ORF ISSUE BRIEF
NOVEMBER 2015
ISSUE NO. 114

The US-China Cyber-Agreement: Implications for India

ARINDRAJIT BASU

ABSTRACT This essay considers the implications of the new cyber-security agreement between China and the United States in terms of the evolution of an international legal regime governing the use of cyberspace. This agreement lays down the foundations for norm emergence in the arena, which could also carry implications for India by shaping the country's response and carving its path towards becoming a crucial international stakeholder in the cyberspace regime. As international relations today is characterised by an overwhelming lack of consensus on crucial issues ranging from the high seas to the climate, it is imperative that the progress made by China and the US be built upon and internalised by other states.

INTRODUCTION

The aftermath of Chinese President Xi Jinping's September 2015 visit to the United States[1] was marked by an abundance of discourse on, *inter alia*, the merits of the US-China cyber-security agreement.[2] The agreement was quickly dismissed by various foreign-policy pundits on grounds that it was "ambiguous",[3] "lacking teeth",[4] "missing essential aspects of a comprehensive agreement"[5] and thereby, an inconsequential diplomatic endeavor. Such criticisms, however, fail to appreciate the potential of the agreement in laying out a normative framework with positive implications not just for US-China relations but also for the emergence of universal rules for the regulation of cyberspace in the near future.

The use of the term "deal" in reference to the agreement has also led to misinterpretation of its nature and purpose. It is imperative to clarify at the outset that the agreement is not a binding bilateral legal instrument and, in its present form, exists only in the form of a White House Press Release (in English)[6] and a Chinese translation. Unlike, say, the Joint Comprehensive Plan of Action on Iran's nuclear programme,[7] the purpose of this agreement was not to lay down a

comprehensive set of rules for the regulation of state action in cyberspace. Expecting concrete rules to emerge at this heads of state summit imposes an unfair burden on both leaders. The agreement in itself is significant as it acknowledged the existence of certain issues by both states with regard to the use of cyberspace. It is certainly an attempt to work out the prospects that emerge with the establishment of this normative framework. This Brief will describe the salient features in the text of the agreement. It will then explain the significance of this agreement in terms of norm creation at the international level. Finally, it will explore what the emergence of this norm means for India by comparing it with its response to other international legal regimes.

THE AGREEMENT AT A GLANCE

In order to satisfactorily evaluate the merits of the agreement, it is necessary to scrutinise the semantics employed by the press release—a task which current responses to the agreement have failed to do, ending up either misinterpreting terms or engaging in selective reading.[8] The text can be broken down into four broad operative components.

First: Both states declared that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property or other business information, with the intent of providing competitive advantages to companies or commercial sectors. This declaration is crucial because China recognised,[9] for the first time, the difference between cyber espionage directed at military and political secrets and industrial espionage through the cyber-theft of business plans and intellectual power. As both states have declared that they will not conduct industrial espionage ("knowingly support cyber-enabled theft of intellectual property") it is clear that they explicitly outlaw this form of espionage without making any commitments regarding espionage for non-commercial purposes. For China, both forms of espionage were aimed at increasing national influence, which diluted the distinction between public and private gain.[10] In fact, as stated by former US National Security Agency Director Michael Hayden, a long-standing grudge harboured by the US was that the Chinese government was passing on information gathered through cyber-espionage to both state-run and private corporate enterprises. ("Look, you spy, we spy but you steal the wrong stuff".[11])Pundits are partially correct when they argue, that the lack of an explicit provision in the agreement outlawing espionage for non-commercial gains is a fatal flaw.[12] Yet, considering that both sides admittedly engage in widespread cyber-espionage, supposedly for purposes of national security, the concretisation of such a provision at this stage may be an unrealistic expectation. The absence of this provision, however, does not detract from the significance of the affirmation by China, of a distinction between industrial and non-industrial espionage.

The agreement does, however, include declarations outlawing cyber attacks and lays down measures to combat them. Both states recognised their mutual commitment to further identify and promote appropriate norms of state behavior in cyberspace within the international community. In that context, both countries also welcomed the July 2015 Report of the UN Group of Governmental Experts in the Field of Information and Telecommunications, (UN-GGE).[13] The UN-GGE Report lays down a comprehensive framework outlining norms for state behavior for the regulation of the legitimate use of cyberspace, suggests multiple confidence-building measures, and encourages cooperation towards capacity building in order to move towards a more equitable use of cyberspace. Both US and China were part of the UN-GGE and contributed to its 2015 Report.[14] The Report identifies existing and emerging threats in Section II.[15] These include attacks targeted against "critical infrastructure and associated information systems" of a state; the use of Information and Communication Technologies (ICTs) for terrorist purposes; and the diversity of malicious non-state actors including criminal groups who seek to exploit cyberspace with

varying motives. In Section III, it discusses various norms, rules and principles for responsible state behavior. These include not knowingly allowing their territory to be used for intentionally wrongful acts using ICTs; to cooperate for the exchange of information using ICTs; and to not knowingly support ICT activity contrary to the principles of International Law including humanity, necessity, proportionality and distinction.[16] In Section IV, it delineates various Confidence-Building Measures that states could adopt for a more sustainable use of cyberspace. These include creating procedures for mutual assistance in responding to incidents and addressing short-term problems; providing access to technologies necessary for ICT security; and facilitating cross-border cooperation that would address critical infrastructure vulnerabilities.[17]

In line with these confidence-building measures, in the cyber-security agreement, the US and China agreed that timely responses should be provided to requests for information and assistance concerning malicious cyber activities. They also agreed to cooperate with the other state to investigate cyber crimes, collect electronic evidence and mitigate malicious cyber activity emanating from their territories and provide updates to the other side on the status and results of investigations. The significance of this part of the agreement has been unfortunately ignored by pundits who have rather focused on the fact that the agreement limits itself solely to economic espionage. The fact that both countries agreed to cooperate and exchange information is in itself a significant feat in light of the prevailing mutual distrust between the two countries on security issues ranging from cyberspace to the high seas. While the scope of what is to be considered as "malicious cyber activities" has not been explicitly defined in the text of the treaty, the 2015 report of the UN-GGE outlines the existing and emerging threats with regard to the exploitation of cyberspace.[18] Till the codification of a universally recognised definition of "cyber attacks", the scope delineated by the UN-GGE Report is normatively sufficient to regulate the scope of cooperation envisaged in this agreement.

Finally, the two sides also created a senior experts group for further discussions on the topic and established a high-level bi-annual dialogue mechanism on fighting cyber crime, which is expected to review the timeliness and quality of requests for information and assistance with regard to malicious activity of concern. They also agreed to establish a hotline which could serve as an Emergency Measure in times of unprecedented escalation of issues. Many analysts question the credibility of the follow-up mechanisms as they distrust China's intentions to comply with them. So does US President Barack Obama, it would seem. In a media statement[19] made shortly after the issuance of the Press Release, Obama said,"The question now is: are words followed by actions? And we will be watching carefully to make an assessment as to whether progress has been made in this area." This would indicate that Obama is not deluded by China's promises of compliance. Instead, he has chosen to adopt the "Trust but Verify[20] approach undertaken by then President Ronald Reagan when he sought to normalise relations with the Soviet Union towards the end of the Cold War. The setting up of the hotline and regular dialogues give both nations an adequate platform to do so.

NORM CREATION FOR THE CYBERSPACE REGIME

The breakthrough in the agreement stems from the fact that it alters the normative realm within which future international discourse on cyber security will take place. Principles of public international law do not embody any restrictions on espionage and therefore have historically failed to distinguish between traditional and economic espionage.[21] Prior to this agreement, the United States was the lone voice in the case against economic espionage through cyber-theft. The fact that two critical states have acknowledged this distinction lays down the normative foundations for universal recognition in the future.

Experts identify three theoretical phases of the evolution of norms at the international level.[22] The

first phase, called "norm-emergence", is the recognition of the norm by a set of "critical states"(States who are either directly affectedby the issue at hand or have the requisite capacity to influence it.) After recognising this norm, the critical states seek to promote such norm at the international level by generating discourse, in a phase termed as "norm cascade". Finally, subsequent to the establishment of the legitimacy of the said norm at the international level, nations internalise these norms into State Policy either out of a desire to conform to peer pressure from other States or to increase international legitimacy. Scholars of international law[23] have also argued that the participation of states in a transnational legal process creates a normative and constitutive dynamic which could alter national interests and shape national identity upon the internalisation of the principles of international law into domestic legislation. This agreement marks the first phase of the emergence of an international norm prohibiting the misuse of cyberspace. Two critical states have publicly acknowledged the existence of issues that need to be resolved along with possible solutions as delineated by the UN-GGE Report. Thus the normative foundations for a sustainable international cyber-security regime have been laid.

As stated by former US Deputy Secretary of State Robert Zoellick, an international regime is sustained by a norm-sharing mechanism that establishes and enforces behavioral standards through the participation of what he calls international stakeholders.[24] International stakeholders, according to Zoellick, help to defend or create the international system.[25] With a vibrant democracy, a strong military, and diplomatic influences across many parts of the world, India has the capacity to become a prominent international stakeholder in the evolution of the cyberspace regime.[26] Over the past two decades, India has embraced economic growth and development while retaining its position as a champion of the developing world. It has shown its support for norm-building at the international level through its membership in regional organisations, engagement in both multilateral and bilateral agreements, and internalisation of norms that have emerged at the international level.[27] For example, the Indian government has stated that it has an "exemplary non-proliferation record" and "supports the highest non-proliferation standards and goals"[28] despite not being a signatory to the Non-Proliferation Treaties (NPT). India also shows evidence of its conformity with the nuclear non-proliferation regime by regularly expressing its concurrence and support of agreements such as the Missile Technology Control Regime which seeks to control the spread of sensitive nuclear technologies.[29] India has also contributed to the discourse and responded to the emergence of norms in the regime on the law of the seas.[30] India was one of the prominent developing countries which advocated for the establishment of a territorial sea of 12 miles and an Exclusive Economic Zone of 200 miles and a continental shelf to prevent the exploitation of resources in this zone by other sea-faring nations during the negotiations building up.[31] In accordance with the provisions of the United Nations Convention on the Law of the Seas (UNCLOS), India has also[32] satisfactorily concluded maritime boundary agreements with Sri Lanka, Indonesia, Maldives, Thailand and Indonesia. India must similarly shape and respond to norm emergence in the cyberspace regime. To do so effectively, India should not only contribute to multi-stakeholder oriented discourse overseas but also create an effective democratic space at home for debating cyber policies.[33]

CONCLUSION

This theoretical understanding of norm evolution does not claim to guarantee conformity with these standards or predict state behavior accurately. In this case, the letter of the agreement may be tailored to suit the interests of either party, selectively adhered to, or used as a bargaining chip in other spheres of Sino-American competition. However, that possibility alone does not negate the importance of this consensus. An analogy can be drawn with the

evolution of the international regimes on the Use of Outer Space and Nuclear Non-Proliferation. While international standards prevailing under both regimes have been crystallised into more concrete rules, they owe their genesis to recognition of and bilateral consensus on these issues between the USA and USSR in the 1960s and 1970s, even though the Cold War was then at its peak.[34] This agreement could be a similar hallmark that catalyses the concretisation of universal standards on cyber security. With the prevailing lack of consensus between the two powerhouses on a catena of issues ranging from maritime security to climate change, this agreement cannot be characterised as anything short of a normative leap in cyber diplomacy.

ABOUT THE AUTHOR

Arindrajit Basu is a researcher with ORF's Cyber Initiative.

ENDNOTES:

1. Jane Perlez, "Xi Jinping's US Visit", *The New York Times*, September 29, 2015, accessed October 31, 2015, http://www.nytimes.com/interactive/projects/cp/reporters-notebook/xi-jinping-visit.
2. "Fact Sheet: President Xi Jinping's State Visit to the United States", *The White House Office of the Press Secretary*, September 25,2015, accessed October 31,2015, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.
3. Jack Goldsmith, "What Explains the U.S.-China Cyber "Agreement"?", *Lawfare*, September 26, 2015, https://www.lawfareblog.com/what-explains-us-china-cyber-agreement.
4. Robert Lemos, "U.S.-China Cyber-Security Agreement Lacks Teeth, Has Holes", *e-Week*, September 30, 2015, http://www.eweek.com/security/u.s.-china-cyber-security-agreement-lacks-teeth-has-holes.html.
5. Joseph Steinberg, "10 Issues with the China-US Cybersecurity Agreement", *INC.edu*, September 27, 2015, http://www.inc.com/joseph-steinberg/why-the-china-us-cybersecurity-agreement-will-fail.htm.
6. Fact Sheet: President Xi Jinping's State Visit to the US" .
7. The Joint Comprehensive Plan of Action (JCPOA) (also referred to as the 'Iran Nuclear Deal' is an international agreement on the nuclear program of Iran signed in Vienna on 14 July 2015 by Iran, the P5+1 (the five permanent members of the United Nations Security Council—China, France, Russia, United Kingdom, United States—plus Germany), and the European Union. Its purpose was to limit the capability of Iran's Nuclear Program by laying out a roadmap for the reduction of centrifuges, which would increase the 'break-out 'time to operationalize a nuclear bomb. See Karen DeYoung and Carol Morello," The path to a final Iran nuclear deal: Long day and short tempers," *The Washington Post*, July 15,2015, accessed November 3,2015,https://www.washingtonpost.com/world/national-security/long-days-and-short-tempers-the-path-to-a-final-nuclear-deal/2015/07/15/bb90235c-2b1d-11e5-bd33-395c05608059_story.html.
8. Jack Goldsmith, for example, argues that the agreement is a mere reiteration of the long-stated US and Chinese positions without acknowledging the fact that the agreement does incorporate multiple follow-up mechanisms See Jack Goldsmith, "What Explains the U.S.-China Cyber "Agreement"?", *Lawfare*, September 26,2015, https://www.lawfareblog.com/what-explains-us-china-cyber-agreement.
9. Adam Segal, "Attribution Proxies and U.S.-China Cyber Security Agreement" *Council on Foreign Relations*, September 28, 2015, accessed October 31,2015, http://blogs.cfr.org/cyber/2015/09/28/attribution-proxies-and-u-s-china-cybersecurity-agreement/.
10. Adam Segal, "Attribution Proxies and U.S.-China Cyber Security Agreement".
11. Marc Hujer and Holger Stark, "Former NSA Director 'Shame on Us'" *Spiegel Online*, Mar 24,2014 , accessed October 31, 2015, http://www.spiegel.de/international/world/spiegel-interview-with-former-nsa-director-michael-hayden-a-960389-2.html.
12. Joseph Steinberg, "10 Issues with the China-US Cybersecurity Agreement" *INC.edu* September 27, 2015, accessed October 31, 2015 http://www.inc.com/joseph-steinberg/why-the-china-us-cybersecurity-agreement-will-fail.htm.
13. United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" (Item 93 of The Provisional Agenda, Seventieth Session of the General Assembly), July 22,2015 accessed October 31,2015http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.
14. United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", 16-17.

15. United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", 6.
16. United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", 7.
17. United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", 9.
18. United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", 6.
19. "US, China reach deal on cyber-theft amid hacking accusations," *RT*, September 26, 2015, accessed October 31, 2015, https://www.rt.com/usa/316539-us-china-deal-security/.
20. Frank Carlucci, "Remembering Reagan's Foreign Policy Legacy", *The Daily Caller*, September 15,2015, accessed October 31, 2015, http://dailycaller.com/2015/09/15/remembering-reagans-foreign-policy-legacy/.
21. Christopher.S.Yoo, "Cyber Espionage or Cyber War: International Law, Domestic Law, and Self-Protective Measures in *Cyberwar : Law and Ethics for Virtual Conflicts*, eds. Jens David Ohlin, Kevin Govern, Claire Finkelstein (Oxford, United Kingdom : Oxford University Press, 2015), 175-194.
22. Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change"4 *International Organizations* 52(1998):887-917.
23. Louis Henkin, *How Nations Behave* (2nd ed, New York, Council on Foreign Relations,1979); Harold Hongju Koh, "Why Do Nations Obey International Law?" *Yale L.J.* 106 (1996): 2995.
24. Robert Zoellick, "Whither China: From Membership to Responsibility?" (Remarks to National Committee on U.S.-China Relations, New York, September 21, 2005), accessed October 31, 2015, http://www.cfr.org/china/whither-china-membership-responsibility/p8916.
25. Robert Zoellick, "Whither China: From Membership to Responsibility?"
26. *See* Parminder Jeet Singh, "Why is India a Follower in Cyberspace when it can lead?" *The Wire*, July 7,2015,accessed October 31, 2015, http://thewire.in/2015/07/06/why-is-india-a-follower-in-cyberspace-when-it-can-lead-5568/.
27. Xavier Dormandy, "Is India, or Will it Be, a Responsible International Stakeholder?" 30 *Washington Quarterly 3*, (2007):119.
28. Shyam Saran, "Indo-U.S. Relations: An Agenda for the Future" (Remarks delivered to the Heritage Foundation, Washington D.C., March 30,2006), accessed October 31, 2015, http://www.heritage.org/events/2006/03/indo-us-relations-an-agenda-for-the-future.
29. Xavier Dormandy, "Is India, or Will it Be, a Responsible International Stakeholder?" *30 Washington Quarterly 3*,117-130 (2007).
30. G.M. Hiranandani, *Transition to Triumph: History of the Indian Navy 1965-1975* (New Delhi, Lancer Publishers,2000),347.
31. Hiranandani, *Transition to Triumph*, 350.
32. Hiranandani, *Transition to Triumph*, 351.
33. Arun Mohan Sukumar, "India's New 'Multistakeholder Line Could Be a Gamechanger in Global Cyberpolitics" *The Wire*, June 22,2015, accessed October 31, 2015, http://thewire.in/2015/06/22/indias-new-multistakeholder-line-could-be-a-gamechanger-in-global-cyberpolitics-4585/.
34. *See* Nick Miller, "U.S. Non-Proliferation policy is an invisible success story", *The Washington Post*, Oct 16,2014,accessed October 31, 2015 https://www.washingtonpost.com/blogs/monkey-cage/wp/2014/10/16/u-s-nonproliferation-policy-is an-invisible-success-story/and Bin Cheng, *Studies in International Space Law* (Clarendon Press, London, 1997).

Ideas • Forums • Leadership • Impact

ORF, 20, Rouse Avenue Institutional Area, New Delhi - 110 002, INDIA
Ph. : +91-11-43520020, 30220020. Fax : +91-11-43520003, 23210773
E-mail: contactus@orfonline.org
Website: www.orfonline.org