least its updated version) is no longer viewed as the product solely of the disparaged military paradigm.

66. In sum, despite some strongly worded statements on both sides, the concern that the divide between them is impassable and therefore fosters the militarization of cyberspace appears exaggerated. It would be unreasonable to expect any major world power to refrain altogether from developing military capabilities in the cyber domain. Yet, the vast majority of cyber operations—whether State-sponsored or conducted exclusively by non-State actors—have not and will not exceed the threshold of the use of force as understood under international law. Most States now recognize, albeit to different degrees, that it is unhelpful to rely on the military paradigm as the first port of call when analysing inter-State malicious cyber operations.

VII. Cyber espionage and international law

67. Espionage is sometimes described as "the second oldest profession" in

177 US, James R. Clapper, Statement for the Record: Worldwide Cyber Threats (10 Sept. 2015), (docs.house.gov/meetings/IG/IG00/20150910/103797/HHRG-114-IG00-Wstate-ClapperJ-20150910.PDF).

178 NATO CCD COE, Over 50 States Consult Tallinn Manual 2.0 (2 Feb. 2016), (ccdcoe.org/over-50-states-consult-tallinn-manual-20.html).

179 China's attitude towards Tallinn 2.0 can be partly explained by its active participation in the two governmental consultative meetings held in the Hague in 2014 and 2015. According to private conversations between one of the present authors and an official from the Chinese Ministry of Foreign Affairs, the Chinese government was invited to attend both meetings, and based on careful preparation, it made numerous comments on various topics in the Tallinn 2.0 process.

180 NATO CCD COE, Experts: Multiple International Law Regimes Apply to Cyber Operations (11 Feb. 2016), (ccdcoe.org/experts-multiple-international-law-regimes-apply-cyber-operations.html).

human history.[181] Before the emergence of cyber espionage, the legality of espionage as such was the subject of some debate among international legal scholars. The majority position is that with the exception of certain limited rules, such as those concerning espionage during an international armed conflict,[182] espionage is largely left unregulated by international law and as such it is not internationally unlawful.[183] Albeit criminalized in the domestic law of nearly every country, as far as the international law is concerned, espionage has long been part and parcel of lawful inter-State relations.

68. Following the end of the Cold War, in the West there was a noticeable shift of concern about espionage from that which is political and military in nature to economic espionage, especially when carried out by cyber means. For instance, the 2011 *International Strategy for Cyberspace* noted:

> The persistent theft of intellectual property, whether by criminals, foreign firms, or state actors working on their behalf, can erode competitiveness in the global economy, and businesses' opportunities to innovate. The United States will take measures to identify and respond to such actions to help build an international environment that recognizes such acts as unlawful and impermissible, and hold such actors accountable.[184]

69. General Keith Alexander, then director of the US NSA and commander of the US Cyber Command, echoed this concern the following year when he claimed that the loss of industrial information and intellectual property through cyber espionage constituted the "greatest transfer of wealth in history," and that US companies were losing about $250 billion per year through intellectual property theft, with another $114 billion lost due to cyber crime.[185]

---

181 Simon Chesterman, The Spy Who Came from the Cold War: Intelligence and International Law, 27 Michigan JIL (2005-2006), 1072.

182 See, in particular, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Art. 46. For discussion of espionage under the law of armed conflict, see further Christian Schaller, Spies, in: Rüdiger Wolfrum (ed.), The Max Planck Encyclopedia of Public International Law (2008), online edition (www.mpepil.com), paras.6–12.

183 See e.g. Christopher Baker, Tolerance of International Espionage: A Functional Approach, 19 American University ILR (2003-2004), 1094–1095.

184 US International Strategy, above n.16, 18.

185 Josh Rogin, NSA Chief: Cybercrime Constitutes the "Greatest Transfer of Wealth in History" (thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history).

70. Moreover, the US has accused China of being "the most threatening actor in cyberspace",[186] and it was claimed that "[t]he easiest way to innovate is to plagiarize" by stealing US intellectual property.[187] It is against this background that in May 2014, the US indicted five officers of the Chinese People's Liberation Army[188] for "serious cybersecurity breaches against six American victim entities", which represented "the first ever charges against known state actors for infiltrating U.S. commercial targets by cyber means".[189]

71. Meanwhile, after the Snowden revelations in 2013, the cyber espionage activities carried out by the United States and some of its Western allies—the so-called "Five Eyes" alliance comprising additionally Australia, Canada, New Zealand and the United Kingdom—also attracted worldwide attention. The documents released by Snowden revealed that these countries had been engaged in a global surveillance programme to collect confidential information stored in or transmitted through cyberspace. As mentioned earlier, the NSA had reportedly monitored the communications of top Chinese leaders for years.[190] Interestingly, some NSA documents that were leaked seem to suggest that—despite public assurances to the contrary[191]—the US and its allies had also engaged in *economic* espionage against targets in

---

186 Bloomberg 2012 (www.bloomberg.com/news/articles/2012-11-05/china-most-threatening-cyberspace-force-u-s-panel-says).

187 Brian Grow & Mark Hosenball, In Cyberspy vs. Cyberspy, China Has the Edge, (www.huffingtonpost.com/2011/04/14/china-us-cyberspy_n_849016.html) (citing James Lewis).

188 US, District Court-Western District of Pennsylvania, United States of America v. Wang Dong et al., Indictment, Criminal No. 14-118 (1 May 2014), (www.justice.gov/iso/opa/resources/512201451913235846 1949.pdf).

189 US Department of Justice, Attorney General Eric Holder Speaks at the Press Conference Announcing U.S. Charges Against Five Chinese Military Hackers for Cyber Espionage (19 May 2014), (www.justice.gov/iso/opa/ag/speeches/2014/ag-speech-140519.html).

190 See, e.g., NSA Spied on Chinese Government and Networking Firm, Der Spiegel (22 Mar. 2014), (www.spiegel.de/international/world/nsa-spied-on-chinese-government-and-networking-firm-huawei-a-960199.html).

191 See, e.g., Barton Gellman and Ellen Nakashima, "U.S. Spy Agencies Mounted 231 Offensive Cyber Operations in 2011, Documents Show," Washington Post (30 Aug. 2013) (www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html) (reporting a statement from the US Department of Defense, according to which "[t]he department does ***not*** engage in economic espionage in any domain, including cyber.") (emphasis original).

Brazil, Venezuela, Mexico, Russia, and elsewhere.[192]

72. While countries may well criminalize foreign cyber espionage activities through domestic law, the enforcement of national criminal laws against perpetrators located in foreign jurisdictions is likely to be extremely difficult, which renders the protection against transboundary cyber espionage to ultimately rest with international law.[193] Against this backdrop, countries tend to reinterpret international law in relation to cyber espionage in different directions.

73. On the one hand, the US government and academics have been trying to distinguish economic from political espionage in international law, in part to justify past and ongoing US conduct. It has been argued that cyber-enabled intellectual property theft may be treated as a violation of the Agreement on Trade-Related Intellectual Property Rights (TRIPs Agreement) and brought before the World Trade Organization (WTO) dispute resolution mechanisms.[194] Additionally, there have been assertions that economically motivated espionage amounts to an "act of economic warfare"[195], or even that it embodies "the newest form of warfare employed by the Chinese government [against the US]".[196]

---

192 Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (2015), 134–139.

193 See Russell Buchan, Cyber Espionage and International Law, in: Nicholas Tsagourias and Russell Buchan (eds.), Research Handbook on International Law and Cyberspace (2014), 172.

194 Richard Clarke, A Global Cyber-crisis in Waiting (www.washingtonpost.com/opinions/a-global-cyber-crisis-in-waiting/2013/02/07/812e024c-6fd6-11e2-ac36-3d8d9dcaa2e2_story.html); James Lewis, Conflict and Negotiation in Cyberspace (Jan. 2013), (csis.org/files/publication/130208_Lewis_Conflict Cyberspace_Web.pdf), 49–51. See also James P. Farwell, Take Chinese Hacking to the WTO, National Interest (15 Mar. 2013), (nationalinterest.org/commentary/take-chinese-hacking-the-wto-8224) ("An internationally-recognized ruling, handed down in legal proceedings that found China guilty of intellectual-property theft or infringement, could render it liable for billions of dollars in compensation, expose it to multinational economic sanctions and cause it to be branded a 'pirate state.'"). Such academic arguments have even received a degree of political support, including from the US Senator Charles Schumer. See Charles Schumer, To Truly Fight Back Against Attacks on U.S. Companies, U.S. Must go to W.T.O, (www.schumer.senate.gov/Newsroom/record.cfm?id=351779).

195 Susan Brenner and Anthony Crescenzi, State-Sponsored Crime: The Futility of the Economic Espionage Act, 28 Houston JIL (2006), 395.

196 Jonathan Lewis, The Economic Espionage Act and the Treat of Chinese

74. On the other hand, the Chinese government declared that the spying operations of the US had "flagrantly breached international laws, seriously infringed upon the human rights and put global cyber-security under threat" and "deserve to be rejected and condemned by the whole world".[197] The Chinese government repeatedly described the accusations by the US and some other Western countries as "unfounded" and countered that it was actually the main target of cyberattacks.[198] Meanwhile, in view of the attempt by the US to make a distinction between economic cyber espionage and other cyber espionage activities, the Chinese government stressed that it opposed what it described as the double standard of some Western countries on the issue of cybersecurity, criticizing the US stance as a remnant of "Cold War mentality".[199] There have even been suggestions that "China should confront the US directly" with evidence of espionage and intrusions directed at China.[200]

Espionage in the United States, 8 Chicago-Kent Journal of Intellectual Property (2008-2009), 227.

197 Xinhua News Agency, The United States' Global Surveillance Record (26 May 2014), (news.xinhuanet.com/english/china/2014-05/27/c_133363178.htm). Brazil also determined that cyber espionage by the United States violates State sovereignty and constitute a "breach of international law". See The Guardian, Brazilian president: US surveillance a "breach of international law" (24 Sept. 2013), (www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance).

198 See, e.g., Ai Yang, Nation needs "more Internet security", China Daily (29 Dec. 2010), (usa.chinadaily.com.cn/2010-12/29/content_11770277.htm) (citing Su Hao, an expert on international security, as saying that "China was accused time and again for launching cyber attacks abroad but there was never any solid proof. Actually, China has become a victim of such repeated claims[.]"). It was reported that the number of attacks against Chinese computers increased by 80 percent annually. Shaun Waterman, China open to cyber-attack, Washington Times (17 Mar. 2011), (www.washingtontimes.com/news/2011/mar/17/china-open-to-cyber-attack/?page=all).

199 Tony Romm, Report Fuels China CyberSpying Concerns (Politico) (23 Apr. 2013), (www.politicopro.com/financial-services/story/2013/04/report-fuels-china-cyberspying-concerns-021337); China Denies Pentagon Cyber-Raid, BBC News (news.bbc.co.uk/2/hi/americas/6977533.stm).

200 See Hacker claims reflect US intention of cyber hegemony, Global Times (21 Feb. 2013), (www.globaltimes.cn/content/763429.shtml) ("China has been too tolerant in previous Internet disputes with the US. Since China's tolerance was not appreciated by the US, *China should confront the US directly. China should gather, testify, and publish evidence of the US' Internet intrusions.* So far,

75. From the Chinese perspective, it seems justified to argue that there is no distinction in international law that disallows economic espionage while permitting other forms of espionage.[201] Yet, it is equally difficult to claim that either cyber espionage in general or the totality of intelligence collection operations conducted by the US would be prohibited under international law. This is also the official position of the US government. For example, when the large-scale online surveillance programs of various US governmental departments and agencies attracted widespread criticism, President Obama declared that "[w]hile our intelligence agencies will continue to gather information about the intentions of governments—as opposed to ordinary citizens—around the world, in the same way that the intelligence services of every other nation do, we will not apologize because our services may be more effective".[202] In a speech delivered in November 2016, Brian Egan, US State Department Legal Adviser, expressly noted that the US legal position is that "there is no *per se* prohibition on such activities under customary international law".[203]

76. Therefore, the two positions are in fact less radically different than they may first appear. In fact, recent developments reflect a growing convergence of the Chinese and Western views on this issue. This was reflected during Chinese President Xi Jinping's State visit to the US in September 2015, when the two sides agreed that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors".[204] Similar statements have been also made

---

the US has sanctioned many Chinese firms and individuals based on its own evidence, while China seldom does the same. Such an unfair state of affairs should end.") (emphasis added). See also James McGregor, Is the Specter of a "Cyber Cold War" Real?, The Atlantic (27 Apr. 2013), (www.theatlantic.com/china/archive/2013/04/is-the-specter-of-a-cyber-cold-war-real/275352).

201 For a discussion of the relevance of the TRIPS Agreement of the WTO, see David Fidler, Why the WTO is Not an Appropriate Venue for Addressing Economic Cyber Espionage (11 Feb. 2013), (armscontrollaw.com/2013/02/11/why-the-wto-is-not-an-appropriate-venue-for-addressing-economic-cyber-espionage).

202 The White House, President Obama Discusses US Intelligence Programs at the Department of Justice (17 Jan. 2014), (www.whitehouse.gov/blog/2014/01/17/president-obama-discusses-us-intelligence-programs-department-justice).

203 Egan, above n.32, 12.

204 The White House, FACT SHEET: President Xi Jinping's State Visit to the

at bilateral meetings between China and other major Western countries, such as the United Kingdom,[205] and at multilateral fora like the G20 Antalya Summit in November 2015.[206] Moreover, the United States has been vigorously proposing this constraint on economic cyber espionage as one of the voluntary norms of responsible state behaviour during peacetime in the UN GGE.[207] It remains to be seen whether over time a new customary norm constraining the conduct of State-sponsored economic cyber espionage will be crystallized.

VIII. Concluding remarks

77. Although philosophers and international law theorists may find the search for the precise meaning of the international rule of law vexing,[208] in practical terms it is a value and a principle shared by the entire international community. For instance, in a prominent display of unanimity, member States of the UN gathered at the World Summit in 2005 collectively recognized "the need for universal adherence to and implementation of the rule of law at both the national and international levels".[209] In 2012, UN member States reaffirmed this commitment to the rule of law in a more detailed declaration, again adopted unanimously.[210]

United States, above n.28.

205 Full text: China-UK Joint Declaration on Building a Global Comprehensive Strategic Partnership (22 Oct. 2015), (en.cnci.net.cn/html/2015-10/33328.html) ("China and the UK agree not to conduct or support cyber-enabled theft of intellectual property, trade secrets, or confidential business information with the intent of providing competitive advantage").

206 G20 Leaders' Communiqué at Antalya Summit, above n.27 ("no country should conduct or support cyber-enabled theft of intellectual property with the intent of providing competitive advantages to companies or commercial sectors").

207 Christopher Painter, Testimony Before Policy Hearing Titled: "Cybersecurity: Setting the Rules for Responsible Global Behavior", Senate Foreign Relations Committee Subcommittee on East Asia, the Pacific, and International Cybersecurity, Washington, DC (14 May 2015), (www.state.gov/s/cyberissues/releasesandremarks/243801.htm); Egan, above n.32, 23.

208 See, e.g., Chesterman, above n.13, 340 ("The content of the term 'rule of law,' … remains contested across both time and geography."); McCorquodale, above n.13, 288–291 (examining previous attempts to define the international rule of law).

209 GA Res 60/1 (24 Oct. 2005), para.134.

210 GA Res 67/1 (24 Sept. 2012) ("Declaration of the high-level meeting of the

78. These general proclamations have been echoed in the context of international law regulation of cyber activities. Key players on both sides of the supposed East-West divide, led respectively by China and the US, have affirmed and reaffirmed their commitment to the international rule of law in cyberspace. The shared readiness of States to embrace the principle of the rule of law likely reflects their growing understanding of common interests and of mutual interdependence in the cyber domain.

79. However, consensus between China and Western States on the general level seems to weaken measurably when particular aspects of the regulation of state conduct online are taken into account. Due to this perception, scholarly accounts speak of two competing "camps" of countries holding divergent views of the crucial facets of the rule of law in cyberspace.[211] Yet, we submit that this binary depiction is but a part of the story, one that is insufficiently nuanced to capture the whole picture.

80. We have identified five areas of this supposed divergence. In each of them, it may indeed appear at first glance that two competing views have emerged, sharply dividing the East from the West. While China has proposed binding codes of conduct, Western countries have maintained that existing rules of international law suffice. China supposedly believes in "multilateralism", while the US advocates a "multi-stakeholder" approach. China is pro-sovereignty; Western States promote Internet freedom. The West, led by the US, is said to have adopted a "military paradigm", which China and other countries find unacceptable. Western States have condemned supposed Chinese economic cyber espionage, as China protests against the more traditional political espionage conducted by the US using cyber means.

81. On closer analysis, such black-and-white depictions prove little more than a caricature of the actual complex web of positions, views, and relationships in this area. To the extent that an overarching trend can be identified at all, it is—we submit—one of a trajectory towards convergence. Analysis leads to five conclusions.

82. Firstly, although States may take different positions on the preferred method of identification and development of international law, they have reached a consensus on the baseline issue of the applicability of international law to cyberspace as such. The prospects of a comprehensive binding treaty on cyber security remain dim, but the existence of a plurality of diverse non-binding norm initiatives, as well as several recent bilateral agreements reached between the main cyber powers, demonstrate that cyber

---

General Assembly on the rule of law at the national and international levels").

211 See, e.g., Shackleford and Craig, above n.14, 135; Eichensehr, above n.14, 333; Inkster, above n.14, 9.

norms development has not ended.

83. Secondly, the supposed choice between the multilateral and multi-stakeholder modes of Internet governance is a false dilemma. Top Chinese representatives have acknowledged the importance of multi-stakeholder processes and Western countries have allowed the quintessential embodiment of multilateralism, the United Nations, to gain ground in cyberspace governance. The US release of control over ICANN as well as the growing importance of the IGF are two important signs of convergence in this area.

84. Thirdly, the importance and role of sovereignty in cyberspace has now been recognized by countries across the supposed East/West divide. An erstwhile either-or question has become one of degree. In other words, the central issue today is the type of State conduct, particularly the extent of State online content control, that can be justified by recourse to sovereignty. But any suggestion of a "camp" of States rejecting the applicability of the concept of sovereignty to cyberspace is simply counterfactual.

85. Fourthly, accusations of the militarization of cyberspace are not entirely baseless. However, States and scholars alike have gradually realized that the so-called military paradigm is unhelpful as the first port of call when analysing inter-State malicious cyber operations. Most cyber operations do not cross the use of force threshold and must be analysed through the prism of peacetime international law. This reality is reflected in recent developments, including US statements separating cyber warfare from cyber security and the new Tallinn Manual 2.0, with its primary focus on peacetime regulation of cyberspace.

86. Finally, cyber espionage is (perhaps unsurprisingly) the murkiest of the five areas analysed. What is reasonably uncontroversial is that there still is no general prohibition of espionage under international law. Additionally, it is conceivable that the US has set in motion a process that will at some point result in the emergence of a new customary norm constraining the conduct of State-sponsored economic (as opposed to political) espionage conducted by cyber means. However, for now, statements made in that regard (particularly in various bilateral fora) remain too unspecific and unrepresentative to amount to expressions of legally relevant *opinio juris*.[212]

87. All in all, this article maps out the main areas of difference between the Western and Chinese approaches to the rule of law in cyberspace. As should be apparent, it is inaccurate to describe these two as sharply divided and competing camps. Rather, the emerging picture reveals a web of

---

212 But see, e.g., Catherine Lotrionte, Countering State-Sponsored Cyber Economic Espionage Under International Law, 40 North Carolina JIL (2015), 443, 497–512 (arguing that economic cyber espionage is illegal under customary international law when it is so serious as to amount to a form of coercive intervention).

relationships and views that reflect an overall trajectory of convergence, even if modest in scope and velocity. Ultimately, all involved States bear responsibility for understanding the benefits of collaboration and the dangers of isolation in this area. We hope that this article will improve the general understanding of the potential and space for convergence and thus contribute, at least in small part, to the moderately positive trend it has identified.