US-China Relations in Cyberspace: The Benefits and Limits of a Realist Analysis

https://www.e-ir.info/2016/08/28/us-china-relations-in-cyberspace-the-benefits-and-limits-of-a-realist-analysis/

ELIZABETH THOMAS, AUG 28 2016

Cybersecurity issues have increasingly been singled out as an irritant in the United States(US)-China bilateral relationship. US-China relations in cyberspace exemplify tensions in the broader bilateral relationship, canvassing military competition, trade barriers, intelligence activity, and pathways to long-term economic and political strength.[1] However, cybersecurity is still a nascent foreign policy issue. Much of the existing literature on cybersecurity in international relations addresses the issue through the lens of policy rather than theory.

This paper is a contribution to bridging the gap between policy and theory. It examines the extent to which offensive realist theory helps us understand how the US and China are managing their relations on cybersecurity. I argue that the US is a hegemon in cyberspace, and China a revisionist power. Based on that assessment, I consider the likelihood of cyberwar, the issue of economic espionage, their respective approaches to Internet governance, and conclude that offensive realism provides a useful framework for considering security-related issues. However, it cannot explain the full range of bilateral cyber-related activity, including examples of cooperation and norm-building in cyberspace. I briefly touch on liberal theories' ability to explain other elements of the relationship and conclude that given the breadth of cyber-related issues, an issue-specific or analytically eclectic approach may be the most fruitful.

The framework for analysis: offensive neorealism

Offensive realism refers to a sub-school of neorealist international relations theory, which developed from Kenneth Waltz's work on structural realism.[2] The classical realism of thinkers like Hans Morgenthau had focused on human nature.[3] Waltz shifted realism's focus to the international system, positing that the anarchic structure of the international system forces states to pursue power to ensure their survival. Power – measured by the relative distribution of economic and military capabilities across the system – is a state's only guarantee of security. Subsequently, sub-schools of defensive and offensive realism have developed based on Waltz's work.[4]

This paper focuses on the applicability of John J. Mearsheimer's offensive realism to US-China cybersecurity relations.[5] I have chosen offensive realism as the basis for my analysis because the relationship is popularly characterized as conflictual. Offensive neorealism posits that great powers seek to ensure their security by maximising their share of world power. Being the dominant power – a hegemon – is the best means to ensure survival. States therefore are "primed for offense".[6] Mearsheimer makes five key assumptions about the international system, which together cause states to formulate aggressive policies.[7] These are: (1) anarchy is the ordering principle of the international system; (2) great powers possess some military capability; (3) states can never be certain about other states' intentions; (4) survival is the primary goal of great powers; and (5) that great powers are rational actors.[8] I will treat these assumptions as given for the purposes of my analysis.

Combined, these factors result in three patterns of behaviour: fear, self-help, and power maximisation.[9] Unable to trust other states, and aware that they operate in a self-help system, states view becoming the most powerful states in the system as the best way to ensure survival.[10] States look to maximise their power and alter the balance of power using a variety of tools – even if doing so makes other states suspicious or hostile.[11] Capability is what

matters, given the intentions of other states are uncertain. States will lie, cheat and use force if it can help them gain an advantage.[12] All great powers will have revisionist tendencies until they achieve hegemony, resulting in constant security competition.[13] Finally, in Mearsheimer's view, multipolar systems are more likely to result in conflict than bipolar systems, and multipolar systems with an emerging hegemon are the most dangerous ("unbalanced multipolarity").[14]

What is the current balance of power in cyberspace?

In order to understand whether there is a security competition in cyberspace, it is necessary to assess the current balance of power. Because I am considering cybersecurity in isolation from the wider bilateral relationship this analysis necessarily will be artificial, focusing only on relative cyberpower (broadly defined). Mearsheimer defines a hegemon as a "state that is so powerful that it dominates all the other states in the system."[15] A state that is substantially more powerful than other powers in the system is not a hegemon – a hegemon is the only great power.[16] Mearsheimer concludes that it is virtually impossible for a state to become a global power because of the difficulties in projecting power across the world's oceans.[17]

However, the US arguably has hegemonic power in cyberspace, where geographic boundaries do not affect power projection. The US, thanks to its role in the Internet's creation and development, retains a huge amount of influence over its operations and governance. Ten of the Internet's 13 root servers are on US soil, and China, like many other states, is still reliant on technology from American firms like Microsoft.[18] Secondly, the US is generally believed to have the most significant cyber offensive capabilities in the world. While cyber capability is shrouded in secret, the US is likely to have a good chance at dominating other great powers in cyberspace.

The question is then whether there are any other great powers in cyberspace. China has arguably risen as a cyber power, though its (known) activities to date are computer-network exploitation for intelligence rather than attacks causing disruption.[19] China sees cyber power as a cost effective, long range way to counter a superior adversary in conflict.[20] China has also become increasingly influential in global policy debates on Internet governance issues, as will be discussed below. However, the US has considerably more experience in managing complex network operations and the Peoples' Liberation Army faces sizeable challenges implementing cyber tactics.[21]

Cyberspace also is not a simple bipolar world. Russia, for instance, is widely considered to be one of the most capable actors in cyberspace and is believed to have deployed offensive cyber capability in support of its wider objectives (most recently shutting down a power grid in the Ukraine). Cyber capabilities also are proliferating widely, in part because of low barriers to entry.[22] Cyberspace therefore can loosely be characterized as a multipolar system.

In an unbalanced multipolar system, we should expect to see an ongoing security competition, based on calculations of relative state power. The US will seek to check China's activity to maintain its hegemony. China, as an aspiring hegemon and revisionist power, will use force to alter the status quo if the benefits outweigh the costs.[23] The polarity of the system will make states fearful and security competition is likely to be particularly acute in the cyber context. The secrecy shrouding states' cyber capabilities makes it difficult to measure relative capability, which will increase suspicion.

A spiral of mistrust – should we expect the outbreak of cyberwar?

Relations between the US and China indeed have been marked by fear and mistrust. Growing concerns about competitive advantage have exacerbated that mistrust, along with ongoing intelligence activities and political rhetoric. China is suspicious that the US is using its dominance in cyberspace to undermine other states, which suggests a sense of vulnerability, and US has a deep sense of unease about a rising China.[24] Offensive realism suggests that how much states fear each other determines the severity of their security competition as well as the likelihood that they will fight a war.[25]

As signaled above, states cannot accurately assess their relative cyberpower because offensive cyber capabilities

tend to be highly classified. Fear has therefore driven both states to invest in offensive and defensive capabilities.[26] There is also an incentive for both to misrepresent their strength, so the true balance of power is unclear.[27] This may lead to a misperception of dominance, particularly when the effectiveness of 'cyberweapons' is poorly understood.[28]

However, a cyber conflict between the US and China is highly unlikely. Examples of attacks with destructive or physical consequences are still very rare (although the number may be increasing). Since the late 1980s, there have been 61 attacks conducted by states against during peacetime, and 24 during wartime.[29] Examples include Russian attacks on Georgia in 2008 and the infamous Stuxnet attack on Iranian nuclear infrastructure (usually attributed to the US and Israel).[30]

No state has ever declared a 'cyberwar'.[31] This is partly because to develop sophisticated attacks like Stuxnet is very difficult, requiring high levels of technical expertise.[32] Attribution is also notoriously difficult in cyberspace. It is extremely tough to trace attacks and states may also use proxy or non-state actors, further confusing the issue.[33] Until recently, the failure to develop an effective deterrence policy has been related to the difficulty in attributing cyberattacks.

Nevertheless, the US has "reserve[d] the right to use all necessary means – diplomatic, informational, military, and economic – as appropriate and consistent with applicable international law" to respond to hostile acts in cyberspace.[34] China has not used 'force' against the US in cyberspace but it is clear that cyberattacks would feature in any broader military clash. Difficulties arise in considering what constitutes a proportionate response to low-level attacks like hacking or cybercrime. It is very unlikely that any incident of that nature could justify a traditional military response.[35] To date, countermeasures have fallen well below the use of military force. The US has instead relied on diplomatic and law enforcement tools: attribution, indictments, and the threat of sanctions.[36]

Cyber-enabled espionage – a constant, low level conflict?

Intense security competition between the US and China is much more evident when considering the issue of cyber-enabled espionage. As a trading state, China has benefited from Internet connectivity, but it is still a net importer of advanced technology.[37] To maintain high growth levels in an innovation-driven world, economic espionage is a useful shortcut, and economic power is fungible.[38]

The US has consistently alleged that China is conducting economic espionage on a massive scale to support Chinese firms. Good evidence exists to support this allegation. For instance, one study found that "96 percent of recorded, state-affiliated attacks targeting businesses' trade secrets and other intellectual property in 2012 could be traced by to Chinese hackers."[39] While each loss might be small, the net effect has been described as "the most significant transfer of wealth in history."[40] In response, China has consistently accused the US of hypocrisy, supported by evidence in the Snowden disclosures of the extent to which the US had penetrated a range of Chinese companies and networks.[41] Chinese officials point out that China is the largest victim of cyber attacks in the world, many emanating from the US.[42]

In China's view, the US has no "moral standing" to make accusations against China or define norms of appropriate behaviour online.[43] Despite this, the US has attempted to draw a distinction between espionage for national security purposes and economic espionage for the benefit of a states' firms (such as China's state-owned enterprises). While China has historically refused to acknowledge this distinction, US policy has been calibrated both to develop this norm and to raise the costs of Chinese activity.

Until recently, actions in cyberspace had been largely penalty-free. Over the last two years, the US has executed the first steps in a new strategy to change the cost-benefit-risk calculus for its cyber adversaries.[44] In May 2014, the Department of Justice indicted of five members of the Chinese Peoples' Liberation Army (PLA) for hacking and commercial espionage against major US companies.[45] Following the high-profile hack of Sony pictures in December 2014, the US attributed the attack to North Korean actors – the first time that the US had publicly attributed an attack on a US company to a foreign government.[46] Then, in April 2015, President Obama signed an

executive order allowing the US to impose severe financial restrictions on individuals or entities who engage in or benefit from cyber-enabled economic espionage.[47] In advance of President Xi Jinping's first state visit to the US in 2015, there were serious indications that the Obama administration might impose sanctions against China in a second major volley on economic espionage.[48] Shortly before the visit, Obama described theft of intellectual property and trade secrets as an "act of aggression" and a "core national security threat".[49]

Despite previously refusing to accept the US distinction between 'acceptable' espionage for national security and 'unacceptable' economic espionage, President Xi reached a landmark agreement with President Obama in September 2015. The two leaders agreed that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[50][51] The agreement was an unexpected reversal of the Chinese position.

Offensive realism suggests that China may have signed the agreement for two reasons. Threatened with sanctions, China made a rational choice – the costs of cyber activity against the US were rising and it was in China's interest to agree. More pessimistically, China may also have signed with no intention of adhering to the agreement. Offensive realism suggests that concerns about cheating will hinder cooperation, as states fear that the other side will cheat, putting them at a disadvantage. [52] Subsequent evidence suggests that China is not complying with the agreement. The Director of National Intelligence noted in February 2016 that "China continues to have success in cyber espionage against the U.S. government, our allies, and U.S. companies."[53]

Continuing Chinese activity suggests that the US has not succeeded in raising the real costs of economic espionage. The costs of an indictment and the threat of sanctions are slight in comparison to the benefits China is reaping from its economic espionage practices.[54] Cheating on a cyber agreement may also be simpler because deception is a core part of network intrusions.[55] As long as the benefits to China outweigh the risks, there is no reason to stop. For the US, it appears that more significant punishments may be too costly or escalatory to pursue.[56] Some of this reluctance likely derives from concerns about damaging relations with a state with a major economic market.[57]

Internet governance and China as a revisionist power

As discussed earlier, part of what facilitates US hegemony in cyberspace is the economic gains it realises and its influence on global Internet governance issues. To date, the US has set the terms for Internet governance[58] and key organisations often are seen as "captive to US interests."[59] The global Internet governance system is also closely aligned with the US vision of "an open, interoperable, secure, and reliable" Internet that supports global commerce, strengthens international security and fosters free expression and innovation.[60] Internet governance is currently based on a multi-stakeholder model with states, civil society, technical experts and private companies all working together. Internet governance currently tends to reinforce the US' economic competitiveness, and works indirectly to realize a US vision of a liberal, integrated world founded on an open internet.[61] The Internet is a platform for expanding free market commerce and free speech, and for information and economic exchanges.[62]

In contrast, Chinese cyber foreign policy is premised on an interpretation of the United Nations (UN) system as protecting absolute sovereignty, which stops other states from interfering in its domestic political affairs.[63] This approach, along with a perception of excessive US influence, has shaped China's proposals for Internet governance reforms. Based on a principle of "Internet sovereignty", China is promoting an agreement that states refrain from interference of any kind with another state's cyberspace, and a proposal that the Internet be run by a multilateral international forum.

China's proposed Internet governance reforms would bolster the role of governments in Internet governance. The US and others fear that increasing governmental authority in cyberspace would legitimate authoritarian control, and could result in the balkanisation of cyberspace along territorial lines.[64] The Internet governance debate reflects two different visions for global political order. Offensive realism characterises the international order at any time as largely resulting from the self-interested actions of the great powers.[65] Currently, that order reflects US interests, while China's recent diplomatic efforts comprise an effort to revise the system. China is perhaps "best seen as the

most assertive and the most potent of a new of new powers that challenge the existing international order and the American role in it."[66]

The limitations of offensive realism

While offensive realism can help characterize the security competition between the US and China, it does not adequately account for a range of related cybersecurity issues. One of the key challenges in considering cybersecurity is that the concept encompasses a wide range of overlapping issues – not only security, but also economic, political, social and cultural issues. As a result, more than one international relations theory is required to help explain the entire US-China cybersecurity relationship. As a counterpoint to the offensive realist analysis above, I shall briefly highlight how liberal theories can contribute.

Liberalism is very broad school of thought, but its contributions are likely to provide another valuable tool for understanding relations in cyberspace, especially given its insistence that the economy matters as much as security. China and the US are highly economically interdependent, so the trade elements of the relationship should not be neglected. For example, there have been signs of declining interest in bilateral trade and investment in the technology sector because of China's new cybersecurity laws requiring companies to comply with contentious policies such as installing backdoors in software.[67] Other key contributions include acknowledging the importance of domestic political factors in determining states' international behaviour and the role of institutions in establishing rules for state behaviour.[68] I will briefly address each of these in the context of US-China relations.

The domestic landscape is ignored by neorealism but it is critical to understanding China's Internet governance policies. Increased Internet uptake in China (now around 618 million Internet users) provides a platform for dissenting voices and challenges to the Chinese Communist Party regime's legitimacy.[69] For China, control of the Internet and flows of information through its extensive censorship regime is not a human rights violation, but a necessary tool for political stability.[70] Risk of political interference and subversion means that China takes a highly regulated approach to its domestic Internet (including the "Great Firewall)."[71] So while the US defines cybersecurity in terms of technical threats, China includes ideological threats and the control of information content.[72] China's push to strengthen the role of states in controlling cyberspace cannot be understood without considering its domestic concerns.[73]

Finally, offensive realism is very sceptical of the impact of norms and institutions on the international system – these are seen as vehicles for the interests of the powerful. Cooperation also is limited because states do not seek mutual security.[74] However, there are clear examples of cooperative activity, including through institutions, evident in the US-China relationship. Both the US and China have a formal position that security in cyberspace can only be achieved through international cooperation.[75] For instance, both states have been engaged in creating regional cyber confidence-building measures in the ASEAN Regional Forum (ARF).[76] There has also been a concerted effort by both the US and China to help develop norms of online behaviour, in particular through a UN Group of Governmental Experts (GGE) process kicked off in 2010. Defensive realism can offer a more nuanced picture of cooperation (if states are happy to live with the status quo), but liberalism, in particular neoliberal institutionalism, is likely to have greater explanatory power in this context.

Conclusion

The overriding feature of cyberspace is its complexity. Cybersecurity policy incorporates a web of linked security, economic and social issues. A focus on cyberspace therefore highlights both the deep economic interdependence between China and the US, as well as the rivalry and lack of trust on security issues.[77] Offensive realism provides a useful framework for considering the national security rivalry in cyberspace and illuminates the current security competition. However, neorealism fails to capture the full range of issues that affect cybersecurity relations. Other approaches will be required. Aspects of liberal theories can help explain factors such the impact of domestic policies. The nature of engagement in cyberspace (and the construction of cyberspace itself) is also amenable to constructivist analysis.

Accordingly, to understand US-China cybersecurity relations in their entirety is likely to require an analytically eclectic approach to international relations theory. An eclectic approach also is likely to be the most useful for policymakers in both countries who are seeking to understand how state behaviour will be shaped by both the "incentives of the anarchic structure of world politics, as well as the economic potential of interdependent networks".[78]

[1] James A. Lewis, "Cyber War and Competition in the China-U.S. relationship." Remarks delivered at the China Institute of Contemporary International Relations, May 13 2010, 1. Last accessed May 5 2016. http://csis.org/publication/cyber-war-and-competition-china-us-relationship

[2] See Kenneth Waltz *Theory of International Politics* (Reading, MA: Addison-Wesley, 1979).

[3] See Hans Morgenthau, *Politics Among Nations: The Struggle for Power and Peace*, 5th ed. (revised) (New York: Alfred Knopf, 1978).

[4] Defensive realists argue that too much power is counterproductive and security results from maintaining a balance of power.

[5] John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York and London: W.W. Norton & Company, 2001).

[6] *Ibid.*, 3.

[7] *Ibid.*, 29.

[8] *Ibid.*, 31-32.

[9] *Ibid.*, 32.

[10] *Ibid.*, 33.

[11] *Ibid.*, 34.

[12] *Ibid.*, 35.

[13] *Ibid.*, 2.

[14] *Ibid.*, 5.

[15] Ibid., 40.

[16] *Ibid.*

[17] *Ibid.*, 41.

[18] Jon R. Lindsay, "China and Cybersecurity: Controversy and Context", in*China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain*, eds. Jon R. Lindsay, Jai Ming Cheung and Derek S. Reveron. (New York: Oxford University Press, 2015), 3.

[19] Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," *International Security* 39:3 (Winter 2014/15), 33.

[20] *Ibid.*, 29-30.

[21] Jon R. Lindsay, "Conclusion: The Rise of China and the Future of Cyberspace," in*China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain*, eds. Jon R. Lindsay, Jai Ming Cheung and Derek S. Reveron. (New York: Oxford University Press, 2015), 344-5.

[22] For example, Australia announced in April 2016 that it will develop offensive cyber capabilities. See https://cybersecuritystrategy.dpmc.gov.au/.

[23] Mearsheimer, 2.

[24] Simon Hansen, *Special Report: Australia-China relations in the next Internet era* (Canberra, Australian Strategic Policy Institute, 2015), 7.

[25] Mearsheimer, 42.

[26] Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," 35.

[27] Jon R. Lindsay, "Tipping the scales: The attribution problem and the feasibility of deterrence against cyberattack," *Journal of Cybersecurity,* 0:0 (2015), 3.

[28] Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction, 37 & 46.

[29] Robert Morgus, "Rules of Cyber Engagement," *Slate.com*, March 10 2016, accessed March 15 2016. http://www.slate.com/articles/technology/future_tense/2016/03/the_fuzzy_international_rules_for_war_in_cyberspace.html

[30] See for example https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ for more detail on Stuxnet.

[31] Morgus.

[32] P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014): 154.

[33] Morgus.

[34] United States Government, "International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World," May 2011, 14.

[35] James A. Lewis, "Indictment, Countermeasures and Deterrence," March 25 2016, last accessed May 2 2016. http://csis.org/publication/indictments-countermeasures-and-deterrence.

[36] *Ibid.*

[37] James A. Lewis, "Economic Warfare and cyberspace," ASPI Special Report (Canberra: Australian Strategic Policy Institute, 2014), 3.

[38] Singer and Friedman, 94.

[39] *Ibid* .,95.

[40] Quoted in Malcolm R. Lee, "Will the United States impose cyber sanctions on China?" September 22 2015, last accessed May 2 2016. http://www.brookings.edu/blogs/order-from-chaos/posts/2015/09/22-will-us-impose-cyber-sanctions-china-lee.

[41] Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," 7-8.

[42] Singer and Friedman, 140.

[43] Roger Hurwitz, "The State of Play: Norms and Security in Cyberspace," *American Foreign Policy Interests* 36:5 (2014), 329.

[44] Lewis, "Indictment, Countermeasures and Deterrence". This approach has not only been demonstrated against China, but also in the May 2016 indictment of seven hackers associated with the Iranian government for hacking to disrupt key US industries, and in sanctions applied to North Korean officials following the December 2014 Sony pictures hack. The US is yet to take any action against Russia.

[45] See https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[46] Ellen Nakashima, "U.S. attributes cyberattack on Sony to North Korea," *The Washington Post*, December 19 2014, last accessed May 2 2016. https://www.washingtonpost.com/world/national-security/us-attributes-sony-attack-to-north-korea/2014/12/19/fc3aec60-8790-11e4-a702-fa31ff4ae98e_story.html

[47] See https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf.

[48] See for example Ellen Nakashima, "US developing sanctions against China over cyberthefts"*The Washington Post* August 30 2015, last accessed May 2 2016. https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html

[49] Quoted in Lee.

[50] The White House, "FACT SHEET: President Xi Jinping's visit to the United States," September 25 2015, last accessed May 2 2016. https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

[51] The prohibition on commercial espionage was replicated in a joint statement between the United Kingdom and China a month later, and by the G20 in November 2015.

[52] Mearsheimer, 52.

[53] James A. Clapper, quoted in Franz-Stefan Gady, "Top US Spy Chief: China Still Successful in Cyber Espionage Against US," *The Diplomat*, February 16 2016, last accessed May 2 2016. http://thediplomat.com/2016/02/top-us-spy-chief-china-still-successful-in-cyber-espionage-against-us/

[54] Jack Goldsmith, "China and Cybertheft: Did Action Follow Words?" *Lawfare Blog*, March 18 2016, last accessed May 2 2016. https://www.lawfareblog.com/china-and-cybertheft-did-action-follow-words

[55] Lindsay, "Tipping the scales",3.

[56] *Ibid*., 2.

[57] Lewis, "Economic Warfare and cyberspace," 6.

[58] Nazli Choucri, *Cyberpolitics in International Relations* (Cambridge, MA: The MIT Press, 2012): 183; 230.

[59] Singer and Friedman, 30.

[60] United States Government, "International Strategy for Cyberspace: Prosperity, Security and Openness in a

Networked World," May 2011, 8.

[61] Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," 43.

[62] Ryan David Kiggins, "US Leadership in Cyberspace: Transnational Cyber Security and Global Governance," in *Cyberspace and International Relations: Theory, Prospects and Challenge*, eds. Benedikt Muller and Jan-Frederik Kremer (Berlin: Springer, 2004), 163.

[63] Liselotte Odgaard, *The Balance of Power in Asia-Pacific Security: US-China Policies on Regional Order* (London and New York: Routledge, 2007): 196; 220.

[64] Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," 13.

[65] Mearsheimer, 49.

[66] Lewis, "Economic Warfare and cyberspace," 7.

[67] Hansen, *Special Report: Australia-China relations in the next Internet era*, 14.

[68] Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?" *International Political Science Review* 27:3 (2006), 230.

[69] Simon Hansen, "China's emerging cyberpower: Elite discourse and political aspirations," ASPI Special Report (Canberra: Australian Strategic Policy Institute, 2014), 14.

[70] Singer and Friedman, 107.

[71] Hansen, *Special Report: Australia-China relations in the next Internet era*, 15-16.

[72] Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," 15.

[73] Hansen, "China's emerging cyberpower", 19.

[74] Robert Jervis, "Realism, Neorealism, and Cooperation: Understanding the Debate," *International Security* 24:1 (1999), 48.

[75] Greg Austin, "2015 is the year of Chinese cyber power," *East Asia Forum*. July 31 2015, last accessed April 6, 2016. http://www.eastasiaforum.org/2015/07/31/2015-is-the-year-of-chinese-cyber-power/

[76] Christopher M.E. Painter, Testimony before the Senate Foreign Relations Committee Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy, May 14 2015. Last accessed May 5 2016. http://www.foreign.senate.gov/download/051415_Painter_Testimony

[77] Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," 45.

[78] Lindsay, "China and Cybersecurity: Controversy and Context", 21.

References

Austin, Greg. "2015 is the year of Chinese cyber power," East Asia Forum. July 31 2015, last accessed April 6, 2016. http://www.eastasiaforum.org/2015/07/31/2015-is-the-year-of-chinese-cyber-power/.

Choucri, Nazli. Cyberpolitics in International Relations. Cambridge, MA: The MIT Press, 2012.

Eriksson, Johan and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?" International Political Science Review 27:3 (2006): 221-244.

Gady, Franz-Stefan. "Top US Spy Chief: China Still Successful in Cyber Espionage Against US," The Diplomat, February 16 2016, last accessed May 2 2016. http://thediplomat.com/2016/02/top-us-spy-chief-china-still-successful-in-cyber-espionage-against-us/.

Gertz, Bill. "China Continuing Cyber Attacks on U.S. Networks," March 18 2016, last accessed May 2 2016. http://freebeacon.com/national-security/china-continuing-cyber-attacks-on-u-s-networks/.

Goldsmith, Jack. "China and Cybertheft: Did Action Follow Words?" Lawfare Blog, March 18 2016, last accessed May 2 2016. https://www.lawfareblog.com/china-and-cybertheft-did-action-follow-words.

Hansen, Simon. Special Report: Australia-China relations in the next Internet era. Canberra, Australian Strategic Policy Institute, 2015.

Hansen, Simon. "China's emerging cyberpower: Elite discourse and political aspirations," ASPI Special Report. Canberra: Australian Strategic Policy Institute, 2014.

Hurwitz, Roger. "The State of Play: Norms and Security in Cyberspace," American Foreign Policy Interests 36:5 (2014): 322-331.

Jervis, Robert. "Realism, Neorealism, and Cooperation: Understanding the Debate," International Security 24:1 (1999): 42-63.

Kiggins, Ryan David. "US Leadership in Cyberspace: Transnational Cyber Security and Global Governance," in Cyberspace and International Relations: Theory, Prospects and Challenge, eds. Benedikt Muller and Jan-Frederik Kremer. Berlin: Springer, 2004: 169.

Lee, Malcolm R. "Will the United States impose cyber sanctions on China?" September 22 2015, last accessed May 2 2016. http://www.brookings.edu/blogs/order-from-chaos/posts/2015/09/22-will-us-impose-cyber-sanctions-china-lee.

Lewis, James A. "Cyber War and Competition in the China-U.S. relationship." Remarks delivered at the China Institute of Contemporary International Relations, May 13 2010. Last accessed May 5 2016. http://csis.org/publication/cyber-war-and-competition-china-us-relationship.

Lewis, James A. "Economic Warfare and cyberspace," ASPI Special Report. Canberra: Australian Strategic Policy Institute, 2014.

Lewis, James A. "Indictment, Countermeasures and Deterrence," March 25 2016, last accessed May 2 2016. http://csis.org/publication/indictments-countermeasures-and-deterrence.

Lindsay, Jon R. "China and Cybersecurity: Controversy and Context", in China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain, eds. Jon R. Lindsay, Jai Ming Cheung and Derek S. Reveron. New York: Oxford University Press, 2015: 1-28.

Lindsay, Jon R. "Conclusion: The Rise of China and the Future of Cyberspace," in China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain, eds. Jon R. Lindsay, Jai Ming Cheung and Derek S. Reveron. New York: Oxford University Press, 2015: 353-355.

Lindsay, Jon R. "The Impact of China on Cybersecurity: Fiction and Friction," International Security 39:3 (Winter 2014/15): 7-47.

Lindsay, Jon R. “Tipping the scales: The attribution problem and the feasibility of deterrence against cyberattack,” Journal of Cybersecurity, 0:0 (2015): 1-15.

Mearsheimer, John J. The Tragedy of Great Power Politics. New York and London: W.W. Norton and Company, 2001.

Morgus, Robert. “Rules of Cyber Engagement,” Slate.com, March 10 2016, accessed March 15 2016. http://www.slate.com/articles/technology/future_tense/2016/03/the_fuzzy_international_rules_for_war_in_cyberspace.html.

Nakashima, Ellen. “U.S. attributes cyberattack on Sony to North Korea,” The Washington Post, December 19 2014, last accessed May 2 2016. https://www.washingtonpost.com/world/national-security/us-attributes-sony-attack-to-north-korea/2014/12/19/fc3aec60-8790-11e4-a702-fa31ff4ae98e_story.html.

Nakashima, Ellen. “U.S. developing sanctions against China over cyberthefts.” The Washington Post August 30 2015, last accessed May 2 2016. https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html.

Odgaard, Liselotte. The Balance of Power in Asia-Pacific Security: US-China Policies on Regional Order. London and New York: Routledge, 2007.

Painter, Christopher M.E. Testimony before the Senate Foreign Relations Committee Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy, May 14 2015. Last accessed May 5 2016. http://www.foreign.senate.gov/download/051415_Painter_Testimony.

Singer, P.W. and Friedman, Allan. Cybersecurity and Cyberwar: What Everyone Needs to Know. New York: Oxford University Press, 2014.

The White House, “FACT SHEET: President Xi Jinping’s visit to the United States,” September 25 2015, last accessed May 2 2016. https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

Written by: Elizabeth Thomas
Written at: The Australian National University
Written for: Dr Benjamin Zala
Date written: June 2016