International Cyber Norms:
Legal, Policy & Industry Perspectives,
Anna-Maria Osula and Henry Rõigas (Eds.),
NATO CCD COE Publications, Tallinn 2016

CHAPTER 9

International Legal Norms in Cyberspace: Evolution of China's National Security Motivations

Greg Austin

China, like most states, has sought to ensure that its interests are protected both by existing international law and in any discussion of emerging international legal norms. This chapter addresses China's pursuit of that goal in respect of its national security interests in cyberspace.[1] There is a brief overview of four essential background issues: the political character of norm diplomacy by any state, the security interests China has in cyberspace, the epistemic community in China involved in norm diplomacy, and the evolution of China's military cyber policy. The chapter then outlines three phases in cyber norm diplomacy by China: slow start (1998-2005), higher tempo where cyber war is more central (2006-2013), and the upgrade to a 'cyber power' ambition (2014 and beyond). The chapter ends with a short conclusion.

1. Legal Norms in Practical Diplomacy for Cyberspace

Diplomacy is in part a contest over the right to dictate international legal norms, how to have the upper hand in shaping them, or how to interpret and implement existing norms. Table 1 sets out this author's assumptions about the politicised terrain of norm formation in general and in respect of cyberspace in particular.

[1] The author would like to acknowledge the useful comments by Professor Shen Yi of Fudan University, Jamie Collier of Oxford University and several anonymous reviewers.

An international legal norm can be one that is universally agreed (and therefore of universal application), or one limited to a group of consenting states (applying only to them). This distinction can be seen in the approach of the United States to the United Nations Convention on the Law of the Sea, which has near universal force in its entirety (subject to reservations lawfully registered and where permissible) but which the US honours only in so far as it reflects (in the US view) customary international law.[2] Universality of a norm, including implementation of all parts of it in its entirety, is not a prerequisite for it to be regarded as an international legal norm.

Under international law, each state is equal to all others in its right to offer interpretations of the meaning of its normative obligations. It must however rely on the court of international public opinion to win such claims. Therefore, China is as much a subject of norms and norm formation (along with almost 200 other states) as it is a state seeking to shape norms. China is obliged to be a norm-taker (analogy with 'price taker' in economics)[3] to a large degree, even as it aspires to be a norm-maker.

There should be no presumption of any kind regarding the potential universal appeal or moral rectitude of a normative proposition advanced by one state or another. A legal norm is the result of diplomatic compromise among the states which crafted it. Moral rectitude is in the eye of the beholder. Thus any privileging of one country's normative position over that of another state – for example suggesting that the US position is preferred over China's – is a statement of an individual ethical choice not one of political or legal analysis. The ethical terrain of cyberspace carries important dilemmas for states of all political stripes yet the need for new normative behaviours is urgent, as many of them have argued,[4] with considerable support from scholars.[5]

[2] There are many iterations of this principle by the US. See for example, Office of the General Counsel of the National Oceanic and Atmospheric Administration, 'Law of the Sea Convention,' http://www.gc.noaa.gov/gcil_los.html: 'Although not yet a party to the treaty, the US nevertheless observes the UN LOSC as reflective of customary international law and practice'; see also Hillary Rodham Clinton, US Department of State, *Testimony before the Senate Committee on Foreign Relations* (Washington DC: 2012), http://www.state.gov/secretary/20092013clinton/rm/2012/05/190685.htm: 'As a non-party to the convention, we rely – we have to rely – on what is called customary international law as a legal basis for invoking and enforcing these norms'.

[3] See for example Paul Krugman and Robin Wells, *Economics*, third edition (New York: Palgrave Macmillan, 2012), 16, https://books.google.com.au/books?id=_2YdBQAAQBAJ: 'A producer is a price taker when its actions cannot affect the market price of the good or services it sells'.

[4] The best locations for government statements and analyses include UN documents, documentation on various conferences in the London Process accessible through the website of the 2015 conference in The Hague (GCCS2015, https://www.gccs2015.com/), and the INCYDER database of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn (NATO Cooperative Cyber Defence Centre of Excellence, 'INCYDER,' https://ccdcoe.org/incyder.html).

[5] Michael Portnoy and Seymour Goodman, eds., *Global Initiatives to Secure Cyberspace: An Emerging Landscape*, Vol. 42 (New York: Springer US, 2009); Markus Maybaum, Anna-Maria Osula and Lauri Lindström, eds., *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace* (Tallinn: NATO CCD COE Publications, 2015); Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013); Michael N. Schmitt and Liis Vihul, 'The Nature of International Law Cyber Norms,' *The Tallinn Papers* 5 (2014), Special Expanded Issue; Roger Hurwitz, 'The Play of States: Norms and Security in Cyberspace,' *American Foreign Policy Interests* 36 (2014): 322-331; Ludovica Glorioso and Anna-Maria Osula, eds., *1st Workshop on Ethics of Cyber Conflict: Proceedings* (Tallinn: NATO CCD COE Publications, 2014); American Bar Association, 'A Call to Cyber Norms: Discussions at the Harvard-MIT-University of Toronto Cyber Norms Workshops, 2011 and 2012' (2015), https://www.americanbar.org/content/dam/aba/uncategorized/GAO/2015apr14_acalltocybernorms.authcheckdam.pdf; Tim Maurer, 'Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security,' Discussion Paper 2011-11, *Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School* (2011); Eneken Tikk-Ringas, *Developments in the Field of Information and Telecommunications in the Context of International Security: Work of UN First Committee 1998-2012* (Geneva: ICT4Peace, 2012); Camino Kavanagh, Tim Maurer and Eneken Tikk-Ringas, *Baseline Review: ICT-Related Processes & Events: Implications for International and Regional Security (2011-2013)* (Geneva: ICT4Peace, 2014); Abdul Paliwala, 'Netizenship, Security and Freedom,' *International Review of Law, Computers and Technology* 27 (2013): 104-123.

Table 1. Indicative list of assumptions about the normative terrain of cyberspace.

Assumptions about the terrain of norms in international law
1. Politics, like diplomacy, is a contest over the right to dictate norms or at least have the upper hand in shaping norm development OR shaping an argument about how to interpret and implement existing norms.
2. An international legal norm can be one that is universally agreed (with universal application) or one limited to a group of consenting states (applying only to the consenting states).
3. Most new international legal norms with universal application usually take decades to develop and become accepted as norms.
4. Norms are often constituted by 'regimes' (of practice) that subsequently become legal norms.
5. Normative behaviours (such as consultation, self-restraint and dispute resolution by peaceful means) can be adjuncts to or even substitutes for legal norms.
6. Practices unregulated by norms coexist with emerging norms, universally accepted norms, and contested norms.
7. Discussions are often confounded by loose usage of the term 'norms' which has several meanings depending on the context (international legal norms, domestic legal norms, moral norms, political norms, professional norms, business norms, and so on).

Additional assumptions about cyberspace norms
1. Cyberspace is ubiquitous and highly variegated: the contest over norms, laws and practices of cyberspace is ubiquitous and highly variegated.
2. Some examples of the wide scope of cyberspace norms can be found in many areas of international law that directly touch on cyberspace issues, including intellectual property law, trade law, investment law, labour law, human rights, state responsibility, diplomatic (sovereign) immunity, law of the sea (cable protection), air and space law (satellite protection), air traffic control, disaster relief, pandemic control, laws of armed conflict, private international law, extradition treaties, and non-aggression treaties.
3. Ethical and political contest between states over the meaning of existing or emerging norms is severely magnified and exaggerated at all levels by the power of citizens accessing the internet and of private corporations who choose to mount active opposition to state preferences.
4. States are only one category of actor in cyberspace and they cannot exercise a monopoly position on shaping legal norms (power and authority are distributed away from states).

2. China Security Interests for Norms in Cyberspace

China has participated constructively in most international regimes governing cyberspace and observed most existing international law (legal norms), while contesting aspects of others, or pushing for new regimes and new norms. On the whole, it has maintained a positive record, with the main exception being its approach to human rights norms and a lesser exception being its approach to norms on protection of intellectual property rights affected by cyber espionage. China has been a participant in what Benson described as the 'spontaneous evolution of cyber law'.[6] In looking at the full scope of the regime complex underpinning the evolution of norms for cyberspace,[7] it is clear that China has been active in most of the forums identified by Joe

[6] Bruce L. Benson, 'The Spontaneous Evolution of Cyber Law: Norms, Property Rights, Contracting, Dispute Resolution and Enforcement without the State,' *Journal of Law, Economics and Policy* 269 (2005): 265.

[7] Joseph S. Nye Jr, *The Regime Complex for Managing Global Cyber Activities* (Harvard: Belfer Center for Science and International Affairs, 2014), 7, http://belfercenter.hks.harvard.edu/files/global-cyber-final-web.pdf.

Nye. In this, it has often been a cooperative contributor to evolution of certain types of international legal norms, though these have usually been those less politicised and more related to business, the economy, trade, investment and technical standards. One indication of China's intent and exemplary record and attention to detail in these broader areas of economic security can be seen in the fact that a Chinese national, Zhao Houlin, secured international support in 2014 to head the International Telecommunications Union, having served as its Deputy Director General for seven years. Under his chairmanship, the conversations in the World Conference on International Telecommunications in 2015 were markedly different from the confrontational theatrics of the 2012 meeting, a fact that secured praise from the US.[8]

Looking at China's security interests in international aspects of cyberspace somewhat more narrowly, we can see that they are substantial and some cut across issues of the economy, business and technology transfer. They include:

- Preventing foreign interference in China's political sovereignty over Taiwan and Tibet;
- Constraining foreign actors from undermining the rule of the Communist Party;
- Preventing armed conflict;
- Constraining the military capability of its potential enemies;
- Maximising the country's military potential;
- Contingency planning for armed conflict;
- Intelligence collection and assessment;
- Protecting state secrets;
- Development of its defence industry base;
- Development of its national skills base for its military personnel;
- The protection of national critical information infrastructure (CII); and
- Mobilisation of the national economy and society in war-time if needed.[9]

Official Chinese views on these security needs in cyberspace are not usually documented in one place in such a comprehensive fashion but can be found in a variety of documents such as government defence white papers published every two years, especially the 2015 paper,[10] and the 2010 White Paper on the Internet in China.[11]

[8] See Greg Austin, 'US-China Internet Cooperation,' *The Diplomat*, January 19, 2015, http://thediplomat.com/2015/01/us-china-internet-cooperation/.

[9] These national security needs are not unique to China. For more detail on what they mean in the case of China, see Greg Austin, *Cyber Policy in China*, 1st edn (Cambridge UK: Polity Press, 2014), chapter 5; Jon R. Lindsay, Tai Ming Cheung and Derek S. Reveron, eds., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (Oxford: Oxford University Press, 2015); Daniel Ventre, 'Cybersécurité et cyberdéfense chinoise: évolutions', in 'Réflexions sur le cyber: quels enjeux?', ed. Jean-Christophe Pitard, *Bouet Centre d'études stratégiques aérospatiales* (2015): 128-142.

[10] Ministry of National Defense the People's Republic of China, The State Council Information Office of the People's Republic of China, *China's Military Strategy* (May 2015), http://eng.mod.gov.cn/Database/WhitePapers/.

[11] The State Council Information Office of the People's Republic of China, *The Internet in China* (June 8, 2010), http://www.china.org.cn/government/whitepaper/node_7093508.htm.

China, like many states, has not articulated in consistent detail how all of its individual security interests may be served by advocacy of this or that norm in cyberspace. This has left open the opportunity for speculation by analysts.

Security analysts in both the West and in China have often seen its position as focused largely on the fourth point in the list above: the need to constrain the cyber military capability of its potential adversaries. This has indeed been a high interest. Such a preoccupation would explain why China has focused some of its activities within the framework of the arms control mechanisms of the United Nations, especially the First Committee of the General Assembly. But China's interest in framing limitation of cyber weapons as a broad objective does not appear to have been followed up by its officials in any detail at the inter-governmental level.[12] It has subsumed this goal in pushing for reflection on and constraint of impulses toward militarisation of cyberspace, even though it very clearly joined the same trend in February 2014 when President Xi Jinping declared that the government would do everything necessary for China to become a 'cyber power'.[13]

That goal of constraining US cyber military power had in fact been just one of many national security priorities for China in its norm entrepreneurship for cyberspace. A wider view of its goals in cyberspace is both possible and necessary, not just within the international security domain but also outside it. First, China's national security interests are quite diverse and span a vast territory of policy interests. It is almost impossible to disaggregate any single one of them from others as a security motivator for China's position on cyberspace legal norms. Second, China has pursued cyberspace norm development for its national security interests hand in glove with its approach in areas affecting the economy, trade and development. The two domains of policy (national security and economic prosperity) are inextricably linked in China's conceptions of contemporary world order. China sees itself as needing a baseline of normative behaviour on cyberspace issues in order to maximise its economic exchange with the US, Japan and the European Union that it sees as essential for building an advanced military industrial base. Third, conflict prevention (stopping the escalation of political disputes to military confrontation) is also a paramount objective for China's leaders. At the same time, China has not for decades seen armed conflict with major powers as imminent and in that context has not been averse to active cyber probing of other countries' defences and civil infrastructure. It has clearly judged such actions to be low risk and low cost, and not prohibited by international law.

A wider view of national security, extending beyond the narrowly governmental or narrowly military, is also dictated by the fact that in cyberspace affairs, there are few neat boundaries between governments and the private sector, or to put the same point

[12] It has figured prominently in Track 2 discussions involving Chinese officials.

[13] The significance of this announcement is discussed in Austin, *Cyber Policy in China*, and several media commentaries by the author, such as: Greg Austin, '2015 is the Year of Chinese Cyber Power,' *East Asia Forum*, July 31, 2015, http://www.eastasiaforum.org/2015/07/31/2015-is-the-year-of-chinese-cyber-power/; Greg Austin, 'China's Military Dream,' *The Straits Times*, May 29, 2015, http://www.straitstimes.com/news/opinion/more-opinion-stories/story/chinas-military-dream-20150529; Greg Austin, 'How China Plans to Become a World Class Cyber Power,' *The Diplomat*, April 30, 2015, http://thediplomat.com/2015/05/how-china-plans-to-become-a-world-class-cyber-power/.

differently, between the national security aspects and the economic security aspect of cyberspace.

I have found only a small number of independent scholarly works that address the subject of this chapter systematically or in much detail. These include a number of articles by Chinese specialists about their government's approach to legal norms for cyberspace,[14] and these are complemented by a number of reports of international working groups involving Chinese participants.[15]

In terms of analyses outside the country, a short 2014 review on 'China and International Law in Cyberspace' provides a snapshot assessment of the situation around the end of 2013.[16] It observed that China's approach to norms for cyberspace was different to those of the US, though the bulk of the article bears out the opposite conclusion – that there has been more common ground than division. It noted that China strongly advocated the application to cyberspace of the UN Charter norm of non-interference in the internal affairs of other states. The article also discussed the notion, supported by China, that democratisation of Internet governance, and therefore the elimination of the strong US influence over the Internet Corporation for Assigned Names and Numbers (ICANN), conformed to a normative principle of good order, a principle the US also accepts. The analysis concluded that China's agreement to the 2013 report by the UN Group of Governmental Experts (GGE) on cyberspace issues suggests that 'China agrees in principle not only to the general application of international law to cyberspace, but also the application of specific aspects of international law, including the law of state responsibility, concepts in the UN Convention relating to the use of military force, and the law of armed conflict'. This was also the US position. The paper concluded that the 2013 GGE report represented 'an implicit, general consensus on the definitions of key terms such as 'use of force' and 'armed attack' in cyberspace',[17] a view of the GGE report that is not really credible. A 2014 legal analysis from the US, 'An International Law Response to Cyber Economic Espionage', provides a useful analysis of the place of existing norms and organisations such as the WTO to address charges levied at China.[18] By implication, it suggests correctly that China is already party to norms governing this practice. Michael Swaine provides a useful overview of how China views its interests in cyberspace and its general approach to norm development.[19]

[14] See for example, Zhang Xinbao, 'Establishing Common International Rules to Strengthen the Cooperation of Cyber Information Security,' *China Legal Sciences* 121 (2013) [in Chinese]; Shen Yi, 'Protecting Safety by Strength or Achieving Safety by Governance? – Two Cyber Safety Strategies and China's Choice,' *Foreign Affairs Review* (2013): 140-148 [in Chinese]; Chunmei Kang, 'Establishing Norms of Behaviour in Cyberspace: The Chinese Viewpoint,' in *Security in Cyberspace: Targeting Nations, Infrastructures, Individuals*, Revised edition, ed. Giampiero Giacomello (London: Bloomsbury Publishing, 2014), 113-124.

[15] Center for Strategic and International Studies (CSIS), *Bilateral Discussions on Cooperation in Cybersecurity China Institute of Contemporary International Relations (CICIR)* (June 2012), http://csis.org/files/attachments/120615_JointStatement_CICIR.pdf; and Karl Frederick Rauscher and Zhou Yonglin, 'Frank Communication & Sensible Cooperation to Stem Harmful Hacking,' *EastWest Institute* (2013). A full version can be found on the website of CERT China at http://www.cert.org.cn/publish/main/upload/File/China-US%20Anti-Hacking%20Report%20v190.pdf.

[16] Kimberly Hsu and Craig Murray, *China and International Law in Cyber Space, U.S.-China Economic and Security Review Commission Staff Report* (U.S.-China Economic and Security Review Commission, 2014), 1.

[17] Ibid, 4.

[18] Christine Parajon Skinner, 'An International Law Response to Cyber Economic Espionage,' *Connecticut Law Review* 46 (2014): 1165-1207.

[19] Michael D. Swaine, 'China's Views of Cyber Security in Foreign Relations,' *China Leadership Monitor* 42 (2013), http://carnegieendowment.org/files/clm42ms_092013carnegie.pdf.

Since this chapter is about 'China the government', it focuses on official views. A government's view of international legal norms is only what it says it is or, in some cases, what it may unambiguously manifest by its actions over a sustained period. China's official views on international legal norms for cyberspace can be found in UN resolutions that China has supported beginning in 1998, in statements by Chinese officials in the UN General Assembly and its committees, in the World Summit on the Information Society (WSIS), the International Telecommunications Union (ITU), the UN-initiated Group of Governmental Experts (GGE) over several iterations,[20] regional organisations, and in several treaties with a cyberspace aspect, such as the 2009 Treaty among members of the Shanghai Cooperation Organization (SCO),[21] the Beijing Convention 2010[22] on aircraft hijacking (with a clause on technical attack), and the Russia/China information security agreement of 2015.[23] China's views can also be found in consideration of treaties it has rejected, such as the 2001 Budapest Convention on Cyber Crime and the 2012 Multinational Statement on Nuclear Information Security agreed by 31 states at the Nuclear Safety Summit that year. At the same time, unofficial analytical sources or working group reports do reflect opinions of senior government leaders and can be valuable supplementary material if carefully scrutinised.

[20] The work of the Group of Governmental Experts set up by the United Nations to review certain aspects of international law relating to cyberspace provided the Chinese representatives the opportunity to outline Chinese official positions at far greater length and to sound out alternative approaches. Unfortunately, there is no public record of the Chinese representative's positions in these meetings, and only a few passing references from other participants to the positions they believe the Chinese representatives took. The formal reports of the GGE are mentioned later in terms of how they illuminate China's public position.

[21] Shanghai Cooperation Organization, *Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security* (16 June 2009), https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf [Unofficial translation]. The text in Russian of the treaty, with unofficial English translation, can be found at NATO Cooperative Cyber Defence Centre of Excellence, 'Shanghai Cooperation Organisation,' https://ccdcoe.org/sco.html.

[22] The text of the 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation 'was adopted with 55 votes in favour, 14 votes not in favour' and the text of the 2010 Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft was adopted 'with 57 votes in favour, 13 votes not in favour'. See International Civil Aviation Organization, *Final Act of the of the International Conference on Air Law (Diplomatic Conference on Aviation Security) held under the auspices of the International Civil Aviation Organization at Beijing from 30 August to 10 September 2010* (10 September 2010), http://www.icao.int/secretariat/legal/Docs/beijing_final_act_multi.pdf. For the text of the Convention, see *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation*, Beijing, 10 September 2010, No. 21, https://www.unodc.org/tldb/en/2010_convention_civil_aviation.html. For the text of the Protocol, see *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft*, Beijing, 10 September 2010, No. 22, https://www.unodc.org/tldb/en/2010_protocol_convention_unlawful_seizure_aircraft.html. For an excellent analysis of the two treaties, see Damien van der Toorn, 'September 11 Inspired Aviation Counter-Terrorism Convention and Protocol Adopted,' *American Society of International Law* 15 (2011), http://www.asil.org/insights/volume/15/issue/3/september-11-inspired-aviation-counter-terrorism-convention-and-protocol. According to the International Civil Aviation Organization (ICAO), the main changes to pre-existing treaties with similar names were the criminalisation of the acts of using civil aircraft as weapons, using dangerous materials to attack aircraft or other targets, and cyber attacks on aircraft in flight.

[23] For a text in Russian, see Government of the Russian Federation, Order of the Russian Government on signing the Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on Cooperation in the Field of Ensuring International Information Security, 30 April 2015, 788-r, http://government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf [in Russian].

3. China's Epistemic and Policy Communities

The characteristics of a country's epistemic and policy communities will shape how it analyses and proposes norms and normative ideas on the international stage. Much will depend on the values and the discourse about values in domestic politics. In cyberspace affairs, there is a fundamental gulf in domestic approaches to the articulation of international legal norms between, on the one hand, China and like-minded countries such as Russia and, on the other, the US, the European Union, Japan and other Western countries. This chapter is not the place to analyse differences between epistemic communities or its impact on the subject at hand.[24] Let it suffice for current purposes merely to observe that a dialogue with China on norms about cyberspace affairs may be challenging because of differences between the structure and priorities of the epistemic and policy communities inside China compared to those in major Western powers. After all, as Nye has observed, norm development relies on epistemic communities.[25] If the epistemic communities are very different, then we must expect differences between national approaches to norm promotion.

We can cite, as just one example, the fact China has not been as vigorous as its Western counterparts in forensic dissection of existing international legal norms about the permissibility or otherwise of certain actions in cyberspace in time of war or in preparation for war. China has shown little interest even in a scholarly elaboration of possible approaches to cyber norms, such as the Tallinn manual.[26] A far higher priority has been the articulation of cyberspace norms affecting political sovereignty at home in terms of controlling dissent and maintaining Communist Party rule. Simply put, the Government of China has a very basic view on national security aspects of international legal norms for cyberspace and they relate mainly to internal security.

In the absence of legal doctrines on the military uses of cyberspace that might emanate from the Ministry of Foreign Affairs or the Ministry of National Defence, we are left to speculate as to official views on key issues.

We can assume that it is China's view, as it is that of most countries, that all activities preparatory for military combat (and national self-defence) not specifically prohibited by international law are permissible. This is captured well, between the lines, in the text of the 2015 agreement with Russia that commits each country to refrain from 'unlawful' interference in the information infrastructure of the other. This assessment is also captured directly in the language of a 2010 international treaty and associated protocol both signed by China and the US among others, that requires states to criminalise 'technological attack' (i.e. including cyber

[24] An overview of China's values for cyberspace affairs can be found in Austin, *Cyber Policy on China.*

[25] Joseph S. Nye Jr, 'The Information Revolution and American Soft Power,' *Asia-Pacific Review* 9 (2002): 60-76.

[26] Schmitt, *Tallinn Manual.*

attack) against civil aviation. Article 6 of the Protocol excludes situations of armed conflict and the lawful duties of the armed forces of a state from the purview of the treaty and protocol.[27] Similar language can be found in other international treaties excluding their effect from situations of armed conflict and the lawful duties of the armed forces of a state.

Thus this chapter can throw some light on what China has hoped to get out of discussion on legal norms in terms of protecting or advancing its military security interests. But this will look and feel very different from the articulation of such expectations about norms among legal experts and political scientists in the West. The chapter is more useful for seeing how China sees the interaction in the international normative space between national security narrowly defined and broader conceptions of it based on economic interests.

4. Milestones in China's Cyber Military Policy

This section of the chapter gives a very brief summary of how China's military interests in cyberspace have developed from 1998 to the present. The purpose is not to tie subsequent discussion too narrowly to military affairs, but rather to reinforce the proposition that military use of cyberspace is a relatively new area of policy for China (beginning around 2003) and one that has developed only in fits and starts before taking a decisive turn in 2014.

China, like all states, has had to come to terms with a revolution in military affairs as a result of the rapid advance in the military potential of information and communications technologies. In 1998, the US published a formal Joint Staff doctrine on Information Operations (to include offensive computer attack),[28] that had been many years in the making and which brought together elements that had been well practised in the single military services and separate intelligence agencies of the US. The same year, two Chinese military strategists were writing a book called *Unrestricted Warfare*, expressing concern about a range of developments, including information warfare, and foreshadowing an eventual shift by China to a similar strategy that US had adopted.[29] Yet China was behind at the time. Table 2 offers a brief summary overview of milestones in China's military policy in cyberspace.[30]

[27] These treaties are analysed in Greg Austin, Eric Cappon, Bruce McConnell and Nadia Kostyuk, 'A Measure of Restraint in Cyberspace: Reducing Risk to Civilian Nuclear Assets,' *EastWest Institute* (2014): 17-18.

[28] United States of America, Joint Chiefs of Staff, *Joint Doctrine for Information Operations*, Joint Pub 3-13 (9 October 1998), http://www.c4i.org/jp3_13.pdf. This doctrine manual, which included options for computer network attack, was developed to implement a DoD Directive on Information Operations from 1996, the first of its kind in the US at joint force level.

[29] See Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999) [in Chinese], http://www.c4i.org/unrestricted.pdf. The book was written through 1998. A translation more than 200pp of excerpts is available at http://www.c4i.org/unrestricted.pdf. The book is notable for its several references to the breach of international norms or rules by any countries adhering to the concept of 'unrestricted warfare'.

[30] For a discussion of the detail, see Austin, *Cyber Policy in China*, chapter Five.

Table 2. Milestones in China's military development in cyberspace.

1998	Chinese military pays closer attention to military uses of cyberspace
1999	China observes US cyber operations against Belgrade electric grid
2000	Jiang Zemin declares shift to an information society, including in military affairs, and asks PLA to begin to shift focus
2001	PLA joins Informatisation Leading Group which is upgraded from Vice Premier control to Premier
2003	China shifts official military doctrine to take account of informatisation China conducts first mass cyber espionage 'Titan Rain'
2006	Training regulations for information warfare approved National Informatisation Plan 2006-2015 (first such plan in in the civil economy)
2007	China undertakes a kinetic anti-satellite test (US cyber military power depends on space-based assets)
2010	Internet white paper says China's cyber military capabilities are rudimentary
2011	Changes in General Staff communications structure Academy of Sciences publishes 2050 Roadmap for Information Technology
2013	Edward Snowden revelations deliver a sharp wake-up call to China's leaders and security elites
2014	Xi declares China will become a 'cyber power' and takes over Leading Group; six months later Xi calls for a cyber military strategy
2015	China issues first 'Military Strategy' recognising outer space and cyberspace as the 'commanding heights' of international security

A simple time-line like this cannot convey the complexity of the military policy changes contemplated by China in the past 15 years, the immense bureaucratic and practical obstacles China would face in implementing any policy change, or the character of its international relations over the protracted time frame the changes would need to be made.

One essential conclusion to draw from this timeline is that China's approach to international legal norms for cyberspace would have trailed behind this timetable, and not got ahead of it. If the pace of adjustment in cyber military affairs was gradual, then so too would have been the pace of development of an approach to international legal norms governing military affairs. Moreover, since the most radical changes in cyber military policy only occurred in 2014 and 2015, we can probably expect to see some acceleration in the pace around development of approaches to international legal norms for security in cyberspace. The situation with respect to internal security was markedly different, with China staking its positions in that area quite early by comparison.

5. Slow Start: 1998-2005

National security concerns only began to surface in China's international legal practice for cyberspace around 1998 when it supported a resolution introduced by Russia in the First Committee on security aspects of information and telecommunications.[31] The Resolution (less than two pages long) seemed unremarkable. It cited three normative propositions: optimum exploitation of information and communications technologies (ICT) for development through broad international cooperation; fostering strategic stability and state security; and the need to prevent criminal or terrorist use of the technologies. Key elements of the original Russian draft had been dropped at the urging of the US. These deletions involved references to the use of information technology for military purposes, specific definitions of 'information weapons' and 'information war', the need for a regime of prohibition of the creation and use of information weapons, and provisions on the comparability of the impact of information weapons and weapons of mass destruction.[32] In the same UNGA session, China supported a resolution (passed without a vote) which contained a section on 'Information in the Service of Humanity' in which it called for freedom of the press, a diverse media and rapid transfer to developing countries of information technologies.[33] This resolution had carried over from previous years. Thus, in 1998, China was not really thinking in terms of crafting new international legal norms to govern cyberspace and there was wide agreement on the need to foster strategic stability and state security (expressed in the most general terms).

Throughout 1998 and 1999 China got a foretaste of the potential of international cooperation on cyberspace security issues when it found itself working alongside the rest of the world to prevent any dangers from the Y2K problem.[34] At this time, Russia's relations, under Boris Yeltsin, with the US were quite strong. Russia had just been admitted to the G8, and the two Presidents had agreed to include cyber security in their official bilateral agenda.[35] Yet the divergence in approaches in the international community that the Russian-sponsored 1998 Resolution (53/70) was to open up were more fully revealed in a 1999 report by the UN Secretary General recording the formal position of ten member states provided by them in accordance with the terms of the Resolution.[36] In its statement, Russia called for work to 'begin on the development of international principles (e.g. a regime, a code of conduct for states)' to strengthen international information security, with such principles subsequently 'incorporated into a multilateral international legal instrument', and working in partnership with the UN Conference on Disarmament.[37] In its response,

[31] United Nations, General Assembly resolution 53/70, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/53/70 (4 January 1999), http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70.

[32] Aleksandr Berditskii, 'An International Agreement on Cyber Security: Is Consensus Possible?' *Perspektivy*, October 24, 2014, http://www.perspektivy.info/table/mezhdunarodnyje_dogovoronnosti_po_kiberprostranstvu_vozmozhen_li_konsensus_2013-10-24.htm [in Russian].

[33] United Nations, General Assembly resolution 53/59, *Questions relating to information*, A/RES/53/59 (18 February 1999), http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/53/59. Section A in this resolution related to 'information in the service of humanity'.

[34] This was the concern that when the century and millennium rolled over at midnight on 31 December 1999, then many automated controllers in sensitive systems (such as aircraft, nuclear power stations, financial institutions or hospitals) might malfunction since programmers may not have provided for a '00' or '000' date after '99' or '999'.

[35] See Franz-Stefan Gady and Greg Austin, 'Russia, the United States and Cyber Diplomacy: Opening the Doors,' *EastWest Institute* (2010): 1-2.

[36] United Nations, General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*: *report of the Secretary-General,* A/54/213 (10 August 1999).

[37] Ibid, 9.

the US was silent on emerging doctrines of information warfare, and declared that 'it would be premature to formulate overarching principles pertaining to information security in all its aspects'.[38] The US and its allies had a clear preference to keep cyberspace issues at the United Nations out of the purview of the First Committee (disarmament) where the Russians had introduced it. China was silent on this emerging debate about a new treaty held up by Russia in 1999.

Thus in 1999, the US position was identical with the position of China in 2015 outlined later: that it may be premature to formulate over-arching principles, especially in regard to cyber warfare.

Subsequent versions of the annual resolution became more strident on security issues of concern to China and Russia. In the 1999 NATO war against the former Yugoslavia, the potential of information warfare was played out in several ways on which the public historical record is incomplete.[39] Regardless of what actually transpired, there was some currency to the idea that network attack weapons had been used by the US for the first time ever in war. President Jiang Zemin was prepared to credit the reports as fact[40] and his mind had been focused no doubt by what China saw as a precision (kinetic) attack by NATO on the Chinese Embassy in Belgrade. The 2000 version of the UN ICT/security resolution for the first time called on states to promote 'possible measures to limit the [security] threats emerging in this field'.[41] Thus the idea was born that China and Russia wanted to use an arms control process of some sort to constrain US and allied capability, even though the US also supported this new language.

In 2000, Jiang Zemin appealed in a brief reference during a speech in Beijing to the World Computer Congress for a global Internet treaty in order to jointly strengthen information security management and to give full play to the 'positive role of the internet'.[42] His interventions coincided with the emergence in the G8 of the Okinawa Declaration on a Global Information Society[43] which sought to promote a globally inclusive approach, but which remained largely a G8 exercise, including through its Digital Opportunity Task Force. At this time, China did not have a fully articulated diplomatic strategy for international security aspects of the information society, beyond those that affected economic settings, science

[38] Ibid, 13.

[39] For one account, see Myriam Dunn Cavelty, 'Cyberwar' in *The Ashgate Research Companion to Modern Warfare*, eds. George Kassimeris and John D. Buckley (England: Ashgate Publishing Limited, 2010), 123-144.

[40] See Jiang Zemin, 'Informationize the Army, Excerpts form a speech to the Central Military Commission, 27 December 2002,' in *On the Development of China's Information Technology Industry*, ed. Jiang Zemin (Oxford: Elsevier, 2010) (Oxford: 2010), Kindle edition. Jiang cited NATO's rout of the Yugoslav army as an example of informatised, non-contact warfare.

[41] United Nations, General Assembly resolution 55/28, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/55/28 (20 November 2000), Article 1, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/55/28. In the 1998 resolution, this language did not appear. In the 1999 resolution, it appeared only in a preambular reference.

[42] Jiang Zemin, 'Speech at the Opening Ceremony of the 16th World Computer Congress', in *On the Development of China's Information Technology Industry*, ed. Jiang.

[43] See Ministry of Foreign Affairs of Japan, *Okinawa Charter on Global Information Society* (2000), http://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html.

and technology or domestic security, including cyber crime.[44] Nevertheless, it was actively trying to position itself in the diplomatic space especially with reference to a possible new treaty, Internet governance and ICANN.[45] In 2000, a Chinese candidate for a seat on the Council of ICANN was unsuccessful but a researcher from the Chinese Academy of Sciences was elected as Council Chairman of Asia Pacific Top Level Domain Association (APTLD) by a unanimous vote. For China, ICANN arrangements have related directly to international security order because of the presumption that if governments like the US and like-minded countries controlled the governance of the Internet, they would continue to stimulate the flow of subversive material over it against the interests of states like China.[46]

China took a more robust and engaged position on international collaboration on cyberspace issues in the framework of the Asia Pacific Economic Cooperation (APEC) group in support of its international economic security interests, including protection of critical infrastructure. One factor that facilitated China's willingness to extend itself in APEC on debate about cyber-related norms or normative behaviour was that this group was fairly tightly focused on economic issues, studiously avoiding politically contentious issues (to the extent that China had ten years earlier agreed to Taiwan's membership as an 'economy'). This consideration meant that China did not have the same need or the potential in APEC to deal with political and security issues as it did in the UN framework. In October 2001, in the month after the 9/11 attacks in the US, China joined the APEC leaders in a statement after their summit in Shanghai that called for strengthening cooperation at all levels in counter-terrorism, including the protection of critical infrastructure, such as telecommunications.[47] The leaders also issued a lengthy action plan on developing *e*-APEC, which included many commitments by China to normative behaviour in the economic and social spheres of cyberspace development, including security, privacy protection, and consumer trust.[48]

In May 2002, APEC Telecommunications Ministers, including China, agreed the Shanghai Declaration,[49] which included as Annex A the Work Programme for their officials,[50] and at Annex B, a more detailed 'Statement on the Security of Information and

[44] On 4 December 2000, China supported a UN General Assembly Resolution 'Combating the criminal misuse of information technologies'. See United Nations, General Assembly resolution 55/63, *Combating the criminal misuse of information technologies*, A/RES/55/63 (22 January 2001), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf.

[45] ICANN was incorporated as non-profit, non-governmental organization in 1998, but remained formally associated with the US Department of Commerce until 2015.

[46] See for an example of hundreds of commentaries to this effect over many years, Guo Ji, 'The Internet Cannot Be Allowed to Become a New Tool of US Hegemony,' *English Edition of Qiushi Journal* 6 (2014), http://english.qstheory.cn/magazine/201401/201401/t20140121_315162.htm. *Quishi* is a journal of the Chinese Communist Party.

[47] Asia-Pacific Economic Cooperation, *APEC Leaders Statement on Counter Terrorism* (21 October 2011), http://www.apec.org/Meeting-Papers/Leaders-Declarations/2001/2001_aelm/statement_on_counter-terrorism.aspx.

[48] Asia-Pacific Economic Cooperation, *APEC Economic Leaders Declaration Appendix 2: e-APEC Strategy*' (21 October 2001), http://www.apec.org/Meeting-Papers/Leaders-Declarations/2001/2001_aelm/appendix2_eAPEC_strategy.aspx.

[49] Asia-Pacific Economic Cooperation, *The Fifth APEC Ministerial Meeting of the Telecommunications and Information Industry (TELMIN5), Shanghai Declaration*, TELMIN5/1 (29-30 May 2002), http://www.apec.org/Meeting-Papers/Ministerial-Statements/Telecommunications-and-Information/2002_tel/.

[50] Asia-Pacific Economic Cooperation, *Annex A – Program of Action*, *Shanghai Declaration* (29-30 May 2002), http://www.apec.org/Meeting-Papers/Ministerial-Statements/Telecommunications-and-Information/2002_tel/annex_a.aspx.

Communications Infrastructures.[51] The annex expressed shared recognition of interdependence of the information infrastructure in cyberspace and, indeed, the interdependence of the information security of all members. The Programme of Action provided an impetus for convening expert groups on security related issues. As the APEC host, China has to be credited at least in part with the emergence of these processes.

These moves early in the decade were largely declaratory but provided a strong foundation for a leading role later by China in regional approaches and they closely foreshadowed the agreements on critical infrastructure supported by the Chinese representative in the 2013-2015 GGE convened by the United Nations.

At the Ministerial Meeting of APEC in Los Cabos, Mexico, on 23-24 October 2002, the participants agreed the 'importance of protecting the integrity of APEC's communications and information systems while allowing the free flow of information'.[52] They 'supported' the 'Cybersecurity Strategy' which had been presented by the APEC Telecommunications and Information Working Group (in fact drafted by the US), and they 'instructed Officials to implement the Strategy'. By this time, China had decided on a policy of social control of the Internet, realising that it could not ever achieve the technology to censor it completely.[53] At the same time, China continued to maximise its technical capacities, and build the foundations of the biggest and most intrusive cyber-enabled internal surveillance system in the world.[54]

In the United Nations setting, the 2002 version of the annual Russian-instigated ICT resolution saw a slight change in language. The preambular clause on the threats, previously very broad ('may affect the security of states'), now specifically called out a 'threat to the integrity of the infrastructure of states to the detriment of their security in both civil and military fields'.[55] At this time, China began to stake out its independent views (unilaterally expressed) on legal norms for cyberspace, flagging them for the first time in a rather general statement in 2002,[56] and reiterated in similar statements in 2004[57] and 2006.[58] China called for the use of

[51] Asia-Pacific Economic Cooperation, *Annex B – Statement on the Security of Information and Communications Infrastructures, Shanghai Declaration* (29-30 May 2002), http://www.apec.org/Meeting-Papers/Ministerial-Statements/Telecommunications-and-Information/2002_tel/annex_b.aspx.

[52] See Asia-Pacific Economic Cooperation, *2002 APEC Ministerial Meeting. Joint Statement - Expanding the Benefits of Cooperation for Economic Growth and Development - Implementing the Vision* (23-24 October 2002), http://www.apec.org/Meeting-Papers/Ministerial-Statements/Annual/2002/2002_amm.aspx.

[53] See Austin, *Cyber Policy in China*, chapter 3.

[54] Arguably, the US has the biggest and best capability for surveillance, but in terms of negative impact, relatively speaking, on the lives of people, it is China which has the more intrusive surveillance system.

[55] General Assembly resolution 57/53, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/57/53, (30 December 2002), http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/57/53.

[56] 'Statement by Ambassador Sha Zukang Head of the Chinese Delegation at the First Meeting of the Intergovernmental Preparatory Committee of the World Summit on the Information Society' (The First Meeting of the Intergovernmental Preparatory Committee of the World Summit on the Information Society, Geneva, 1 July 2002), http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t25077.shtml.

[57] See United Nations, General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security: report of the Secretary-General*, A/59/116 (23 June 2004), 4, http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N04/407/04/PDF/N0440704.pdf?OpenElement: 'China holds that use of information technology should abide by the United Nations Charter and other internationally accepted principles'.

[58] United Nations, General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security: report of the Secretary-General*, A/61/161 (18 July 2006), 4, https://disarmament-library.un.org/UNODA/Library.nsf/df4241a26771ddbd852571a8006cd413/8cc65546257a1692852571cb00566c6e/$FILE/sg61.161.pdf.

information technologies in accordance with the UN Charter, including in respect of international security. As indicated in Table 2 above, it was at precisely this time that China was preparing the ground for its first shift to information war strategies in response to what it had seen the US and Russia developing.[59]

In the 2002 statement, China's Ambassador to the United Nations in Geneva, Sha Zukang,[60] articulated the need for innovations in diplomacy to respond to the information society: 'establishing international organisations and mechanisms that ensure the security and reliability of communication networks by fighting against viruses and cyber crimes'.[61] China's engagement in the preparations for the World Summit on the Information Society became an additional opportunity (a workshop) for the development of its normative positions. Sha offered an assessment of the current global situation with respect to the information society. Alongside unprecedented technological conditions for global economic and social development, and valuable 'digital opportunities' for economic development and social progress, he observed that the 'infocom' development around the world is 'seriously unbalanced'. The digital divide is 'widening instead of narrowing, putting the developing countries in a more disadvantageous position'. He warned that this would 'inevitably further aggravate the social and economic disparity' and that the digital divide had to become a major focal point of international action.

His also laid out a six-point position statement on what states might do. First, he said, since 'countries vary in their social and cultural traditions and level of economic development and informatisation, plans and measures they formulate for their own informatisation may well differ'. Second, information infrastructure is the 'physical foundation of the information society' and in the future it needs to 'satisfy our demand for intelligence, diversification, personalisation, multimedia and globalisation as well as universal service'. Considerable attention needed to be given to developing countries to 'accelerate their information infrastructure build-out'.

The third point addressed security more directly. He noted that this was multi-level, from promoting consumer confidence to countering terrorism. He said that this involved technologies as well as laws and regulations and would require international cooperation. Fourth, to foster the expansion of knowledge and skills, innovative mechanisms for training and human resources development were needed. Fifth, developed countries needed to 'truly shoulder their responsibilities in helping the developing countries accelerate their informatisation processes'. Assistance could take the form of financial support, technology transfer and human resources training. Sixth, the private sector and the civil society would need to be closely involved but in international policy, 'governments obviously should play the leading role'.

Subsequently, China started to firm up its commitment to the goals of common security in an interdependent cyberspace. This can be seen in its support for the

[59] See Austin, *Cyber Policy in China*, 132-35.

[60] Sha subsequently became the Under-Secretary-General of the United Nations responsible for the Department of Economic and Social Affairs (UNDESA). He was succeeded by compatriot, Wu Hongbo.

[61] Statement by Ambassador Sha Zukang.

December 2002 UN General Assembly Resolution (ARes/57/239) on 'Creation of a global culture of cybersecurity' and for the 2003 Geneva Declaration of Principles of the World Summit on the Information Society. This latter document observed that '[s]trengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs'.[62] The Association of South East Asian Nations (ASEAN) agreed with China in 2003 to implement an ASEAN-China Strategic Partnership for Peace and Prosperity, with a declaration that expressed their joint intent: 'to formulate cooperative and emergency response procedures for purposes of maintaining and enhancing cybersecurity, and preventing and combating cybercrime'.

The earlier UN resolutions beginning in 1998 had the effect of saying that information technologies were of concern to international and national security, whereas the other documents of 2002 and 2003 mentioned above saw China signing up to more explicit statements of what that meant and what should be done about it with other states. These themes as canvassed at the time were not much different in effect from what China's GGE representative agreed to in 2015.

In 2004, the United Nations convened its first GGE to consider security aspects of ICT. That year, in its first statement to the Secretary General in connection with the call that was made in the first ICT/security resolution in 1998 for states to register their views, China made a fairly strong if brief intervention.[63] It said that 'information security has become a grave challenge in the field of international security'. China declared its support for 'international efforts aimed at maintaining and promoting information security of all countries', and it also supported the establishment of governmental expert group to discuss how common understandings on the issues might be advanced at the international level. The statement called for special attention to 'information criminality and terrorism'. It reiterated the view that the 'imbalanced development of countries in the field of telecommunications' mandated a need for the international community to deepen cooperation in the research and application of information technology. In 2004, as part of a consultation mechanism for trilateral relations in the broad, which had been established at head of state level the year before, China, Japan and Korea agreed a work plan that included 'projects on network and information security policies and mechanisms, joint response to cyber attacks (including hacking and viruses), information exchange on online privacy protection information, and creation of a Working Group to promote this cooperation'.[64]

In 2005, China supported the Lima declaration by APEC Telecommunications

[62] First Phase of the World Summit on the Information Society, *Declaration of Principles, Building the Information Society: A Global Challenge in the New Millennium*, WSIS-03/GENEVA/DOC/4-E (12 December 2003), http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf.

[63] United Nations, General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/59/116 (2004).

[64] Portnoy and Goodman, eds., *Global Initiatives to Secure* Cyberspace, 55.

Ministers[65] which mentions their recognition of the 'importance of ensuring the security and integrity of the APEC region's communications infrastructure, in particular the Internet, in order to bolster the trust and confidence of users and enable the continued advancement of this infrastructure'. Several other APEC policy documents, signed off by China, were adopted that year:

- Guiding Principles for PKI-Based Approaches to Electronic Authentication;
- Principles for Action against Spam; and
- Strategy to Ensure a Trusted, Secure and Sustainable Online Environment.

By August 2005, it had become apparent that the first GGE, which had been set up in 2004, would not reach 'consensus on a final report'.[66] According to the Russian representative, all members of the group (including China) but not the US representative, had agreed a number of points:

- The capability of ICT as an effective means of negatively affecting the civil and military affairs of a state;
- The powerful destructive force of information aggression;
- The potential for harmful acts in the information space both from states and non-state actors (criminals and terrorists);
- The existence of capabilities within states for covert use of cyber criminals; and
- The need for mutual efforts to reduce threats and strengthen trust in the information sphere.[67]

Thus, by 2005, China had moved decisively on normative approaches to economic security aspects of cyberspace on the diplomatic and international legal stages. In party with other states, it had called out counter-terrorism as a key security issue to be addressed through legal norms or normative behaviours in cyberspace and was calling out the need to be prepared for 'information aggression'. China's experience reviewed above shows that APEC and a number of regional mechanisms (such as Japan-China-Korea trilateral) were more productive than the UN as a forum on cyberspace norms.

[65] Asia-Pacific Economic Cooperation, *2005 APEC Telecommunications and Information Ministerial Meeting, Lima Declaration* (1-3 June 2005), http://www.apec.org/Meeting-Papers/Ministerial-Statements/Telecommunications-and-Information/2005_tel.aspx.

[66] See United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: report of the Secretary-General*, A/60/202 (5 August 2005), 2, http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/453/63/PDF/N0545363.pdf?OpenElement.

[67] Andrey Krutskikh, 'Towards a Politico-Legal Foundation for Global Information Security,' *International Trends*, http://www.intertrends.ru/thirteen/003.htm [in Russian].

6. Higher Tempo: Cyber War more Central 2006-2013

China took a dramatic step in 2006 through its membership of the Shanghai Cooperation Organization (SCO) when it supported a declaration by it on information security.[68] This manifestation of China's strategic intent in normative debates on cyberspace included an assessment of the revolutionary impact of ICT on security: 'ICTs are shaping the global information environment, on which foundation rests the political, economic, defence, socio-cultural and other components of national security and of the entire system of international security and stability'. The statement expressed concern about a 'real danger that ICT would be used for the purposes of bringing serious harm to the security of the individual, society and states by breaching fundamental principles of equality and mutual respect, non-interference in internal affairs of sovereign states, the peaceful settlement of disputes, non-use of force, and the observance of human rights'. The signatories called for a range of unspecified measures at bilateral, multilateral and global levels to address the new threats.

This declaration was referred to in the final communique of the summit as 'Statement of Heads of State of Member States of the Shanghai Cooperation Organisation on International Information Security'.[69] The communique declared that 'Threats of a military-political, criminal or terrorist nature to information security constitute common challenges for all member states that need to be dealt with through prompt joint measures'. It noted that an SCO experts' panel had been 'entrusted with the task of producing a long-term plan of action for the maintenance of information security before the next Summit in 2007, including ways of solving this problem within the SCO framework'. One import of this was that the membership of the SCO (all authoritarian states) strongly identified with China's positions on most issues, especially the balance to be struck between state sovereignty and international openness. According to a later Russian study, the Heads of State agreed that the threats to international information security should be dealt with through the observance of international law.[70] (This presaged China's support for the same proposition in the 2013 report of the UN GGE report discussed later.)

In a statement to the UN in 2006, China went much harder on the need for states to respect the differences in political systems, asserting that understanding of the principle that the free flow of information 'should be guaranteed under the premises that national sovereignty and security must be safeguarded and that the historical, cultural and political differences among countries be

[68] *Declaration of the Heads of Member States of the Shanghai Cooperation Organization on International Information Security* (15 June 2006), http://www.sectsco.org/RU123/show.asp?id=107 [in Russian].

[69] 'Joint Communiqué of the Meeting of the Council of Heads of State of the Shanghai Cooperation Organization' (The Council of Heads of State of the Shanghai Cooperation Organization, Shanghai, 15 June 2006), http://www.china.org.cn/english/features/meeting/171590.htm.

[70] Berditskii, 'An International Agreement on Cyber Security: Is Consensus Possible?'

respected'.[71] It asserted its doctrine that there is a legally-bounded, sovereign cyberspace, a Chinese Internet: 'each country has the right to manage its own cyberspace in accordance with its domestic legislation'. It positively appraised the work of the GGE because it offered the opportunity for a 'profound exchange of ideas and offered numerous valuable proposals', even though it failed to produce a consensus report. It indicated its support for reconvening a similar group.

In 2006, the ASEAN Regional Forum (ARF), a cooperative security and preventive diplomacy forum for heads of states and/or foreign/defence ministers of the ASEAN states plus China, Russia, the US, Japan, North and South Korea and Australia, among others,[72] issued a statement on security in cyberspace, acknowledging the 'importance of a national framework for cooperation and collaboration in addressing criminal, including terrorist, misuse of cyberspace and encourage the formulation of such a framework'.[73] It recognised the 'serious ramifications of an attack via cyberspace to critical infrastructure on the security of the people and on the economic and physical well-being of countries in the region', as well as 'stressing the need for cooperation between governments and the private sector in identifying, preventing, and mitigating cyber-attacks'. The statement was largely focused on cyber crime and cyber terrorism, and it called on states to make necessary changes to domestic law enforcement as we cooperate internationally.

At the summit of SCO Heads of State in August 2007, the members signed a series of documents, among which was an 'SCO member countries' action plan to safeguard international information security'.[74] It committed them to 'work together to jointly address growing network and information security threats'. It expressed 'concern over the threat of using [information technology] for purposes inconsistent with the tasks of protecting international stability and security'. An SCO seminar in June has already raised the idea of creating a 'unitary Eurasian information space'[75] (an SCO Internet?).

In 2009, the SCO formally agreed a treaty on the subject.[76] This was the first international treaty on information security that specifically addressed the range of issues that had been canvassed in the annual UN resolutions 'in the context of international security' since the expanded version of 1999. Article 3 of the 2009 treaty commits the parties to cooperate to eliminate a wide range of threats; and 'to work up collective measures for the development of international legal norms in the area of limiting the proliferation and application of information weapons that create

[71] United Nations, General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security,* A/61/161.

[72] Bangladesh, Canada, European Union, India, Mongolia, New Zealand, Pakistan, Sri Lanka, and Timor-Leste.

[73] 'ASEAN Regional Forum, Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyberspace' (The Thirteenth ASEAN Regional Forum 2006, Kuala Lumpur, 28 July 2006), http://www.mofa.go.jp/region/asia-paci/asean/conference/arf/state0607-3.html.

[74] *Bishkek Declaration of the Heads of the Member States of the Shanghai Cooperation Organisation* (16 August 2007), http://www.sectsco.org/EN123/show.asp?id=92.

[75] See Shanghai Cooperation Organization, *Chronicle of main events at SCO in 2007*, 31 December 2007, http://www.sectsco.org/EN123/show.asp?id=97.

[76] Shanghai Cooperation Organization, *Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation.*

threats to defence preparedness, and national or collective security'. Annex 2 over three pages describes five categories of threat:

- Development and use of information weapons, and the preparation and conduct of information war;
- Information terrorism;
- Information crime;
- Use of a dominant position in information space to harm the interests and security of other countries; and
- Spreading of information impacting negatively on the socio-political and socio-economic systems, spiritual, moral and cultural environment of other countries.

Annex 1 carries definitions of 13 basic concepts, among which the most important is the overarching concept of 'international information security', defined as the 'maintenance of international relations excluding the breach of peaceful stability and the creation of a threat to the security of states and world society in the information space'.

Also in 2009, China and ASEAN signed a framework agreement on network and information security emergency response,[77] as a follow-up to their agreement in 2005 on ICT cooperation for development (the Beijing Declaration) and a related agreement in 2007.[78] The 2007 agreement had also set up an ASEAN-China experts group on network security. The two sides commenced an annual seminar on network security in 2009, meeting for the first time in China.

In 2010, China published a White Paper on the Internet in China, an event that came a full fifteen years after the technology began to be introduced into the country outside of its universities.[79] One of the primary motivations for publishing the White Paper was to set out the public values around use of the Internet. The White Paper affirms freedom of speech, democratic supervision of government policies and the citizens' constitutional right to know. In one of six main sections, China discussed its commitment to collaborate internationally in cyber security, referencing a number of its activities mentioned above.

It was in this 2010 White Paper that China staked out a more comprehensive vision of international order concerning the Internet. It said 'China supports the establishment of an authoritative and just international internet administration organisation under the UN system through democratic procedures on a worldwide scale'. It said China was looking for all countries to 'have equal rights in participating in the administration of the fundamental international resources of the

[77] China-ASEAN Coordination Framework for Network and Information Security Emergency Responses. See 'The Internet in China,' *English.news.cn*, June 8, 2010, http://news.xinhuanet.com/english2010/china/2010-06/08/c_13339232_8.htm. Text of this agreement does not appear to be readily available.

[78] See Association of Southeast Asian Nations, *Plan of Action to Implement the Beijing Declaration on ASEAN-China ICT Cooperative Partnership for Common Development*, http://www.asean.org/news/item/plan-of-action-to-implement-the-beijing-declaration-on-asean-china-ict-cooperative-partnership-for-common-development-2.

[79] China.org.cn, *Active International Exchanges and Cooperation*, http://www.china.org.cn/government/whitepaper/2010-06/08/content_20207975.htm.

internet', with a 'multilateral and transparent allocation system' to be established 'on the basis of the current management model'. It noted that the 'development of the internet industry brings with it a series of new scientific and moral problems'. It reaffirmed that China would share with other countries the 'opportunities brought by the development of the Chinese Internet industry', 'unswervingly stick to its opening-up policy, open the Chinese internet market in accordance with the law, welcome enterprises from other countries to enter the Chinese internet market', continue to abide by its general obligations and specific commitments as a WTO member, and 'protect the legitimate rights and interests of foreign enterprises in China'.

In 2010, a new UN GGE, constituted one year earlier with China participating, reached important agreements. First, on the threats, it concluded that there is 'increased reporting that states are developing ICTs as instruments of warfare and intelligence, and for political purposes'; and that 'uncertainty regarding attribution and the absence of common understanding regarding acceptable state behaviour may create the risk of instability and misperception'.[80] The GGE made the following recommendations 'for the development of confidence-building and other measures to reduce the risk of misperception resulting from ICT disruptions':

- Further dialogue among states to discuss norms pertaining to state use of ICTs, to reduce collective risk and protect critical national and international infrastructure;
- Confidence-building, stability and risk reduction measures to address the implications of state use of ICTs, including exchanges of national views on the use of ICTs in conflict;
- Information exchanges on national legislation and national information and communications technologies security strategies and technologies, policies and best practices;
- Identification of measures to support capacity-building in less developed countries; and
- Finding possibilities to elaborate common terms and definitions relevant to General Assembly resolution 64/25.[81]

In addition, the APEC Working Group on Telecommunications agreed in 2010 an action plan for 2010-2015 in which one of five streams was devoted to a 'safe and trusted ICT environment', with a focus on domestic policies: capacity-building, cyber security awareness, security initiatives with industry, safer online environments, and promotion of the Internet economy.[82]

[80] United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/65/201 (30 July 2010), 7, http://www.unidir.org/files/medias/pdfs/information-security-2010-doc-2-a-65-201-eng-0-582.pdf.

[81] Ibid, 8.

[82] 'TEL Strategic Action Plan: 2010-2015, 2010/TELMIN/024' (Asia-Pacific Economic Cooperation, 8th Ministerial Meeting on Telecommunications and Information Industry, Okinawa, 30-31 October 2010), http://www.apec.org/Meeting-Papers/Ministerial-Statements/Telecommunications-and-Information/2010_tel/ActionPlan.aspx.

China's preparedness to collaborate in international rule making for security in cyberspace was demonstrated when it supported the clause in the 2010 Beijing Convention calling on states to criminalise 'technical attack' on aircraft in flight or air traffic control systems.[83]

In January 2011, the US and China committed for the first time a Head of State level to work together on a bilateral basis on issues of cyber security, but this was a passing mention in a set of more than twenty additional issues listed in one long sentence that were judged less important than the substantial number already covered in the statement with some elaboration.[84] This relatively low public prominence for cyberspace issues belied the high importance that both sides privately attached to them, not least in China's case after the revelations the previous year about the US use of the Stuxnet worm. For the US, there was a rising concern about China's use of cyber espionage, especially activities that threatened the safe functioning of its national critical infrastructure.

In a 2011 speech to UN, China's disarmament ambassador Wang Qun acknowledged the transformative aspect of the influence of ICT on security: 'information and cyberspace security represents a major non-traditional security challenge confronting the international community. Effective response to this challenge has become an important element of international security'.[85] Use of the term 'non-traditional' has been a device used by Chinese leaders and officials to avoid giving the impression that the information age has totally transformed the traditional approaches to security. He went on to say that the international community should view this issue from the new perspective of 'a community of common destiny' and 'work together towards a peaceful, secure and equitable information and cyber space'. We can probably assume that this approach contrasts quite strongly with that of mainstream military strategists in China. (It is equivalent to the shift by the Soviet Union under Gorbachev to the idea of common security, a shift that was essential for ending the Cold War.) Wang advocated five principles, as set out in Table 3.

Of some note, Wang directly appealed for the rules of the road, a call heard earlier in the year from the US. Wang said:

> '[I]n this virtual space where traffic is very heavy, there is, hitherto, no comprehensive 'traffic rules'. As a result, 'traffic accidents' in information and cyberspace constantly occur with ever increasing damage and impact. Therefore, the development of international norms and rules guiding the activities in information and cyberspace has become an urgent task.'[86]

[83] *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation.*

[84] For related information, see Greg Austin and Franz-Stefan Gady, 'Cyber Detente between the United States and China,' *EastWest Institute* (2012), http://www.ewi.info/sites/default/files/ideas-files/detente.pdf.

[85] 'Speech by H.E. Ambassador Wang Qun at the First Committee of the 66th Session of the GA on Information and Cyberspace Security' (The First Committee of the 66th Session of the GA on Information and Cyberspace Security, New York, 20 October 2011), http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t869580.shtml.

[86] Ibid.

Table 3. China's normative principles for cyberspace (2011).

Peace
War avoidance, active preventive diplomacy, and promote the use of information and cyber technology in maintaining security; commit to non-use of information and cyber technology for hostile actions and non-proliferation of information and cyber weapons; while retaining the right of self-defence against 'threats, disturbance, attack and sabotage'; prevent a cyber arms race and settle disputes peacefully.

Sovereignty
States remain the main actor in governance of information and cyberspace; sovereignty and territorial integrity remain basic norms; countries should build a comprehensive and integrated national management system for all aspects of cyberspace; cyber technology should not be used as 'another tool to interfere in internal affairs of other countries'.

Balance between freedom and security
Uphold the rule of law to keep order in information and cyberspace; practicing power politics in cyberspace in the name of cyber freedom is untenable.

Cooperation
Interdependence of cyber networks ('interlink with each other and belong to different sovereign jurisdictions') means that 'no country is able to manage only its own information and cyber business' or 'ensure its information and cyber security by itself'; all countries need to work together.

Equitable development
Developed countries have an obligation 'to help developing countries enhance capacity in information and cyber technology and narrow the digital divide'.

In 2011, in order to promote such a policy agenda on the international stage, China and several other countries (Russia, Tajikistan and Uzbekistan) submitted to the United Nations General Assembly a proposal for an International Code of Conduct for Information Security.[87] The draft code calls on states to observe international law as set out in the UN Charter as well as 'universally recognised norms governing international relations that enshrine, inter alia, respect for the sovereignty, territorial integrity and political independence of all states'. The code also calls on states 'not to use information and communications technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies'.

Russia was the driving force behind this, not China, but it nevertheless represented a new level of international mobilisation by China. These proposals go close to matching those previously elaborated by Chinese representatives. This idea of common security received further expression in 2012 (not referencing information security in particular) in a speech by Vice Minister of Foreign Affairs Cui Tankai to the Asia Society in Hong Kong: 'we believe countries should build mutual trust and seek common security … Security at the expense of others will only make us less secure'.[88]

[87] United Nations, General Assembly, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, A/66/359 (14 September 2011), http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/496/56/PDF/N1149656.pdf?OpenElement.

[88] Wendy Tang, 'Cui: Toward 'Common Security' and Cooperation in the Asia Pacific,' *Asia Society*, July 5, 2012, http://asiasociety.org/hong-kong/cui-toward-common-security-and-cooperation-asia-pacific/.

In August 2011, a political commentator from the Chinese National Defence University observed:

> 'I think that first we should follow the basic norms of the Charter of the United Nations and other internationally recognised norms, establish and improve cyberspace theory around national interests and sovereignty with Chinese characteristics, build our own network warfare theory, develop a cyberspace policy and legal system with our own characteristics, and in the world support the principle of building a harmonious cyberspace.'[89]

In October 2012, a Chinese diplomat elaborated the same point differently, including a direct invocation of existing international law:

> 'Peaceful use of cyberspace benefits the interests of every country and the common interests of mankind. We call upon all countries to observe the UN Charter and universally recognised international laws and norms governing international relations, not to take advantage of their internet technologies and resources to jeopardise the national security of other countries, not to conduct hostile activities against other countries or threaten international peace and security, and not to research, develop or use cyber weapons.'[90]

Work on the Code of Conduct between Russia and China had proceeded in tandem with a series of discussions in various forums in 2012 on a draft UN Convention on Information Security which had been prepared by a group of Russian experts. China was actively involved in several of these forums to discuss the draft.[91] Track 2 discussions on China's approach to international legal norms for cyberspace also became more focused and productive by 2012, showing areas of agreement and disagreement between unofficial representatives of China and the US.[92]

In March 2013, China had to deal with an unusually robust set of public demands on it to curtail what the US saw as its malicious activities in cyberspace. The US National Security Adviser, Thomas Donilon, called on China to undertake a bilateral dialogue with the US to establish 'acceptable norms of behaviour in cyberspace'.

In June 2013, the GGE, with a Chinese representative participating, reached consensus that the rules of international law do apply in cyberspace and called for more development work on future norms and the promotion of confidence

[89] Liu Zenglian, 'How to Build the Network Border Defense,' *People's Forum*, August 19, 2011 [in Chinese].

[90] 'Statement at Budapest Conference on Cyber Issues' (Huang Huikang, Budapest Conference, Budapest, 4 October 2012), http://www.chinesemission-vienna.at/eng/zgbd/t977627.htm.

[91] Anastasia Matvejeva, 'The Concept of Freedom is Not Absolute,' *Gazeta.ru*, February 9, 2012, http://www.gazeta.ru/business/2012/02/09/3994965.shtml [in Russian].

[92] There were several forums for such meetings, including those organised between US think tanks and a range of counterparts in China. Those organised (separately) by the EastWest Institute and the Centre for Strategic and International Studies (CSIS) had begun in 2009. Those conducted by the EastWest Institute included contacts with the Central Military Commission, at the time China's highest decision-making body in strategic policy. The summary report of the CSIS meetings in 2012 is particularly illuminating. See Center for Strategic and International Studies (CSIS), *Bilateral Discussions on Cooperation in Cybersecurity*.

building.[93] The GGE also called out what this meant in terms of the application of norms of sovereignty, human rights and state responsibility. Key excerpts are here *verbatim*:

- 'The application of norms derived from existing international law relevant to the use of ICTs by States is an essential measure to reduce risks to international peace, security and stability'.
- 'Common understandings on how such norms shall apply to State behaviour and the use of ICTs by States requires further study'.
- 'Given the unique attributes of ICTs, additional norms could be developed over time.
- 'International 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 environment'.
- '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'.
- 'State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments'.
- 'States should intensify cooperation against criminal or terrorist use of ICTs, harmonise legal approaches as appropriate and strengthen practical collaboration between respective law enforcement and prosecutorial agencies'.
- 'States must meet their international obligations regarding internationally wrongful acts attributable to them'.

In the debate in the First Committee in October 2013, China's delegate presented an enriched picture of Chinese threat perception by referencing pre-emptive military strike while referring to earlier ideas, such as some countries using their dominant position in cyberspace to interfere in internal affairs of others, export controls on ICTs, and militarisation by some countries of cyberspace.[94] He reiterated the idea of common security: 'Cold War mentality and zero sum game theory is neither feasible nor tenable in the information space'. He advocated four principles and three measures.

[93] United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note by the Secretary-General*, A/68/98 (24 June 2013), http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

[94] 'Statement by the Chinese Delegation on Information and Cyber Security at the Thematic Debate at the First Committee of the 65th Session UNGA' (United Nations, New York, October 2013), http://www.un.org/disarmament/special/meetings/firstcommittee/68/pdfs/TD_30-Oct_ODMIS_China.pdf.

The principles were familiar:

- States should observe the UN Charter and not threaten each other in cyberspace;
- States should not use ICT dominance to interfere in other states affairs;
- There should be equitable and democratic governance of the Internet; and
- States should promote exchange of ICT for peaceful development across the digital divide.

The three measures were:

- '[D]evelop a set of universal and effective international norms and rules governing activities in information space';
- Make full use of the GGE to 'deepen mutual understanding and explore the international norms and rules'; and
- '[G]ive play to the leading role of governments', who have a leadership role domestically in stimulating private-public initiatives and multi-stakeholder approaches, while at the international level to drive cooperation in combating cyber crime and cyber terrorism, and in protecting critical information infrastructure.

The delegate then observed that China had an exemplary record in promoting global cooperation through its work in various global and regional organisations.

7. China Resets Its Cyber Ambitions 2014-2015: Norm Entrepreneurship Will Change

Starting from 2014, the pace of China's efforts around international legal norms in cyberspace has been the most intense since China joined the global information economy in 1993.[95] The quickening of pace can be traced to February 2014, when President Xi Jinping declared that China would do everything necessary to become[96] a cyber power and that there could be no national security without cyber security.

Key policy developments that demonstrate Xi's earnestness have been his call in September 2014 for China to develop a military strategy for cyberspace, and the delivery of elements of such a cyber concept (in broad terms) in May 2015 in

[95] This is the year China set up its first national body for the information economy, a technocratic policy group which eventually transformed itself through several iterations, expansion and political upgrading into the Central Leading Group for Informatisation and Cyber Security, a leadership group of the Communist Party and the State Council formally (re)constituted in 2014 and chaired by President Xi Jinping.

[96] Zhu Ningzhu, ed., 'Xi Jinping Leads Internet Security Group,' *English.news.cn*, February 27, 2014, http://news.xinhuanet.com/english/china/2014-02/27/c_133148273.htm.

'China's Military Strategy',[97] the first official document of its kind released in public with that title. The depth of the commitment was also revealed in a governmental restructuring to create the Cyberspace Administration of China, an organisation that was assigned to support the freshly reorganised Central Leading Group on Informatisation and Cyber Security, upgraded by Xi when he took it over at the time of the 'cyber power' announcement. We could reasonably conclude that these moves might have been accompanied by some adjustment in China's approach to international legal norms for cyberspace. For example, if China was now committed in public to joining the ranks of military cyber power powers, one might have expected its position to shift more toward accommodating the views of other major cyber military powers.

As this chapter was being completed, China played its strongest card yet in the diplomacy of cyber norms. In early September 2015, it sent the Politburo member with responsibility for China's non-military spy agencies, Meng Jianzhu,[98] to Washington for four days for official discussions to try to dampen controversies with the US about the norms of cyber espionage in advance of a state visit by President Xi Jinping.[99] This was the high point in direct official contact on the subject resulting from a robust diplomatic campaign by the US which reached a peak in March 2013 when National Security Adviser Thomas Donilon made public demands on China to abide by rules of the road prohibiting cyber espionage for commercial purposes.[100]

Just weeks earlier, the United Nations published the report of the fourth Group of Governmental Experts (GGE) on certain aspects of information and telecommunications affecting international security.[101] With Chinese representation in the GGE, this report marked a new high point in intergovernmental consensus on some related issues, including most importantly the endorsement of a range of possible 'voluntary, non-binding norms, rules or principles' for restraint in international cyber practices.

The 2015 GGE report reached an agreement on three important and potential 'voluntary non-binding norms' for state behaviour in cyberspace:

[97] The State Council Information Office of the People's Republic of China, *China's Military Strategy* (May 2015), Beijing, http://www.chinadaily.com.cn/china/2015-05/26/content_20820628.htm.

[98] Of special note, Meng controls the civilian spy agencies (Ministry of State Security for external intelligence and Ministry of Public Security for domestic intelligence). He does not control the main signals intelligence agency of China which sits in the People's Liberation Army, under the control of the Central Military Commission of the Chinese Communist Party (CCP). Meng is the Secretary of the Central Political and Legal Commission, one of the most powerful political bodies in the country because of its role is the protection of all aspects of the 'political and legal' system in the country.

[99] The White House, Office of the Press Secretary, *Readout of Senior Administration Officials' Meeting with Secretary of the Central Political and Legal Affairs Commission of the Communist Party of China Meng Jianzhu*, 12 September 2015, https://www.whitehouse.gov/the-press-office/2015/09/12/readout-senior-administration-officials-meeting-secretary-central.

[100] Greg Austin, 'Cybersecurity: The Toughest Diplomatic Challenge Is China's Weakness,' *The Global Journal*, April 5, 2013, http://theglobaljournal.net/article/view/1049/.

[101] United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174 (22 July 2015), http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

- States should not attack each other's critical infrastructure for the purpose of damaging it;
- States should not target each other's cyber emergency response systems; and
- States should assist in the investigation of cyber attacks and cyber crime launched from their territories when requested to do so by other states.[102]

These proposals represented important refinements of previous Chinese positions in UN forums in providing that states should be held accountable for acts that were more precisely defined than simply being against the UN Charter principles. At the same time, all three of these proposed norms had been foreshadowed in China's diplomatic activity in some way, principally in APEC beginning of 2001, with ASEAN after 2003, and in China's support for the formation of the Asia Pacific Computer Emergency Response Team (APCERT) in 2003 (at a meeting in Taipei).

In the first half of 2015, China made three other important advances in its approach to international legal practice for cyberspace. First, on 8 May, it concluded a formal agreement with Russia not to interfere unlawfully in each other's information resources and networks.[103] Second, China and the US agreed to negotiate a 'code of conduct' of some kind in cyberspace.[104] Third, though less important, in January, China had participated in tabling a slightly revised draft of the proposed code of conduct for cyberspace initially submitted to the United Nations in 2011.[105]

By signing the new bilateral agreement in May, China and Russia together appear to have pre-empted the advisory effect of the GGE report, and its recent predecessors, to give legal effect to some of the principles proposed. The bilateral agreement goes very close to constituting a formal military alliance in cyberspace, since it lays out a mutual obligation of assistance in the event of a wide range of cyber attacks.

The Russia/China agreement is the fulfilment of a decade of involvement by the two countries in cooperative measures on cyberspace governance, including through the Shanghai Cooperation Organization talks beginning in 2006. The new agreement formalises at a bilateral level the countries' proposal in the UN system for a code of conduct in cyberspace. The agreement is as much about that effort as it is about strengthening each other in the face of US cyber pre-eminence. Article one describes malicious use of cyberspace 'as a fundamental threat to international

[102] Ibid.

[103] For a text of the approved agreement, see Government of the Russian Federation, *Order of the Russian Government on signing the Agreement between the Government of the Russian Federation and the Government of the People's Republic of China.*

[104] The US Secretary of State, John Kerry, announced on 23 June 2015 the following: 'We believe very strongly that the US and China should be working together to develop and implement a shared understanding of appropriate state behavior in cyberspace, and I'm pleased to say that China agreed that we must work together to complete a code of conduct regarding cyber activities.' See John Kerry, U.S. Department of State, *The Strategic & Economic Dialogue / Consultation on People-to-People Exchange Closing Statements* (Washington DC: 2015), http://www.state.gov/secretary/remarks/2015/06/244208.htm. While Kerry implies that this was a US proposal, it appears to have been a Chinese proposal, flagged in the opening remarks several days earlier by China, rather than a US proposal, and it had been China's policy since 2011 at least.

[105] See United Nations, General Assembly, *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, A/69/723 (13 January 2015), https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.

security'. Article 4 only commits the two countries not to undertake actions like 'unlawful use or unsanctioned interference in the information resources of the other side, particularly through computer attack'.

This is not a commitment to refrain from all use of military cyber assets against each other. Article 4 only says that each country has an equal right of self-defence in cyberspace against 'unlawful use or unsanctioned interference in the information resources of the other side, particularly through computer attack'. Neither Russia nor China regards cyber espionage or preparations for war in cyberspace as 'unlawful' or 'unsanctioned'. Of some note, Article 6.2 commits both parties to protect the state secrets of the other in cyberspace, and references a prior bilateral treaty with that general effect dating from 24 May 2000. The Russia/China agreement in its totality may put some pressure on other states to follow suit in the diplomacy of military cyberspace cooperation.[106]

The preamble has extensive new language on the sovereignty principle, with both sides reaffirming that 'state sovereignty and the international norms and principles flowing from state sovereignty, extend to the conduct of states in their use of information and communications technologies and the jurisdiction of states over the information space, and in the same way, a state has sovereign rights to define and undertake state policy on questions connected with the information and telecommunications network of the Internet, including the maintenance of security'.

It should be noted that the idea of a 'code of conduct' long advocated by China and Russia is just another way of laying down a set of voluntary non-binding norms of the kind agreed by the GGE in 2015. In sharp contrast, the 2015 agreement with Russia delivers to China an alliance relationship to buttress its information security and support its capacity development as it keeps its sights on Xi's goal of China becoming a cyber power. Furthermore, as I have often argued, China's interests in economic security aspects of cyberspace may now be driving it to some accommodation with the US on normative behaviours. Thus, between 2014 and 2015, China could feel it was making headway both in its political contest with the US over cyber norms and in its quest to become a cyber power even if that meant winning some diplomatic battles and losing others.

8. Conclusion

China's approach to international legal norms for cyberspace has not changed fundamentally at least since 2002 when the country made its first major statement

[106] The agreement followed a Japan-US agreement on cyberspace cooperation in military affairs. Japan Ministry of Defense, *Joint Statement of the U.S.-Japan Cyber Defense Policy Working Group*, 30 May 2015, http://www.mod.go.jp/j/press/news/2015/05/30a_1.pdf.

on the subject in the UN General Assembly. There has been useful elaboration by China on some of the detail, especially concerning protection of critical infrastructure and emergency response, which contributed to the meeting of minds in the UN GGE in 2015.

One important change has been in China's sense of urgency in using such norms to restrain countries like the US from more rapid strengthening of what China sees as the US hegemonic position in cyberspace. The cause of this change is China's deepening sense of insecurity in cyberspace, both domestically and on the international stage. Even though the place of espionage in China's exploitation of cyberspace has also expanded dramatically since 2002, this represents no change in its approach to international legal norms for cyberspace. China's interests in international cooperation to protect critical cyber infrastructure and, separately, to counter terrorism in cyberspace have deepened. At the same time, China has been sending conflicting signals about how to strike a balance between sovereign rights for control of sensitive cyber technologies in the name of national security and norms that allow for continued deep integration in a globalised ICT industry and a global cyberspace. China's interest in using advanced ICTs, especially for domestic political control has deepened enormously, and this carries important implications for its positioning on international legal norms in cyberspace.

China's main international security concerns have been military cyber conflict and foreign interference in Chinese domestic networks for the promotion of political dissent. China's position has largely been one about which norms should apply and in what circumstances, while emphasising the need for discussions about new normative behaviour and possible new norms, including a possible code of conduct or treaty that is specific to the action of states in cyberspace. While recognising that the normative position China takes on certain issues (its interpretation of international law) is ethically distinguishable from those taken by the US and like-minded countries, or from those that various scholars including me might take, suggestions that China has not been prepared to engage or promote new norms, or that such negotiations must be a zero sum game,[107] are not ones I would support. Moreover, we need to recall that the normative differences between the US and the European Union are also significant, if not perhaps as big as those between the US and China.

There have been multiple sources of confusion about China's position: under-appreciation of the overriding importance to China of existential security needs in cyberspace; lack of clarity in discussion by Chinese participants in Track 2 meetings, and even in the GGE, between international legal norms and other norms; reliance on unofficial interlocutors who, while working for the Chinese government, have few qualifications to represent a formal view of the Chinese government; and

[107] See for example James A. Lewis, *Cyber War and Competition in the China-U.S. Relationship* (China Institutes of Contemporary International Relations, 2010), http://csis.org/files/publication/100510_CICIR%20Speech.pdf.

mistaking norm entrepreneurship (and its relentless propagandistic pursuit) in military affairs as the totality of China's position. A state's position on an international legal norm is only what the state's plenipotentiary representatives say it is.

By September 2015, there are increasing signs that China feels obliged to cooperate in cyberspace rather than risk the fabric of its economic ties. China's economy is almost certainly not immune from serious damage that could be brought on by a US cyber attack. In both countries, elements of the civil infrastructure dependent on the cyber domain (mobile communications, Internet, electricity grids, land lines, undersea cables, banking) are inter-mingled with military assets. In most countries, the mingling is so profound that it is called 'entanglement'. In broad terms, this characteristic is shared with all countries. But exactly just how this entanglement, and its impact on China's normative behaviour looks from Beijing's perspective is worthy of much deeper study.