2014-12

A rising China: shifting the economic balance of power through cyberspace

Kihara, Stacy A.

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A RISING CHINA: SHIFTING THE ECONOMIC BALANCE OF POWER THROUGH CYBERSPACE

by

Stacy A. Kihara

December 2014

Thesis Advisor: Carolyn Halladay
Co-Advisor: Wade L. Huntley

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2014	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
A RISING CHINA: SHIFTING THE ECONOMIC BALANCE OF POWER THROUGH CYBERSPACE

5. FUNDING NUMBERS

6. AUTHOR(S) Stacy A. Kihara

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

The growing evidence of Chinese government complicity in commercial cyber espionage and theft of intellectual property, costing the United States billions of dollars, has blurred the distinction between the geopolitical and economic realms, complicating an already complex relationship. Yet, China's cyber activity takes place in the context of an extensive economic interdependence between the two countries that may be seen as a source of stability in the relationship. Taking into consideration the economic interdependence between the United States and China, the rise of China as a potential global power, and the threat of state-sponsored malicious cyber activity, the major question driving this thesis is: What does China's cyber behavior tell us about the role of economic interdependence in U.S.-China relations? This thesis applies the complex interdependence framework to demonstrate that China has systematically conducted cyber-enabled economic espionage against the United States in an effort to shift the economic balance of power. Furthermore, this thesis shows China's ability to use asymmetric interdependence as a source of power and instrument of political coercion and prove its willingness to use these instruments against the United States. Finally, this thesis reasons that if China continues its persistent cyber espionage campaign, it would indicate that the potential costs of its cyber programs outweigh the benefits of its relationship with the United States.

14. SUBJECT TERMS China, Economic Interdependence, Complex Interdependence, Cyberspace, International Relations, Economic Espionage, Intellectual Property, Economic Growth, U.S.-China Relations, Balance of Power, Internet, Indigenous Innovation, Economic Rebalancing.

15. NUMBER OF PAGES 125

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01-280-5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

A RISING CHINA: SHIFTING THE ECONOMIC BALANCE OF POWER THROUGH CYBERSPACE

Stacy A. Kihara
Major, United States Air Force
B.A., St. John's University, 1997

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2014**

Author: Stacy A. Kihara

Approved by: Carolyn Halladay
Thesis Advisor

Wade L. Huntley
Co-Advisor

Mohammed M. Hafez
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The growing evidence of Chinese government complicity in commercial cyber espionage and theft of intellectual property, costing the United States billions of dollars, has blurred the distinction between the geopolitical and economic realms, complicating an already complex relationship. Yet, China's cyber activity takes place in the context of an extensive economic interdependence between the two countries that may be seen as a source of stability in the relationship. Taking into consideration the economic interdependence between the United States and China, the rise of China as a potential global power, and the threat of state-sponsored malicious cyber activity, the major question driving this thesis is: What does China's cyber behavior tell us about the role of economic interdependence in U.S.-China relations? This thesis applies the complex interdependence framework to demonstrate that China has systematically conducted cyber-enabled economic espionage against the United States in an effort to shift the economic balance of power. Furthermore, this thesis shows China's ability to use asymmetric interdependence as a source of power and instrument of political coercion and prove its willingness to use these instruments against the United States. Finally, this thesis reasons that if China continues its persistent cyber espionage campaign, it would indicate that the potential costs of its cyber programs outweigh the benefits of its relationship with the United States.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

FBI	Federal Bureau of Investigation
FDI	foreign direct investment
FYP	five-year plan
GAO	Government Accounting Office
GDP	gross domestic product
HPSCI	House Permanent Select Committee on Intelligence
IMF	International Monetary Fund
IP	intellectual property
IR	international relations
LOC	lines of communication
MLP	Medium to Long-Term Plan for the Development of Science and Technology
OSD	Office of the Secretary of Defense
PLA	People's Liberation Army
PPP	purchasing power parity
PRC	People's Republic of China
REE	rare earth element
R&D	research and development
RMB	Renminbi
WTO	World Trade Organization

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Although the thesis is just a portion of the graduate education I received at Naval Postgraduate School, it became a labor of love for me. I was lucky enough to have family, friends, and advisors who encouraged and supported me throughout this academic process and to which I owe a debt of gratitude.

I would like to give a sincere thank-you to Dr. Robert Looney for the considerable help and guidance he provided me on this thesis. It was during his Global Economic Relations class that I really became interested in the economic relationship between the United States and China, and was able to turn the subject into a premise for a thesis. Chapter II would not have been possible without his guidance, support, and remarkable expertise.

I would also like to thank my co-advisor, Dr. Wade Huntley, for his assistance. He introduced me to the concept of complex interdependence. When I presented a proposal, he guided me to the analytical framework that made my thesis possible.

Additionally, I would like to offer a special thank-you to Dr. Carolyn Halladay for the guidance and assistance throughout the thesis process and my educational journey at NPS. She was a perfect match as my advisor, immediately understanding my personality, and helping me use it to my advantage. Her support and counsel allowed me to find a topic I was truly interested in and turn it into a thesis I am proud to have written.

Last, but certainly not least, thank you to my amazing husband and children. This thesis and my success at NPS would not have been possible without their unwavering support. My husband, Shane, had the toughest job of all, staying home with our babies, yet he always found time to read my papers, listen to my ideas, and walk every step through this thesis process with me. I don’t know many partners that would do their own independent research to make sure they understood the thesis topic enough to provide valuable feedback. His dedication to my success and our family is incredible, and I can never thank him enough. Finally, I would like to thank Scarlett and Sai, the little loves of

my life. They pushed me without even knowing that and kept me going when I wanted to quit. I only hope that I inspire them as much as they both inspire me.

I. INTRODUCTION

In an environment of greater global economic interdependence, astounding technological advancement, the challenge of U.S. hegemony with the rise of new global superpowers, and the ease with which conflict and war can and have been waged, the nature of interstate relationships has never been more important. While U.S-China economic ties have significantly increased over the past three decades, the bilateral relationship continues to be riddled with complexities, friction, and tension. The growing evidence of Chinese government complicity in commercial cyber espionage and theft of intellectual property (IP), costing the United States billions of dollars, has blurred the distinction between the geopolitical and economic realms, further complicating the relationship.

During bilateral discussions in June 2013, President Barack Obama warned Chinese President Xi Jinping that if cyber security issues, such as the theft of U.S. property, were not addressed, it would "be a very difficult problem in the economic relationship and was going to be an inhibitor to the relationship really reaching its full potential."[1] The possibility of this distrust spilling over into other areas of U.S.-China relations is a major concern that could determine whether the relationship becomes one of cooperation or more adversarial in nature.[2] "Distrust of each other's actions in the cyber realm is growing between the U.S. and China," according to Kenneth Lieberthal and Peter Singer, political scientists and senior fellows at Brookings Institute.[3] The effect of cyber security on other aspects of the U.S.-China relationship is more important than with any other bilateral relationship because of the emerging world order and potential challenge to U.S. hegemony.

---

[1] Wayne M. Morrison, *China-U.S. Trade Issues*, (CRS Report No. RL33536) (Washington, DC: Congressional Research Service, 2014), 1, http://fas.org/sgp/crs/row/RL33536.pdf.

[2] Ibid., 6.

[3] Kenneth Lieberthal and Peter W. Singer, *Cybersecurity and U.S.-China Relations* (Washington, DC: Brookings Institute, 2012), 6, http://www.brookings.edu/~/media/Research/Files/Papers/2012/2/23%20cybersecurity%20china%20us%20singer%20lieberthal/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.PDF.

China is believed to have engaged in cyber espionage and intelligence collection as far back as 2004 when the Federal Bureau of Investigation (FBI) investigated intrusions, code-named Titan Rain, by Chinese hackers against U.S. military labs.[4] In 2012, computer networks and systems around the world continued to be targets of intrusions and data theft, many of which originated in China and were attributable directly to the Chinese government and military.[5] Though it would seem that China took a step in the direction of cooperation by agreeing in a 2013 United Nations report that international law does extend to cyberspace, there are no indications that China's cyber espionage and the theft of IP against the United States has waned.[6]

China's cyber activity against the United States takes place in the context of an extensive economic interdependence between the two countries that could be seen as a source of accommodation and stability in the relationship. Taking into consideration the economic interdependence between the United States and China, the rise of China as a potential global power, and the threat of state-sponsored malicious cyber activity, the major question driving this thesis is: What does China's cyber behavior tell us about the role of economic interdependence in U.S.-China relations? Other aspects of this question include: Is China's current use of cyberspace intended to shift the symmetry within U.S.-China economic interdependence and create a source of power for China? Does the use of cyberspace strengthen or weaken China's position within the U.S-China relationship? How has China's cyber behavior been shaped by U.S.-China interdependence?

A. CHINA'S EMERGING ECONOMY

Economists agree that there is no emerging economy more important than China to the health of the global economy and that China will face difficult challenges that will

[4] Timothy Thomas, "Google Confronts China's 'Three Warfares,'" *Parameters* (Summer 2010): 102.

[5] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* (Washington, DC: Department of Defense, 2013), 37, http://www.defense.gov/pubs/2013_china_report_final.pdf.

[6] U.S.-China Economic and Security Review Commission, *2013 Annual Report to Congress* (Washington, DC:,Government Printing Office, 2013), 249, http://www.uscc.gov/Annual_Reports/2013-annual-report-congress.

require both economic and political change.[7] Where economists diverge is in predicting whether China can maintain the significant growth seen of the last three decades to surpass the United States as the largest global economy and what that means for the global power structure. "The next 40 years may see one of the greatest shifts in economic and military power in history," according to Uri Dadush, an author and economist with the Carnegie Endowment for International Peace.[8]

By 2050, the world's three largest economies will be the United States, China, and India.[9] This shift in economic power will significantly affect global economic governance and regional and global interstate relationships. However, "distortive economic policies that have resulted in over-reliance on fixed investment and exports for economic growth (rather than on consumer demand), government support for state-owned firms, a weak banking system, widening income gaps, growing pollution, and the relative lack of the rule of law in China" have been identified as potential weak points in China's economic development, according to a U.S. Congressional Research Service report.[10] Predicting the economic growth or potential for any nation is difficult, but for China, it is especially difficult with the significant economic reforms identified in the country's Twelfth Five-Year Plan (FYP).

B. CYBER REVOLUTION

Similar to the degree of difficulty in predicting the economic growth of China, forecasting and analyzing China's behavior in cyberspace is equally problematic. There is no space more unpredictable than cyberspace, yet states are becoming increasingly dependent on information technology to drive political and economic development. The United States and China are two of the major players in cyberspace, but they hold vastly

---

[7] Robert E. Looney, *Handbook of Emerging Economies*, ed. Robert E. Looney (London and New York: Routledge, 2014), 5.

[8] Uri Dadush, "Key Trends in the World Economy" in *Handbook of Emerging Economies*, ed. Robert E. Looney (London and New York: Routledge, 2014), 26.

[9] Ibid., 16, 21.

[10] Wayne M. Morrison, *China's Economic Rise: History, Trends, Challenges, and Implications for the United States* (CRS Report No. RL33534) (Washington, DC: Congressional Research Service, 2014), 1–2, http://fas.org/sgp/crs/row/RL33534.pdf.

different views on acceptable behavior in the cyber domain. Even among close allies, there is little consensus among researchers on what constitutes a cyber attack or the threshold for an act of war in cyberspace. James Lewis, author and preeminent expert on cyber security, reasons that "an obstacle to managing cyber competition among states is the blurred boundaries between cyber-crime, cyber-espionage, and cyber-attack among states."[11] The Internet was originally designed for the free flow of information with security as an afterthought. "The only distinction between computer network exploitation and attack is the intent of the operator at the keyboard," argues Brian Krekel, author and subject matter expert on China.[12]

Despite the difficulty in attribution of cyber operations and ability of a nation to potentially disguise cyber operations, the interdependence between two nations may be enough of a deterrence to prevent a cyber attack. "Even when the source of an attack can be successfully disguised under a 'false flag,' other governments may find themselves sufficiently entangled in interdependent relationships that a major attack would be counterproductive. China, for example, would itself lose from an attack that severely damaged the American economy, and vice versa," argues Joseph Nye, Distinguished Service Professor at Harvard University and co-founder of complex interdependence theory.[13] But knowing where these lines are is a serious problem for both the United States and China. Offensive cyber operations require a deep knowledge of cultural or military sensitivities, potential "red lines," and how an attack or intrusion will be perceived. For instance, China's government sees Tibetan exiles and Falun Gong hackers as national security threats, while the United States sees them as hacktivists advancing human rights and Internet freedom. Similarly, U.S. leaders view Twitter and YouTube as outlets for personal expression, but their Beijing counterparts identify the websites as

---

[11] James Lewis, *Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia* (Washington, DC: Center for Strategic and International Studies, 2013), 2, http://csis.org/publication/hidden-arena-cyber-competition-and-conflict-indo-pacific-asia.

[12] Bryan Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation* (Falls Church, VA: Northrop Grumman, 2009), 8, http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-030.pdf.

[13] Joseph S. Nye Jr., "Cyber Power," Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010, 16, http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

instruments of attack.[14] "Failure to understand an enemy's potential 'red lines' can lead to unintentional escalation of the conflict," states Krekel.[15]

In addition, cyberspace represents a domain in which a nation's economic, political, and military capabilities and vulnerabilities converge. "The Internet thus may have no formal state borders, but it is increasingly a place that state entities both operate in and care deeply about," affirm Lieberthal and Singer.[16] IP, sensitive source code, proprietary data, business records, research and development, sensitive economic information, and advanced technology all exist in digital medium, enabling foreign actors to quickly gather massive quantities of data with little risk. The most important change facilitating economic espionage through cyberspace, or cyber-enabled economic espionage, is the sheer quantity of data produced digitally and stored electronically. With China's long-term economic growth and prosperity riding on technological innovation, China's actions in cyberspace will be a major factor in determining future U.S.-China political and economic relations, as well as whether the rise of China as a regional hegemon will be peaceful.

C. LITERATURE REVIEW

Work for this thesis draws on and conjoins four distinct areas of prior research: the role of economic interdependence in the relationships of states, the "rise of China" and how China's rise is shaping U.S.-China relations, and the impact of cyber technologies on such relationships.

1. Economic Interdependence, War, and Peace

Understanding International Relations (IR) theory is key to understanding the nature of the changing relations between nation states, and there is no relationship more important to the international system than the relationship between the United States and China. As China continues its rise, the United States struggles with how to address

[14] Ibid., 18.

[15] Krekel, *Capability of the People's Republic of China*, 21.

[16] Lieberthal and Singer, *Cybersecurity and U.S.-China Relations*, 6.

China's emergence as a potential great power. Each school of thought provides a different perspective on China's rise and what it means for U.S.-China relations. From one perspective, the economic interdependence between the United States and China makes conflict impractical.[17] From another perspective, there is a real likelihood that the United States and China will engage in an intense security competition that could very well lead to conflict.[18] While this literature review will examine a number of IR perspectives, the complex interdependence framework, seen as an integration of realist and liberal thought, is the framework used throughout this thesis.

In *The Great Illusion*, originally published in 1909, Norman Angell disputes the idea that nations could gain from war, conquest, or armed conflict.[19] Rather than bringing profit or other advantages, Angell argues that the prevailing economic interdependence between industrial countries made war obsolete in the 20th century, since even military victors lose far more than they gain.[20] This proposition became an article of faith among policy- and opinion-makers of the age, and informed the heady promises that the "boys" who marched into the battles brewing in Europe in August 1914 would "be home by Christmas" that year. When instead, World War I wore on for several years, expending the blood and treasure of the leading western powers in unprecedented measure, critics lambasted Angell and his argument. The critics missed a key point, however: Angell did not say war was impossible but rather that the economic consequences would devastate the participants.[21]

Some observers believe that Angell's principle—of economic prowess inhibiting all-out military conflict—operates in China today. Thomas Friedman advanced a position similar to Angell, arguing that "to the extent that countries tied their economies and futures to global integration and trade, it would act as a restraint on going to war with their neighbors. As countries got woven into the fabric of global trade and rising living

---

[17] Norman Angell, *The Great Illusion* (New York and London: Garland Publishing: 1972), 54–55.

[18] John J. Mearsheimer, "China's Unpeaceful Rise," *Current History* (April 2006): 160–161, http://www.currenthistory.com/pdf_org_files/105_690_160.pdf.

[19] Angell, *The Great Illusion*, 27.

[20] Ibid.

[21] Ibid., 54–55.

standards, the cost of war for victor and vanquished became prohibitively high."[22] Friedman believes that China's push toward a more free-market economy is in the best interest of the United States and of the world. Political upheaval or a potential war could devastate economic progress, risk a state's place in the global supply chain, and ruin business credibility. He contends that countries intertwined in global supply chains will have to carefully consider engaging in anything but a war of self-defense.[23]

Kenneth Waltz argues the contrary by stating that the structure of the international system limits cooperation and forces states to compete in order to ensure survival: "States do not willingly place themselves in situations of increased dependence. In a self-help system, considerations of security subordinate economic gain to political interest."[24] Furthermore, states seek to maximize their relative power in order to ensure their own survival and "because any state may at any time use force, all states must constantly be ready either to counter force with force or to pay the cost of weakness."[25] Waltz states that "in the end, power will balance power, and there isn't any doubt that the Chinese are very uncomfortable with the extent to which the United States dominates the world militarily. But China, if it maintains its political coherence, its political capabilities will have in due course the economic and the technological means of competing."[26] While countries have always competed for security, it has often led to conflict. The world is witnessing what Waltz describes as "the all-but-inevitable movement from unipolarity to multipolarity" in Asia as China emerges as a great power.[27]

John Mearsheimer reiterates this point when he states that "the ultimate goal of every great power is to maximize its share of world power and eventually dominate the

---

[22] Thomas L. Friedman, The World is Flat: Brief History of the Twenty-First Century (New York: Picador, 2007), 586.

[23] Ibid., 587.

[24] Kenneth N. Waltz, *Theory of International Politics* (McGraw-Hill, 1979), 107.

[25] Kenneth N. Waltz, *Man, the State, and War: A Theoretical Analysis* (New York: Columbia University Press, 2001), 160.

[26] Kenneth N. Waltz, "Conversations with History: Conversation with Kenneth Waltz," Institute of International Studies, University of California at Berkeley, February 10, 2003, 5, http://globetrotter.berkeley.edu/people3/Waltz/waltz-con5.html.

[27] Kenneth N. Waltz, "Structural Realism after the Cold War," *International Security* 25, no. 1 (2000): 32, http://www.columbia.edu/itc/sipa/U6800/readings-sm/Waltz_Structural%20Realism.pdf.

system."[28] He writes that "the best way to survive in the international system is to be as powerful as possible, relative to potential rivals."[29] Great powers don't only strive to be the strongest power but to be the only great power in the system and prevent others from accomplishing the same. This type of intense security competition has the potential to lead to conflict or war.[30] Mearsheimer states, "China cannot rise peacefully, and if it continues its dramatic economic growth over the next few decades, the United States and China are likely to engage in an intense security competition with considerable potential for war."[31]

2. The Rise of China and U.S.-China Relationship

It is no secret that China has developed into a major global economic and trade power over the last three decades. While many experts expect that China will surpass the United States as the world's largest economy, others argue that China's ability to maintain the rapid economic growth it has seen over the past decade will depend on whether it implements comprehensive economic reforms and completes the transition to a free market economy.[32] Uri Dadush contends that China will overtake the United States as the world's largest economic power to become a global economic leader. Even under a lower-growth scenario, China will emerge as one of the three largest economies in the world. Although it will remain smaller than the United States in dollar terms, it will surpass the purchasing power parity (PPP) gross domestic product (GDP) of the United States to become the largest in the world by 2050.[33] The World Bank affirms this position, stating that China's economic performance over the last three decades has been impressive: "Even if China grows a third as slowly in the future compared with its past (6.6 percent a year on average compared with 9.9 percent over the past 30 years), it will

---

[28] John J. Mearsheimer, "China's Unpeaceful Rise," *Current History* (April 2006): 160, http://www.currenthistory.com/pdf_org_files/105_690_160.pdf.

[29] Zbigniew Brzezinski and John J. Mearsheimer, "Clash of the Titans," *Foreign Policy*, no. 146 (January/February 2005): 48.

[30] Mearsheimer, "China's Unpeaceful Rise," 160–161.

[31] Brzezinski and Mearsheimer, "Clash of the Titans," 47.

[32] Morrison, *China's Economic Rise*, Summary page.

[33] Dadush, "Key Trends in the World Economy," 13, 28.

become a high-income country sometime before 2030 and outstrip the United States in economic size (its per capita income, however, will still be a fraction of that in advanced countries)."[34]

On the contrary, an International Monetary Fund (IMF) paper in January 2014 shows a continued decline in China's growth since 2007 despite high levels of investment and credit growth. The authors contend that these factors "would imply diminishing returns to investment, a misallocation of resources, and a limit to how far an economy can grow by reallocating labor from the country side into factories," and suggest significant reform implementation is needed.[35] Wayne Morrison makes the same assessment claiming that China's ability to maintain the rapid economic growth it has seen over the past decade will depend on the implementation of comprehensive economic reforms and completion of the transition to a free market economy.[36] Although Friedman argues that China has the potential to become a free-market version of the United States, without implementation of a standard rule of law, free press, and a more open political system that allows people to vent their grievances, China will never become efficient, eradicate corruption, nor be capable of coping with the inevitable downturns in its economy.[37]

3. Strategic Questions of the U.S.-China Relationship

One aspect of Chinese economic rise that seems to be clear is the growing trade relationship between the United States and China and "sharp expansion in U.S.-China commercial ties" since its entrance into the World Trade Organization (WTO) in 2001.[38]

---

[34] The World Bank, "China 2030: Building a Modern, Harmonious, and Creative Society," 2013, 3, http://www.worldbank.org/content/dam/Worldbank/document/China-2030-complete.pdf.

[35] Rahul Anand, Kevin C. Cheng, Sidra Rehman, and Longmei Zhang, "Potential Growth in Emerging Asia," (IMF Working Paper, International Monetary Fund, 2014), 6,13, http://www.imf.org/external/pubs/ft/wp/2014/wp1402.pdf.

[36] Morrison, *China's Economic Rise*, Summary page.

[37] Friedman, *The World is Flat*, 149.

[38] Morrison, *China-U.S. Trade Issues*, 1.

What is relatively unclear among experts is whether the relationship will remain cooperative and peaceful or end in eventual conflict.[39]

In 2011, both the United States and China committed to building a more cooperative partnership and a military-to-military relationship in an effort to encourage China's cooperation in the international forum and as a responsible power.[40] In a visit to China in February 2014, Secretary of State John Kerry spoke about the U.S. and China's relationship as having great potential and a partnership that can come together to build stability and prosperity in the region. Secretary Kerry reiterated the commitment to a bilateral relationship based on "practical cooperation" and "constructive management of differences."[41] Additionally, the Office of the Secretary of Defense (OSD) contends that China's priorities for the early 21st century are economic growth and development, maintaining peace and stability in the region, expanding their influence to access new markets and resources, and avoiding direct confrontation with the United States and other nations.[42]

Zbigniew Brzezinski argues that China is "determined to sustain economic growth" and that a "confrontational foreign policy could disrupt that growth, harm hundreds of millions of Chinese, and threaten the Communist Party's hold on power."[43] A position that China confirmed in a December 2012 essay, when State Councilor of China Dai Bingguo wrote: "The notion that China wants to replace the United States and dominate the world is a myth."[44] Brzezinski posits that the leadership in China is conscious of its strengths but also of its weaknesses: "In a conflict, Chinese maritime

---

[39] Lieberthal and Singer, *Cybersecurity and U.S.-China Relations*, 1; Adam Lowther et al., "Chinese-US Relations: Moving Toward Greater Cooperation or Conflict?," *Strategic Studies Quarterly* (Winter 2013): 20, http://www.au.af.mil/au/ssq/digital/pdf/winter_13/2013winter-Lowther.pdf.

[40] John Kerry, *Solo Press Availability in Beijing, China* (Washington, DC: Department of State, 2014), http://www.state.gov/secretary/remarks/2014/02/221658.htm.

[41] Ibid.

[42] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013*, (Washington, DC: Department of Defense, 2013), 15–16.

[43] Brzezinski and Mearsheimer, "Clash of the Titans," 47.

[44] Dai Bingguo, "坚持走和平发展道路 [Stick to the road of peaceful development]," December 6, 2010, http://www.gov.cn/ldhd/2010-12/06/content_1760381.htm. Translated with the assistance of Karen Li.

trade would stop entirely. The flow of oil would cease, and the Chinese economy would be paralyzed."[45]

In contrast, Mearsheimer argues against the conjecture that China's desire for continued economic growth makes conflict with the United States unlikely: "One of the principle reasons that China has been so successful economically over the past 20 years is that it has not picked a fight with the United States."[46] Both the German and Japanese economies were growing strongly prior to World War II, but Hitler still started World War II and Japan started conflict in Asia, combatting the idea that economic strength predominates all else or that economic interdependence will restrain states from engaging in war.[47]

Many U.S. policymakers and senior leaders have similar concerns. Michael Schuman argues that while the rise of China is good for the global economy, it concerns the United States in the same way that Japan's economic might did back in the 1980s.[48] Fear that a competing economic system that challenges U.S. ideals can generate superior results. According to Schuman, "China is not just competing with the U.S. in the world markets, but offering up an entirely different economic and political system. China is succeeding based on ideas that Americans despise."[49]

But possibly the biggest concern for some U.S. policy makers is the increasing trade deficit between the United States and China with China having amassed $2.5 trillion in foreign exchange reserves, $1.3 billion of it in U.S. Treasury securities as of 2013.[50] Adam Lowther, John Geis, Panayotis Yannakogeorgos, and Chad Dacus argue that if China faces economic stagnation, Chinese Communist Party leaders could alter their behavior to ensure power is maintained.[51] They argue that "considering China's

---

[45] Brzezinski and Mearsheimer, "Clash of the Titans," 47.

[46] Ibid., 49.

[47] Ibid.

[48] Michael Schuman, "Why Do We Fear a Rising China?," *Time*, June 7, 2011, http://business.time.com/2011/06/07/why-do-we-fear-a-rising-china/.

[49] Ibid.

[50] Morrison, *China-U.S. Trade Issues*, 13.

[51] Lowther et al., "Chinese-US Relations," 26–27.

strategic culture and the geopolitical environment, antagonistic actions by the PRC toward the United States are more likely to be economic than military."[52]

In 2010, People's Liberation Army academic advisers called on China to dump U.S. Treasuries in retaliation for a proposed arms deal between the United States and Taiwan.[53] The United States responded that "the ability of China to affect the market for U.S. Treasuries, and U.S. financial markets more broadly, is limited."[54] While China held $1.17 trillion in U.S. Treasury Securities in 2012 and $1.3 trillion in 2013, China's holdings of U.S. Treasury securities accounted for 11 percent of federal debt held by the public, 7.5 percent of total public debt, and only slightly more than 2 percent of total U.S. credit market debt in 2012, according to the OSD.[55] The report asserts that in the most aggressive scenario, China could abruptly dump its holdings of U.S. Treasuries, causing short-term market disruptions, decreased secondary market values, and increased interest rates—though such a move also would impose significant direct financial losses for itself. Thus, "attempting to use U.S. Treasury securities as a coercive tool would have limited effect and likely would do more harm to China than to the United States."[56] Still, Lowther et al. believe that movement away from the dollar would serve to destabilize U.S. hegemony.[57] The question, then, is only which economy would suffer more.

Lowther et al. argue that it is when—not if—China will become the world's largest economy and eventually lead to military superiority.[58] "Even with modest economic growth (by Chinese standards), a consistent share of its gross domestic product devoted to defense spending, and relatively optimistic projections of U.S. defense expenditures, China's military outlays are likely to eclipse U.S. defense spending shortly

---

[52] Ibid.

[53] Office of the Secretary of Defense, *Report to Congress, Assessment of the National Security Risks Posed to the United States as a Result of the U.S. Federal Debt Owed to China as a Creditor of the U.S. Government* (Washington, DC: Department of Defense 2012), 3, https://www.hsdl.org/?view&did=723112.

[54] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2012*, 3.

[55] Ibid.

[56] Ibid., 4.

[57] Lowther et al., "Chinese-US Relations," 26.

[58] Ibid., 26–27.

after 2025."[59] While there is little perceived danger of offensive U.S. military, economic, or other policy actions, according to Robert Sutter, China's emergence as a power in the region alarms many regional states.[60] As China's economy grows, so does its military strength, making many of its regional neighbors (Australia, South Korea, Vietnam, Japan, and Taiwan) nervous.[61] Mearsheimer claims that it is unlikely that China will build its military force to conquer nations, but rather to gain regional hegemony. "An increasingly powerful China is also likely to try to push the United States out of Asia, much the way the United States pushed the European great powers out of the Western Hemisphere."[62] Mearsheimer points out that the United States has a historical track record of intolerance toward peer competitors: "As it demonstrated in the twentieth century, it is determined to remain the world's only regional hegemon."[63] He reasons that much like the behavior the United States displayed toward the Soviets during the cold war, the United States will likely look to a policy of containment against China. In addition, China's neighbors will look to the United States to build a coalition of nations aimed at preventing China from achieving regional hegemon status.[64]

Despite the U.S. and Chinese rhetoric that maintaining peace and stability in the Pacific remains a priority for both nations, Lowther et al. believe that the "regular employment of ambiguity, disinformation, and secrecy in PRC foreign affairs has left the United States and countries throughout Asia reticent to believe that China's military modernization is solely for defensive purposes."[65] Consequently, they maintain that many of China's acquisition and development choices, such as the DF-21D missile system, dubbed the "carrier killer," are subtle indicators that China sees a threat arising

---

[59] Ibid., 26.

[60] Robert Sutter, "Rebalancing, China and Asian Dynamics – Obama's Good Fit," Center for Strategic and International Studies, January 6, 2014, https://csis.org/publication/pacnet-1-rebalancing-china-and-asian-dynamics-obamas-good-fit.

[61] Schuman, "Why Do We Fear a Rising China?"

[62] Mearsheimer, "China's Unpeaceful Rise," 162.

[63] Ibid.

[64] Ibid.

[65] Lowther et al., "Chinese-US Relations," 35.

from the United States that requires a military modernization program aimed at mitigating U.S. strengths.[66]

While many experts believe the potential for military conflict remains low, China's military modernization, cyberspace endeavors, weapons proliferation activities, and aggressive behavior in the South China Sea in 2012 and East China Sea in 2013 and 2014 continue to be a concern for the U.S. and regional allies. Daniel Russel, assistant secretary of state of the Bureau of East Asian and Pacific Affairs, testified that "well over half the world's merchant tonnage flows through the South China Sea, and over 15 million barrels of oil per day transited the Strait of Malacca last year, with most of it continuing onward through the East China Sea to three of the world's largest economies."[67] China's provocative actions and lack of clarity with respect to territorial claims in the region increase tensions, lead to concerns about China's overall objectives, and are a great concern to the United States as a maritime nation, dependent on freedom of the seas and unimpeded lawful commerce for economic and security interests.[68]

4. The U.S.-China Cyberspace Race

In spite of perceived aggression and provocation by China, Lowther et al. contend that unless there is a serious challenge to China's core interests, their domestic and international political and economic environments will ensure they remain nonaggressive in the near term.[69] They continue: "Historically, great powers have found it difficult to become close friends. At the same time, a non-confrontational relationship is possible and preferred by China. Chinese cultural writings place particular importance on avoiding direct confrontation, especially with a superior adversary"[70] China may very well have

---

[66] Ibid., 34.

[67] *Maritime Disputes in East Asia: Hearings Before House Committee on Foreign Affairs Subcommittee on Asia and the Pacific*, *House Committee on Foreign Affairs*, 113th Cong., 1 (2014) (statement of Daniel R. Russel, Assistant Secretary of State, Bureau of East Asian and Pacific Affairs), http://www.state.gov/p/eap/rls/rm/2014/02/221293.htm.

[68] Ibid.

[69] Lowther et al., "Chinese-US Relations," 22.

[70] Ibid., 22, 38.

identified cyberspace as the mechanism to compete with the United States while avoiding direct confrontation.

According to the OSD, "Chinese actors are the world's most active and persistent perpetrators of economic espionage. Chinese attempts to collect U.S. technological and economic information will continue at a high level and will represent a growing and persistent threat to U.S. economic security."[71] In 2013, The U.S. government openly accused the Chinese government of directing and executing cyber espionage against U.S. diplomatic, economic, and defense industrial base sectors in order to "benefit China's defense industry, high technology industries, policymaker interest in U.S. leadership thinking on key China issues, and military planners building a picture of U.S. network defense networks, logistics, and related military capabilities that could be exploited during a crisis.[72] In what might be the most significant unclassified analytic report released on cyber espionage against the United States, the Mandiant Intelligence Report bridged the gap between one of the most persistent Chinese cyber actors and the Chinese government, attributing global cyber intrusion victims to the 2nd Bureau of China's People's Liberation Army (PLA).[73]

Krekel asserts China's cyber exploits are more economic in nature: "China's defense industry is producing new generations of weapon platforms with impressive speed and quality, and while these advancements are due to a variety of domestic factors, Chinese industrial espionage is providing a source of new technology without the necessity of investing time or money to perform research."[74] Lowther et al. support this view stating, "China's rapid rise as an economic power is in part the result of effective economic reforms but also of its use of cyberspace to conduct wide-spread state-sponsored espionage against governmental and industrial targets to 'catch up' with

---

[71] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2012*, 10.

[72] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013*, 36.

[73] Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Alexandria, VA: Mandiant, 2013), 2–3, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

[74] Krekel, *Capability of the People's Republic of China*, 58.

advanced nations."[75] Lewis observes that "information technology and cyberspace occupy a central position in Chinese politics, strategy, and economic policy." He submits that economic espionage through the use of cyberspace is standard practice in China aimed at gaining a military and economic advantage.[76]

Robert Keohane and Joseph Nye reason that information technology will likely be the most important power resource in the next century.[77] Nye suggests that "information technology is likely to be the most crucial power resource" and "asymmetries in information can greatly strengthen the hand of the less vulnerable party."[78] Lewis attests to Keohane and Nye's position by stating, "China uses cyber techniques to redress what it sees as an imbalance of power, using cyber espionage to compensate for its technological lag and weak national innovation capability, as well as an element of a larger strategy on how to gain advantage in any military conflict."[79]

However, China maintains that U.S. allegations are groundless. China continues to deny claims of cyber espionage arguing that the anonymity of cyberspace and the lack of verifiable technical forensic data make it near impossible to identify China as the origin. China's leadership insists that the "accusation that the Chinese government participated in cyber attacks, either in an explicit or inexplicit way, is groundless and aims to denigrate China. We [are] firmly opposed to that."[80] China asserts that it has the same concerns about cyber security as other nations, claiming to also be subject to hacking and online threats: "The Ministry of Public Security has noted that the number of cyber attacks on Chinese computers and websites has soared by more than 80 percent annually, and, by the raw numbers, China is the world's largest victim of cyber

---

[75] Lowther et al., "Chinese-US Relations," 29.

[76] Lewis, *Hidden Arena*, 2.

[77] Robert O. Keohane and Joseph S. Nye, Jr., "Power and Interdependence in the Information Age," *Foreign Affairs* 77, no. 5 (September/October 1998): 87.

[78] Joseph S. Nye Jr., *American Power in the Twenty-First Century: Two Examples* (Berkeley, CA: University of California at Berkeley, 1999), 34, 36.

[79] Lewis, *Hidden Arena*, 6.

[80] "Accusation of Chinese Government's Participation in Cyber Attack "Groundless": Ministry," *Xinhua News*, January 25, 2010, http://news.xinhuanet.com/english2010/china/2010-01/25/c_13149276.htm.

attacks."[81] Lewis concurs that China is genuinely concerned about the risk of malicious cyber activity occurring against large nation states and more importantly, the ability of cyberspace to affect policies and political stability in China such as they did in the Middle East during the Arab Spring in 2010 when social media became a critical component in the social revolutions that occurred in much of the Arab world.[82]

Contrary to the denial of allegations of cyber espionage, Chinese professional military literature highlights the importance of information superiority to China and its military leaders. Major General Wang Pufeng writes that information warfare will "control the form and future of war" and that the goal is to use "information superiority to achieve greater victories at a smaller cost."[83] Wei Jincheng takes Major General Wang's position one step further by declaring that "the multidimensional, interconnected networks on the ground, in the air (or outer space), and under water, as well as terminals, modems, and software, are not only instruments, but also weapons."[84]

Despite the diverging theories on China's cyber activity, Lowther et al. suggest that by observing Chinese behavior in cyberspace, the United States can develop an accurate sense of the U.S.-China relationship.[85] While they look at economic interests and activity in cyberspace to determine the direction U.S-China relations may take, even identifying China's use of cyberspace to advance economic power, they fall short of identifying what China's cyber behavior tells us about the role of economic interdependence in U.S.-China relations. Keohane and Nye address the economic interdependence between the United States and China and the importance of information technology as a future source of power, but do not explore how it could affect U.S.-China political or economic relations. Stephen Roach dedicates massive amounts of research on economic interdependence between the United States and China, but limits his focus to

---

[81] Lieberthal and Singer, *Cybersecurity and U.S.-China Relations*, 4.

[82] Lewis, *Hidden Arena*, 2, 4.

[83] Wang Pufeng, "The Challenge of Information Warfare," in *Chinese Views of Future Warfare*, revised ed., ed. Michael Pillsbury (Washington, D.C.: National Defense university Press, 1998), 318.

[84] Wei Jincheng, "Information War: A New Form of People's War," in *Chinese Views of Future Warfare*, revised ed., ed. Michael Pillsbury (Washington, D.C.: National Defense university Press, 1998), 411.

[85] Lowther et al., "Chinese-US Relations," 29.

the economic aspect of the relationship, with little attention paid to economic espionage or cyberspace as a means to conduct economic espionage. In addition, research exists that either independently addresses China's cyber activity or its economic interdependence, failing to establish any predictive relationship between these two variables.

As the literature review illustrates, researchers have given extensive attention to the role of economic interdependence in international relations, the rise of China as an economic power, and the contentiousness of Chinese cyber behavior. This thesis examines the intersection of these three topics.

D. COMPLEX INTERDEPENDENCE

This thesis applies the complex interdependence framework to demonstrate China's efforts to gain leverage through cyberspace in an effort to shift the balance of power within its economic interdependent relationship with the United States. Within the structure of complex interdependence, Keohane and Nye argue that the more states become economically interconnected, the more states will seek to structure their interdependence to achieve joint gains and create asymmetries in order to increase power relative to the other state.[86] They propose that states try to forge issue linkages by creating an asymmetric advantage in one area to overcome a disadvantage in another.[87] Nye argues that "manipulating the asymmetries of interdependence is an important dimension of economic power. If both states value the interdependent relationship, the state that stands to lose the least possesses a source of power."[88]

Nye asserts that a relationship of interdependence has developed today between the United States and China, both vulnerable to the actions of the other: "The asymmetries reveal a 'balance of financial terror' analogous to the Cold War military interdependence (mutually assured destruction) in which the United States and the Soviet Union each had the potential to destroy the other in a nuclear exchange but never did."[89]

---

[86] Robert O. Keohane and Joseph S. Nye, Jr., *Power and Interdependence* (HarperCollins: 1989), 30–31.

[87] Ibid.

[88] Joseph S. Nye, Jr., *The Future of Power* (New York: Public Affairs, 2011), 55.

[89] Nye, Jr., *The Future of Power*, 56–57

He argues that although some analysts believe that China's impressive success in overcoming the financial crisis and its increased holdings of dollars have greatly increased its power over the United States, China's reliance on the United States' economic well-being levels the playing field. While China threatening to sell its dollars would cause a shift in the global balance of power and bring the United States to its knees, it "might also bring itself to its ankles."[90] Neither the United States nor China is willing to break the symmetry of their interdependence, yet both nations continue to shape the structure of their market relationship in an attempt to create asymmetrical advantages over the other. Nye argues that this type of balance does not guarantee stability and it is likely that both nations will seek to reduce their vulnerabilities.[91]

This thesis employs the analytic concept of complex interdependence to show that China's use of cyber-enabled economic espionage and cyber theft is used as a mechanism to overcome scientific and technological innovation and intellectual property deficits that threaten economic stagnation, prevent long-term economic growth, and ensure China's dependence on the United States for sustained economic expansion.

E. THESIS ORGANIZATION

This research examines whether China is using cyberspace as a mechanism to create asymmetries in the economic interdependent relationship between the United States and China in order to shift the current balance of power. This first chapter established the basic framework for further examination of U.S.-China economic interdependence, China's cyber behavior, and the implications for future U.S.-China relations.

Chapter II examines the economic interdependence that has transpired between the United States and China over the last 30 years, resulting in a somewhat symmetrical dependence that has enabled both nations to sustain long-term economic growth. This chapter provides a historical look at the development of U.S.-Chinese economic interdependence followed by a section on how the current economic growth models of

90 Joseph S. Nye, Jr., "American and Chinese Power after the Financial Crisis," *Washington Quarterly* 33, no. 4 (October 2010): 148, doi: 10.1080/0163660X.2010.516634.

91 Nye, Jr., *The Future of Power*, 60 and Nye, "American and Chinese Power after the Financial Crisis," 148.

each nation have resulted in a symmetrical dependence. The chapter concludes by describing how China is attempting to implement an economic rebalancing that will ensure long-term economic growth while shifting the balance of power within U.S.-Chinese economic interdependence.

Chapter III analyzes Chinese use of cyberspace to conduct economic espionage and IP theft in an effort to create an asymmetrical advantage over the United States. This chapter provides case studies of Chinese cyber-enabled economic espionage that show the pervasiveness of China's economic espionage and how cyberspace is being used to alter the balance of economic power between the United States and China. Additionally, this chapter will identify parallels between China's cyber-enabled economic espionage, its Twelfth FYP, and its 2006 National Medium to Long-Term Plan for the Development of Science and Technology, 2006–2020 (MLP).

Taking into consideration the assessments made in Chapters II and III that China is using cyberspace as a mechanism to create asymmetries in their economic interdependent relationship, Chapter IV examines how China's cyber economic espionage could affect the economic relationship between the United States and China and what it may mean for the future of U.S.-China relations.

It is important to note that this thesis is purposely kept at the unclassified level, utilizing only unclassified sources and material. While the primary source material for this thesis is unclassified, it is understood that there may be a number of classified sources that would add to this research topic. The intent is for this thesis and the methodologies used within this thesis to be used as a future framework for additional research incorporating materials at higher levels of classification. The source material for this thesis consists of U.S. government documents, strategies, and policy as well as cybersecurity sources with extensive knowledge and understanding of cyberspace such as Mandiant, McAfee, Northrup Grumman, and the Rand Corporation. Although most of the source material on China will consist primarily of U.S.-authored literature, translated Chinese works, such as *Chinese Views of Future Warfare* and *The Art of War*, will be used whenever possible.

II. U.S.-CHINA ECONOMIC INTERDEPENDENCE

Since opening up to foreign trade and investment and implementing free market reforms in 1979, China has been among the world's fastest-growing economies, with real annual GDP growth averaging nearly 10 percent through 2013.[92] In recent years, China has emerged as a major global economic and trade power. It is currently the world's second-largest economy, largest trading economy, second largest destination of foreign direct investment (FDI), largest manufacturer, and largest holder of foreign exchange reserves.[93]

Although the economic relationship between the United States and China was mutually beneficial at the start, with each nation drawing on the other's strengths to expand economic growth, the connection has its downsides, as well. The United States, enabled by China's surplus capital and low-cost production, has pushed its consumption to the max while continuously spending its savings. China, supported by the perpetual U.S. demand for Chinese products, has focused solely on its export-led growth, causing significant economic imbalances and a "destabilizing surplus in its international current account balance."[94] As time goes on, China and the United States need each other more than ever to sustain the economic growth each desires, building a symbiotic relationship neither is comfortable maintaining. Although both the United States and China continue to voice growing concerns over the interdependence that has developed over the previous two decades, neither has been able to rebalance the economy enough to create an asymmetrical advantage over the other.

A. THE ROAD TO INTERDEPENDENCE

The second half of the 20th century was considered by many as the golden age of American capitalism. Postwar economic expansion and consumer prosperity from the end

[92] Morrison, *China's Economic Rise*, 1.

[93] Morrison, *China's Economic Rise*, Summary page.

[94] Stephen S. Roach, *Unbalanced: The Codependency of America and China* (New Haven and London: Yale University Press, 2014), 3.

of World War II to the early 1970s led to an increased middle-class, upsurge in productivity, and steady GDP growth. Sara Burke and Claudio Puty assert: "Spectacular conditions of profitability in the system during the Golden Age made it possible to redistribute gains from increased productivity back to workers in the form of real wage increases. The result was increased middle-class demand, which created a growing market for mass-produced goods that is now one of the fundamental features of modern industrialized societies."[95] Unable to maintain the post-war economic expansion, economic growth began to slow in the late 1960s and by the early 1970s Americans faced soaring inflation, collapse of the Bretton Woods system, rising interest rates, a stock market crash, and an oil crisis.[96] Additionally, the post-World War II reconstruction of Japan and Germany and emergence of new centers of manufacturing in Asia in the 1960s led many American companies to shift manufacturing and production overseas. Industrial cities such as Chicago and Detroit lost more than 50 percent of the manufacturing jobs that existed 30 years prior.[97] Between 1960 and 1980, the number of manufacturing workers decreased by 10 percent and by 1975, unemployment rose to 9 percent—levels not seen since the Great Depression (see additional information below).[98]

Despite weakening income growth, increasing trade deficits, and mounting national debt, the United States had solidified itself as a consumption-based economy by the 1980s. U.S. monetary and fiscal policies encouraged consumer spending by identifying new ways to increase purchasing power, allowing Americans to live beyond

---

[95] Sara Burke and Claudio Puty, "The Post-World War II *Golden Age* of Capitalism and the Crisis of the 1970s," Gloves Off, accessed July 23, 2014, http://www.glovesoff.org/features/gjamerica_1.html.

[96] E. Philip Davis, "Comparing Bear Markets - 1973 and 2000," *National Institute Economic Review* 183, no. 78 (January 2003): 78–79, http://ner.sagepub.com/content/183/1/78.full.pdf+html and Floyd Norris, "1974 Redux: Why Bear Market May Be Over," *New York Times* online, October 4, 2002, http://www.nytimes.com/2002/10/04/business/1974-redux-why-bear-market-may-be-over.html.

[97] Eric Foner, *Give Me Liberty! An American History*, 3rd ed. (New York: W. W. Norton & Company, 2011) 1094–1095, 1096 and U.S. Department of Labor Bureau of Labor and Statistics, "Labor Force Statistics from the Current Population Survey," data extracted July 23, 2014, http://data.bls.gov/timeseries/LNS14000000. While Public Law 95–523, 95th Congress, H.R. 50: Full Employment and Balanced Growth Act [Humphrey-Hawkins Act] states that unemployment rates should be no more than 3% for persons aged 20 or over and not more than 4% for persons aged 16 or over, a Non-Accelerating Inflation Rate of Unemployment (NAIRU) or "full employment" rate between 4 percent and 5.5 percent has been deemed acceptable.

[98] Foner, *Give Me Liberty! An American History*, 1095.

their means. Personal consumption rose to a record 69 percent of GDP in 2011 from 64 percent in 1990, the highest of any nation (see Figure 1).[99]

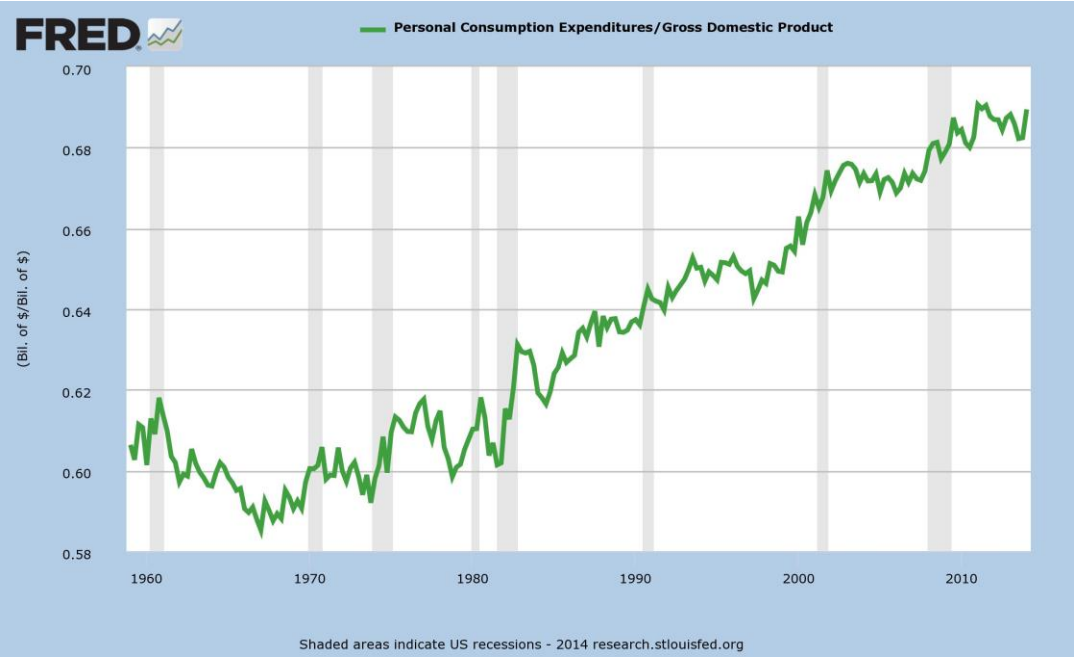


Figure 1. U.S. Personal Consumption as percent of GDP: 1960–2011[100]

Increased spending combined with weak labor income growth resulted in a personal savings rate in 2005 that mirrored the post-World War II low of 2.3 percent, 7 percent below the norm.[101] By 2008, household sector indebtedness swelled to 132 percent of disposable personal income resulting in a "savings-short U.S. economy."[102] Financial experts contend that the insatiable spending habits of Americans caused U.S. personal savings rates to dip below 50-year averages between 1993 and 2009.[103] Following deregulation in the late 1970s and 1980s, credit became increasingly easier to

[99] Roach, *Unbalanced*, 8–10.

[100] Federal Reserve Bank of St. Louis, "Graph: Personal Consumption Expenditures/Gross Domestic Product," Federal Reserve Bank of St. Louis website, accessed July 22, 2014, http://research.stlouisfed.org/fred2/graph/?g=hh3.

[101] Roach, *Unbalanced*, 9.

[102] Roach, *Unbalanced*, 9.

[103] Federal Reserve Bank of St. Louis, "Graph: Personal Consumption Expenditures/Gross Domestic Product."

obtain. Households financed large purchases instead of saving for them, often spending more than their real wage earnings. The lack of personal savings and decrease in personal net worth was a major contributor to financial market instability leading up to and exacerbating the financial crisis that started in 2008 (see Figure 2).[104]

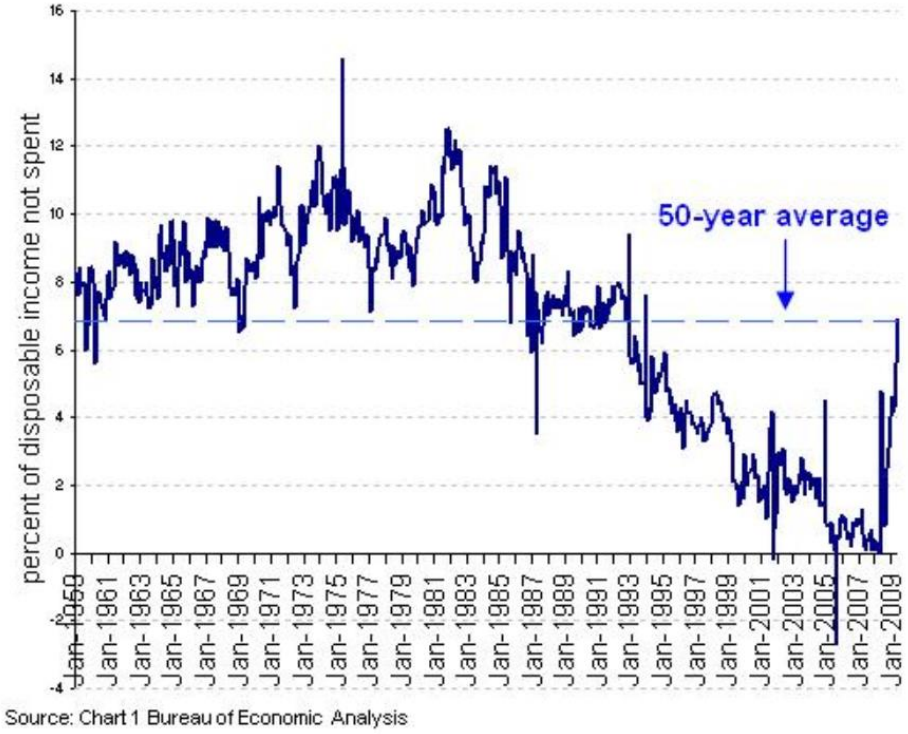


Figure 2. U.S. Personal Savings Rate: 1959–2009 (percent)[105]

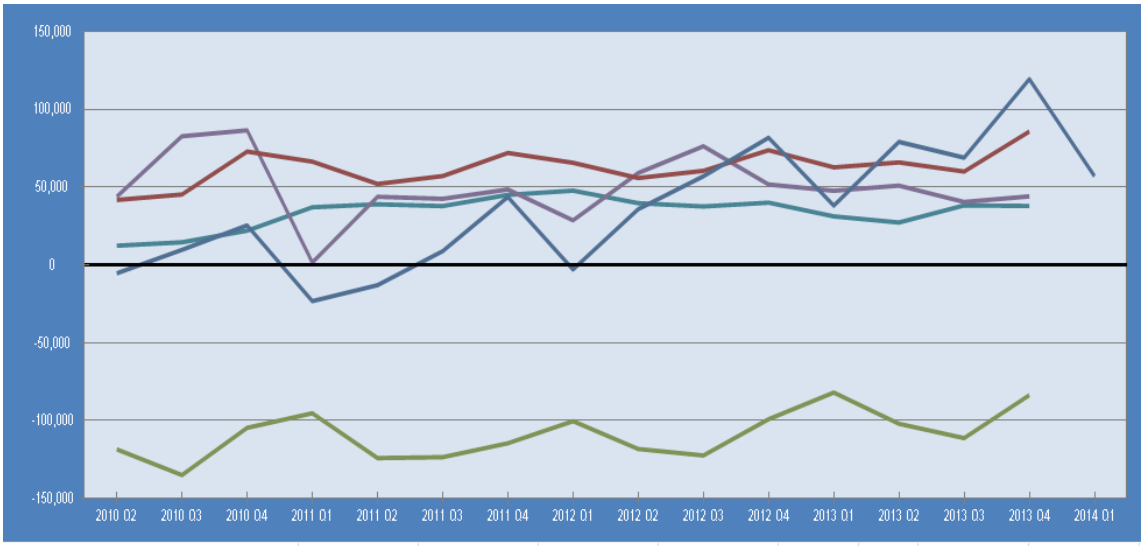
Seeking ways to increase growth with stagnant labor income generation, the United States "aggressively borrowed surplus savings from abroad, running massive current account and foreign trade deficits."[106] In 2011, the United States accounted for 17 percent of global consumer demand, spending $10.7 trillion on personal consumption.

[104] Patrick J. Catania, "Lack of Personal Savings: The Weakest Link," Baxter Credit Union website, accessed July 22, 2014, https://www.cdwcu.com/FRCPersonalSavingsarticle.aspx and Catherine Rampell, "Savings Rates Rising Toward Mediocrity," *Economix (blog), New York Times*, June 26, 2009, http://economix.blogs.nytimes.com/2009/06/26/savings-rates-rising-toward-mediocrity/?_php=true&_type=blogs&_r=0.

[105] Catania, "Lack of Personal Savings."

[106] Roach, *Unbalanced*, 9–10.

The United States accounts for only 4.5 percent of the world's population, but U.S. consumption is 35 percent larger than pan-European consumption and four times Chinese and Indian combined consumption.[107] With U.S. consumers, businesses, and government spending well beyond U.S. export income and an inability to draw on domestic savings, the United States turned to savings from abroad to fund excess spending. The United States has run a balance of payments deficit almost every year since 1982, with a deficit in 2013 of $379 billion—approximately $295 billion more than the world's second-largest deficit, held by the United Kingdom.[108] The tremendous disparity between the United States and other top current account balance holders appears in Figure 3.



	2010	2011	2012	2013
Euro Area	12,240.20	15,972.35	171,381.00	305,175.79
Germany	212,156.13	247,217.57	255,382.68	273,971.46
United States	-449,477.00	-457,729.00	-440,423.00	-379,276.00
China, P.R.: Mainland	237,810.39	136,096.76	215,391.75	182,807.19
Saudi Arabia	66,750.99	158,545.22	164,763.65	134,330.26

Figure 3. Balance of Payment Statistics (US $ millions): 2010–2013[109]

[107] Roach, *Unbalanced*, 10.

[108] International Monetary Fund, "World Economic Outlook Database: Current Account Balance Statistics," April 2014, http://www.imf.org/external/pubs/ft/weo/2014/01/weodata/index.aspx. The second-largest current account balance deficit was the United Kingdom at -$84.624.

[109] IMF eData Library, "Balance of Payment Statistics," International Monetary Fund, http://elibrary-data.imf.org/FindDataReports.aspx?d=33061&e=170784. Statistics and chart were downloaded and reformatted to reduce query size and make the data readable. Actual data has not been altered.

Economist and Yale lecturer Stephen Roach argues that "an economy as large as America's with an outsize savings shortfall must run trade deficits with many countries in order to secure the incremental funding it needs to maintain economic growth."[110] In essence, lack of savings and excess spending by the United States resulting in substantial trade and current account deficits and reliance on foreign investment, has ultimately led to the development of an economic interdependent relationship with China.

The history of China's economic growth is vastly different. After the establishment of the People's Republic of China in 1949, Chairman Mao Zedong adopted a Soviet economic model that incorporated a series of five-year economic plans aimed at Chinese socialist industrialization based on the self-sufficiency of Chinese producers and consumers (see additional information below).[111] Unfortunately, the 1950s through the 1970s in China were fraught with major economic recessions as a result of unrealistic development ambitions and political upheaval during the first four five-year economic plans. The First and Second FYPs resulted in a drop in national income from 21.3 percent in 1952 to 8.3 percent in 1957.[112] The Great Leap Forward implemented by Chairman Mao from 1958 to 1960 during the Second FYP, was an economic campaign designed to transform China from an agrarian economy into an industrialized communist society that resulted in mass famine and took the lives of approximately 40 million people.[113] China's Third and Fourth FYPs fared just as poorly because of the political chaos that arose during the Cultural Revolution from 1966 to 1976. Although China's economic policies and basic economic model remained the same during this period, the political and social

---

[110] Roach, *Unbalanced*, 129.

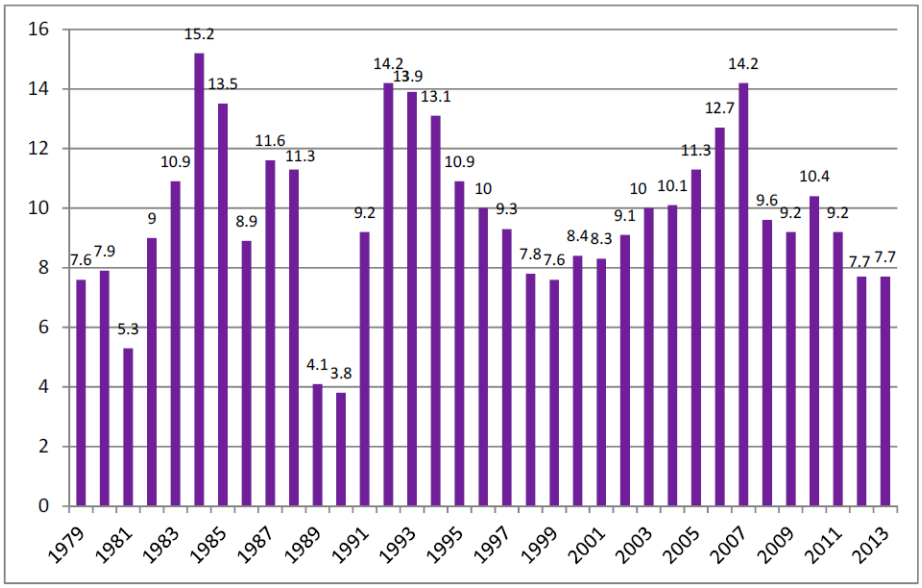
[111] Thomas R. Gottschang, "A Country Study: China," Library of Congress, Library of Congress Call Number DS706 .C489 1988, Chapter 5, http://lcweb2.loc.gov/frd/cs/cntoc.html#cn0149**.** Under Communist Party of China (CPC) leadership, Chairman Mao Zedong adopted the Soviet economic model of rapid industrial growth and socialization. China's economic development plans were manifested in a series of Five-Year Plans (FYPs) aimed at achieving high rates of economic growth through industrial development. China's five-year economic plans continue to be a detailed outline for the country's economic goals for a given five-year period, aligning China's economy with government policy goals. The FYPs are broken down as follows: First FYP (1953–1957), Second FYP (1958–1962), Third FYP (1966–1970), Fourth FYP (1971–1975), Fifth FYP (1976–1980), Sixth FYP (1981–1985), Seventh FYP (1986–1990), Eighth FYP (1991–1995) , Ninth FYP (1996–2000), Tenth FYP (2001–2005), Eleventh FYP (2006–2010), Twelfth FYP (2011–2015).

[112] Roach, *Unbalanced*, 12–13.

[113] Roach, *Unbalanced*, 12–13 and Morrison, *China's Economic Rise*, 3.

instability that ensued had negative long-term effects on the economy. Production halts, extensive disruption of transportation to support the Red Guards, curtailment of foreign equipment imports required for technological advancement, and a critical shortage of highly educated personnel due to the closing of universities and demotion or imprisonment of technical experts led to a 14 percent decrease in industrial production by 1967.[114]

While the FYP framework has been a mainstay of Chinese economic policy, Deng Xiaoping led China from a Soviet-style economy to a socialist market economy in the 1980s in an effort to develop growth by opening the nation to the forces of market competition. From 1979 to 2007, China's "opening up" led to a rise in exports and large-scale fixed investment from 31 percent to 75 percent of the GDP, surging China's real GDP an average of 10 percent annually between 1979 and 2013 (see Figure 4).[115]



Source: Economist Intelligence Unit and official Chinese government data.

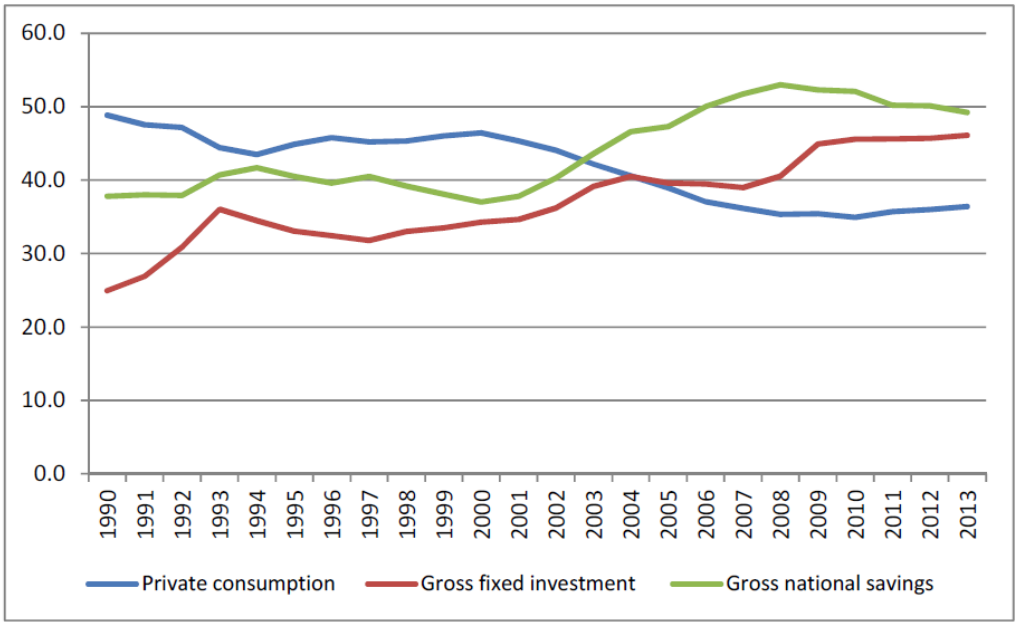
Figure 4. Chinese Real GDP Growth: 1979–2013 (percent)[116]

[114] Gottschang, "A Country Study: China," Chapter 5.

[115] Morrison, *China's Economic Rise*, 4.

[116] Ibid.

Exports alone increased from 5 percent of GDP to 36 percent from 1979 to 2007, while internal consumption dropped from 50 percent to 35 percent during the same period. The steep drop in consumption and diminishing import demand was driven largely by economic policies that encouraged high savings rates and favored export-oriented industries.[117] Because China lacked the ability to generate growth internally, it became heavily dependent on production and exports to sustain its phenomenal economic growth.[118] Although China has pushed to modernize its economy through major economic reforms in the Eleventh and Twelfth FYPs, a continued overdependence on exports and fixed investment and sharp decline in private consumption was evident through 2013 (see Figure 5).



Source: Economist Intelligence Unit.

Figure 5. Chinese Gross Savings, Gross Fixed Investment, and Private Consumption as a Percent of GDP: 1990–2013 (percent)[119]

[117] Roach, *Unbalanced*, 12–13 and Morrison, *China's Economic Rise*, 3.

[118] Roach, *Unbalanced*, 14, 15, 21.

[119] Morrison, *China's Economic Rise*, 28.

"Just as the world has never seen a consumer like the American consumer, it has never seen a producer like China," posits Roach.[120] He argues that a marriage of convenience has occurred with the ever-increasing consumer demand of the United States and a never-ending supply of goods and surplus savings offered by China.[121] While neither nation intended to develop the interdependence that has occurred between both economies, disestablishing the relationship would require long-term economic restructuring for both nations.[122]

B. ALMOST PERFECT SYMMETRY

China's unprecedented economic growth and performance over the last three decades has increased the importance of its role in the world economy and transformed it into a global economic power, but China's growth remains dependent on U.S. economic strength and health. Likewise, U.S. reliance on Chinese foreign investments to fund budget deficits is equally dependent on China's economic well-being. Though Nye argues that perfect symmetry in an interdependent relationship is quite rare because "most cases of economic interdependence also involve a potential power relationship," the United States and China appear to have unintentionally achieved a nearly equivalent economic dependence, such that neither nation has accrued a particular power advantage over the other.[123] With economic strength as a dominant source of state power, the current economic interdependent relationship between the United States and China has been fraught with tension, yet sustained to ensure continued economic growth.

Most economists agree that China's economy will continue to grow over the next 15–20 years; however, there is little consensus on the rate of China's growth or when it will rival the United States as the world's largest economy.[124] Estimating the actual size

---

[120] Roach, *Unbalanced*, 16.

[121] Ibid., 21.

[122] This is an argument also made by Stephen Roach in *Unbalanced* and "China's 12th Five-Year Plan: Strategy vs. Tactics," Morgan Stanley, April 2011, http://www.law.yale.edu/documents/pdf/cbl/China_12th_Five_Year_Plan.pdf.

[123] Nye, *The Future of Power*, 55.

[124] "China 2030: Building a Modern, Harmonious, and Creative Society," 3; Morrison, *China's Economic Rise*, 6; Dadush, "Key Trends in the World Economy," 26.

of China's economy is a major debate among economists and is dependent on how GDP and GDP per capita are measured. For instance, in 2013, China's nominal GDP was $9.4 trillion, 56 percent the size of the of the U.S. nominal GDP of $16.8 trillion.[125] However, because the PPP basis increases the estimated measurement of China's economy, when looking at China's GDP for 2013 on a PPP basis, China's GDP increases to $13.6 trillion, making it 81 percent the size of the U.S. economy and significantly closer to reaching parity with the U.S. economy (see Table 1 and additional information on PPP below).[126] Despite the significant jump in GDP from nominal to PPP, per capita GDP paints a much starker picture for China when comparing economies. Even with a per capita increase from $6,960 to $10,060, China was still only 19 percent of the U.S. level and relatively poor in per capita terms (see Table 1).[127]

Table 1. Chinese, Japanese, and U.S. GDP and Per Capita GDP in Nominal U.S. Dollars and a Purchasing Power Parity Basis: 2013[128]

	China	Japan	United States
Nominal GDP ($ billions)	9,394	4,907	16,786
GDP in PPP ($ billions)	13,579	4,618	16,786
Nominal Per Capita GDP ($)	6,960	39,040	53,060
Per Capita GDP in PPP ($)	10,060	36,740	53,060

Source: Economist Intelligence Unit estimates using World Bank PPP data.

[125] Morrison, *China's Economic Rise*, 6.

[126] Wayne M. Morrison and Marc Labonte, *China's Holdings of U.S. Securities: Implications for the U.S. Economy* (CRS Report No. RL34314) (Washington, DC: Congressional Research Service, 2013), 7, http://fas.org/sgp/crs/row/RL34314.pdf. There are two ways to measure GDP per capita: nominal and PPP. Nominal is a fixed standard that remains the same from country to country, reflecting the prices of foreign currency to the U.S. dollar and excluding differences in the prices for goods and services between countries. For example, $1 exchanged for 1 yuan (RMB) would buy more in China than it would in the United States because prices for goods and services in China are relatively cheaper than in the United States. PPP is an attempt at estimating exchange rates based on actual purchasing power, taking factors of each country into consideration in order to put a number on a person's standard of living within that country. According to Joe Kern, http://applebutterdreams.wordpress.com/the-difference-between-gdp-nominal-and-gdp-ppp/, "PPP is how much of a local good a person can buy in their country, and nominal is roughly how much of an internationally traded good a person can buy in their country."

[127] Morrison, *China's Economic Rise*, 7.

[128] Ibid., 7.

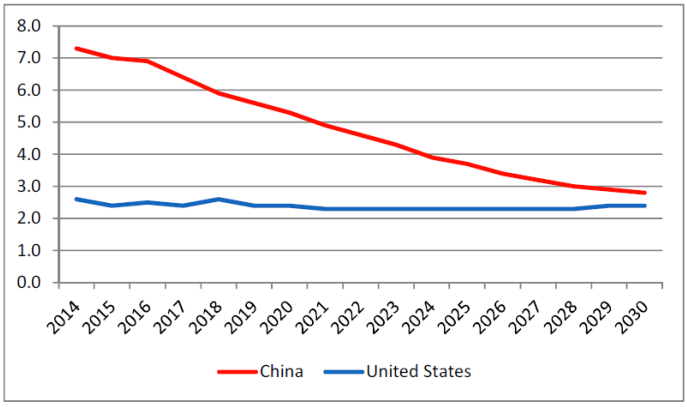
Although some analysts project that China may overtake the United States as the world's largest economy on a PPP basis as early as 2015, it will take years for its living standards to catch up to the United States (see additional information below).[129] China's PPP position may be used to improve its global economic stature and decision-making power within financial organizations like the IMF, but "China can't buy missiles and ships and iPhones and German cars in PPP currency," contends Tom Wright.[130] Even as the second-largest world economy on a PPP basis, China ranked 99th on a per capita basis and contributed half as much as the United States to the world GDP in 2011 (see Table 2). With China's real GDP growth projected to slow significantly and U.S. real GDP growth projected to maintain its current trajectory, it would be approximately 2030 before China truly challenges the United States as the world's largest economic power (see Figure 6).

[129] Tom Wright, China's Economy Surpassing the U.S.? Well, Yes and No," Real Time Economics (blog), *The Wall Street Journal*, April 30, 2014, http://blogs.wsj.com/economics/2014/04/30/chinas-economy-surpassing-u-s-well-yes-and-no/. In April 2014, the International Comparison Program, under the World Bank, introduced new calculations on the size on economies using a PPP basis. Based on the new calculations, China could overtake the United States in GDP on a PPP basis by late 2014/early 2015. The current GDP on a PPP basis for the United States is $16.8 trillion while China is now at $16.2. However, on a per capita basis, China still trails the U.S. by 78 percent.

[130] Ibid.

Table 2. Twelve Largest Economies by Share of World GDP: 2011[131]

Ranking by GDP (PPP-based)	Economy	Share of world GDP (PPP-based, world = 100)	Share of world GDP (exchange rate–based, world = 100)	Ranking by GDP per capita (PPP-based)
1	United States	17.1	22.1	12
2	***China***	***14.9***	***10.4***	***99***
3	***India***	***6.4***	***2.7***	***127***
4	Japan	4.8	8.4	33
5	Germany	3.7	5.2	24
6	***Russian Federation***	***3.5***	***2.7***	***55***
7	***Brazil***	***3.1***	***3.5***	***80***
8	France	2.6	4.0	30
9	United Kingdom	2.4	3.5	32
10	***Indonesia***	***2.3***	***1.2***	***107***
11		2.3	3.1	34
12	***Mexico***	***2.1***	***1.7***	***72***



Source: Economist Intelligence Unit.

Note: Long-range economic projections should be viewed with caution.

Figure 6. Projections of U.S. and Chinese Real GDP Growth Rates: 2014–2030[132]

131 International Comparison Program, "Purchasing Power Parities and Real Expenditures of World Economies: Summary of Results and Findings of the 2011 International Comparison Program," The World Bank, 2014, 81, http://siteresources.worldbank.org/ICPINT/Resources/270056-1183395201801/Summary-of-Results-and-Findings-of-the-2011-International-Comparison-Program.pdf. The country ranked number 11 was blank in the original report and no further details were provided explaining which country may be filling that position.

132 Morrison, *China's Economic Rise*, 6.

While bilateral tensions continue to grow over the current economic relationship, each equally encourages unsustainable monetary and fiscal policies. In the United States, despite an increase in personal savings rates since 2007, significant government budget deficits have slowed any real growth in U.S. savings. With the U.S. net national savings rate of only 1.4 percent of gross national income in the first quarter of 2014, the U.S. economy remains dependent on foreign capital inflows from China to fund the federal budget deficit, meet domestic investment needs, and keep U.S. real interest rates low.[133] Equally reliant on foreign capital, China's sizeable current account surpluses and an exchange rate policy that limits appreciation of Chinese currency—renminbi (RMB)—has led China to accumulate $3.5 trillion in foreign exchange reserves, 70 percent of which are estimated to be dollar holdings.[134] By 2013, the United States was the world's largest importer of foreign capital and China was the second largest exporter of foreign capital (see Figure 7).[135]

[133] Morrison and Labonte, *China's Holdings of U.S. Securities*, summary page and U.S. Department of Commerce Bureau of Economic Analysis, "National Income and Product Accounts Tables: 2010–2014," last revised June 25, 2014, Section 5 – Savings and Investment, http://www.bea.gov/iTable/iTable.cfm?ReqID=9&step=1#reqid=9&step=3&isuri=1&904=2010&903=137&906=q&905=2014&910=x&911=0.

[134] Morrison and Labonte, *China's Holdings of U.S. Securities*, 1.

[135] International Monetary Fund, "Global Financial Stability Report: Moving from Liquidity- To Growth-Driven Markets," April 2014, Statistical Appendix, http://www.imf.org/external/pubs/FT/GFSR/2014/01/index.htm.

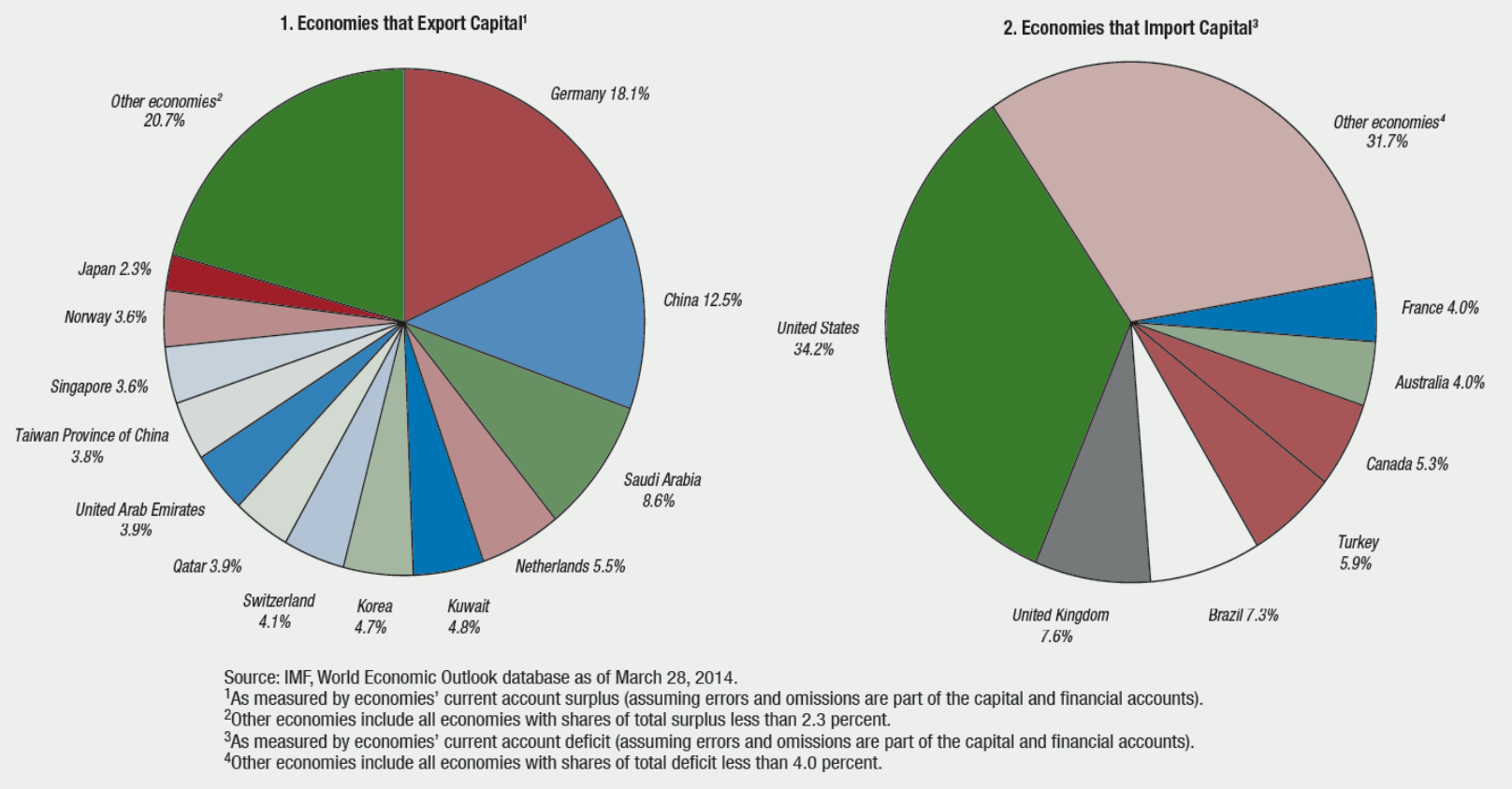


Figure 7. Major Net Exporters and Importers of Foreign Capital in 2013[136]

[136] "Global Financial Stability Report: Moving from Liquidity- To Growth-Driven Markets."

Decades of budget deficits and savings shortfalls in the United States have led private holdings of U.S. public debt to soar to $12.3 trillion in 2013, with 47 percent ($5.8 trillion) held by foreign private investors (see Table 3).[137] Of that 47 percent, China held 21.9 percent of all foreign holdings in U.S. federal debt totaling $1.3 trillion by the end of 2013 (see Table 4).[138]

Table 3. Estimated Ownership of U.S. Treasury Securities ($ Billions)[139]

End of Month	Total Publicly Held Debt	Foreign Holdings of Publicly Held Debt	Foreign Holdings as a Share of Total Publicly Held Debt
Dec. 2013	$12,328.3	$5,803.8	47.1%
Dec. 2012	$11,568.9	$5,573.8	48.2%
Dec. 2011	$10,428.3	$5,006.9	48.0%
Dec. 2010	$9,361.5	$4,458.8	47.6%
Dec. 2009	$7,781.9	$3,670.6	47.2%
Dec. 2008	$6,338.2	$3,253.0	51.3%

Source: Federal Reserve Board of Governors Flow of Funds, Table L.209 Treasury Securities, June 5, 2014 available at http://federalreserve.gov/releases/z1/.

[137] Marc Labonte and Jared C. Nagel, *Foreign Holdings of Federal Debt* (CRS Report No. RS22331) (Washington, DC: Congressional Research Service, 2014), 1, http://fas.org/sgp/crs/misc/RS22331.pdf.

[138] Labonte and Nagel, *Foreign Holdings of Federal Debt*, 2. According to Morrison and Labonte in *China's Holdings of U.S. Securities*, The People's Bank of China as the largest holder of U.S. public debt.

[139] Ibid., 1.

Table 4. The Top 10 Foreign Holders of Federal Debt by Country: 2009 and 2013[140]

	As of December 2013			As of December 2009	
Country	Amount Held ($ billions)	Percentage of all foreign holdings in federal debt	Country	Amount Held ($ billions)	Percentage of all foreign holdings in federal debt
Mainland China	$1,270.0	21.9%	Mainland China	$ 894.8	24.3%
Japan	$1,182.5	20.4%	Japan	$ 765.7	20.8%
Caribbean Banking Centers	$295.3	5.1%	Oil Exporters	$ 201.1	5.5%
Belgium	$256.8	4.4%	United Kingdom	$ 180.3	4.9%
Brazil	$245.4	4.2%	Brazil	$ 169.2	4.0%
Oil Exporters	$238.3	4.1%	Hong Kong	$ 148.7	4.0%
Taiwan	$182.2	3.1%	Russia	$ 141.8	3.9%
Switzerland	$176.7	3.1%	Caribbean Banking Centers	$ 128.2	3.5%
United Kingdom	$163.7	2.8%	Taiwan	$ 116.5	3.2%
Hong Kong	$158.8	2.7%	Switzerland	$ 89.7	2.4%
Total Top 10 Countries of Foreign Investors in Federal Debt	$4,169.7	71.9%	Total Top 10 Countries of Foreign Investors in Federal Debt	$2,836.0	77.0%
Total All Foreign Investment in Federal Debt	$5,802	100%	Total All Foreign Investment in Federal Debt	$3685.1	100%

Source: Treasury Department International Capital System (TIC), at http://www.treasury.gov/resource-center/data-chart-center/tic/Documents/mfhhis01.txt.

Notes: Data, including estimated foreign holders of federal debt historically by month, in these Treasury Department tables are periodically adjusted. Current monthly estimates are available at http://www.treas.gov/tic/

According to Wayne Morrison and Marc Labonte, "rather than hold dollars (and other foreign currencies), which earn no interest, the Chinese central government has converted some level of its foreign exchange reserve holdings into U.S. financial securities, including U.S. Treasury securities, U.S. agency debt, U.S. corporate debt, and U.S. equities."[141] With U.S. Treasury securities as the main mechanism for the U.S. government to finance the federal debt and the largest category of U.S. securities, foreign holdings of U.S. Treasury securities grew to $5.6 trillion by June 2013. China alone held $1.3 trillion of that $5.6 trillion in U.S. Treasury securities (see Table 5). This substantial amount accounts for 22.8 percent of total foreign holdings of U.S. Treasury securities (see Table 6).[142]

[140] Ibid., 2.

[141] Morrison and Labonte, *China's Holdings of U.S. Securities*, 1.

[142] Ibid., 8.

Table 5. China's Year-End Holdings of U.S. Treasury Securities: 2003–2012 and as of May 2013[143] ($ Billions and as a Percentage of Total Foreign Holdings)

	2003	2005	2007	2009	2010	2011	2012	May 2013
China's Holdings ($billions)	159.0	310.0	477.6	894.8	1,160.1	1,151.9	1,220.4	1,275,8
Holdings as a % of Total Foreign Holdings	10.4%	15.2%	20.3%	24.2%	26.1%	23.0%	21.9%	22.8%

Source: Department of Treasury, Major Foreign Holders of Treasury Securities Holdings, August 15, 2013.

Table 6. Top 5 Foreign Holders of U.S. Treasury Securities as of June 2013[144]

	Total Foreign Holdings ($ billions)	Country Holdings as a Share of Total Foreign Holdings (%)
China	1,275.8	22.8
Japan	1,083.4	19.3
Caribbean Banking Centers	290.8	5.2
Oil Exporters	256.8	4.6
Brazil	253.7	4.5
Total Foreign Holdings	5,600.6	100.0

Source: Department of Treasury, *Major Foreign Holders of Treasury Securities Holdings*, August 15, 2013.

Although a number of U.S. policymakers have raised concerns over the U.S. dependency on China to help fund the U.S. budget deficit through purchase of U.S. securities, the ability to borrow from China keeps U.S. interest rates low, increases private investment, and prevents GDP stagnation. In 2010 and 2011, the U.S. Congress attempted to enact trade sanctions against China to counter its alleged currency manipulation, failing to understand that the steep tariffs placed on goods from China

[143] Ibid., 9.

[144] Ibid.,10.

could backfire on the United States by raising the costs of U.S. imports, rapidly depreciating the dollar's value, and causing interest rates to soar.[145] Simply put by Labonte and Nagel, "foreign purchases of Treasury securities reduce the federal government's borrowing costs and reduce the costs the deficit imposes on the broader economy."[146] The problem for the United States is not foreign holdings of U.S. debt, but rather massive and sustained deficits. According to Derek Scissors, the longer the United States maintains enormous budget deficits, "the more likely it is that U.S. treasuries will become relatively less attractive, thereby tipping the balance of influence toward China."[147]

China has also voiced concerns over the growing economic interdependence and the safety of its large accumulation of U.S. debt.[148] Morrison and Labonte write: "Chinese officials have criticized U.S. fiscal and monetary policies, such as quantitative easing by the U.S. Federal Reserve, arguing that they could lead to higher U.S. inflation and/or a significant weakening of the dollar, which could reduce the value of China's U.S. debt holdings in the future."[149] Despite China's apprehensions, U.S. securities continue to be its investment of choice for a number of reasons: U.S. securities are considered to be safe and liquid compared to other types of investments; interest and principal payments are guaranteed and backed by the full faith and credit of the U.S. government; and "in order to maintain the exchange rate effects that lay behind the acquisition of U.S. dollars, those dollars must be invested in dollar-denominated securities."[150]

---

[145] Roach, *Unbalanced*, x, xi and Morrison and Labonte, *China's Holdings of U.S. Securities*, 14.

[146] Labonte and Nagel, *Foreign Holdings of Federal Debt*, 4.

[147] *China's Role in the Origins of and Responses to the Global Recession: Testimony before the U.S.-China Economic and Security Review Commission*, (2009) (statement of Derek Scissors, Research Fellow for Asia Economic Policy, The Heritage Foundation), http://www.heritage.org/research/testimony/testimony-before-the-us-china-economic-and-security-review-commission-on-chinas-role-in-the-origins-of-and-responses-to-the-global-recession.

[148] Morrison and Labonte, *China's Holdings of U.S. Securities*, 10.

[149] Ibid., summary page.

[150] Ibid., 5.

Above all, the massive accrual of foreign reserve holdings is likely the biggest driver in Chinese investment in U.S. securities. As the world's largest economy and biggest capital market, the United States is the only global market large enough to accommodate China's substantial foreign holdings. The financial crisis in Europe and economic issues in Japan have left China with few options to invest its sizeable foreign reserves.[151] In his hearing before the U.S.-China Economic and Security Review Commission, Research Fellow for Asia Economic Policy at The Heritage Foundation, Derek Scissors testified that "Chinese investment is largely involuntary, a function of having a great deal of money and no place else to put it. Who needs the other more varies with American and international financial conditions.

The more money the U.S. borrows, the more the American economy needs the PRC. The more desirable Treasury bonds are, the more China needs us."[152] The ultimate goal in any interdependent relationship between states is to create asymmetries in order to become the less dependent and increase power relative to another state. Less dependence can mean more power. Clearly articulating the dangers to the United States of a Chinese economic rebalancing, Stephen Roach writes:

> Therein lies what could be a critical source of global tension – an asymmetrical global rebalancing scenario. China, the world's largest surplus saver, could well rebalance before the United States, the world's largest deficit saver. Such an outcome could prove quite problematic for the U.S. economy and for world financial markets.[153]

C. CHINA TIPPING THE SCALES

In March 2007, Premier Wen Jiaboao publicly stated that China's economy had become unstable, unbalanced, uncoordinated, and unsustainable.[154] China has recognized the need for major economic structural rebalancing. Economic reforms in China are not

---

[151] Morrison and Labonte, *China's Holdings of U.S. Securities*, 5, 14 and Labonte and Nagel, *Foreign Holdings of Federal Debt*, 4.

[152] *China's Role in the Origins of and Responses to the Global Recession*.

[153] Stephen S. Roach, "China's 12th Five-Year Plan: Strategy vs. Tactics," Morgan Stanley, April 2011, 8, http://www.law.yale.edu/documents/pdf/cbl/China_12th_Five_Year_Plan.pdf.

[154] Stephen S. Roach, *The Next Asia: Opportunities and Challenges for a New Globalization* (Hoboken, NJ: John Wiley & Sons Inc., 2009), 229.

only required to lessen dependence on the United States, but to fix substantial underlying structural problems that threaten to hamper its long-term growth. The question is now more about how China will go about such a significant economic transformation.

Acknowledging the need for major economic restructuring to sustain economic growth, China's last two FYPs (Eleventh FYP from 2006 to 2010 and Twelfth FYP from 2011 to 2015) shifted economic emphasis from an export and investment-led economy to a consumer-led economy, placing heavy emphasis on indigenous innovation.[155] Thus, far, China's real GDP growth has been dependent on fixed investment and exports, but as China's technological development reaches the levels of major developed nations, it must implement widespread economic reforms and become a major center for new technology and innovation to prevent economic stagnation.[156] In 2013, Chinese President Xi Jinping re-emphasized the need for increased indigenous innovation to strengthen economic development by stating: "Implementing a strategy of innovation-driven development will be fundamental in accelerating the transformation of China's growth pattern, solving deep-rooted problems concerning economic development, and enhancing economic vitality."[157]

Deeming science and technology crucial to economic development and international competitiveness, China adopted a policy of indigenous innovation (*zizhu chuangxin*) in 2006, defining indigenous innovation as "enhancing original innovation through co-innovation and re-innovation based on the assimilation of imported technologies."[158] Consequently, the 2006 National Medium to Long-Term Plan for the Development of Science and Technology, 2006–2020 (MLP) was developed in an effort

---

155 Joseph Casey and Katherine Koleski, *Backgrounder: China's 12th Five-Year Plan* (Washington, DC: U.S.-China Economic and Security Review Commission, 2011), 1, 3, 8, http://www.uscc.gov/Research/backgrounder-china%E2%80%99s-12th-five-year-plan.

156 Morrison, *China's Economic Rise*, 5.

157 "Xi Urges Innovation-Driven Growth," *Xinhua*, March 4, 2013, http://news.xinhuanet.com/english/china/2013-03/04/c_132207617.htm.

158 James McGregor, "Drive for 'Indigenous Innovation': A Web of Industrial Policies," APCO Worldwide, July 2010, 4, https://www.uschamber.com/sites/default/files/legacy/reports/100728chinareport_0.pdf.

to shift from its current growth model to a more sustainable model by making scientific modernization and indigenous innovation the drivers of future economic growth.[159]

Micah Springut, Stephen Schlaikjer, and David Chen argue however, that indigenous innovation means something vastly different in China than it does in the United States. For China, indigenous innovation is not necessarily technological self-sufficiency or the creation of new ideas, but rather extracting desired technology and adapting it for the needs of the nation.[160] The MLP clearly identifies foreign technology as a key component to the development of Chinese IP and technological innovation.[161] "As a result, the plan is considered by many international technology companies to be a blueprint for technology theft on a scale the world has never seen before," writes James McGregor.[162] Despite China's push for a significant reduction in foreign technology dependence, Chinese policies that inhibit research creativity, favor particular government industries, and neglect protection of IP rights prevent Chinese indigenous innovation from reaching its full potential and have led to technological gaps that can only be filled by foreign research and technology.

As China's dependence on foreign technology has grown, so have its conflicts with the United States over IP rights and technology transfer standards. Unfair trade practices, policies that support and protect particular government favored Chinese industries, widespread infringement of U.S. intellectual property rights, and trade and investment barriers that limit opportunities for U.S. in China have done little to quell U.S. concerns.[163]

---

[159] Micah Springut, Stephen Schlaikjer, and David Chen, *China's Program for Science and Technology Modernization: Implications for American Competitiveness*, Prepared for The U.S.-China Economic and Security Review Commission (Arlington; VA: CENTRA Technology, Inc., 2011), 6, 11, http://origin.www.uscc.gov/sites/default/files/Research/USCC_REPORT_China%27s_Program_forScience_and_Technology_Modernization.pdf. The 2006 National Medium to Long-term Plan for the Development of Science and Technology (2005-2020) is also commonly referred to as the MLP and 15-Year Science and Technology Plan.

[160] Ibid., 7.

[161] McGregor, "Drive for 'Indigenous Innovation,'" 4.

[162] Ibid., 4.

[163] Morrison, *China-U.S. Trade Issues*, 1.

William Hannas, James Mulvenon, and Anna Puglisi argue that "China's quest for foreign technology goes well beyond the modest efforts to supplement indigenous research that most countries pursue as common practice. Rather, it is part of a deliberate, state-sponsored project to circumvent the costs of research, overcome cultural disadvantages, and 'leapfrog' to the forefront by leveraging the creativity of other nations."[164] Given the economic interdependence between the United States and China, and the fact that the United States is one of the biggest leaders in technology and innovation, it makes sense that China would seek to fill important capability gaps through espionage and theft of U.S. IP. Roach argues that although China and the United States have become increasingly more reliant on each other for economic growth, "there are no guarantees that both nations are equally afflicted," resulting in the development of an "asymmetrical coping mechanism."[165]

The following chapter investigates how, because U.S. innovation and IP is a critical source of U.S. economic growth and global competitiveness, China has chosen cyber-enabled illicit acquisition of U.S. technology and intellectual property as its asymmetrical coping mechanism to shift the balance of power within U.S.-China economic interdependence.

[164] William C. Hannas, James Mulvenon, and Anna B Puglisi, *Chinese Industrial Espionage: Technology acquisition and military modernization* (New York: Routledge, 2013), 78.

[165] Roach, *Unbalanced*, ix.

III. CHINESE CYBER-ENABLED ECONOMIC ESPIONAGE

Although concerns about cyberspace and cyber security have leapt to the forefront of U.S.-China relations, China's cyber behavior cannot be dissociated from its political and economic relations. "China poses an especially difficult problem [to the United States], given the size and importance of its economy and the interdependence of the Chinese economy with those of the United States, Europe, and Japan," argues the IP Commission.[166] As the interdependence between U.S. and China expands U.S. markets, it also provides Chinese government agencies and Chinese businesses greater opportunities to collect sensitive U.S. economic information while leapfrogging the Research and Development (R&D) phase.[167] Hannas, Mulvenon, and Puglisi emphasize how important timing has been for China, reasoning that China is "emerging as a global economic power at a time when nearly every secret worth stealing sits on a computer server."[168]

With the global rise of the Internet, the United States has witnessed massive intrusion and data exfiltration campaigns against U.S. public and private industries by the Chinese government and Chinese government-owned enterprises. According to McAfee, "Numerous sources of intellectual property exist inside today's global companies…to say these intellectual property sources represent the heart and core value of companies worldwide is an understatement. When these intellectual property sources get compromised, capitalism and commerce are compromised on a global scale."[169]

---

[166] The Commission on the Theft of American Intellectual Property, *The IP Commission Report* (Washington, DC: The National Bureau of Asian Research, 2013), 21, http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

[167] Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011* (Washington, DC: Office of the Director of National Intelligence, 2011), 8, http://www.ncix.gov/publications/reports/fecie_all/.

[168] Hannas, Mulvenon, and Puglisi, *Chinese Industrial Espionage*, 78.

[169] McAfee, "Protecting Your Critical Assets: Lessons Learned from 'Operation Aurora,'" McAfee Labs and McAfee Foundstone Professional Services, January 2010, 4, http://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf.

Economic espionage not only affects revenue and income, but undermines corporate innovation, having devastating effects on the national and global economy. "In a world where the highest-value assets are intangible and easy to transfer over networks, espionage has taken on a new dimension," argues the IP Commission.[170] China has swiftly adapted to this new environment by shifting its traditional intelligence collection operations to cyber collection operations. "Given the choice between traditional espionage and cyber espionage, it is only natural that intelligence services would increasingly pick the less risky, cheaper, and faster way of doing business," state Hannas, Mulvenon, and Puglisi.[171] China has taken economic espionage to a new level through cyberspace, stealing sensitive U.S. economic data at an unprecedented rate and with significant costs to the U.S. economy.

A. COSTS TO THE U.S. ECONOMY

Many analysts believe that trade secrets, proprietary information, copyrights, patents, and trademarks, all considered IP, represent the U.S. advantage in the global economy. Theft of IP by foreign economic competitors jeopardizes this advantage by inhibiting the business sector's "ability to create jobs, generate revenues, foster innovation, and lay the economic foundation for prosperity and national security."[172] The IP Commission Report assesses the damage to the U.S. economy to be approximately $300 billion a year, with 50 percent to 80 percent of international IP theft originating in China (see additional information below).[173]

Yet the cost of cyber-enabled economic espionage includes more than the stolen property itself. James Lewis argues that "there are opportunity costs, damage to brand

---

[170] The Commission on the Theft of American Intellectual Property, *The IP Commission Report*, 43.

[171] William C. Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology acquisition and military modernization* (New York: Routledge, 2013), 218.

[172] *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets* (Washington, DC: The White House, 2013), 1, 3, http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

[173] The Commission on the Theft of American Intellectual Property, *The IP Commission Report*, 2. According to the U.S.-China Economic and Security Review Commission in its *2013 Annual Report to Congress*, although the economic impact of cyber espionage to the United States is significant, precise economic costs are difficult to calculate because of the intangible nature of the assets themselves.

and reputation, consumer losses from fraud, the opportunity costs of service disruptions 'cleaning up' after cyber incidents, and the cost of increased spending on cyber security."[174] Moreover, IP theft slows the development of new inventions and new industries by undermining the means and the incentive for entrepreneurs to innovate, causing stagnation of innovation and inhibiting expansion of the world economy.[175]

To put the intellectual property loss into perspective, the U.S. Department of Commerce identified 75 of 313 U.S. industries as IP-intensive that directly accounted for 27.1 million U.S. jobs and 18.8 percent of all employment in the 2010 economy. These IP-intensive industries also accounted for 34.8 percent of U.S. GDP while indirectly supporting 12.9 million additional supply-chain jobs throughout the economy. All in all, the most IP-intensive industries either directly or indirectly accounted for 27.7 percent of all jobs (40 million jobs) in the United States and 60.7 percent of total U.S. merchandise exports ($775 billion) in 2010.[176]

China, however, has threatened U.S. technological competitiveness and economic prosperity for more than a decade through the use of cyberspace. In a hearing before the House Committee on Foreign Affairs, Lewis stated the United States has always been upfront with China that "espionage is a two-way street, something that all great powers do, and that espionage against military and political targets is legitimate" but that the United States "objects to economic espionage" and "rampant commercial cyber espionage."[177] The U.S. International Trade Commission estimates Chinese theft of U.S. intellectual property in the form of lost sales, royalties, and license fees to be $48.2 billion in 2009 alone with another $4.8 billion spent by firms to address Chinese

---

[174] James Lewis and Stewart Baker, *The Economic Impact of Cybercrime and Cyber Espionage* (Washington, DC: Center for Strategic and International Studies, 2013), 5, 6, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf.

[175] The Commission on the Theft of American Intellectual Property, *The IP Commission Report*, 10.

[176] Economics and Statistics Administration and U.S. Patent and Trademark Office, *Intellectual Property and the U.S. Economy: Industries in Focus* (Washington, DC: U.S. Department of Commerce, 2012), vi-viii, http://www.uspto.gov/news/publications/IP_Report_March_2012.pdf.

[177] *Asia: The Cybersecurity Battleground: Hearings Before House Committee on Foreign Affairs Subcommittee on Asia and the Pacific*, *House Committee on Foreign Affairs*, 113th Cong., 1 (2013) (statement of James A. Lewis, Director and Senior Fellow, Technology and Public Policy Program, Center for Strategic International Studies), https://foreignaffairs.house.gov/hearing/subcommittee-hearing-asia-cyber-security-battleground.

infringement.[178] Because "the entire U.S. economy relies on some form of IP," with every industry using or producing it, the theft of IP by China directly affects U.S. strength in the global economy.[179]

B. SEIZING THE ADVANTAGE

With cyber espionage forming such a significant portion of Chinese economic growth, Chinese leadership likely will be unwilling to put this at risk. "There will be a domestic political price for Beijing to bring cyber espionage under control and little incentive for the party's leadership to pay this price absent external pressure and a changed view of what best serves China's own interests," asserts Lewis.[180] Lewis continues: "China uses cyber techniques to redress what it sees as an imbalance of power, using cyber espionage to compensate for its technological lag and weak national innovation capability."[181] While economic espionage is a problem in many developing nations, it is especially prevalent in China where its future as a regional hegemon rests on continued economic growth and prosperity.

Despite U.S. condemnation, the number of cyber-espionage and cyber-theft intrusions attributed to private Chinese companies, Chinese state-owned enterprises, and the Chinese government continues to grow. The following cases of Chinese cyber-enabled economic espionage clearly show the pervasiveness of China's economic espionage and how cyberspace is being used to alter the balance of economic power between the United States and China.

Night Dragon: Beginning in late 2009, China conducted coordinated covert cyber attacks against the global energy sector, specifically sensitive competitive proprietary operations and project-financing information on global oil, energy, and petrochemical

---

[178] *China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy* (USITC Publication No. 4226) (Washington, DC: U.S. International Trade Commission, 2011), xiv, xv, http://www.usitc.gov/publications/332/pub4226.pdf.

[179] Economics and Statistics Administration and U.S. Patent and Trademark Office, *Intellectual Property and the U.S. Economy*, vi.

[180] *Asia: The Cybersecurity Battleground*.

[181] *Ibid*.

companies.[182] Using servers in the United States and the Netherlands, files focusing on operational oil and gas field production systems and financial documents related to field exploration and bidding were copied and downloaded from oil, energy, and petrochemical companies as well as executives in Kazakhstan, Taiwan, Greece, and the United States for at least two years.[183] Based on the operations originating from several locations within China and the use of cyber tools and techniques developed in China, McAfee publicly attributed these attacks, named *Night Dragon*, to China in 2011.[184]

APT1: In one of the most important unclassified documents released on cyber attacks against the United States, the Mandiant Intelligence Report attributed 141 cyber intrusion victims to the 2nd Bureau of the People's Liberation Army (PLA), also known by its cover name of Unit 61398, bridging the gap between one of the most persistent Chinese cyber actors and the Chinese government.[185] Since 2006, APT1 has stolen hundreds of terabytes of data including technology blueprints, proprietary manufacturing processes, minutes from meetings involving high-ranking personnel, test results, business plans, pricing documents, partnership agreements, and emails of high-ranking employees from 20 major industries.[186]

The Mandiant report claims the reason the economic espionage was so persistent, extensive, and successful was because it received direct support from the Chinese government. The report states: "APT1 has demonstrated the capability and intent to steal from dozens of organizations across a wide range of industries virtually simultaneously…The scope of APT1's parallel activities implies that the group has significant personnel and technical resources at its disposal."[187] Although Mandiant has witnessed the exfiltration of massive volumes of valuable intellectual property from

---

[182] McAfee, "Global Energy Cyberattacks: 'Night Dragon,'" McAfee Foundstone Professional Services and McAfee Labs, February 10, 2011, 4, 7, http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf.

[183] Ibid.

[184] Ibid., 3, 7.

[185] *APT1*, 2–3.

[186] Ibid.

[187] Ibid., 22.

APT1, they believe this is only a small portion of the cyber espionage that APT1 has executed since its inception.[188]

Operation Shady Rat: In 2011, McAfee published the results of a five-year targeted cyber operation that hit at least 71 global organizations, including U.S. federal, county, and state governments; defense contractors; Fortune 100 companies, the United Nations, and the International Olympic Committee. Of the 71 victims, 49 were U.S. companies, government agencies, defense contractors, and non-profit organizations. The most heavily targeted victims were U.S. government entities (15 total) and U.S. defense contractors (12 total).

While McAfee does not directly attribute the attacks to a specific actor, one only has to read the facts in the report to understand that a direct finger was being pointed at China.[189] McAfee emphasizes the importance of these intrusions stating:

> What we have witnessed over the past five to six years has been nothing short of a historically unprecedented transfer of wealth—closely guarded national secrets (including those from classified government networks), source code, bug databases, email archives, negotiation plans and exploration details for new oil and gas field auctions, document stores, legal contracts, supervisory control and data acquisition (SCADA) configurations, design schematics, and much more has "fallen off the truck" of numerous, mostly Western companies and disappeared in the ever-growing electronic archives of dogged adversaries.[190]

Operation Aurora: *Operation Aurora*, also referred to as the Google hacking attack that occurred in January 2010, targeted at least 34 companies in the technology, financial, and defense sectors to gain access to and potentially modify source code repositories that Dmitri Alperovitch states are "the crown jewels of most of these companies" and "much more valuable than any financial or personally identifiable

---

[188] Ibid., 2–4, 20. Of the 141 victims, 115 were in the United States.

[189] Dmitri Alperovitch, *Revealed: Operation Shady RAT* (Santa Clara, CA: McAfee, 2011), 3–6, http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

[190] Ibid., 2.

data."[191] McAfee, which attributes the attacks to the Chinese government, called these attacks a "watershed event" for two reasons.

First, a new precedent had been set by a company as large as Google with openly admitting to a security breach. Second, while cyber espionage is common between foreign governments, it was a "big game-changer" for corporations to witness attacks from a government into corporate entities.[192] Alperovitch stated that "we have never ever, outside of the defense industry, seen commercial industrial companies come under that level of sophisticated attack."[193] Directly after the attacks were identified, Google publicly announced that the highly sophisticated attacks successfully targeted IP at Google and other high-value companies.[194]

American Superconductor Corporation: Between 2008 and 2011, the American Superconductor Corporation (AMSC) lost 90 percent of its stock value after its wind-energy software code was stolen by a major customer in China. While AMSC engineers were troubleshooting a turbine malfunction in China, they discovered the hardware had been running on a pirated version of AMSC's software. In March 2011, China's Sinovel Wind Group, AMSC's largest customer, abruptly ended the contract, which accounted for more than $210 million in 2010 revenue, causing investors to flee. Within six months, AMSC lost 84 percent of its value.[195]

In 2011, a software engineer for AMSC's research facility confessed to being hired by Sinovel to create turbine software using stolen source code from AMSC's server. According to Michael Riley and Ashlee Vance, the Chinese government was equally complicit. Sinovel was given advanced information on state-planned wind farms

---

[191] Kim Zetter, "'Google' Hackers Had Ability to Alter Source Code," *Wired*, March 3, 2010, http://www.wired.com/2010/03/source-code-hacks/.

[192] William Jackson, "How Google attacks changed the security game," Global Compliance Network, Sep 01, 2010, http://gcn.com/articles/2010/09/06/interview-george-kurtz-mcafee-google-attacks.aspx.

[193] Kim Zetter, "Google Hack Attack Was Ultra Sophisticated, New Details Show," Wired, January 14, 2010, http://www.wired.com/2010/01/operation-aurora/.

[194] Zetter, "Google Hack Attack Was Ultra Sophisticated, New Details Show."

[195] Michael A. Riley and Ashlee Vance, "China Corporate Espionage Boom Knocks Wind Out of U.S. Companies," *Bloomberg Businessweek*, March 15, 2012, http://www.bloomberg.com/news/2012-03-15/china-corporate-espionage-boom-knocks-wind-out-of-u-s-companies.html.

by the Chinese government prior to government bidding for a mega-wing project in 2008 and eventually awarded 47 percent of the project. Adding insult to injury, the day after the IP theft went public, AMSC computer networks were hit by a cyber attack in which company executives were emailed spyware designed to copy confidential data and internal communications.[196]

Fortune 500 Manufacturing Company: In 2010, Mandiant reported that an APT compromised computers of senior executives within a U.S. Fortune 500 manufacturing company that was negotiating the acquisition of a Chinese corporation. During the negotiation period between the two companies, sensitive pricing data and details on U.S. negotiation strategies was exfiltrated on a weekly basis. Mandiant assessed that because the executives targeted were directly involved in the negotiations with the Chinese company, it was most likely an effort by the Chinese company to gain an advantage during negotiations. Although early notification of the compromise allowed the U.S. manufacturing corporation to cancel the acquisition, their business objectives were unable to be fulfilled.[197]

DuPont and Cargill: In 2011, a Chinese scientist was convicted of Economic Espionage and Theft of Trade Secrets for providing scientists at Hunan Normal University, the National Natural Science Foundation of China, and China's 863 Program (all three funded by the Chinese government) with sensitive data on agrochemical and biotechnology products from Dow AgroSciences and Cargill Inc. Kexue Huang, a research scientist and research leader in the development of biotechnology development for organic insecticides for Dow AgroSciences from 2003–2008 and as a biotechnologist for Cargill, Inc., from 2008–2009, transferred stolen proprietary data with the intent of benefiting the government of China.

Huang used the stolen materials to conduct unauthorized research with students from Hunan Normal University, earning grant money from the National Natural

---

196 Ibid.

197 Mandiant, *Mandiant M-Trends: the advanced persistent threat* (Alexandria, VA: Mandiant, 2010), 20, https://dl.mandiant.com/EE/assets/PDF_MTrends_2010.pdf?elq=3c9ad31542594c9184e8dcf552d66792&elqCampaignId=.

Foundation of China to conduct further research and publish findings in scientific journals in China. Additionally, Huang identified manufacturing facilities in China that could produce products based on the stolen research and compete directly with Dow in the established organic pesticide market.[198] Huang also admitted to downloading DNA sequences for a key component in the manufacture of a new food product while at Cargill and providing it to scientists at Hunan Normal University. The Department of Justice estimates the loss from misappropriated trade secrets somewhere between $7 million and $20 million.[199]

Chinese Telecommunications: In October 2012, the House Permanent Select Committee on Intelligence (HPSCI) issued an investigative report on two Chinese telecommunication companies, Huawei Technologies and ZTE Inc., concluding that "risks associated with Huawei's and ZTE's provision of equipment to U.S. critical infrastructure could undermine core U.S. national-security interests."[200] During a year-long investigation requested by Huawei Technologies, the HPSCI discovered evidence of both economic espionage, through the extraction of sensitive information and IP from U.S. companies; and state-sponsored support from the Chinese government, with Huawei having direct ties to China's Signals Intelligence Division.[201]

During testimony before the HPSCI during the investigation, Huawei and ZTE attested that the backdoors (illegal remote access to a computer) found in their software were not intentional vulnerabilities, but rather flaws in the software itself.[202] Though the

---

[198] United States of America versus Kexue Huang, Plea Agreement, Docket Number: 1:10-cr-00102, August 9, 2011, http://tsi.brooklaw.edu/sites/tsi.brooklaw.edu/files/filings/united-states-v-huang/20110809plea-agreement.pdf .

[199] *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*, Annex B, 23.

[200] House Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE* (Washington, DC: U.S. House of Representatives, 2012), vi, https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf.

[201] House Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, 14 and Michael S. Schmidt, Keith Bradsher, and Christine Hauser, "U.S. Panel Cites Risks in Chinese Equipment." *New York Times*, October 8, 2012, http://www.nytimes.com/2012/10/09/us/us-panel-calls-huawei-and-zte-national-security-threat.html?pagewanted=all&_r=0.

[202] Schmidt, Bradsher, and Hauser, "U.S. Panel Cites Risks in Chinese Equipment."

precedence set by the HPSCI report has significant national security implications, it also signifies U.S. government understanding of China's attempts to shift the economic balance of power in their favor using advanced technology in cyberspace. The report affirms: "The capacity to maliciously modify or steal information from government and corporate entities provides China access to expensive and time-consuming research and development that advances China's economic place in the world."[203]

While China continues to deny allegations of economic espionage and cyber intrusions into U.S. systems, the depth of resources necessary to sustain the current scope of computer network exploitation far exceeds the capabilities of hackers and cyber criminals and is nearly impossible without some type of state-sponsorship.[204] The overwhelming evidence presented by Mandiant in its *APT1* report is a testament to this premise.[205] Furthermore, the existence of a government program, identified by the Office of the National Counterintelligence Executive as Project 863, aimed at directing and funding the procurement of sensitive economic data and U.S. technology through clandestine means, highlights the magnitude of the operations China is undertaking to shift the balance of power.

C. ECONOMIC GROWTH PLANS OR CYBER ROAD MAPS?

The proliferation of cyberspace and upsurge in computer technology combined with a number of major economic challenges has made cyber-enabled economic espionage vital to China's economic development. Cyber-enabled economic espionage allows China to produce new sources of technology without having to invest the time and money to conduct R&D and without having to address distortive economic policies such as government support for state-owned firms and the lack of the rule of law in China.[206] While China continues to deny allegations of economic espionage and cyber intrusions into U.S. systems, China's cyber-enabled economic espionage clearly corresponds to the

---

[203] House Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, 3.

[204] Krekel, *Capability of the People's Republic of China*, 8.

[205] *APT1*, 6, 19.

[206] Morrison, *China's Economic Rise*, 1–2.

technological advancement and indigenous innovation initiatives identified in both its Twelfth FYP and National Medium to Long-Term Plan for the Development of Science and Technology, 2006–2020 (MLP). This section discusses how, essentially, China is using advanced cyber tools to steal the data it needs to meet the technology and innovation goals outlined in both plans.

China's Twelfth FYP, designed like previous FYPs as an economic roadmap to communicate policy goals, differs from previous plans by placing a much larger emphasis on scientific development and indigenous innovation.[207] One of the major features of the Twelfth FYP is the concept of seven strategic emerging industries (SEIs) that are instrumental in China's push for a more advanced technology-driven economy and increasing the global competitiveness of Chinese businesses to support sustained economic growth. Three of the SEIs are designed to promote sustainable growth, while the remaining four are designed to move China up in global competitiveness. The seven SEIs within the Twelfth FYP are as follows:[208]

Sustainable Growth:

1. Clean Energy Technology: Including high-efficiency and energy saving equipment, pollution control, and advanced environmental protection.

2. Alternative Energy: Including smart power grids; and nuclear, solar, wind, and biomass power.

3. Clean Energy Vehicles: Including electric hybrid cars, pure electric cars, and fuel cell cars.

Increase Global Competitiveness:

4. Next-Generation Information Technology: Including cloud computing, integrated circuits, smart devices, high-end software and servers, next-generation Internet equipment, and telecommunications.

5. Biotechnology: Including biopharmaceuticals, biomedicine, biomanufacturing, marine biology, and innovative pharmaceuticals.

6. New Materials: Including high-performance composites, new function materials, semiconductors, LED, special glass, and structural materials.

---

207 Casey and Koleski, *Backgrounder: China's 12th Five-Year Plan*, 1, 4, 8.

208 Ibid., 1, 4, 8.

7. High-End Equipment Manufacturing: Including aerospace and space, rail and transportation, ocean engineering, and smart assembly.

Intended as "the backbone of China's next phase of industrial modernization and technological development," the Twelfth FYP may also be viewed as a blueprint for economic espionage and theft of IP.[209] Mandiant states that "organizations in all industries related to China's strategic priorities are potential targets of *APT1's* comprehensive cyber espionage campaign" pointing out that 115 of the 141 *APT1* victims "match industries that China has identified as strategic to their growth, including four of the seven strategic emerging industries that China identified in its 12th Five-Year Plan" (see Figure 8).[210]

[209] The U.S.-China Business Council, "China's Strategic Emerging Industries: Policy, Implementation, Challenges, & Recommendations," March 2013, 1, http://uschina.org/sites/default/files/sei-report.pdf.

[210] *APT1: Exposing One of China's Cyber Espionage Units*, 4.

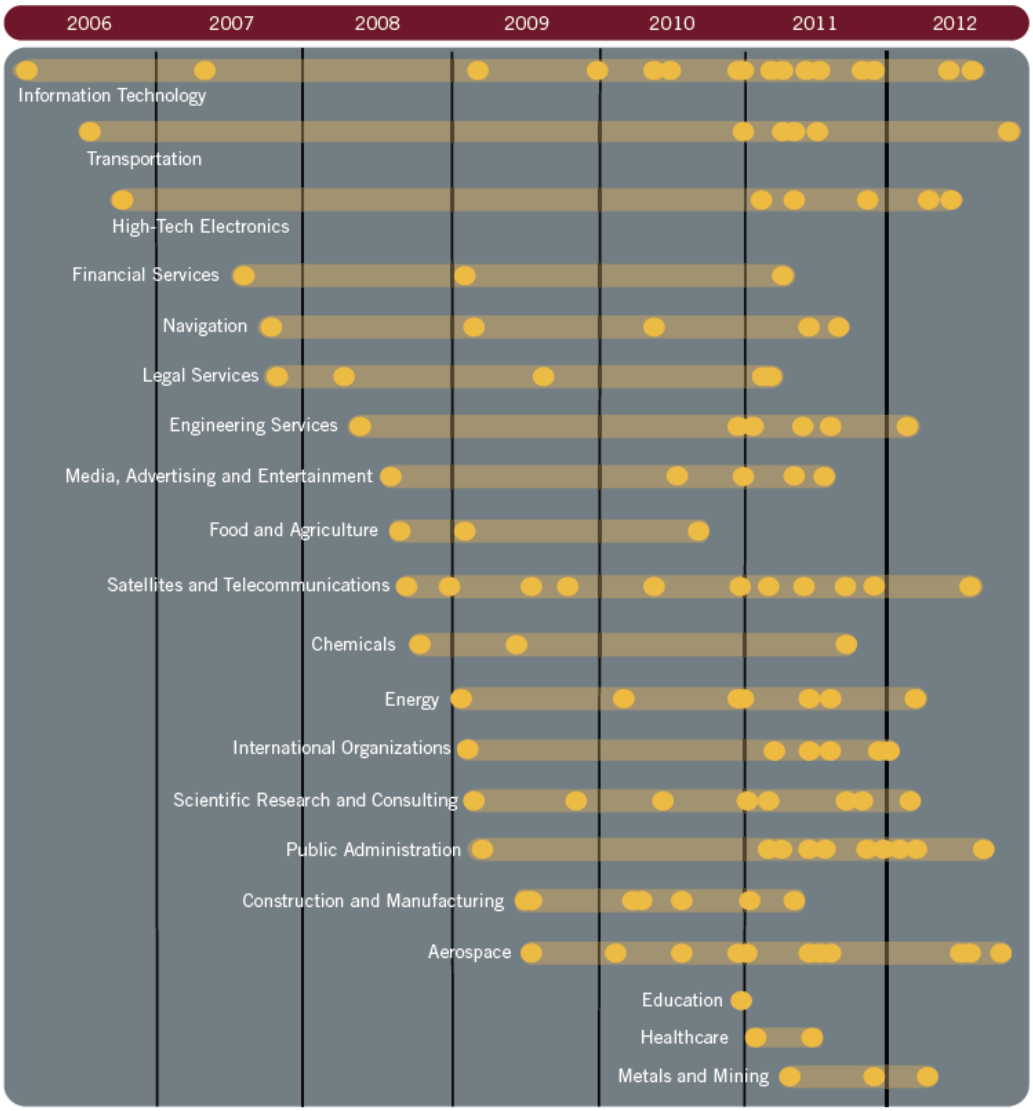


Figure 8. Timeline of APT1 Compromises by Industry Sector[211]

The similarities among major policy plans and Chinese cyber-enabled economic espionage are not restricted to just China's Twelfth FYP. China's MLP, designed as a 15-year science and technology plan, shares similar goals to the Twelfth FYP, while focusing more specifically on technological development and indigenous innovation. The MLP is China's plan to turn the Chinese economy into a "technology powerhouse by 2020 and a global leader by 2050" through indigenous innovation.[212] According to

[211] Ibid., 23.

[212] McGregor, "Drive for 'Indigenous Innovation," 4.

Springut, Schlaikjer, and Chen "the MLP calls for an unprecedented mobilization of resources for R&D projects in 11 'priority fields,' eight areas of 'frontier technology,' and another eight areas of 'cutting-edge science' challenges."[213] The eight areas of "frontier technology" within the MLP are as follows:

1. Advanced Energy
2. Information Technology
3. Biotechnology
4. New Materials
5. Advanced Manufacturing
6. Aerospace and Aeronautics
7. Lasers
8. Ocean Technologies

The areas share an uncanny resemblance to the Twelfth FYP's SEIs as well as Chinese cyber intrusions and cyber-enabled economic espionage against the United States.

Although the MLP calls for "establishing the nation's credibility and image in international cooperation" and "to perfect the nation's intellectual property rights system," preferential government policies, forced technology transfer, lacking incentives for research creativity and innovation, and disregard for IP rights create an environment in which illicit technology transfer is necessary to meet national priorities.[214] McGregor argues that "with these "indigenous innovation industrial policies, it is very clear that China has switched from defense to offense."[215] Using Mandiant and McAfee cyber intrusion reports and Department of Justice economic espionage and trade secret criminal cases (see Appendix for the Department of Justice cases presented), Figure 9 depicts the similarities among China's Twelfth FYP and MLP and specific cases of Chinese cyber-enabled economic espionage against the United States. The unmistakable overlaps

[213] Springut, Schlaikjer, and Chen, *China's Program for Science and Technology Modernization*, 42.

[214] McGregor, "Drive for 'Indigenous Innovation," 4.

[215] Ibid., 4.

between the MLP, Twelfth FYP, and cases of Chinese cyber-enabled economic espionage are difficult to dispute.

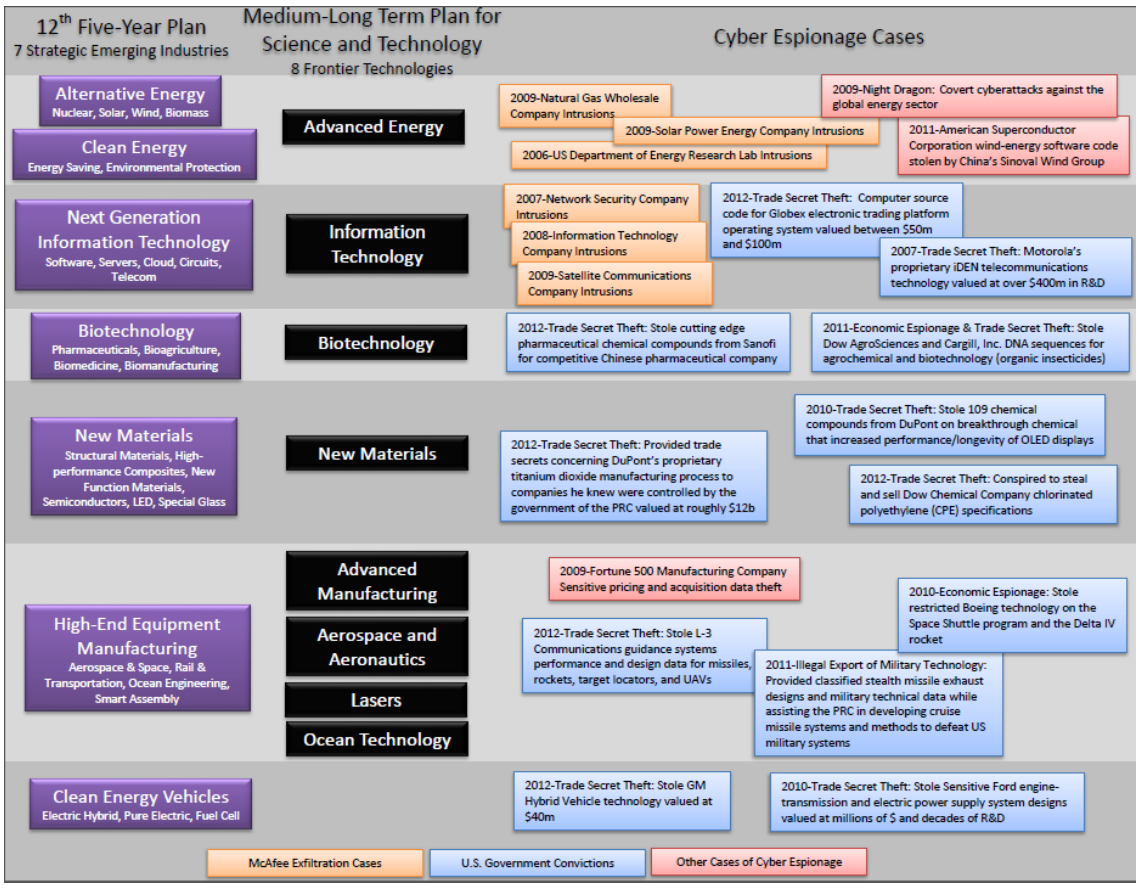


Figure 9. Similarities Among China's 12th Five-Year Plan, National Medium Long-Term Plan for Science and Technology (2006–2020), and Specific Cases of Chinese Cyber Espionage Against the United States.[216]

[216] Alperovitch, *Revealed: Operation Shady RAT*, 7–9; *Mandiant M-Trends: the advanced persistent threat*, 20; Riley and Vance, "China Corporate Espionage Boom Knocks Wind Out of U.S. Companies"; "Global Energy Cyberattacks," 3, 7; "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets," Annex B, 23; U.S. Department of Justice, "Hawaii Man Sentenced to 32 Years in Prison for Providing Defense Information and Services to People's Republic of China," January, 25, 2011, http://www.justice.gov/opa/pr/hawaii-man-sentenced-32-years-prison-providing-defense-information-and-services-people-s; U.S. Department of Justice, "Former CME Group Software Engineer Pleads guilty to Stealing Globex Computer Trade Secrets While Planning Business to Improve Electronic Trading Exchange in China," September 19, 2012, http://www.justice.gov/usao/iln/pr/chicago/2012/pr0919_01.pdf.

D. CHINESE RESOLVE

Recognizing the power potential in the cyber domain, China has aggressively used cyberspace to gain a competitive advantage in the economic and political domains. Lewis echoes this point when he writes: "China has integrated the use of cyber techniques into its military doctrine and economic policies far more comprehensively than any other nation in the region."[217] Through cyber-enabled economic espionage, China has not only identified a mechanism to overcome its lacking domestic innovation, but also a way to weaken the U.S. economy. If a major problem for China's continued economic growth is the lack of innovation, and the United States is the largest innovator in the world, why expend the time and resources on domestic innovation when it can be retrieved through cyber espionage?

As China continues to syphon U.S. trade secrets and IP at an alarming rate, it races to overtake the United States as the world's largest economy and possibly challenge U.S. hegemony. Despite international backlash, public exposure, and direct accusations from the U.S. government, China continues to maintain its persistent state-sponsored economic espionage. Rightly stated in Mandiant's *2104 Threat Report*, China's unwillingness to discontinue its intrusive cyber operations suggests China "believes the benefits of its cyber espionage campaigns outweigh the potential costs of an international backlash."[218]

This chapter's demonstration of China's extensive use of the cyber domain to conduct economic espionage demonstrates China's resolve to shift the balance of economic power, given by asymmetric interdependence, away from the United States. This chapter also underscores the importance of the next chapter's investigation on China's use of asymmetric interdependence as a coercive political tool and potential source of power against the United States.

---

[217] Lewis, *Hidden Arena*, 8.

[218] Mandiant, *2014 Threat Report: Beyond the Breach* (Alexandria, VA: Mandiant, 2014), 18, 21, https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf.

IV. U.S.-CHINA RELATIONS: CAN CHINA RISE PEACEFULLY?

With China's rise as a potential great power—owing much to its significant economic growth that, in turn, has expanded its political and military power—the U.S.-China relationship has become one of the most important bilateral relationships in the world. The ascent of China is changing the international order, making global stability increasingly more dependent on U.S.-China relations.[219] This relationship is not without its problems, however. "Hanging over the relationship is the larger question of whether, as China grows in economic and military power, the United States and China can manage their relationship in such a way as to avoid debilitating rivalry and conflict that have accompanied the rise of new powers in previous eras," states Susan Lawrence.[220] If the past provides any indication of the future, history does not offer a favorable outcome for U.S.-China relations. Looking solely at the rise and fall of great powers over the last 500 years, in "11 of 15 cases since 1500 in which a rising power rivaled a ruling power, the outcome was war."[221]

As the United States struggles with how to address China's massive cyber-enabled economic espionage campaign, threatening U.S. economic growth and stability, it does so in an environment in which China is emerging as a potential great power. "China's rise has occurred within a world system still dominated by American unilateral authority. Because of these imbalances, China has naturally sought to find asymmetrical advantages, and cyberspace at first glance appears to be a dimension of national power in which the United States is asymmetrically vulnerable," state Hannas, Mulvenon, and Puglisi.[222] What is clear so far is that both the United States and China are entangled in an

---

219 Joshua Cooper Ramo, *The Beijing Consensus* (London: Foreign Policy Centre, 2004), 12.

220 Susan V. Lawrence, *U.S.-China Relations: An Overview of Policy Issues* (CRS Report No. R41108) (Washington, DC: Congressional Research Service, 2013), 33, http://fas.org/sgp/crs/row/R41108.pdf.

221 Graham T. Allison, "Obama and Xi Must Think Broadly to Avoid a Classic Trap," *New York Times*, June 6, 2013, http://www.nytimes.com/2013/06/07/opinion/obama-and-xi-must-think-broadly-to-avoid-a-classic-trap.html?_r=0.

222 Hannas, Mulvenon, and Puglisi, *Chinese Industrial Espionage*, 217–218.

economically interdependent relationship that neither is comfortable maintaining in its current state.

With the United States leading the world in global innovation and China's long-term economic growth relying on innovation and technological advancement, China continues to seek cyber-enabled economic espionage as a mechanism to create an asymmetry in the interdependent economic relationship. China's use of cyberspace allows China to increase the global competitiveness of Chinese businesses and overcome its lacking domestic innovation in order to support sustained economic growth, all the while weakening the U.S. economy. While China has demonstrated its willingness to use cyber-enabled economic espionage to shift the balance of economic power it its favor, the larger question is whether China is willing to then use the asymmetric interdependence as a source of power to affect other areas of the U.S.-China relationship. This chapter explains why previous patterns of Chinese behavior indicate that the answer is yes.

A. CHINA'S USE OF ASYMMETRIC ECONOMIC INTERDEPENDENCE AS A SOURCE OF POWER

In September 2010, a Chinese fishing boat collided with a Japanese Coast Guard vessel near the disputed Senkaku Islands in the East China Sea resulting in a major diplomatic dispute between China and Japan. When China's numerous demands for the captain's release were refused, China halted shipments of rare earth elements (REEs) to Japan—vital elements in high-tech products and cutting-edge modern technology.[223]

Consisting of 17 related chemical elements essential to the production of hybrid cars, wind turbines, guided missiles, Unmanned Aerial Vehicles, computer hard-drives, and cellphones, REEs are actually not that rare. REEs can be found throughout the world; however their geochemical properties limit concentration as minerals making exploitation

[223] Keith Bradsher, "Amid Tension, China Blocks Vital Exports to Japan," *New York Times*, September 22, 2010, http://www.nytimes.com/2010/09/23/business/global/23rare.html?pagewanted=all&_r=0.

extremely difficult and potentially devastating to the environment.[224] China however, is willing to overlook the environmental effects in order to meet the needs of a growing market and maintain a dominant foothold in a lucrative REE business. According to Ed Dolan, with China's embargo against Japan, "suddenly the world became aware that China, home to some 95 percent of global REE production, held an alarming strategic monopoly."[225]

Although China's market share does not represent a true natural monopoly according to Dolan, the ownership of these unique resources does create an asymmetry within the China-Japan economic interdependent relationship. With Japan being the principal consumer of Chinese REEs, China was willing and able to leverage this vulnerability as a coercive tool that succeeded in gaining the release of the Chinese fishing boat and its captain. Keith Bradsher echoes this sentiment when he states that "until recently, China typically sought quick and quiet accommodations on trade issues. But the interruption in rare earth supplies is the latest sign from Beijing that Chinese leaders are willing to use their growing economic muscle."[226]

Key to what China deemed as successful diplomatic negotiations was the ability of China to manipulate the system. "Despite a widely confirmed suspension of rare earth shipments from China to Japan, Beijing has continued to deny the existence of an embargo," Bradsher states.[227] China's denial of the export suspension and lack of official policy trail prevented Japan from immediately lodging a WTO complaint for violating free trade rules and allowed China to "wield an undeclared trade weapon."[228] Bradsher argues that "China has refrained until now from using its near monopoly on rare earth

---

224 David Stringer, "China's Rare Earth Toxic Time Bomb to Spur Mining Boom," *Bloomberg*, June 4, 2014, http://www.bloomberg.com/news/2014-06-03/china-s-rare-earth-toxic-time-bomb-to-spur-12-billion-of-mines.html. The mining of REEs run the risk of radiation leaks and release of carcinogens. The U.S. mine in California was closed in 2002 as a result of a radiation leak and was unable to renew its operating license until 2012.

225 Ed Dolan, "China's Fragile Rare Earth Monopoly," *Ed Dolan's Econ blog*, October 24, 2010, http://dolanecon.blogspot.com/2010/10/chinas-fragile-rare-earth-monopoly.html.

226 Keith Bradsher, "China Said to Widen Its Embargo of Minerals," *New York Times*, October 19, 2010, http://www.nytimes.com/2010/10/20/business/global/20rare.html?pagewanted=all.

227 Ibid.

228 Ibid.

elements as a form of leverage on other governments."[229] Yet China's use of asymmetric economic interdependence as a source of diplomatic power was not only directed at Japan, but extended to the United States as well.

With China the sole sources of REEs and Japan the main manufacturing capacity of REEs at the time, disruption of REE exports to Japan would make the United States completely reliant on China for crucial components used in defense assets such as jet fighter engines, missile guidance systems, antimissile defense, space-based satellites, and communication systems.[230] "Rare earth elements are essential for a diverse and expanding array of high-technology applications, which constitute an important part of the industrial economy of the United States," emphasizes the U.S. Geological Survey.[231]

Although China's original intent was to leverage its asymmetric economic interdependence to politically coerce Japan, China simultaneously created an asymmetry in the U.S.-China economic interdependent relationship with the same embargo. This asymmetry would almost instantly be leveraged by China when approximately a month after the exports to Japan stopped flowing, so too did the flow of REEs to the United States. Just days after U.S. trade officials announced an impending investigation against China for imposing export restraints on raw materials and breaking WTO rules by distorting trade and competition in the green technology sector, Chinese customs officials imposed broader REE export restrictions, halting nearly all shipments of REEs to the United States.[232]

But as Keohane and Nye argue, "strategies of manipulating interdependence are likely to lead to counterstrategies," and the United States was unwilling to let China use its dependence on REEs as a coercive political tool.[233] Instead, the United States met

---

229 Bradsher, "Amid Tension, China Blocks Vital Exports to Japan."

230 Marc Humphries, *Rare Earth Elements: The Global Supply Chain* (CRS Report No. R41347) (Washington, DC: Congressional Research Service, 2013), Summary page, http://fas.org/sgp/crs/natsec/R41347.pdf.

231 Gordon B. Haxel, James B. Hedrick, and Greta J. Orris, *Rare Earth Elements—Critical Resources for High Technology* (Fact Sheet 087–02) (Reston, VA: U.S. Geological Survey, 2005), http://pubs.usgs.gov/fs/2002/fs087-02/.

232 Bradsher, "China Said to Widen Its Embargo of Minerals."

233 Keohane and Nye, Jr., *Power and Interdependence*, 16.

China's challenge by filing a two formal cases with the WTO citing China's steady reduction of REE quotas since 2005 and exorbitant export taxes on rare earths were "illegal attempts to force multinational companies to produce more of their high-technology goods in China," giving domestic companies in China a competitive advantage in particular markets.[234] Unlike Japan, the United States has the luxury of directly challenging China. With China home to only around 37 percent of world reserves and the United States sitting on significant REE reserves, a once self-reliant United States could once again look to extract REEs at home.[235] In fact, as a result of China's embargos and unfair trade practices in rare earths, U.S. policy makers continuously seek legislation to fiscally support reinvigoration of the U.S. REE industry in addition to negotiating additional capacity from Australia, Canada, Malaysia, and India.[236]

Nonetheless, Keohane and Nye point out that "sensitivity interdependence can provide the basis for significant political influence only when the rules and norms in effect can be taken for granted, or when it would be prohibitively costly for dissatisfied states to change their policies quickly."[237] With production lines in the United States and Japan set up to produce specific high-tech products, REE-dependent technologies cannot simply be shifted to alternative methods of production.[238] "You can't just substitute nickel for the neodymium in a magnet and expect the product still to do its job," states Dolan.[239] Although both Japan and the United States are sensitive to a Chinese REE embargo, with Japan more so than the United States, "the underlying capabilities of the United States reduces its vulnerability and makes its sensitivity less serious politically."[240]

---

234 Bradsher, "China Said to Widen Its Embargo of Minerals."

235 Keith Bradsher, "After China's Rare Earth Embargo, a New Calculus," *New York Times*, October 29, 2010, http://www.nytimes.com/2010/10/30/business/global/30rare.html.

236 Valerie Bailey Grasso, *Rare Earth Elements in National Defense: Background, Oversight Issues, and Options for Congress* (CRS Report No. R41744) (Washington, DC: Congressional Research Service, 2013), 8, http://fas.org/sgp/crs/natsec/R41744.pdf and Humphries, *Rare Earth Elements*, Summary page.

237 Keohane and Nye, Jr., *Power and Interdependence*, 18.

238 Dolan, "China's Fragile Rare Earth Monopoly."

239 Ibid.

240 Keohane and Nye, Jr., *Power and Interdependence*, 13.

Keohane and Nye continue that "the vulnerability dimension of interdependence rests on the relative availability and costliness of the alternatives various actors face."[241] Japan's vulnerability stems from a lack of available organic resources and costliness of finding substitutions, making it a prime target for Chinese manipulation. Despite numerous joint venture agreements and potential partnerships to obtain REEs, thus far, Japan has been unable to secure enough sources of particular REEs to break its vulnerability dependence with China.

While economic interdependence can be used as a source of power, actors face potential consequences in doing so. In the case of China, although it holds a dominant position in the global supply chain, the temporary embargo immediately raised the global prices of rare earths and damaged China's long-term trade interests.[242] Chinese efforts to exploit its market advantage pushed dependent countries to develop alternative REE sources and new technologies states Dolan. Dolan argues that "after the East China Sea incident, concerns over reliability of supply, as much as concerns over price, are triggering research and investment to an extent that suggests that the long run—as in "long-run elasticity"—is fast approaching."[243] The United States, Japan, Canada, Australia, and India started looking both internally and externally for alternate sources of REEs. With more than 400 exploration projects popping up outside of China between 2011 and 2013, prices of most REEs dropped approximately 60 percent.[244]

Additionally, both WTO cases filed by the United States against China resulted in rulings against China for violation of trade obligations and WTO commitments. In the second WTO case filed against China for rare earth export restrictions, the United States was joined by the European Union, Japan, and Canada as complainants on the case, "indicating a degree of cooperation among some of the world's largest economies, which

---

241 Keohane and Nye, Jr., *Power and Interdependence*, 13 and Saurav Jha, "China's Rare Earths Advantage," *The Diplomat*, April 29, 2014, http://thediplomat.com/2014/04/chinas-rare-earths-advantage/.

242 Shiro Armstrong, "Rare earth metals export ban, a Chinese own goal," East Asia Forum, September 19, 2011, http://www.eastasiaforum.org/2011/09/19/rare-earth-metals-export-ban-a-chinese-own-goal/.

243 Dolan, "China's Fragile Rare Earth Monopoly."

244 Grasso, *Rare Earth Elements in National Defense*, 8.

also constitute China's largest trading partners."[245] China's embargo against Japan demonstrated China's willingness to use economic interdependence as a source of power to bend the political will of other states in its favor. This episode did little to build trust or credibility with major players within the international community, therefore also demonstrating the potential long-term costs of wielding such power for short-term gain in another issue area.

China's future willingness to use economic interdependence as a source of power in the broader U.S.-China relationship therefore is likely conditioned by Beijing's perception of whether such long-term costs are manageable or avoidable. Based on China's continued cyber espionage against the United States, it would appear that China believes the long-term costs of such behavior are manageable. In fact, according to Lowther et al., "a refusal by the Chinese government to control state sponsored cyber espionage will serve as a clear indication of how China's leadership views the United States—with a lack of cooperation indicating it views the United States as a weakening power."[246] But just as China seeks the use of power derived from asymmetric interdependence, so too does the United States.

B. U.S. STRONGHOLD ON INFORMATION POWER

For decades, the United States has maintained a deliberate policy of using information as a source of power and a strategic instrument used to shape political, economic, and military behavior. U.S. doctrine identifies information as one of the four instruments of national power, U.S. presidential administrations publish a *National Strategy for Strategic Communication and Public Diplomacy*, and military service branches possess information warfare units—highlighting the importance of information power to U.S. strategy. The Chinese embargo of REEs provides more than just an example of Chinese use of asymmetric economic interdependence as an instrument of political

[245] Wayne Morrison and Rachel Tang, *China's Rare Earth Industry and Export Regime: Economic and Trade Implications* (CRS Report No. R42510) (Washington, DC: Congressional Research Service, 2012), 35, http://fas.org/sgp/crs/row/R42510.pdf.

[246] Lowther et al., "Chinese-US Relations," 31.

coercion. It also provides an example of how the United States leverages its asymmetric advantage in the information domain to create a source of power against China.

In the REE embargo example, the WTO dispute settlement cases filed by the United States served these two purposes in terms of information power. The first was to discredit China as a reliable economic and trade partner, emphasizing its disregard for following basic rules of free trade to which China agreed when it joined the WTO in 2001. As Keohane and Nye point out, "credibility is the crucial resource [in information power], and asymmetrical credibility is a key source of power."[247] By formally filing a WTO case, the United States brought China's credibility into question, publicizing that China violated global trade rules by imposing export restrictions on rare earths to create an unfair competitive advantage at the "expense of the economic interests of other countries."[248]

Keohane and Nye argue that "much of the traditional conduct of foreign policy occurs through the exchange of promises, which can be valuable only insofar as they are credible. Hence, governments that can credibly assure potential partners that they will not act opportunistically will gain advantages over competitors whose promises are less credible."[249] China's implementation of trade embargoes, distortive economic and trade policies, and aggressive territorial disputes provides the United States with a distinct advantage over China in terms of credibility—one the United States is more than willing to exploit.

The second purpose for filing a settlement case against China is to leverage the information power inherent in the collective action of international institutions. The United States, having helped create influential international organizations such as the United Nations, the IMF, the World Bank, and the General Agreement on Tariffs and Trade (later becoming the WTO), understands the power in bringing "a measure of law

247 Keohane and Nye, Jr., "Power and Interdependence in the Information Age," 89.

248 Morrison and Tang, *China's Rare Earth Industry and Export Regime*, 35.

249 Keohane and Nye, Jr., "Power and Interdependence in the Information Age," 87.

and reciprocity to international politics."[250] As the world's largest economy and sole superpower, the United States possesses great shaping power in the establishment of multilateral partnerships and development of international norms—especially when its interests are at stake. The U.S. use of the WTO for dispute resolution in the REE case established legitimacy in U.S. grievances against China's trade restrictions. It was no longer simply a bilateral disagreement between the United States and China, but rather a legitimate complaint lodged to a recognized international arbiter such as the WTO.

The settlement case and subsequent WTO ruling in favor of the United States not only forces China to take corrective action (action that would likely not be taken otherwise), but validates the U.S. position and highlights China's missteps to the international community. To China, its accession into the WTO in 2001 substantiated its position as a global economic power, but to the United States, it means the ability to formally hold China accountable through the collective action of member states without having to threaten economic sanctions or a potential military show of force. The use of international organizations by the United States is not limited to the REE issue. Through the WTO alone, the United States has submitted 15 of the 31 cases brought against China since its acceptance into the organization in 2001, indicating the willingness of the United States to leverage international institutions in an attempt to achieve desired behaviors from China.[251]

The use of information power by the United States against China is not limited to traditional economic issues. With cyberspace enabling foreign economic espionage activities against U.S. enterprises and government agencies, risking long-term economic growth, the United States has a vested interest in leveraging information power to shape its interests in the cyber domain. "If a state can make its power legitimate in the eyes of others and establish international institutions that encourage others to define their interests in compatible ways, it may not need to expend as many costly traditional

---

[250] David M. Kennedy, "What Would Wilson Do?," *The Atlantic*, January 1, 2010, http://www.theatlantic.com/magazine/archive/2010/01/what-would-wilson-do/307844/3/.

[251] "Dispute Settlement: The Disputes; Disputes by country/territory," The World Trade Organization, accessed October 20, 2014, http://www.wto.org/english/tratop_e/dispu_e/dispu_by_country_e.htm.

economic or military resources," state Keohane and Nye.[252] As China continues its cyber-enabled economic espionage campaign against the United States, the United States works diligently with other nations to develop an international consensus on acceptable behavior in cyberspace that reflects U.S. interests and normative principles. "The U.S. Government Accounting Office (GAO) states that U.S. involvement in developing international agreements and standards on cyberspace security and governance is essential to promoting U.S. national and economic security to the rest of the world."[253]

With the United States and China holding very different views on the rights and obligations of states in cyberspace, cyber security initiatives with a heavy U.S. influence could give the United States a significant source of power. Of the 19 organizations identified by the GAO as "key entities and efforts whose international activities significantly influence the security and governance of cyberspace," the United States is either the lead or a key member.[254] A U.S. led cyber security initiative leveraging international institutions benefits the United States in three ways: first, it shows a U.S. willingness to adhere to internationally established rules, adding legitimacy to its position as a global leader; second, it allows the United States to encourage China's participation in international forums on cyber security as a show of U.S. good faith and acceptance of China as a rising power; and third, it makes China accountable for adhering to normative behavior in cyberspace heavily influenced by the United States. "As this effort [to create norms and agreement on state behavior in cyberspace] progresses and there is international consensus on responsible behavior in cyberspace, China's cyber espionage will be difficult to sustain," states Lewis.[255]

Lewis argues that China's maritime and cyber actions have created an "implicit commonality of interests among other regional powers" that "creates a powerful

---

[252] Keohane and Nye, Jr., "Power and Interdependence in the Information Age," 86.

[253] *Cyberspace: U.S. Faces Challenges in Addressing Global Cybersecurity and Governance* (GAO-10-606) (Washington, DC: U.S. Government Accountability Office, 2010), 1, http://gao.gov/assets/310/308401.pdf.

[254] Ibid.

[255] *Asia: The Cybersecurity Battleground*.

incentive for cooperation and collective action."[256] Even without ratified international norms, the United States and other nations affected by China's illicit cyber behavior could move beyond information power and seek to use existing international mechanisms, such as the WTO, to address China's government-sponsored cyber espionage. The United States has made clear in its *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets* that it will use "trade policy tools to increase international enforcement against trade secret theft to minimize unfair competition against U.S. companies."[257]

The United States, long having used information as a strategic instrument of power, has also executed a persistent information campaign against China and its cyber behavior. After numerous failed attempts to address the cyber espionage issues directly with China, the United States took the issue public to call attention to China's cyber espionage behavior:

- In 2010 after Google announced China as being responsible for computer hacks into its corporate infrastructure, Secretary of State Clinton specifically asked the Chinese government for an explanation.[258]

- In 2011, the Office of the National Counterintelligence Executive released a report to Congress specifically naming "China as the 'most active and persistent' perpetrator of cyber intrusions into the United States."[259]

- In 2011, McAfee indirectly accused China of a five-year targeted cyber operation that hit at least 71 global organizations.[260]

- In 2012, the HPSCI "issued a blistering bipartisan report" accusing two of China's largest telecommunications companies, Huawei and ZTE, of being Chinese proxies empowered to steal intellectual property from American companies.[261]

---

256 Lewis, *Hidden Arena*, 12.

257 *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*, 3.

258 Bobbie Johnson, "US asks China to explain Google hacking claims," *The Guardian*, January 13, 2010, http://www.theguardian.com/technology/2010/jan/13/china-google-hacking-attack-us.

259 Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace*, i.

260 Alperovitch, *Revealed: Operation Shady RAT*, 3–6.

261 Schmidt, Bradsher, and Hauser, "U.S. Panel Cites Risks in Chinese Equipment."

- In 2013, a number of U.S. senior officials publicly demanded that China cease its cyber-enabled economic espionage.[262]

- In February 2013, with U.S. government knowledge, Mandiant released its report on *APT1: Exposing One of China's Cyber Espionage Units*, linking economic espionage conducted since 2006 directly to the Chinese government.[263]

One goal in publicizing China's cyber behavior is to tarnish China's credibility as a responsible world power. "Governments compete with each other and with other organizations to enhance their own credibility and weaken that of their opponent," states Nye.[264] By continuously publicizing technical details on China's illicit cyber endeavors, the United States seeks to systematically weaken China's position as a responsible stakeholder within the international community. China has done little to change public perceptions. China's repeated denial of cyber espionage in the face of credible evidence has caused significant damage to its reputation. Additionally, China's emphasis on cyber security cooperation and coordination while simultaneously maintaining its cyber espionage undermines its efforts to build trust with its international partners and plays right into the hands of the United States. With asymmetrical credibility a key source of power, the United States increases its power by drawing attention to China's hypocrisy on cyber security issues.

The information campaign against China, however, has not occurred without engagement and strategic dialogue between the two nations. In June 2013, during a one-on-one meeting between President Obama and President Xi, cyber security was made the main focus of economic discussions in which President Obama "made clear the threat posed to U.S. economic and national security by cyber-enabled economic espionage."[265] In July 2013, the first meeting of the U.S.-China Working Group on Cybersecurity

---

262 Editorial Board, "Getting China to talk about cyberespionage," *Washington Post*, June 5, 2013, http://www.washingtonpost.com/opinions/getting-china-to-talk-about-cyberespionage/2013/06/05/d69f5446-cdec-11e2-8845-d970ccb04497_story.html.

263 Alperovitch, *Revealed: Operation Shady RAT*, 2–4, 20.

264 Nye Jr., *American Power in the Twenty-First Century*, 38.

265 Tom Donilon, *Press Briefing by National Security Advisor Tom Donilon* (Washington, DC: The White House, 2013), http://www.whitehouse.gov/the-press-office/2013/06/08/press-briefing-national-security-advisor-tom-donilon.

successfully took place in which both nations engaged in straightforward dialogue in an effort to improve cooperation in cyberspace.[266] Additionally, "representing a new milestone in Sino-U.S. military-to-military information-sharing," the U.S. Secretary of Defense traveled to Beijing in April 2014 to provide details on U.S. cyber forces, cyber policies, and potential red lines in cyberspace in the hopes of Chinese reciprocation and sharing.[267]

Not only did the Chinese fail to reciprocate after the U.S. government laid their cards on the table, but after years of continued pressure by the United States to stop cyber economic espionage, China has proved unwilling. China's unwillingness to address cyber-enabled economic espionage and its persistent economic espionage campaign against U.S. companies has pushed the U.S. government to take a different approach. In a bold move rarely taken against other foreign government employees, the Department of Justice charged five China's People's Liberation Army members on May 19, 2014, with economic espionage and requested extradition of the individuals to stand trial.[268] Knowing that the PLA members will not show up for trial, the indictment served more of a "signaling tool" to China that the United States "will not remain silent on state-sponsored acts that harm U.S. national interests, including the competitiveness of U.S. firms."[269] China immediately suspended its participation in the bilateral Cybersecurity Working Group "given the U.S. lack of sincerity in resolving Internet security issues through dialogue and cooperation," putting a halt to cooperation between the two nations

---

[266] Adam Segal, "The Positive That Might Have Come Out the U.S.-China Cybersecurity Working Group," *Asia Unbound (blog), Council on Foreign Relations*, July 10, 2013, http://blogs.cfr.org/asia/2013/07/10/the-positive-that-might-have-come-out-the-u-s-china-cybersecurity-working-group/.

[267] Joe McReynolds, "In a Fortnight: Cyber Transparency for Thee, But Not for Me," *China Brief* 14, no. 8 (April 2014): 1, http://www.jamestown.org/chinabrief/.

[268] Michael S. Schmidt, "U.S. Charges Chinese Army Personnel With Cyberspying," *New York Times*, May 19, 2014, http://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html?action=click&contentCollection=World&region=Footer&module=MoreInSection&pgtype=article

[269] Ankit Panda, "Why Did the U.S. Indict PLA Officers for Hacking, Economic Espionage?," *The Diplomat*, May 21, 2014, http://thediplomat.com/2014/05/why-did-the-us-indict-pla-officers-for-hacking-economic-espionage/.

on cyber security and signaling the limits of the previous U.S. approach to China's illicit cyber behavior.[270]

C. CHINA'S WILLINGNESS TO USE CYBERSPACE

Despite the U.S. advantage in information power, China is keenly aware of the importance of the power in the information domain. Like the United States, China too has used strategic communications to discredit the United States and its cyber security agenda. After release of the U.S. indictment against PLA members, China's state news agency called the actions a "deliberate fabrication" that "grossly violates the basic norms governing international relations and jeopardizes China-U.S. cooperation and mutual trust."[271] Xinhua news alleged that information revealed during the recent intelligence leaks demonstrates U.S. "hypocrisy" on cyber security issues and a "typical case of a thief crying thief" with the United States is at the center of the largest global hacking network.[272] China also highlights what it believes is an unfair advantage in the U.S. use of its development of the Internet and major cyber technologies to influence cyber security initiatives.[273] Additionally, China argues that its own cyber capabilities are a "defensive response to what it views as 'hegemonic' efforts by the United States to militarize cyberspace with offensive capabilities."[274]

China's use of information power, however, goes well beyond influence and propaganda. China's strength in the information domain is in its willingness to use cyberspace as a mechanism to create asymmetries in its interdependent relationships—asymmetries that could potentially be used as a source of power in other issue areas. Hannas, Mulvenon, and Puglisi assert that "China seems much more comfortable with

---

270 Schmidt, "U.S. Charges Chinese Army Personnel With Cyberspying."

271 Zhu Dongyang, "Commentary: Cyber-spying charges against Chinese officers an indictment of U.S. hypocrisy," *Xinhua*, May 20, 2014, http://news.xinhuanet.com/english/china/2014-05/20/c_133347543.htm.

272 Ibid.

273 Lieberthal and Singer, *Cybersecurity and U.S.-China Relations*, 5.

274 Kimberly Hsu and Craig Murray, *China and International Law in Cyberspace* (Washington, DC: U.S.-China Economic and Security Review Commission, 2014), 1, http://origin.www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf.

cyber power as a legitimate, overt tool of state power, especially compared with the United States, which still treats cyber operations as a highly classified, compartmented capability."[275]

Although China's cyber-enabled economic espionage provides China with a long-term economic advantage in the U.S.-China economic interdependent relationship, it could also provide China with a significant source of power. The ability to go from stealing information to manipulating information to possibly destroying information in cyberspace can be a very powerful tool against a nation whose infrastructure and economic survivability has become dependent on cyberspace. China has proven its willingness to steal and manipulate information through cyber operations to shift the balance of power in particular issue areas, but its willingness to sacrifice key relationships with major powers such as the United States by conducting cyber attacks aimed at political coercion is a topic of debate. According to Jayson Spade, China is "conducting cyberspace reconnaissance; creating the ability to do economic harm and damage critical infrastructure; preparing to disrupt communications and information systems necessary to support conventional armed conflict; and readying to conduct psychological operations to influence the will of the American people.[276]

If China's REE embargo against Japan and subsequently the United States is any indication of its willingness to use asymmetric interdependence as a source of power, the likelihood of using cyber power as a coercive tool against the United States is more than feasible. In fact, during periods of heightened tension between the United States and China, Chinese hackers initiated cyber-attack campaigns against U.S. government entities. In 1999 after a U.S. aircraft accidently bombed the Chinese Embassy in Belgrade, Chinese hackers attacked government websites causing the Department of Energy website to go down for an entire day.[277] Again, in 2001, Chinese hackers

---

[275] Hannas, Mulvenon, and Puglisi, *Chinese Industrial Espionage*, 218.

[276] Jayson M. Spade, "Information as Power: China's Cyber Power and America's National Security," U.S. Army War College, May 2012, 3, http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-072.pdf.

[277] Ann Kellan, "Hackers hit government Websites after China embassy bombing," *CNN*, May 11, 1999, http://www.cnn.com/TECH/computing/9905/10/hack.attack.02/index.html?_s=PM:TECH.

launched a number of cyber-attacks against U.S. Government websites following the collision of a U.S. Navy EP-3 Aries reconnaissance aircraft and a People's Liberation Army Navy (PLAN) F-8 Finback fighter aircraft.[278] In addition to the cyber-attacks against the United States, Chinese hackers were deemed responsible for attacks against the Japanese government in 2004 after a Senkaku Island dispute, the French Embassy website in 2008 in protest over a meeting with the Dalai Lama, and South Korean banks in 2013 amid tensions with North Koreas over nuclear weapons and missile testing.[279] The attacks against South Korea were attributed to North Korea but reportedly supported by China when the attacks were traced back to IP address in China.[280]

While there is no direct evidence of Chinese government sponsorship of these attacks, China has long been known to use hackers to carry out cyber espionage and "engage in politically coercive acts."[281] Lowther, Geis, Yannakogeorgos, and Dacus argue however, that "whether such activities are state-sponsored or not, China is proving unwilling to undertake efforts to stop them."[282] China's cyber behavior indicates a level of comfort in the use of cyberspace as a coercive tool which, if left unchecked, strengthens China's position within the U.S.-China relationship. For instance, in response to the U.S. indictment of the five PLA members, China's state-owned news agency wrote: "China needs to respond. Suspending the operations of a bilateral group on cyber affairs is a reasonable start, but more countermeasures should be prepared in case Washington obstinately sticks to the wrong track."[283] The statement is a clear warning that China may look beyond diplomatic processes to address what it sees as an injustice.

---

278 William Hagenstad II, *21st Century Chinese Cyberwarfare* (Cambridgeshire: IT Governance Publishing, 2012), 269.

279 Hagenstad II, *21st Century Chinese Cyberwarfare*, 270, 274 and K.J. Kwon, Jethro Mullen, and Michael Pearson, "Hacking attack on South Korea traced to Chinese address, officials say," *CNN*, March 21, 2013, http://edition.cnn.com/2013/03/21/world/asia/south-korea-computer-outage/.

280 Kwon, Mullen, and Pearson, "Hacking attack on South Korea traced to Chinese address, officials say."

281 Lewis, *Hidden Arena*, 4.

282 Lowther et al., "Chinese-US Relations," 29.

283 Dongyang, "Commentary: Cyber-spying charges against Chinese officers an indictment of U.S. hypocrisy."

The use of offensive cyber operations against the United States as a means of political coercion cannot be ruled out. In fact, as the United States continues to become more dependent on cyberspace for its economic growth and national security, it becomes more vulnerable to illicit Chinese cyber behavior. *The National Strategy to Secure Cyberspace* claims that "the threat of organized cyber attacks capable of causing debilitating disruption to our Nation's critical infrastructures, economy, or national security" is a major concern.[284]

Lowther et al., argue that China could use cyber attacks against U.S. commercial lines of communication (LOC), having potentially devastating effects on both the economy and national security. They state that "while closing sea and air LOCs to commercial traffic would clearly be seen as antagonistic and cause a loss of global goodwill, cyber attacks aimed at commercial interests (LOCs) can serve much the same purpose without arousing the same ire from the international community."[285] The difficulty of attribution in cyberspace provides China the ability to plausibly deny responsibility.

Although China might consider certain actions to be below the threshold of what could be considered the use of force or an act of war, especially when denying responsibility, the United States has made clear in its *Department of Defense Strategy for Operating in Cyberspace* "that harmful action within the cyber domain can be met with a parallel response in another domain."[286] Should China be willing to use cyber power as a coercive tool against the United States, it risks the potential for conflict.

D. POTENTIAL FOR CONFLICT

"Because of the newness of technology, the lack of agreement on norms, and the potential to misidentify an espionage exploit as the opening phase of a military action, cyber conflict entails a greater risk of miscalculation and inadvertent escalation of

---

[284] *The National Strategy to Secure Cyberspace* (Washington, DC: The White House, 2003), viii, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

[285] Lowther et al., "Chinese-US Relations," 31.

[286] *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, 2011), 10, http://www.defense.gov/news/d20110714cyber.pdf.

conflict," states Lewis.[287] While it would be naïve to assume that nations would not preserve some cyber capability for intelligence collection and to support military actions, lack of agreement on the acceptable use of cyber capabilities plagues U.S.-China relations.

The United States considers China's cyber-enabled economic espionage intolerable behavior not only because of the damage it does to the U.S. economy, but also because of the ease at which a cyber exploit can become a cyber attack. The strategic goal for China however, is to avoid conflict, viewing armed conflict as an indication of failure.[288] According to Joshua Cooper Ramo, "asymmetry represents the most efficient way to deal with the incredibly complex security environment China inhabits. China is in the process of building the largest asymmetric superpower in history."[289] Ramo argues that "true success" to China is the ability to manipulate a situation so effectively that the outcome favors Chinese interests in a way that enables China to acquire the power to avoid conflict.[290] Thomas validates this notion when he asserts that China's persistent cyber reconnaissance efforts against global powers indicate that China is trying to seek vulnerabilities that can be exploited to achieve an economic or military victory.[291]

Despite China's desire to avoid conflict and its assurance that it seeks a peaceful rise to great power status, its recurrent acts of aggression undermine its efforts to build confidence among its regional neighbors and strategic partners.[292] Lewis points out that "China's cyber activities cannot be divorced from the larger security and political context in Asia, where Chinese actions have alienated many of its neighbors and have increased tensions by attempting to assert its regional authority."[293] As a result, no matter what China does to signal good intentions, China's aggressive behavior coupled with its

---

287 Lewis, *Hidden Arena*, 2.

288 Joshua Cooper Ramo, *The Beijing Consensus* (London: Foreign Policy Centre, 2004), 39.

289 Ibid., 37, 48.

290 Ibid., 39.

291 Thomas, "Google Confronts China's 'Three Warfares,'" 108.

292 Lowther et al., "Chinese-US Relations," 35.

293 *Asia: The Cybersecurity Battleground*.

strategic culture of "ambiguity, disinformation, and secrecy," make other nations skeptical of a peaceful Chinese rise.[294]

The United States holds a similar view to China's in that it too wants to prevent the escalation of hostilities by developing cooperative mechanisms on cyber security. If China ignores U.S. overtures to deal with illicit cyber behavior such as cyber-enabled economic espionage, the United States has conveyed its willingness to respond with military force. In a speech on Defense Department's Cyber Strategy, former Deputy Secretary of Defense William Lynn, III, stated that "just as our military organizes to defend against hostile acts from land, air, and sea, we must also be prepared to respond to hostile acts in cyberspace. Accordingly, the United States reserves the right, under the laws of armed conflict, to respond to serious cyber attacks with a proportional and justified military response at the time and place of our choosing."[295] Though China may have prescribed a peaceful rise to great power status, its manipulation of asymmetrical interdependence as a means of achieving its rise, could very well push the United States to the brink of conflict. Keohane and Nye submit the following:

> It must always be kept in mind, furthermore, that military power dominates economic power in the sense that economic means alone are likely to be ineffective against the serious use of military force. Thus, even effective manipulation of asymmetrical interdependence within a nonmilitary area can create risks of military counteraction. When the United States exploited Japanese vulnerability to economic embargo in 1940–41, Japan countered by attacking Pearl Harbor and the Philippines.[296]

Although war between the United States and China is not inevitable, the persistent and mutual mistrust between the United States and China, exacerbated by China's illicit cyber behavior, continues to afflict U.S.-China relations and could determine whether China's rise will be a peaceful one. Thus, far, the United States and China have made the overall stability of the bilateral relationship a priority, with accommodation and

---

294 Sun Tzu, *Art of War* (Boulder, CO: Westview Press, 1994), 185–95.

295 William J. Lynn, III, "Remarks on the Department of Defense Cyber Strategy," As Delivered by Deputy Secretary of Defense William J. Lynn, III, National Defense University, July 14, 2011, http://www.defense.gov/speeches/speech.aspx?speechid=1593.

296 Keohane and Nye, Jr., *Power and Interdependence*, 16.

cooperation central to its success. Lewis argues that "the rise of China means that other Asian nations must decide where to accommodate and where to confront a newly powerful China with aspirations to restore its regional position and power. In turn, China's leaders must decide where an acceptance of international norms and systems best serves China's interest and where challenging the existing order provides greater benefit."[297] Should China continue its persistent cyber-enabled economic espionage campaign or threaten to use the cyber domain as a source of coercive power, it would likely indicate China's willingness to sacrifice relations with the United States to meet its own core interests and that the costs of that sacrifice no longer exceed the tangible benefits.

E. CONCLUSION

While it would be difficult to say with any certainly what the future holds for U.S.-China relations or if China's ascent to great power status will be a peaceful one, China's cyber behavior does provides some indication about the role of economic interdependence in U.S.-China relations. Over the last three decades, the United States and China have become heavily reliant on each other as a major source of economic growth. The United States has turned to China for its inexpensive goods and abundance of foreign capital to support its consumption model.[298] Similarly, China has turned to the United States as the world's single largest import market to support an export- and investment-led growth model.[299] "Two large economies had large gaps to fill and they quickly became hooked on what each could offer the other in their collective quest for economic growth," states Roach.[300]

Now intertwined in a somewhat balanced economic interdependent relationship, both the United States and China seek to manipulate the relationship in an effort to become the less dependent actor. Despite increasing concerns from both nations, neither

297 Lewis, *Hidden Arena*, 6.

298 Roach, *Unbalanced*, 3.

299 Ibid. According to the WTO, the European Union is the largest import market in the world, but the United States is the single largest import market when looking at individual nations.

300 Ibid.

has been able to rebalance their economies enough to create an asymmetrical advantage over the other. Instead, through cyberspace operations, China has systematically conducted an economic espionage campaign against U.S. companies and government entities to acquire technology and IP and shift the economic balance of power in its favor.

China's theft of IP, costing the United States billions of dollars annually, clearly provides China an advantage.[301] With China's push for increased indigenous innovation to strengthen economic development, cyber-enabled economic espionage allows China to bypass the costs of R&D and jump to the forefront of technological innovation by stealing other nations' hard work. As a result, China's cyber espionage threatens U.S. technological competitiveness and economic prosperity. Although China denies accusations of cyber-enabled economic espionage, the capacity to conduct computer network exploitation operations to the extent that has been attributed to China is nearly impossible without some type of state-sponsorship.[302] Furthermore, China's Twelfth FYP and National Medium to Long-Term Plan for the Development of Science and Technology, 2006–2020 (MLP), both focusing on indigenous innovation and technological advancement, read like a cyber espionage blueprint when compared directly to Chinese cyber intrusions and cyber-enabled economic espionage against the United States.[303] While the United States uses its power in the information domain to call attention to China's brazen cyber espionage behavior and gain collective support against China's cyber-enabled economic espionage, there are no indications the public exposure of Chinese cyber espionage has led China to stop its cyber-enabled economic espionage.[304]

Beyond China's use of cyber-enabled economic espionage to shift the balance of power in the U.S-China economic interdependent relationship, China also recognizes the

---

[301] The Commission on the Theft of American Intellectual Property, *The IP Commission Report*, 2.

[302] Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, 8.

[303] Alperovitch, *Revealed: Operation Shady RAT*, 7–9; Mandiant, *Mandiant M-Trends: the advanced persistent threat*, 20; Riley and Vance, "China Corporate Espionage Boom Knocks Wind Out of U.S. Companies"; "Global Energy Cyberattacks," 3, 7; *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*, Annex B, 23.

[304] U.S.-China Economic and Security Review Commission, *2013 Annual Report to Congress*, 253.

power potential in the cyber domain. China has aggressively used cyberspace to gain a competitive advantage in the economic domain. But is China willing to then leverage the asymmetric economic interdependence as a source of power? Furthermore, is China willing to use its cyber capabilities as a means of political coercion? Based on the research conducted for this thesis, the answer is yes.

China has used asymmetric economic interdependence as a source of power and instrument of political coercion and China would likely be willing to do so against the United States should the economic balance of power shift in its favor. However, even if the United States becomes the more dependent party in the economic relationship, China's ability to use the asymmetry as a source of power will depend on United States sensitivity and vulnerability dependence to particular Chinese actions. For instance, if after understanding the implication to its own economy China decided to use U.S. Treasury securities as a coercive tool against the United States by dumping mass quantities on the market in an effort to destabilize the U.S. economy, the United States would be sensitive to the immediate effects of U.S. Treasury security devaluation and increased inflation. Yet, with the Federal Reserve prepared to purchase U.S. Treasuries dumped on the market in such a situation, the economic impact to the United States is significantly reduced as is its vulnerability to this particular Chinese action.[305]

Alternatively, if China decided to conduct cyber attacks against U.S. banks in response to U.S. trade sanctions or arms deals with Taiwan, devoid of any changes to U.S. policy, the United States would be substantially more vulnerable since U.S. government protection is in cyberspace is not extended to most of the private sector.[306] With the United States having articulated its intent to respond to serious cyber attacks with a proportional and justified response in another domain, China's potential use of cyberspace to conduct offensive operations makes escalation of hostilities and the potential for conflict a real possibility.[307]

---

[305] Office of the Secretary of Defense, *Report to Congress, Assessment of the National Security Risks Posed to the United States as a Result of the U.S. Federal Debt Owed to China as a Creditor of the U.S. Government*, 3.

[306] *The National Strategy to Secure Cyberspace*, viii.

[307] *Department of Defense Strategy for Operating in Cyberspace*, 10.

China's approach to cyber espionage reflects its willingness to risk its economic relationships to achieve its own economic and political policy goals. China, "motivated by the desire to achieve economic, strategic, and military parity with the United States" will likely continue to use cyber espionage as a means to acquire U.S. technology and sensitive economic information.[308] China has little need to accept international norms, especially in cyberspace, if it is willing to bully its way to the top. However, to peacefully maintain its continued ascent to great power status, China will have to demonstrate a willingness to accept normative behavior set by international institutions and multilateral agreements or face potential collective action by embittered major powers. "Cyber security is a fundamental test of China's willingness to play by the rules and whether its integration into the international system will be peaceful," states Lewis.[309] Should China continue its cyber-enabled economic espionage campaign against the United States, it could indicate that China judges that the potential costs of its cyber espionage programs outweigh the benefits of its relationship with the United States.

[308] Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace*, 7.

[309] *Asia: The Cybersecurity Battleground*.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX. DEPARTMENT OF JUSTICE CASES OF CHINESE CYBER ESPIONAGE AGAINST THE UNITED STATES

The following cases are a select number of Department of Justice Economic Espionage and Trade Secret Criminal Cases that were identified in Chapter III, Figure 9, page 57, of this thesis. The information included in each case was taken verbatim from source material.[310]

Military Technical Data and Trade Secrets to China – On Sept. 26, 2012, Sixing Liu, aka Steve Liu, a native of China with a PhD in electrical engineering who worked as a senior staff engineer for Space & Navigation, a New Jersey-based division of L-3 Communications, was convicted in the District of New Jersey of exporting sensitive U.S. military technology to China, stealing trade secrets and lying to federal agents. The jury convicted Liu of nine of 11 counts of an April 5, 2012 second superseding indictment, specifically six counts of violating the Arms Export Control Act, one count of possessing stolen trade secrets in violation of the Economic Espionage Act, one count of transporting stolen property, and one count of lying to federal agents. The jury acquitted Liu on two counts of lying to federal agents. According to documents filed in the case and evidence presented at trial, in 2010, Liu stole thousands of electronic files from his employer, L-3 Communications, Space and Navigation Division. The stolen files detailed the performance and design of guidance systems for missiles, rockets, target locators, and unmanned aerial vehicles. Liu stole the files to position and prepare himself for future employment in China. As part of that plan, Liu delivered presentations about the technology at several Chinese universities, the Chinese Academy of Sciences, and conferences organized by Chinese government entities. However, Liu was not charged with any crimes related to those presentations. On Nov. 12, 2010, Liu boarded a flight from Newark to China. Upon his return to the United States on Nov. 29, 2010, agents found Liu in possession of a non-work-issued computer found to contain the stolen

310 "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets," Annex B, 23; "Hawaii Man Sentenced to 32 Years in Prison for Providing Defense Information and Services to People's Republic of China,"; "Former CME Group Software Engineer Pleads guilty to Stealing Globex Computer Trade Secrets While Planning Business to Improve Electronic Trading Exchange in China."

material. The following day, Liu lied to ICE agents about the extent of his work on U.S. defense technology. The State Department later verified that several of the stolen files on Liu's computer contained technical data that relates to defense items listed on the United States Munitions List. The jury also heard testimony that Liu's company trained him about the United States' export control laws and told him that most of the company's products were covered by those laws. Liu was first arrested on March 8, 2011, in Chicago on a complaint in the District of New Jersey charging him with one count of exporting defense-related technical data without a license. The investigation was conducted by the FBI, ICE and CBP.

Motorola Trade Secrets to China – On Aug. 29, 2012, Hanjuan Jin, a former software engineer for Motorola, was sentenced in the Northern District of Illinois to four years in prison for stealing trade secrets from Motorola, specifically Motorola's proprietary iDEN telecommunications technology, for herself and for Sun Kaisens, a company that developed products for the Chinese military. According to court documents filed in the case, Motorola spent more than $400 million researching and developing iDEN technology in just a matter of years. On Feb. 8, 2012, Jin was found guilty of three counts of stealing trade secrets. Jin, a naturalized U.S. citizen born in China, possessed more than 1,000 electronic and paper Motorola proprietary documents when she was stopped by U.S. authorities at Chicago's O'Hare International Airport as she attempted to travel to China on Feb. 28, 2007. The judge presiding over the case found her not guilty of three counts of economic espionage for the benefit of the government of China and its military. According to the evidence at trial, Jin began working for Motorola in 1998, and took medical leave in February 2006. Between June and November 2006, while still on sick leave, Jin pursued employment in China with Sun Kaisens, a Chinese telecommunications firm that developed products for the Chinese military. Between November 2006 and February 2007, Jin returned to China and did work for Sun Kaisens on projects for the Chinese military. On Feb. 15, 2007, Jin returned to the United States from China and reserved a flight to China scheduled to depart on Feb. 28, 2007. Jin advised Motorola that she was ready to return to work at Motorola, without informing Motorola that she planned to return to China to work for Sun Kaisens. On Feb. 26, 2007,

she returned to Motorola, and accessed hundreds of technical documents belonging to Motorola on its secure internal computer network. As she attempted to depart from Chicago to China, authorities seized numerous materials, some of which provided a description of communication feature that Motorola incorporates into its telecommunications products. Authorities also recovered classified Chinese documents describing telecommunication projects for the Chinese military. Jin was charged with theft of trade secrets in an April 1, 2008 indictment. A superseding indictment returned on Dec. 9, 2008 charged her with economic espionage. The investigation was conducted by the FBI, with assistance from U.S Customs and Border Protection.

Military Technical Data and Trade Secrets to China – On April 5, 2012, a second superseding indictment was returned in the District of New Jersey against Sixing Liu, aka "Steve Liu," a native of China with a Ph.D. in electrical engineering who worked as a senior staff engineer for Space & Navigation, a New Jersey-based division of L-3 Communications, from March 2009 through Nov. 2010. The superseding indictment charged Liu with six counts of illegally exporting defense articles / technical data to China, one count of possessing stolen trade secrets, one count of interstate transportation of stolen property, and three counts of false statements to federal agents. Liu, of Deerfield, Ill., was first arrested on March 8, 2011 in Chicago on a criminal complaint filed in the District of New Jersey charging him with one count of exporting defense-related technical data without a license. At Space & Navigation, Liu allegedly worked on precision navigation devices for rocket launchers, missile launch systems, field artillery, smart munitions, and other components being used by and prepared for the U.S. Department of Defense. Liu was never approved to present information related to Space & Navigation's programs or the technology underlying its programs to any outside person or audience. In 2009 and again in 2010, the indictment alleges that Liu traveled to China where he attended and delivered presentations on export restricted technical data at technology conferences sponsored by Chinese government entities, including the 863 Program. Before leaving for the 2010 conference in China, Liu allegedly downloaded some 36,000 computer files from Space & Navigation to his personal laptop. Upon his return to the United States in November 2010, U.S. Customs inspectors found him to be

in possession of a laptop computer that contained hundreds of documents related to the company's projects, as well as images of Liu making a presentation at a technology conference sponsored by the PRC government. Many of the documents on his computer were marked as containing sensitive proprietary company information and/or export-controlled technical data. The State Department verified that information on the Liu's computer was export-controlled technical data that relates to defense items on the U.S. Munitions List. The investigation was conducted by the FBI and ICE.

DuPont Trade Secrets to China – On March 2, 2012, former DuPont scientist Tze Chao pleaded guilty in the Northern District of California to conspiracy to commit economic espionage, admitting that he provided trade secrets concerning DuPont's proprietary titanium dioxide manufacturing process to companies he knew were controlled by the government of the People's Republic of China (PRC). On Feb. 7, 2012, a grand jury in San Francisco returned a superseding indictment charging Chao and four other individuals, as well as five companies, with economic espionage and theft of trade secrets for their roles in a long-running effort to obtain U.S. trade secrets from DuPont for the benefit of companies controlled by the PRC. The five individuals named in the indictment were Walter Liew, his wife Christina Liew, Hou Shengdong, Robert Maegerle, and Tze Chao. The five companies named as defendants are Pangang Group Company Ltd; Pangang Group Steel Vanadium Industry Company Ltd; Pangang Group Titanium Industry Company Ltd., Pangang Group International Economic & Trading Co; and USA Performance Technology, Inc. According to the superseding indictment, the PRC government identified as a priority the development of chloride-route titanium dioxide (TiO2) production capabilities. TiO2 is a commercially valuable white pigment with numerous uses, including coloring paint, plastics and paper. To achieve that goal, companies controlled by the PRC government, specifically the Pangang Group companies named in the indictment, and employees of those companies conspired and attempted to illegally obtain TiO2 technology that had been developed over many years of research and development by DuPont. The Pangang Group companies were aided in their efforts by individuals in the United States who had obtained TiO2 trade secrets and were willing to sell those secrets for significant sums of money. Defendants Walter Liew,

Christina Liew, Robert Maegerle and Tze Chao allegedly obtained and possessed TiO2 trade secrets belonging to DuPont. Each of these individuals allegedly sold information containing DuPont TiO2 trade secrets to the Pangang Group companies for the purpose of helping those companies develop large-scale chloride route TiO2 production capability in the PRC, including a planned 100,000 ton TiO2 factory at Chongqing, PRC. The Liews, USAPTI, and one of its predecessor companies, Performance Group, entered into contracts worth in excess of $20 million to convey TiO2 trade secret technology to Pangang Group companies. The Liews allegedly received millions of dollars of proceeds from these contracts. The proceeds were wired through the United States, Singapore and ultimately back into several bank accounts in the PRC in the names of relatives of Christina Liew. The object of the defendants' conspiracy was to convey DuPont's secret chloride-route technology to the PRC companies for the purpose of building modern TiO2 production facilities in the PRC without investing in time-consuming and expensive research and development. DuPont invented the chloride-route process for manufacturing TiO2 in the late-1940s and since then has invested heavily in research and development to improve that production process. The global titanium dioxide market has been valued at roughly $12 billion, and DuPont has the largest share of that market. This investigation was conducted by the FBI.

Trade Secrets to U.S. Subsidiary of Chinese Company – On Jan. 17, 2012, Yuan Li, a former research chemist with the global pharmaceutical company Sanofi-Aventis, pleaded guilty in the District of New Jersey to stealing Sanofi's trade secrets and making them available for sale through Abby Pharmatech, Inc., the U.S. subsidiary of a Chinese chemicals company. According to court documents, Li worked at Sanofi headquarters in Bridgewater, N.J., from August 2006 through June 2011, where she assisted in the development of several compounds (trade secrets) that Sanofi viewed as potential building blocks for future drugs. While employed at Sanofi, Li was a 50 percent partner in Abby, which sells and distributes pharmaceuticals. Li admitted that between Oct. 2008 and June 2011, she accessed internal Sanofi databases and downloaded information on Sanofi compounds and transferred this information to her personal home computer. She

also admitted that she made the stolen compounds available for sale on Abby's website. This investigation was conducted by the FBI.

Dow Trade Secrets to China – On Jan. 12, 2012, Wen Chyu Liu, aka David W. Liou, a former research scientist at Dow Chemical Company in Louisiana, was sentenced in the Middle District of Louisiana to 60 months in prison, two years supervised release, a $25,000 fine and was ordered to forfeit $600,000. Liu was convicted on Feb. 7, 2011 of one count of conspiracy to commit trade secret theft for stealing trade secrets from Dow and selling them to companies in China, and he was also convicted of one count of perjury. According to the evidence presented in court, Liou came to the United States from China for graduate work. He began working for Dow in 1965 and retired in 1992. Dow is a leading producer of the elastomeric polymer, chlorinated polyethylene (CPE). Dow's Tyrin CPE is used in a number of applications worldwide, such as automotive and industrial hoses, electrical cable jackets and vinyl siding. While employed at Dow, Liou worked as a research scientist on various aspects of the development and manufacture of Dow elastomers, including Tyrin CPE. The evidence at trial established that Liou conspired with at least four current and former employees of Dow's facilities in Plaquemine, Louisiana, and in Stade, Germany, who had worked in Tyrin CPE production, to misappropriate those trade secrets in an effort to develop and market CPE process design packages to Chinese companies. Liou traveled throughout China to market the stolen information, and he paid current and former Dow employees for Dow's CPE-related material and information. In one instance, Liou bribed a then employee at the Plaquemine facility with $50,000 in cash to provide Dow's process manual and other CPE-related information. The investigation was conducted by the FBI.

Dow and Cargill Trade Secrets to China – On Dec. 21, 2011, Kexue Huang, a Chinese national and former resident of Indiana, was sentenced to 87 months imprisonment and three years' supervised release on charges of economic espionage to benefit a foreign university tied to the People's Republic of China (PRC) and theft of trade secrets. On Oct. 18, 2011, Huang pleaded guilty in the Southern District of Indiana to these charges. In July 2010, Huang was charged in the Southern District of Indiana with misappropriating and transporting trade secrets to the PRC while working as a

research scientist at Dow AgroSciences LLC. On Oct. 18, 2011, a separate indictment in the District of Minnesota charging Huang with stealing a trade secret from a second company, Cargill Inc., was unsealed. From January 2003 until February 2008, Huang was employed as a research scientist at Dow. In 2005, he became a research leader for Dow in strain development related to unique, proprietary organic insecticides marketed worldwide. Huang admitted that during his employment at Dow, he misappropriated several Dow trade secrets. According to plea documents, from 2007 to 2010, Huang transferred and delivered the stolen Dow trade secrets to individuals in Germany and the PRC. With the assistance of these individuals, Huang used the stolen materials to conduct unauthorized research to benefit foreign universities tied to the PRC. Huang also admitted that he pursued steps to develop and produce the misappropriated Dow trade secrets in the PRC. After Huang left Dow, he was hired in March 2008 by Cargill, an international producer and marketer of food, agricultural, financial and industrial products and services. Huang worked as a biotechnologist for Cargill until July 2009. Huang admitted that during his employment with Cargill, he stole one of the company's trade secrets – a key component in the manufacture of a new food product, which he later disseminated to another person, specifically a student at Hunan Normal University in the PRC. According to the plea agreement, the aggregated loss from Huang's conduct exceeds $7 million but is less than $20 million. This investigation was conducted by the FBI.

Ford Motor Company Trade Secrets to China – On Nov. 17, 2010, Yu Xiang Dong, aka Mike Yu, a product engineer with Ford Motor Company pleaded guilty in the Eastern District of Michigan to two counts of theft of trade secrets. According to the plea agreement, Yu was a Product Engineer for Ford from 1997 to 2007 and had access to Ford trade secrets, including Ford design documents. In December 2006, Yu accepted a job at the China branch of a U.S. company. On the eve of his departure from Ford and before he told Ford of his new job, Yu copied some 4,000 Ford documents onto an external hard drive, including sensitive Ford design documents. Ford spent millions of dollars and decades on research, development, and testing to develop and improve the design specifications set forth in these documents. On Dec. 20, 2006, Yu traveled to the

location of his new employer in Shenzhen, China, taking the Ford trade secrets with him. On Jan. 2, 2007, Yu emailed his Ford supervisor from China and informed him that he was leaving Ford's employ. In Nov. 2008, Yu began working for Beijing Automotive Company, a direct competitor of Ford. On Oct. 19, 2009, Yu returned to the U.S. Upon his arrival, he was arrested. At that time, Yu had in his possession his Beijing Automotive Company laptop computer. Upon examination of that computer, the FBI discovered that 41 Ford system design specifications documents had been copied to the defendant's Beijing Automotive Company work computer. The FBI also discovered that each of those design documents had been accessed by Yu during the time of his employment with Beijing Automotive Company. Yu was ultimately sentenced to 70 months in prison in April 2011. This case was investigated by the FBI.

DuPont Trade Secrets to China – On Oct. 26, 2010, Hong Meng, a former research chemist for DuPont, was sentenced in the District of Delaware to 14 months in prison and $58,621 in restitution for theft of trade secrets. Meng pleaded guilty on June 8, 2010. Meng was involved in researching Organic Light Emitting Diodes (OLED) during his tenure at DuPont. In early 2009, DuPont's OLED research efforts resulted in the development of a breakthrough chemical process (trade secret) that increased the performance and longevity of OLED displays. In the Spring of 2009, while still employed at DuPont and without DuPont's permission or knowledge, Meng accepted employment as a faculty member at Peking University (PKU) College of Engineering, Department of Nanotechnology in Beijing, China, and thereafter began soliciting funding to commercialize his OLED research at PKU. In June 2009, he emailed to his PKU account the protected chemical process from DuPont. He also downloaded the chemical process from his DuPont work computer to a thumb drive which he uploaded to his personal computer. In August 2009, he mailed a package containing 109 samples of DuPont intermediate chemical compounds to a colleague at Northwestern University and instructed his colleague at Northwestern to forward the materials to Meng's office at PKU. Eight of the 109 samples were trade secret chemical compounds. Meng also made false statements to the FBI when questioned about these samples. This investigation was conducted by the FBI.

GM Trade Secrets to China – On July 22, 2010, an indictment returned in the Eastern District of Michigan charging Yu Qin and his wife Shanshan Du, both of Troy, Michigan, was unsealed. The indictment charged the defendants with conspiracy to possess trade secrets without authorization, unauthorized possession of trade secrets and wire fraud. According to the indictment, from December 2003 through May 2006, the defendants conspired to possess trade secret information of General Motors Company relating to hybrid vehicles, knowing that the information had been stolen, converted, or obtained without authorization. The indictment alleges that Du, while employed with GM, provided GM trade secret information relating to hybrid vehicles to her husband, Qin, for his benefit and for the benefit of a company, Millennium Technology International Inc. (MTI), which the defendants owned and operated. Five days after Du was offered a severance agreement by GM in January 2005, she copied thousands of GM documents, including trade secret documents, to a computer hard drive used for MTI business. A few months later, Qin moved forward on a new business venture to provide hybrid vehicle technology to Chery Automobile, a Chinese automotive manufacturer based in China and a competitor of GM. The indictment further alleges that in May 2006, the defendants possessed GM trade secret information without authorization on several computer and electronic devices located in their residence. Based on preliminary calculations, GM estimates that the value of the stolen GM documents is over $40 million. This investigation was conducted by the FBI.

Economic Espionage / Theft of Space Shuttle and Rocket Secrets for China – On Feb. 11, 2010 former Rockwell and Boeing engineer Dongfan "Greg" Chung was sentenced to 188 months imprisonment and three years' supervised release after his July 16, 2009 conviction in the Central District of California. Chung was convicted of charges of economic espionage and acting as an illegal agent of the People's Republic of China (PRC), for whom he stole restricted technology and Boeing trade secrets, including information related to the Space Shuttle program and the Delta IV rocket. According to the judge's ruling, Chung served as an illegal agent of China for more than 30 years and kept more than 300,000 pages of documents reflecting Boeing trade secrets stashed in his home as part of his mission of steal aerospace and military trade secrets from Boeing to

assist the Chinese government. Chung sent Boeing trade secrets to the PRC via the mail, via sea freight, via the Chinese consulate in San Francisco, and via a Chinese agent named Chi Mak. On several occasions, Chung also used the trade secrets that he misappropriated from Boeing to prepare detailed briefings that he later presented to Chinese officials in the PRC. Chung was originally arrested on Feb. 11, 2008, in Southern California after being indicted on eight counts of economic espionage, one count of conspiracy to commit economic espionage, one count of acting as an unregistered foreign agent, one count of obstruction of justice, and three counts of making false statements to the FBI. The investigation was conducted by the FBI and NASA.

Illegal Export of Military Technology / Money Laundering / Illegal Communication of Classified Information for China–On Aug. 9, 2010, following six days of deliberation after a trial spanning nearly four months in Honolulu, a federal jury found Noshir S. Gowadia guilty of five criminal offenses relating to his design for the PRC of a low-signature cruise missile exhaust system capable of rendering a PRC cruise missile resistant to detection by infrared missiles. He was sentenced late yesterday to 32 years in prison for communicating classified national defense information to the People's Republic of China (PRC), illegally exporting military technical data, as well as money laundering, filing false tax returns and other offenses. The jury also convicted Gowadia in three counts of illegally communicating classified information regarding lock-on range for infrared missiles against the U.S. B-2 bomber to persons not authorized to receive such information. The B-2 bomber is one of America's most critical defense assets, capable of utilizing its stealth characteristics to penetrate enemy airspace and deliver precision guided weapons on multiple targets. Gowadia was also convicted of unlawfully exporting classified information about the B-2, illegally retaining information related to U.S. national defense at his home, money laundering and filing false tax returns for the years 2001 and 2002. According to information produced during the trial, Gowadia was an engineer with Northrop Grumman Corporation from approximately 1968 to 1986, during which time he contributed to the development of the unique propulsion system and low observable capabilities of the B-2 Spirit bomber, sometimes referred to as the

"Stealth" bomber. Gowadia also continued to work on classified matters as a contractor with the with the U.S. government until 1997, when his security clearance was terminated. Evidence at the trial revealed that from July 2003 to June 2005, Gowadia took six trips to the PRC to provide defense services in the form of design, test support and test data analysis of technologies for the purpose of assisting the PRC with a cruise missile system by developing a stealthy exhaust nozzle. At the time of his arrest, Gowadia had been paid at least $110,000 by the PRC. The jury convicted Gowadia of two specific transmissions of classified information: a PowerPoint presentation on the exhaust nozzle of a PRC cruise missile project and an evaluation of the effectiveness of a redesigned nozzle, and a computer file providing his signature prediction of a PRC cruise missile outfitted with his modified exhaust nozzle and associated predictions in relation to a U.S. air-to-air missile. This case was investigated by FBI, the U.S. Air Force Office of Special Investigations, the IRS's Criminal Investigation Division, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement and the State Department's Directorate of Defense Trade Controls.

Theft of Computer Trade Secrets for China – September 19, 2012, Chunlai Yang, a former senior software engineer for Chicago-based CME Group, Inc., pleaded guilty to theft of trade secrets for stealing computer source code and other proprietary information while at the same time pursuing plans to improve an electronic trading exchange in China. Yang admitted to downloading more than 10,000 files between late 2010, and June 30, 2011, containing CME computer source code that made up a substantial part of the operating systems for the Globex electronic trading platform. The government maintains that the potential loss was between $50 million and $100 million, while Yang maintains that the potential loss was less than $55.7 million. According to the plea agreement, Yang began working for CME Group in 2000 and was a senior software engineer at the time of his arrest. His responsibilities included writing computer code and, because of his position, he had access to the software programs that supported the Globex electronic trading platform, which allowed market participants to buy and sell CME Group products from any place at any time. The source code and algorithms that made up the supporting programs were proprietary and confidential business property of

CME Group, which instituted internal measures to safeguard and protect its trade secrets. Yang also admitted that he and two unnamed business partners developed plans to form a business referred to as the Tongmei (Gateway to America) Futures Exchange Software Technology Company (Gateway), whose purpose was to increase the trading volume at the Zhangjiagang, China, chemical electronic trading exchange (the Zhangjiagang Exchange.) The Zhangjiagang Exchange was to become a transfer station to China for advanced technologies companies around the world. Yang expected that Gateway would provide the exchange with technology through written source code to allow for high trading volume, high trading speeds, and multiple trading functions. To help the China exchange attract more customers and generate higher profits, Gateway proposed to expand the Zhangjiagang Exchange's software by providing customers with more ways of placing orders; connecting the exchange database's storage systems and matching systems; rewriting the trading system software in the JAVA computer programming language; raising the system's capacity and speed by modifying communication lines and structures; and developing trading software based on the FIX computer coding language.

LIST OF REFERENCES

Allison, Graham T. "Obama and Xi Must Think Broadly to Avoid a Classic Trap." *New York Times*, June 6, 2013. http://www.nytimes.com/2013/06/07/opinion/obama-and-xi-must-think-broadly-to-avoid-a-classic-trap.html?_r=0.

Alperovitch, Dmitri. *Revealed: Operation Shady RAT.* Santa Clara, CA: McAfee, 2011. http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

Anand, Rahul, Kevin C. Cheng, Sidra Rehman, and Longmei Zhang. "Potential Growth in Emerging Asia." IMF Working Paper WP/14/2, International Monetary Fund, 2014. http://www.imf.org/external/pubs/ft/wp/2014/wp1402.pdf.

Angell, Norman. *The Great Illusion*. New York: Garland, 1972.

Armstrong, Shiro. "Rare earth metals export ban, a Chinese own goal." East Asia Forum, September 19, 2011. http://www.eastasiaforum.org/2011/09/19/rare-earth-metals-export-ban-a-chinese-own-goal/.

Bingguo, Dai. "坚持走和平发展道路 [Stick to the Road of Peaceful Development]." December 6, 2010. http://www.gov.cn/ldhd/2010-12/06/content_1760381.htm.

Bradsher, Keith. "After China's Rare Earth Embargo, a New Calculus." *New York Times*, October 29, 2010. http://www.nytimes.com/2010/10/30/business/global/30rare.html

———. "Amid Tension, China Blocks Vital Exports to Japan." *New York Times*, September 22, 2010. http://www.nytimes.com/2010/09/23/business/global/23rare.html?pagewanted=all&_r=0.

———. "China Said to Widen Its Embargo of Minerals." *New York Times*, October 19, 2010. http://www.nytimes.com/2010/10/20/business/global/20rare.html?pagewanted=all

Brzezinski, Zbigniew and John J. Mearsheimer. "Clash of the Titans." *Foreign Policy*, no. 146 (January/February 2005): 46–60. http://www.risingpowersinitiative.org/wp-content/uploads/brzezinksi1.pdf.

Burke, Sara, and Claudio Puty. "The Post-World War II *Golden Age* of Capitalism and the Crisis of the 1970s." Gloves Off. Accessed July 23, http://www.glovesoff.org/features/gjamerica_1.html.

Casey, Joseph, and Katherine Koleski. *Backgrounder: China's 12th Five-Year Plan*. Washington, DC: U.S.-China Economic and Security Review Commission, 2011. http://www.uscc.gov/Research/backgrounder-china%E2%80%99s-12th-five-year-plan.

Catania, Patrick J. "Lack of Personal Savings: The Weakest Link." Baxter Credit Union Web. Accessed July 22, 2014. https://www.cdwcu.com/FRCPersonalSavingsarticle.aspx.

China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy. (USITC Publication No. 4226). Washington, DC: U.S. International Trade Commission, 2011. http://www.usitc.gov/publications/332/pub4226.pdf.

Commission on the Theft of American Intellectual Property, The. *The IP Commission Report.* Seattle: The National Bureau of Asian Research, 2013. http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

Cyberspace: U.S. Faces Challenges in Addressing Global Cybersecurity and Governance. (GAO-10-606). Washington, DC: U.S. Government Accountability Office, 2010. http://gao.gov/assets/310/308401.pdf.

Dadush, Uri. "Key Trends in the World Economy." In *Handbook of Emerging Economies*, edited by Robert E. Looney, 13–29. London and New York: Routledge, 2014.

Davis, E. Philip. "Comparing Bear Markets - 1973 and 2000." *National Institute Economic Review* 183, no. 78 (January 2003): 78–79, http://ner.sagepub.com/content/183/1/78.full.pdf+html.

Department of Defense Strategy for Operating in Cyberspace. Washington, DC: Department of Defense, 2011. http://www.defense.gov/news/d20110714cyber.pdf.

World Trade Organization, The. "Dispute Settlement: The Disputes; Disputes by country/territory," Accessed October 20, 2014. http://www.wto.org/english/tratop_e/dispu_e/dispu_by_country_e.htm.

Dolan, Ed. "China's Fragile Rare Earth Monopoly." *Ed Dolan's Econ blog*, October 24, 2010. http://dolanecon.blogspot.com/2010/10/chinas-fragile-rare-earth-monopoly.html.

Dongyang, Zhu. "Commentary: Cyber-spying charges against Chinese officers an indictment of U.S. hypocrisy." *Xinhua*, May 20, 2014. http://news.xinhuanet.com/english/china/2014-05/20/c_133347543.htm.

Donilon, Tom. *Press Briefing by National Security Advisor Tom Donilon.* Washington, DC: The White House, 2013. http://www.whitehouse.gov/the-press-office/2013/06/08/press-briefing-national-security-advisor-tom-donilon.

Economics and Statistics Administration and U.S. Patent and Trademark Office. *Intellectual Property and the U.S. Economy: Industries in Focus*. Washington, DC: U.S. Department of Commerce, 2012. http://www.uspto.gov/news/publications/IP_Report_March_2012.pdf.

Editorial Board. "Getting China to talk about cyber espionage." *Washington Post*, June 5, 2013. http://www.washingtonpost.com/opinions/getting-china-to-talk-about-cyberespionage/2013/06/05/d69f5446-cdec-11e2-8845-d970ccb04497_story.html.

Executive Office of the President of the United States. *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets.* Washington, DC: The White House, February 2013. http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

Federal Reserve Bank of St. Louis. "Graph: Personal Consumption Expenditures/Gross Domestic Product." Federal Reserve Bank of St. Louis. Accessed July 22, 2014. http://research.stlouisfed.org/fred2/graph/?g=hh3.

Foner, Eric. *Give Me Liberty! An American History.* 3rd ed. New York: W.W. Norton, 2011.

Friedman, Thomas L. *The World is Flat: Brief History of the Twenty-First Century*. New York: Picador, 2007.

Gottschang, Thomas R. "A Country Study: China." Library of Congress (Call Number DS706.C489 1988). http://lcweb2.loc.gov/frd/cs/cntoc.html#cn0149**.**

Grasso, Valerie Bailey. *Rare Earth Elements in National Defense: Background, Oversight Issues, and Options for Congress.* (CRS Report No. R41744). Washington, DC: Congressional Research Service, 2013. http://fas.org/sgp/crs/natsec/R41744.pdf.

Hagenstad, II, William. *21st Century Chinese Cyberwarfare*. Cambridgeshire: IT Governance Publishing, 2012.

Hannas, William C., James Mulvenon, and Anna Puglisi. *Chinese Industrial Espionage: Technology Acquisition and Military Modernization.* New York: Routledge, 2013.

Haxel, Gordon B., James B. Hedrick, and Greta J. Orris. *Rare Earth Elements—Critical Resources for High Technology.* (Fact Sheet 087–02). Reston, VA: U.S. Geological Survey, 2005. http://pubs.usgs.gov/fs/2002/fs087-02/.

House Permanent Select Committee on Intelligence. *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*. Washington, DC: U.S. House of Representatives, 2012. https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf.

Hsu, Kimberly and Craig Murray. *China and International Law in Cyberspace.* Washington, DC: U.S.-China Economic and Security Review Commission, 2014. http://origin.www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf.

Humphries, Marc. *Rare Earth Elements: The Global Supply Chain.* (CRS Report No. R41347). Washington, DC: Congressional Research Service, 2013. http://fas.org/sgp/crs/natsec/R41347.pdf.

International Monetary Fund. "Global Financial Stability Report: Moving from Liquidity-To Growth-Driven Markets." April 2014. http://www.imf.org/external/pubs/FT/GFSR/2014/01/index.htm.

International Monetary Fund. "World Economic Outlook Database: Current Account Balance Statistics." April 2014. http://www.imf.org/external/pubs/ft/weo/2014/01/weodata/index.aspx. IMF eData Library. "Balance of Payment Statistics." International Monetary Fund. Accessed July 22, 2014. http://elibrary-data.imf.org/FindDataReports.aspx?d=33061&e=170784.

International Comparison Program. "Purchasing Power Parities and Real Expenditures of World Economies: Summary of Results and Findings of the 2011 International Comparison Program." Washington, DC: The World Bank, 2014. http://siteresources.worldbank.org/ICPINT/Resources/270056-1183395201801/Summary-of-Results-and-Findings-of-the-2011-International-Comparison-Program.pdf.

Jackson, William. "How Google attacks changed the security game." Global Compliance Network. Sep 01, 2010. http://gcn.com/articles/2010/09/06/interview-george-kurtz-mcafee-google-attacks.aspx.

Jha, Saurav. "China's Rare Earths Advantage." *The Diplomat,* April 29, 2014. http://thediplomat.com/2014/04/chinas-rare-earths-advantage/.

Jincheng, Wei. "Information War: A New Form of People's War." In *Chinese Views of Future Warfare,* edited by Michael Pillsbury, 409–412. Revised ed. Washington, D.C.: National Defense University Press, 1998.

Johnson, Bobbie. "U.S. asks China to Explain Google Hacking Claims." *Guardian*, January 13, 2010. http://www.theguardian.com/technology/2010/jan/13/china-google-hacking-attack-us.

Kellan, Ann. "Hackers Hit Government Websites after China Embassy Bombing." *CNN*, May 11, 1999. http://www.cnn.com/TECH/computing/9905/10/hack.attack.02/index.html?_s=PM:TECH.

Kennedy, David M. "What Would Wilson Do?." *The Atlantic*, January 1, 2010. http://www.theatlantic.com/magazine/archive/2010/01/what-would-wilson-do/307844/3/.

Keohane, Robert O. and Joseph S. Nye, Jr. *Power and Interdependence.* City: HarperCollins: 1989.

———. "Power and Interdependence in the Information Age." *Foreign Affairs* 77, no. 5 (September/October 1998): 81–94. http://www.foreignaffairs.com/articles/54395/robert-o-keohane-and-joseph-s-nye-jr/power-and-interdependence-in-the-information-age.

Kerry, John. *Solo Press Availability in Beijing, China*. Washington, DC: Department of State, 2014. http://www.state.gov/secretary/remarks/2014/02/221658.htm.

Krekel, Bryan. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*. Falls Church, VA: Northrop Grumman, 2009. http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-030.pdf.

Kwon, K.J., Jethro Mullen, and Michael Pearson. "Hacking attack on South Korea traced to Chinese address, officials say." *CNN*, March 21, 2013. http://edition.cnn.com/2013/03/21/world/asia/south-korea-computer-outage/.

Labonte, Marc and Jared C. Nagel. *Foreign Holdings of Federal Debt* (CRS Report No. RS22331). Washington, DC: Congressional Research Service, 2014. http://fas.org/sgp/crs/misc/RS22331.pdf.

Lawrence, Susan V. *U.S.-China Relations: An Overview of Policy Issues* (CRS Report No. R41108). Washington, DC: Congressional Research Service. http://fas.org/sgp/crs/row/R41108.pdf.

Lewis, James. *Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia*. Washington, DC: Center for Strategic and International Studies, 2013. http://csis.org/publication/hidden-arena-cyber-competition-and-conflict-indo-pacific-asia.

Lewis, James and Stewart Baker. *The Economic Impact of Cybercrime and Cyber Espionage*. Washington, DC: Center for Strategic and International Studies, 2013. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf.

Lieberthal, Kenneth and Peter W. Singer. *Cybersecurity and U.S.-China Relations*. Washington, DC: Brookings Institute, 2012. http://www.brookings.edu/~/media/Research/Files/Papers/2012/2/23%20cybersecurity%20china%20us%20singer%20lieberthal/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.PDF.

Looney, Robert E. "Introduction." In *Handbook of Emerging Economies*, edited by Robert E. Looney, 3–12. London and New York: Routledge, 2014.

Lowther, Adam, John Geis, Panayotis Yannakogeorgos, and Chad Dacus. "Chinese-US Relations: Moving Toward Greater Cooperation or Conflict?" *Strategic Studies Quarterly*, Winter 2013, 20–45. http://www.au.af.mil/au/ssq/digital/pdf/winter_13/2013winter-Lowther.pdf.

Lynn, III, William J. *Remarks on the Department of Defense Cyber Strategy*. As Delivered by Deputy Secretary of Defense William J. Lynn, III. National Defense University, July 14, 2011. http://www.defense.gov/speeches/speech.aspx?speechid=1593.

Mandiant. *APT1: Exposing One of China's Cyber Espionage Units.* Alexandria, VA: Mandiant, 2013. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

———. *Mandiant M-Trends: the advanced persistent threat.* Alexandria, VA: Mandiant, 2010. https://dl.mandiant.com/EE/assets/PDF_MTrends_2010.pdf?elq=3c9ad31542594c9184e8dcf552d66792&elqCampaignId=.

———. *2014 Threat Report: Beyond the Breach.* Alexandria, VA: Mandiant, 2014. https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf.

McAfee. "Global Energy Cyberattacks: 'Night Dragon.'" McAfee Foundstone Professional Services and McAfee Labs. February 10, 2011. http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf.

———. "Protecting Your Critical Assets: Lessons Learned from 'Operation Aurora.'" McAfee Labs and McAfee Foundstone Professional Services. January 2010. http://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf.

McGregor, James. "Drive for 'Indigenous Innovation': A Web of Industrial Policies." APCO Worldwide, July 2010. https://www.uschamber.com/sites/default/files/legacy/reports/100728chinareport_0.pdf.

Mearsheimer, John J. "China's Unpeaceful Rise." *Current History* (April 2006): 160–162. http://www.currenthistory.com/pdf_org_files/105_690_160.pdf.

McReynolds, Joe. “In a Fortnight: Cyber Transparency for Thee, But Not for Me.” *China Brief* 14, no. 8 (April 2014): 1–3. http://www.jamestown.org/chinabrief/.

Morrison, Wayne M. *China’s Economic Rise: History, Trends, Challenges, and Implications for the United States*. (CRS Report No. RL33534). Washington, DC: Congressional Research Service, 2014. http://fas.org/sgp/crs/row/RL33534.pdf.

———. *China-U.S. Trade Issues*. (CRS Report No. RL33536). Washington, DC: Congressional Research Service, 2014. http://fas.org/sgp/crs/row/RL33536.pdf.

Morrison, Wayne M. and Marc Labonte. *China’s Holdings of U.S. Securities: Implications for the U.S. Economy*. (CRS Report No. RL34314). Washington, DC: Congressional Research Service, 2013. http://fas.org/sgp/crs/row/RL34314.pdf.

Morrison, Wayne and Rachel Tang. *China’s Rare Earth Industry and Export Regime: Economic and Trade Implications.* (CRS Report No. R42510). Washington, DC: Congressional Research Service, 2012. http://fas.org/sgp/crs/row/R42510.pdf.

National Strategy to Secure Cyberspace, The. Washington, DC: The White House, 2003. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

Norris, Floyd. “1974 Redux: Why Bear Market May Be Over.” *New York Times*, October 4, 2002. http://www.nytimes.com/2002/10/04/business/1974-redux-why-bear-market-may-be-over.html.

Nye, Joseph S. Jr., “American and Chinese Power after the Financial Crisis.” *Washington Quarterly* 33, no. 4 (October 2010): 143–153. doi: 10.1080/0163660X.2010.516634.

———. *American Power in the Twenty-First Century: Two Examples*. Berkeley, CA: University of California at Berkeley, 1999.

———. “Cyber Power.” Belfer Center for Science and International Affairs, Harvard Kennedy School. May 2010. http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

———. *The Future of Power*. New York: Public Affairs, 2011.

Office of the National Counterintelligence Executive. *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage*. Washington, DC: Office of the Director of National Intelligence, 2011. http://www.ncix.gov/publications/reports/fecie_all/index.php.

Office of the Secretary of Defense. *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2012*. Washington, DC: Department of Defense, 2012. https://www.hsdl.org/?view&did=723112.

———. *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013*." Washington, DC: Department of Defense, 2013. http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf.

———. *Report to Congress, Assessment of the National Security Risks Posed to the United States as a Result of the U.S. Federal Debt Owed to China as a Creditor of the U.S. Government*. Washington, DC: Department of Defense, 2012. http://www.defense.gov/pubs/pdfs/2012_cmpr_final.pdf.

Panda, Ankit. "Why Did the U.S. Indict PLA Officers for Hacking, Economic Espionage?." *The Diplomat*, May 21, 2014. http://thediplomat.com/2014/05/why-did-the-us-indict-pla-officers-for-hacking-economic-espionage/.

Pufeng, Wang. "The Challenge of Information Warfare." In *Chinese Views of Future Warfare,* edited by Michael Pillsbury, 317–326. Revised ed. Washington, D.C.: National Defense University Press, 1998.

Ramo, Joshua Cooper. The Beijing Consensus. London: Foreign Policy Centre, 2004.

Rampell, Catherine. "Savings Rates Rising Toward Mediocrity." *Economix (blog), New York Times*, June 26, 2009. http://economix.blogs.nytimes.com/2009/06/26/savings-rates-rising-toward-mediocrity/?_php=true&_type=blogs&_r=0.

Riley, Michael A. and Ashlee Vance. "China Corporate Espionage Boom Knocks Wind Out of U.S. Companies." *Bloomberg Businessweek*, March 15, 2012. http://www.bloomberg.com/news/2012-03-15/china-corporate-espionage-boom-knocks-wind-out-of-u-s-companies.html.

Roach, Stephen S. "China's 12th Five-Year Plan: Strategy vs. Tactics." Morgan Stanley, April 2011. http://www.law.yale.edu/documents/pdf/cbl/China_12th_Five_Year_Plan.pdf.

———. *The Next Asia: Opportunities and Challenges for a New Globalization.* Hoboken, NJ: John Wiley & Sons, 2009.

———. *Unbalanced: The Codependency of America and China.* New Haven and London: Yale University Press, 2014.

Schmidt, Michael S. "U.S. Charges Chinese Army Personnel With Cyberspying." *New York Times*, May 19, 2014. http://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html?action=click&contentCollection=World&region=Footer&module=MoreInSection&pgtype=article

Schmidt, Michael S., Keith Bradsher, and Christine Hauser. "U.S. Panel Cites Risks in Chinese Equipment." *New York Times*, October 8, 2012, http://www.nytimes.com/2012/10/09/us/us-panel-calls-huawei-and-zte-national-security-threat.html?pagewanted=all&_r=0.

Schuman, Michael. "Why Do We Fear a Rising China?" *Time*, June 7, 2011. http://business.time.com/2011/06/07/why-do-we-fear-a-rising-china/.

Segal, Adam. "The Positive That Might Have Come Out the U.S.-China Cybersecurity Working Group." *Asia Unbound (blog), Council on Foreign Relations*, July 10, 2013. http://blogs.cfr.org/asia/2013/07/10/the-positive-that-might-have-come-out-the-u-s-china-cybersecurity-working-group/.

Spade, Jayson M. "Information as Power: China's Cyber Power and America's National Security." U.S. Army War College. May 2012. http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-072.pdf.

Springut, Micah, Stephen Schlaikjer, and David Chen. *China's Program for Science and Technology Modernization: Implications for American Competitiveness*. Prepared for The U.S.-China Economic and Security Review Commission. Arlington; VA: CENTRA Technology, Inc., 2011. http://origin.www.uscc.gov/sites/default/files/Research/USCC_REPORT_China%27s_Program_forScience_and_Technology_Modernization.pdf.

Stringer, David. "China's Rare Earth Toxic Time Bomb to Spur Mining Boom." *Bloomberg*, June 4, 2014. http://www.bloomberg.com/news/2014-06-03/china-s-rare-earth-toxic-time-bomb-to-spur-12-billion-of-mines.html.

Sutter, Robert. "Rebalancing, China and Asian Dynamics – Obama's Good Fit." Center for Strategic and International Studies. January 6, 2014. https://csis.org/publication/pacnet-1-rebalancing-china-and-asian-dynamics-obamas-good-fit.

Thomas, Timothy. "Google Confronts China's 'Three Warfares.'" *Parameters* (Summer 2010): 101–113. http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/2010summer/Thomas.pdf

United States of America v. Kexue Huang. Plea Agreement No. 1:10-cr-00102-WTL-KPF-01 (August, 9, 2011). http://tsi.brooklaw.edu/sites/tsi.brooklaw.edu/files/filings/united-states-v-huang/20110809plea-agreement.pdf

U.S.-China Business Council, The. "China's Strategic Emerging Industries: Policy, Implementation, Challenges, & Recommendations." March 2013. http://uschina.org/sites/default/files/sei-report.pdf.

U.S.-China Economic and Security Review Commission. *2013 Annual Report to Congress*. Washington, DC: Government Printing Office, 2013. http://www.uscc.gov/Annual_Reports/2013-annual-report-congress.

U.S. Department of Commerce Bureau of Economic Analysis. "National Income and Product Accounts Tables: 2010–2014." Last modified June 25, 2014. http://www.bea.gov/iTable/iTable.cfm?ReqID=9&step=1#reqid=9&step=3&isuri=1&904=2010&903=137&906=q&905=2014&910=x&911=0.

U.S. Department of Justice. "Former CME Group Software Engineer Pleads guilty to Stealing Globex Computer Trade Secrets While Planning Business to Improve Electronic Trading Exchange in China." September 19, 2012. http://www.justice.gov/usao/iln/pr/chicago/2012/pr0919_01.pdf.

———. "Hawaii Man Sentenced to 32 Years in Prison for Providing Defense Information and Services to People's Republic of China." January, 25, 2011. http://www.justice.gov/opa/pr/hawaii-man-sentenced-32-years-prison-providing-defense-information-and-services-people-s.

U.S. Department of Labor Bureau of Labor and Statistics. "Labor Force Statistics from the Current Population Survey." Accessed July 23, 2014. http://data.bls.gov/timeseries/LNS14000000.

Waltz, Kenneth N. "Conversations with History: Conversation with Kenneth Waltz." Institute of International Studies, University of California at Berkeley. February 10, 2003. http://globetrotter.berkeley.edu/people3/Waltz/waltz-con5.html.

———. *Man, the State, and War: A Theoretical Analysis*. New York: Columbia University Press, 2001.

———. "Structural Realism after the Cold War," *International Security* 25, no. 1 (2000): 5–41. http://www.columbia.edu/itc/sipa/U6800/readings-sm/Waltz_Structural%20Realism.pdf.

———. *Theory of International Politics*. New York: McGraw-Hill, 1979.

World Bank, The. "China 2030: Building a Modern, Harmonious, and Creative Society." 2013. http://www.worldbank.org/content/dam/Worldbank/document/China-2030-complete.pdf.

Wright, Tom. China's Economy Surpassing the U.S.? Well, Yes and No." *Real Time Economics (blog)*, *The Wall Street Journal*, April 30, 2014. http://blogs.wsj.com/economics/2014/04/30/chinas-economy-surpassing-u-s-well-yes-and-no/.

Xinhua News. "Accusation of Chinese Government's Participation in Cyber Attack "Groundless": Ministry." January 25, 2010. http://news.xinhuanet.com/english2010/china/2010-01/25/c_13149276.htm.

Xinhua News. "Xi Urges Innovation-Driven Growth." March 4, 2013. http://news.xinhuanet.com/english/china/2013-03/04/c_132207617.htm.

Zetter, Kim. "'Google' Hackers Had Ability to Alter Source Code." *Wired*. March 3, 2010. http://www.wired.com/2010/03/source-code-hacks/.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California