NEGATIVE BRIEF: Chinese Cyber Piracy

NEGATIVE BRIEF: Chinese Cyber Piracy 3

NEGATIVE PHILOSOPHY 3

Fears of Chinese cyber threat are exaggerated 3

International trade law is the wrong forum to deal with any form of espionage 3

INHERENCY 3

1. China is improving 3

Industrial espionage is done by private parties, and the Chinese government is getting better at stopping it. We need to let the justice system deal with it, not strategic diplomacy 3

HARMS / SIGNIFICANCE 4

1. US does the same thing 4

Who are we to complain? Snowden proves the US does the same thing 4

US spying DOES help US firms economically 4

US intelligence activities offset China’s economic spying: Net result is no clear advantage for either one 4

US spying is what’s hurting US business competitiveness, not Chinese spying 5

2. Threat is receding 5

Increased awareness motivates companies to take more defensive measures now. Golden age of hacking may be over 5

3. Useless data 6

They collect cyber industrial espionage data, fine: But then what do they do with it? 6

China has trouble actually doing anything useful with the stolen data 6

They don’t have the skills to do much with stolen technology: too much bureaucracy and not enough technical skills 6

Just because they’re stealing tons of data doesn’t mean they know what to do with it 7

China can’t easily absorb the information it gets and probably won’t get any enduring technical advantage 7

4. Not much US business impact to IP theft 8

Loss of a trade secret from cyber espionage does not automatically result in economic damage 8

US business impacts of Chinese industrial cyber espionage are exaggerated 8

5. Turn: Hacking leads to Chinese technological dependency – may hurt them more than it helps 8

Reliance on industrial espionage locks them into permanent “second place” status. Example: Soviets during Cold War 8

6. [In case AFF plan links industrial espionage into Chinese military threats] No Chinese military threat from hacking 9

US/China economic cyber threats will not escalate into a cyber war, nor a conventional war 9

Chinese Army (PLA) would be disadvantaged in a cyber war: The US military is better prepared 9

China’s military cyber capabilities aren’t a big threat 9

China’s economic and military cyber capabilities are exaggerated: The gap between them and us is growing (i.e. US capabilities are rising faster than theirs and leaving China behind) 10

SOLVENCY 10

1. Wrong target. Affirmative wants to sanction the Chinese government, but they’re not the primary culprit. 10

Chinese IP theft is mainly a private, not government, activity 10

US government study says Chinese industrial hacking mostly isn’t coming from the Chinese government 10

2. WTO dispute mechanism takes too long 11

3. WTO attorneys working disputes on Intellectual Property don’t understand it 11

4. Text of the WTO doesn’t apply 11

5. Won’t be able to win our case at WTO 12

DISADVANTAGES 12

1. Damage relations with China 12

Link: Using WTO against China over cyber espionage would damage US/China relations 12

Impact: US/China cooperation is the most important foreign policy goal in the world – we need China for solving all major world problems 12

2. Chinese retaliation at WTO 13

Link: Using the WTO against Chinese economic espionage would bring retaliation from China at the WTO 13

Impact: Net benefits. Fighting with China at WTO on balance would not be in US interests 13

3. Increased China mistrust 14

Link: Hype about cyber operations raises US/China mistrust 14

Link: Hyping the cyber threat makes US/China war more likely 14

Impact: War with China would be economic and political disaster for PRC and US 14

NEGATIVE BRIEF: Chinese Cyber Piracy

NEGATIVE PHILOSOPHY

Fears of Chinese cyber threat are exaggerated

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction <http://muse.jhu.edu/login?auth=0&type=summary&url=/journals/international_security/v039/39.3.lindsay.pdf>

Exaggerated fears about the paralysis of digital infrastructure and the loss of competitive advantage contribute to a spiral of mistrust in U.S.-China relations. In every category of putative Chinese cyber threat, there are also considerable Chinese vulnerabilities and Western advantages. China has inadvertently degraded the economic efficiency of its networks and exposed them to foreign infiltration by prioritizing political information control over technical cyber defense. Although China also actively infiltrates foreign targets, its ability to absorb stolen data is questionable, especially at the most competitive end of the value chain, where the United States dominates.

International trade law is the wrong forum to deal with any form of espionage

Prof. David Fidler 2013. (Visiting Fellow for Cybersecurity at the Council on Foreign Relations and is the James Louis Calamaras Professor of Law at Indiana Univ. ) 11 Feb 2013 Why the WTO is not an Appropriate Venue for Addressing Economic Cyber Espionage <http://armscontrollaw.com/2013/02/11/why-the-wto-is-not-an-appropriate-venue-for-addressing-economic-cyber-espionage/>

The potential for trade relations to deteriorate into something more dangerous helps explain why states have never considered international trade law and institutions as appropriate instruments for addressing national security threats posed by any form of espionage.

INHERENCY

1. China is improving

Industrial espionage is done by private parties, and the Chinese government is getting better at stopping it. We need to let the justice system deal with it, not strategic diplomacy

Greg Austin 2013. (Professorial Fellow with the [East-West Institute](http://thediplomat.com/2015/05/what-the-us-gets-wrong-about-chinese-cyberespionage/www.ewi.info) in New York and a Visiting Professor at the Australian Centre for Cyber Security in the University of New South Wales at the Australian Defense Force Academy) 26 Sept 2013 China’s Cyber Espionage Priorities <http://ewipolicy.tumblr.com/post/62325267109/chinas-cyber-espionage-priorities>

Stamping out this public-private espionage at the source is probably not a high priority for Chinese leaders. They do not have the political will to look that deeply into the activities of intelligence agencies. They may and indeed can only respond to facts on the ground that reveal the IP theft through physical production based on it. For fifteen years, China has – in good faith – been progressively strengthening its intellectual property rights (IPR) regime as a primary foundation of its own national innovation strategy. It may be a long way from the standards of the IPR regimes elsewhere, but the civil legal system, not strategic diplomacy, has to be the locus of Western sanction against Chinese actors for cyber-assisted IP theft.

HARMS / SIGNIFICANCE

1. US does the same thing

Who are we to complain? Snowden proves the US does the same thing

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction <http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf>

Indeed, the intelligence leaks from Edward Snowden in 2013 underscored the sophistication and extent of internet surveillance by the United States and its allies against targets worldwide, including in China. The Snowden revelations not only invigorated debate about the balance between security and privacy in a democracy but also undercut the moral force of American complaints about Chinese penetration of commercial, government, and defense networks. Chinese writers hasten to compare the United States to “a thief crying stop thief.”

US spying DOES help US firms economically

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction <http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf>

A White House spokesperson insisted, “We do not give intelligence we collect to U.S. companies to enhance their international competitiveness or increase their bottom line.” In practice, however, this line can blur. The U.S. government might spy on a foreign trade delegation to improve its position in negotiating trade agreements, which would benefit U.S. firms indirectly. It might spy on foreign defense firms and pass on weapon designs to U.S. contractors to develop countermeasures or future requirements, which could improve their profitability.

US intelligence activities offset China’s economic spying: Net result is no clear advantage for either one

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction <http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf>

The chairman of the U.S. House Intelligence Committee alleged that there “is a concerted effort by the government of China to get into the business of stealing economic secrets to put into use in China to compete against the U.S. economy.” Director of the National Security Agency Gen. Keith Alexander described the result of this effect as “the greatest transfer of wealth in history.” Chinese espionage activity alone, however, cannot produce this result. To realize competitive advantage, China needs to be able to absorb and apply the data it steals. Moreover, the United States is also a formidable intelligence actor, which can be expected to offset Chinese advantages to some degree. The category of contested cyberspace highlights the increasing intensity of intelligence competition, not a clear advantage for one side or the other.

US spying is what’s hurting US business competitiveness, not Chinese spying

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction <http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf> (brackets added)

Some of the Snowden leaks suggest a combination of witting and unwitting assistance to the NSA from U.S. internet firms, ranging from the sharing of metadata and technical design information to exploitation of technical control points in cloud infrastructure located on U.S. soil. Notably, it took an insider leak to compromise the NSA, but lax operator tradecraft has compromised Chinese CNE; this imbalance suggests a higher degree of competency and attention to detail in U.S. tradecraft. Ironically, and contrary to the death-by-a-thousand-cuts narrative, it may be American CNE [computer network exploitation] against China, rather than Chinese CNE against the United States, that ends up adversely affecting the competitiveness of American firms. The Snowden trove has provided China with credible evidence of CNE via some major American internet firms. This, in turn, has prompted a wider backlash against the “eight King Kongs” (bada jingang)—Apple, Cisco, Google, IBM, Intel, Microsoft, Oracle, and Qualcomm. Cisco reported an 18 percent drop in orders from China in the fall quarter of 2013, while Hewlett-Packard, IBM, and Microsoft also reported declining Chinese sales.

2. Threat is receding

Increased awareness motivates companies to take more defensive measures now. Golden age of hacking may be over

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction <http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf>

Prior to 2010, Western firms could be accused of complacency regarding cybersecurity. Since then, however, Western cybersecurity defenses, technical expertise, and government assistance to firms have improved. Also, the increased reporting on long-duration APTs (i.e., those that might be expected to be the most difficult to root out) may reflect a growing discovery rate of hard-to-find APTs by network defenders. The potential improvement in Western cyber defense stands in stark contrast to the popular perception of helplessness in the face of growing Chinese intrusion threats. It is possible that one day Chinese cyber operators may look back on 2010–13 much the way German submariners looked back on the “happy time” of 1940–41—namely, as a brief period rich in easy targets before victims learned how to develop active tracking and countermeasures to protect themselves.

3. Useless data

They collect cyber industrial espionage data, fine: But then what do they do with it?

Greg Austin 2013. (Professorial Fellow with the [East-West Institute](http://thediplomat.com/2015/05/what-the-us-gets-wrong-about-chinese-cyberespionage/www.ewi.info) in New York and a Visiting Professor at the Australian Centre for Cyber Security in the University of New South Wales at the Australian Defense Force Academy) 26 Sept 2013 China’s Cyber Espionage Priorities <http://ewipolicy.tumblr.com/post/62325267109/chinas-cyber-espionage-priorities>

As we contemplate the international threat picture for cybersecurity, how can we evaluate claims about China’s cyber espionage intended to aid Chinese firms in production of items copied from competitors’ designs? According to some sources, the country is engaged in the biggest illicit transfer of wealth in history through the theft of intellectual property from the United States and other advanced economies. The United States has, according to newspaper reports, compiled several case studies demonstrating specific IP theft by Chinese government actors that has been converted to competitor production and that undercut the original American IP owner’s profitability. Beyond these few cases, one of the gaps in the publicly available allegations is a fine-grained and comprehensive analysis of how exactly Chinese intelligence agencies handle the information they are allegedly vacuuming up by the terabyte. Do they have an army of technically skilled translators who immediately render all documents into Chinese? Or is there an intermediary team of technically qualified staff brought in from China’s R&D establishments, specific to each design secret being reviewed, to make a judgment that a particular document needs to be translated and then to determine who in the industry should receive it to set about copying it? In the absence of any discussion in public by United States official sources of this sort of fine-grained detail, we are left to make our own thinly-sourced assessment.

China has trouble actually doing anything useful with the stolen data

Dr Jon R. Lindsay 2015 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) May 2015 "Exaggerating the Chinese Cyber Threat" <http://belfercenter.ksg.harvard.edu/publication/25321/exaggerating_the_chinese_cyber_threat.html>

There is strong evidence that China continues to engage in aggressive cyber espionage campaigns against Western interests. Yet it struggles to convert even legitimately obtained foreign data into competitive advantage, let alone make sense of petabytes of stolen data. Absorption is especially challenging at the most sophisticated end of the value chain (e.g., advanced fighter aircraft), which is dominated by the United States. At the same time, the United States conducts its own cyber espionage against China , as the Edward Snowden leaks dramatized, which can indirectly aid U.S. firms (e.g., in government trade negotiations). China's uneven industrial development, fragmented cyber defenses, erratic cyber tradecraft, and the market dominance of U.S. technology firms provide considerable advantages to the United States.

They don’t have the skills to do much with stolen technology: too much bureaucracy and not enough technical skills

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction <http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf>

China faces major challenges in converting foreign inputs into innovative output given the notoriously compartmentalized and hierarchical nature of Chinese bureaucracy, underdeveloped high-end equipment manufacturing capacity, and chronic dependence on foreign technology and know-how. Reliance on Russia for fighter jet engines despite years of access to technical design information and assistance from Russian technicians is a particularly notable but hardly unique example in the Chinese defense industry. Foreign expertise is only one input in the overall innovation process, which also requires “hard” factors such as materials, universities, skilled labor, laboratories, and factories, as well as “soft” factors such as leadership, regulation, contract enforcement, standards and protocols, and an innovative culture. The utility of even the best CNE [computer network exploitation] is sensitive to the performance of the rest of these factors working in synergy, and China still has far to go in integrating them.

Just because they’re stealing tons of data doesn’t mean they know what to do with it

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction <http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf> (brackets added)

Remote access to target networks is only the first step toward developing an intelligence advantage, much less downstream competitive advantage. Although Western cyber defenders can observe the exfiltration of petabytes of data to Chinese servers, they cannot so readily measure China’s ability to use the data. It is possible, for example, that operators in the Third Department of the PLA General Staff are simply rewarded for the number of foreign targets penetrated and terabytes exfiltrated, with little attention to the satisfaction of the intelligence customer, thereby creating lots of measurable CNE [computer network exploitation] with little improvement in national competitiveness. The acquisition, absorption, and application of foreign information from any source is a complicated process. Transaction costs at every step along the way caused by information overload, analytic misinterpretation, or bureaucratic silos can undermine the translation of stolen data into new production knowledge and successful competition in the marketplace.

China can’t easily absorb the information it gets and probably won’t get any enduring technical advantage

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction <http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf>

Chinese espionage is impressive in its scope, but it does not translate easily into industrial absorption, which is a prerequisite for competitive advantage. Furthermore, U.S. intelligence appears to be more technically adept, even if its target set differs somewhat from China’s. Both sides are engaged in commercial and intelligence contests using a range of political, economic, and technical tools. Charges of unfair competition and attempts to redress it will remain a chronic feature of U.S.-China relations. There is no reason to expect the side playing catch-up to realize an enduring advantage for technical reasons alone.

4. Not much US business impact to IP theft

Loss of a trade secret from cyber espionage does not automatically result in economic damage

Greg Austin 2015. (Professorial Fellow with the [East-West Institute](http://thediplomat.com/2015/05/what-the-us-gets-wrong-about-chinese-cyberespionage/www.ewi.info) in New York and a Visiting Professor at the Australian Centre for Cyber Security in the University of New South Wales at the Australian Defense Force Academy) China’s Cyberespionage: The National Security Distinction and U.S. Diplomacy, May 2015 <http://thediplomat.com/wp-content/uploads/2015/05/thediplomat_2015-05-21_22-14-05.pdf>

In the indictments, the United States says it has evidence of transfer of trade secrets to civil sector companies in the cases of Westinghouse and USS, but while other instances have been asserted, few have been evidenced. It is axiomatic that loss of a trade secret does not automatically convert to damaging competition any more than theft of credit card details translates into losses for all of the victims. In fact, very few people suffer personal financial losses as result of the theft and illegal sale of millions of credit card details.

US business impacts of Chinese industrial cyber espionage are exaggerated

Dr Jon R. Lindsay 2015 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) May 2015 "Exaggerating the Chinese Cyber Threat" <http://belfercenter.ksg.harvard.edu/publication/25321/exaggerating_the_chinese_cyber_threat.html>

The rhetorical spiral of mistrust in the Sino-American relationship threatens to undermine the mutual benefits of the information revolution. Fears about the paralysis of the United States' digital infrastructure or the hemorrhage of its competitive advantage are exaggerated. Chinese cyber operators face underappreciated organizational challenges, including information overload and bureaucratic compartmentalization, which hinder the weaponization of cyberspace or absorption of stolen intellectual property. More important, both the United States and China have strong incentives to moderate the intensity of their cyber exploitation to preserve profitable interconnections and avoid costly punishment. The policy backlash against U.S. firms and liberal internet governance by China and others is ultimately more worrisome for U.S. competitiveness than espionage; ironically, it is also counterproductive for Chinese growth. The United States is unlikely to experience either a so-called digital Pearl Harbor through cyber warfare or death by a thousand cuts through industrial espionage.

5. Turn: Hacking leads to Chinese technological dependency – may hurt them more than it helps

Reliance on industrial espionage locks them into permanent “second place” status. Example: Soviets during Cold War

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction <http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf> (brackets added)

The Soviet Union’s reliance on systematic industrial espionage to catch up with the West provides a cautionary tale: the Soviet system became optimized for imitation rather than innovation and was thus locked into a form of second-place dependency, even as it shortened research and development timelines. Chinese espionage can potentially narrow the gap with the West, but only at the price of creating dependency through investment in a large-scale absorption effort. Chinese CNE [computer network exploitation] poses a genuine intelligence threat, to be sure, but it is neither singularly grave nor unprecedented.

6. [In case AFF plan links industrial espionage into Chinese military threats] No Chinese military threat from hacking

US/China economic cyber threats will not escalate into a cyber war, nor a conventional war

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction <http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf>

This article argues that for every type of purported Chinese cyber threat, there are also serious Chinese vulnerabilities and Western strengths that reinforce the political status quo. Cyberwar between the United States and China, much like U.S.-China conventional war, is highly unlikely. Nevertheless, the economically driven proliferation of information technology enables numerous instances of friction to emerge below the threshold of violence.

Chinese Army (PLA) would be disadvantaged in a cyber war: The US military is better prepared

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction <http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf>

If cyberwarfare is as effective as Chinese writers believe it is but they underestimate the costs of mastery, then the PLA is doubly disadvantaged. Chinese attacks can be expected to be less skillfully coordinated against more robust U.S. defenses, and vice versa. The United States already has, while China still struggles to develop, the institutional complements and experience required to plan and control cyber operations in synchrony with the larger battle. Meanwhile the fear of cyberwarfare has prompted considerable U.S. military investment in network protection, active cyber defense measures (e.g., counterintelligence deception and “hack back” counterattack), and exercises in cyber-degraded conditions. The vaunted asymmetry of cyberwarfare, usually posed as an advantage for the weaker power, in fact runs in the opposite direction, giving the stronger and more experienced force the advantage.

China’s military cyber capabilities aren’t a big threat

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction <http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf>

Despite high levels of Chinese political harassment and espionage, there is little evidence of skill or subtlety in China's military cyber operations. Although Chinese strategists describe cyberspace as a highly asymmetric and decisive domain of warfare, China's military cyber capacity does not live up to its doctrinal aspirations. A disruptive attack on physical infrastructure requires careful testing, painstaking planning, and sophisticated intelligence. Even experienced U.S. cyber operators struggle with these challenges. By contrast, the Chinese military is rigidly hierarchical and has no wartime experience with complex information systems. Further, China's pursuit of military "informatization" (i.e., emulation of the U.S. network-centric style of operations) increases its dependence on vulnerable networks and exposure to foreign cyberattack. To be sure, China engages in aggressive cyber campaigns, especially against nongovernmental organizations and firms less equipped to defend themselves than government entities. These activities, however, do not constitute major military threats against the United States, and they do nothing to defend China from the considerable intelligence and military advantages of the United States.

China’s economic and military cyber capabilities are exaggerated: The gap between them and us is growing (i.e. US capabilities are rising faster than theirs and leaving China behind)

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction <http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf>

Although China also actively infiltrates Western networks, its ability to absorb stolen data is questionable, especially at the most competitive end of the value chain, where the United States dominates. Similarly, China’s military cyber capacity cannot live up to its aggressive doctrinal aspirations, even as “informatization” creates vulnerabilities that more experienced foreign cyber operators can attack. Outmatched by the West, China has resorted to a strategy of institutional reform, but it benefits too much from multistakeholder governance to pose a credible alternative. The secrecy of cyber capabilities and operations on all sides makes it difficult to estimate with confidence the magnitude of the gap between China and the United States in the balance of cyber power, but it is potentially growing, not shrinking.

SOLVENCY

1. Wrong target. Affirmative wants to sanction the Chinese government, but they’re not the primary culprit.

Chinese IP theft is mainly a private, not government, activity

Greg Austin 2013. (Professorial Fellow with the [East-West Institute](http://thediplomat.com/2015/05/what-the-us-gets-wrong-about-chinese-cyberespionage/www.ewi.info) in New York and a Visiting Professor at the Australian Centre for Cyber Security in the University of New South Wales at the Australian Defense Force Academy) 26 Sept 2013 China’s Cyber Espionage Priorities <http://ewipolicy.tumblr.com/post/62325267109/chinas-cyber-espionage-priorities>

I believe that China would devote most of its IP espionage activities to purposes other than industrial production in China based on that IP. Relying on the small amount of public evidence available, I find it hard to credit the “illicit transfer of wealth theory” – the belief that cyber espionage by the Chinese government is a threat to United States industrial security because of production based on the IP thus obtained. Based on what I know about the high impunity enjoyed by cyber criminals everywhere and what I know about Chinese legal and corporate culture, I am more inclined to think the that stealing of IP through cyber means by Chinese actors with a view to replicating it for the market is mainly a private activity in China, perhaps with intelligence officials involved on an unauthorized basis.

US government study says Chinese industrial hacking mostly isn’t coming from the Chinese government

Greg Austin 2015. (Professorial Fellow with the East-West Institute in New York and a Visiting Professor at the Australian Centre for Cyber Security in the University of New South Wales at the Australian Defense Force Academy) China’s Cyberespionage: The National Security Distinction and U.S. Diplomacy, May 2015 <http://thediplomat.com/wp-content/uploads/2015/05/thediplomat_2015-05-21_22-14-05.pdf> (brackets added)

For that reason, the [U.S. National Counter Intelligence Executive] 2009-2011 report concentrates on cyber espionage, while keeping up past practice of reporting on other means. The report cites one China-related example from the military sector and one from the civil sector on trade secret theft, and reports that six of the seven cases prosecuted under the Economic Espionage Act in 2010 involved Chinese entities. The report alluded to an “onslaught” of China-related cyber attacks but noted that the U.S. intelligence community “has not been able to attribute many of these private sector data breaches to a state sponsor”. It noted that some private sector companies it had consulted reported Chinese attacks, asserting a variety of differing private or governmental purposes.

2. WTO dispute mechanism takes too long

The Commission on the Theft of American Intellectual Property 2013 (independent and bipartisan initiative of leading Americans from the private sector, public service in national security and foreign affairs, academe, and politics; co-chaired by Dennis C. Blair ,former Director of National Intelligence and Jon M. Huntsman, Jr. former Ambassador to China and Deputy U.S. Trade Representative) May 2013 “The IP Commission Report” <http://www.ipcommission.org/report/ip_commission_report_052213.pdf>

A qualified success, WTO dispute mechanisms have seen more than 339 settlement reports and arbitration awards issued by the organization’s dispute body from 1995 (its year of inception) through 2011. Of these, the United States participated in 140. Participation rates notwithstanding, WTO dispute mechanisms have several problems. Chief among these is the time required to reach a resolution. The process can be so time-consuming that recapturing any damages through this process is often illusory. As noted above, many products today, especially in the software and other high-tech industries, generate the bulk of profits for their companies in the first weeks or months of release.

3. WTO attorneys working disputes on Intellectual Property don’t understand it

The Commission on the Theft of American Intellectual Property 2013 (independent and bipartisan initiative of leading Americans from the private sector, public service in national security and foreign affairs, academe, and politics; co-chaired by Dennis C. Blair ,former Director of National Intelligence and Jon M. Huntsman, Jr. former Ambassador to China and Deputy U.S. Trade Representative) May 2013 “The IP Commission Report” <http://www.ipcommission.org/report/ip_commission_report_052213.pdf>

Dispute mechanisms for trade in goods have worked reasonably well. However, resolutions to disputes involving IP are often reached behind closed doors, by lawyers lacking a sufficient background to make decisions on important issues of IP protection. This stands in contrast to most modern procedural codes, which generally adhere to common transparent guidelines, including that “judicial proceedings must be public and that, in principle, the control of the allegations and proof belongs to the parties.”

4. Text of the WTO doesn’t apply

Prof. David Fidler 2013. (Visiting Fellow for Cybersecurity at the Council on Foreign Relations and is the James Louis Calamaras Professor of Law at Indiana Univ. ) 11 Feb 2013 Why the WTO is not an Appropriate Venue for Addressing Economic Cyber Espionage <http://armscontrollaw.com/2013/02/11/why-the-wto-is-not-an-appropriate-venue-for-addressing-economic-cyber-espionage/>

So, China must accord IP owned by nationals of other WTO members registered or otherwise protected in China certain minimum standards of treatment, such as national treatment (TRIPS, Article 3). If the Chinese government disclosed IP used in China by a company from another WTO member to a competing Chinese enterprise, then China would violate TRIPS by failing to accord national treatment to those foreign-owned IP rights within its territory. But, as noted above, the most serious worries about Chinese economic cyber espionage do not fit within this territorial-centric scenario and focus on espionage conducted outside China. Clarke, Lewis, and others concerned about economic cyber espionage are not, by and large, complaining about theft by the Chinese government of IP owned by US nationals that is already present in Chinese territory. Cybersecurity experts are worried about a more geographically expansive problem. Nothing in the WTO generally or TRIPS specifically mandates that China (or any other WTO member) protect commercially valuable information found in the territories of other countries. TRIPS does not require WTO members to prohibit their nationals or companies from engaging in corporate espionage inside foreign nations, nor does TRIPS regulate government-led economic espionage within other countries. Thus, the US cannot claim that China is violating TRIPS with respect to Chinese economic cyber espionage the US fears is most damaging to US economic and commercial interests. Or, put another way, China has not made commitments under the WTO regarding espionage it conducts outside its territory, meaning the US cannot claim breach of legal obligations that justifies countermeasures involving trade restrictions against China.

5. Won’t be able to win our case at WTO

Prof. David Fidler 2013. (Visiting Fellow for Cybersecurity at the Council on Foreign Relations and is the James Louis Calamaras Professor of Law at Indiana Univ. ) 11 Feb 2013 Why the WTO is not an Appropriate Venue for Addressing Economic Cyber Espionage <http://armscontrollaw.com/2013/02/11/why-the-wto-is-not-an-appropriate-venue-for-addressing-economic-cyber-espionage/>

Further, the US might want to avoid meeting its burden of proof because doing so would require disclosing counter-intelligence means and methods. Allegations not backed with adequate empirical evidence of state responsibility will not satisfy the burden of proof the US would have in pursuing legal complaints in the WTO. The US could seek support within the WTO for amending TRIPS to cover extraterritorial economic espionage (e.g., extending the national treatment principle to cover extraterritorial government actions affecting IP rights protected in other WTO members), but opposition to such a proposal would come from more WTO members than just China, making it nearly impossible for such an amendment to become reality.

DISADVANTAGES

1. Damage relations with China

Link: Using WTO against China over cyber espionage would damage US/China relations

Prof. David Fidler 2013. (Visiting Fellow for Cybersecurity at the Council on Foreign Relations and is the James Louis Calamaras Professor of Law at Indiana Univ. ) 11 Feb 2013 Why the WTO is not an Appropriate Venue for Addressing Economic Cyber Espionage <http://armscontrollaw.com/2013/02/11/why-the-wto-is-not-an-appropriate-venue-for-addressing-economic-cyber-espionage/>

As Lewis acknowledges, for the US to invoke the national security exception in order to restrict trade with China over economic cyber espionage would constitute a dramatic departure from long-standing practice and a potentially destabilizing step. China is unlikely to “turn the other cheek” and could respond in ways that damage US trade and commercial interests. China might respond by arguing that US government efforts under its “Internet freedom” agenda and/or the intense level of cyber espionage the US government conducts against China constitute threats to its essential security interests, justifying Chinese actions against US exports under WTO rules. A high-profile deterioration in trade relations would negatively affect other aspects of Sino-American diplomacy, making this geopolitically important relationship even more adversarial. In this context, espionage of all kinds would likely increase rather than decrease.

Impact: US/China cooperation is the most important foreign policy goal in the world – we need China for solving all major world problems

US-China Smart Power Commission 2009 (chaired by former US Defense Secretary William Cohen and Maurice R. Greenberg), March 2009, "Smart Power in US-China Relations," CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES <http://csis.org/files/media/csis/pubs/090309_mcgiffert_uschinasmartpower_web.pdf>

The evolution of Sino-US relations over the next months, years, and decades has the potential to have a greater impact on global security and prosperity than any other bilateral or multilateral arrangement. In this sense, many analysts consider the US-China diplomatic relationship to be the most influential in the world. Without question, strong and stable US alliances provide the foundation for the protection and promotion of US and global interests. Yet within that broad framework, the trajectory of US-China relations will determine the success, or failure, of efforts to address the toughest global challenges: global financial stability, energy security and climate change, nonproliferation, and terrorism, among other pressing issues. Shepherding that trajectory in the most constructive direction possible must therefore be a priority for Washington and Beijing. Virtually no major global challenge can be met without US-China cooperation.

2. Chinese retaliation at WTO

Link: Using the WTO against Chinese economic espionage would bring retaliation from China at the WTO

Prof. David Fidler 2013. (Visiting Fellow for Cybersecurity at the Council on Foreign Relations and is the James Louis Calamaras Professor of Law at Indiana Univ. ) 11 Feb 2013 Why the WTO is not an Appropriate Venue for Addressing Economic Cyber Espionage <http://armscontrollaw.com/2013/02/11/why-the-wto-is-not-an-appropriate-venue-for-addressing-economic-cyber-espionage/>

Proposals favoring US use of the WTO against Chinese economic cyber espionage sometimes contain more political than legal flavor–that is, raising the issue in the WTO will put the Chinese under increasing diplomatic scrutiny, leading to a curtailment of Chinese economic cyber espionage. In other words, the purpose of taking the issue to the WTO is not to win a legal argument but to put political pressure on China through this high-profile diplomatic forum. However, this strategy could generate “blowback” against the US from China, which could itself attempt to use the WTO to turn the tables on the US by criticizing American political, military, and intelligence community behavior in cyberspace (e.g., intervening in the domestic affairs of other states under the “Internet freedom” agenda, launching Stuxnet against Iran, and engaging in extensive cyber espionage against many countries). Not wanting to be forced to take sides, other WTO members would want this unproductive standoff to go away and stop jeopardizing what the WTO does well, which does not include resolving spats about espionage practices.

Impact: Net benefits. Fighting with China at WTO on balance would not be in US interests

Prof. David Fidler 2013. (Visiting Fellow for Cybersecurity at the Council on Foreign Relations and is the James Louis Calamaras Professor of Law at Indiana Univ. ) 11 Feb 2013 Why the WTO is not an Appropriate Venue for Addressing Economic Cyber Espionage <http://armscontrollaw.com/2013/02/11/why-the-wto-is-not-an-appropriate-venue-for-addressing-economic-cyber-espionage/>

China has made it clear it is willing to pick fights with the US on cyber issues in diplomatic forums, and I doubt whether an American attempt to enlist the WTO will bring a more cooperative Chinese diplomatic response.  
Conclusion  
Let me be clear: The US and other countries face a serious problem with traditional and economic espionage conducted through cyber technologies. I have written on how dangerous cyber espionage is (see David P. Fidler, “Tinker, Tailor, Soldier, Duqu: Why Cyberespionage is More Dangerous than You Think,” International Journal of Critical Infrastructure Protection (March 2012), pp. 28-29). However, the WTO is not an appropriate venue for the US to use in addressing the threat posed by economic cyber espionage. Cold calculation of American interests suggests this idea should be put aside.

3. Increased China mistrust

Link: Hype about cyber operations raises US/China mistrust

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction <http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf>

Cyber operations and the rhetorical reactions to them on both sides of the Pacific have undermined trust in the Sino-American relationship. Exaggerated fears about the paralysis of digital infrastructure and growing concerns over competitive advantage exacerbate the spiral of mistrust. Closer consideration of domestic factors within China and China’s strategic interaction with the United States reveals a more complicated yet less worrisome situation.

Link: Hyping the cyber threat makes US/China war more likely

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction <http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf>

As long as dense interconnection and economic interdependence remain mutually beneficial for powers such as the United States and China, they will be able to tolerate the irritants that they will inevitably inflict on one another. The modern intelligence-counterintelligence contest plays out in a complicated sociotechnical space where states take advantage of economic cooperation and hedge against security competition. If their broader mutual interest frays, however, then cyberwarfare becomes just one facet of a more serious strategic problem involving more dangerous means. Exaggeration of the cyber threat feeds spirals of mistrust, which make this undesirable outcome slightly more likely.

Impact: War with China would be economic and political disaster for PRC and US

Dr. Ted Galen Carpenter 2004 ( PhD in Diplomatic History; vice president for defense and foreign policy studies at the Cato Institute, is the author of eight books on international issues) 10 Aug 2004, "China's Taiwan Policy and America's Difficult Choices" <http://www.cato.org/pub_display.php?pub_id=2778>

And a war in the Taiwan strait would be a disaster for both the PRC and the United States. The mutually beneficial economic relationship (now valued at more than $150 billion a year) would be severed, and America's relations with a major power would be poisoned for decades.