Aargh: The Case For WTO Retaliation for Chinese Cyber Piracy

By Vance Trefethen

Arrgh: The Case for WTO Retaliation for Chinese Cyber-Piracy 3

OBSERVATION 1. We offer the following DEFINITIONS. 3

Substantial: 3

Reform: 3

Policy: 3

OBSERVATION 2. INHERENCY, or the structure of the Status Quo. We offer 2 key FACTS 4

FACT 1. Criminal indictments. The Justice Dept. is prosecuting members of the Chinese Army for cyber espionage. And China won’t cooperate. 4

FACT 2. Not enough. The Justice Department isn’t enough, we need the WTO. 4

OBSERVATION 3. The HARM. Chinese cyber industrial espionage harms the US and global economies. 4

Subpoint A. Thousands of companies hacked. Thousands of American companies are victims of Chinese economic cyber espionage 4

Subpoint B. Massive job losses. Chinese industrial espionage costs the US 100,000 to 200,000 jobs 4

Subpoint C: Loss of technological innovation. Chinese theft of intellectual property does long-term damage to the US and global economy by destroying business incentives for innovation. 5

OBSERVATION 4. The PLAN, implemented by the Congress, the President and the US Trade Representative 5

OBSERVATION 5. SOLVENCY. WTO sanctions are the solution. We see this in 2 sub-points 5

A. We can win. The US can win the WTO complaint 5

B. The right solution. A WTO complaint will make China stop piracy 6

2A EVIDENCE: WTO RETALIATION FOR CHINESE CYBER PIRACY 7

DEFINITIONS & BACKGROUND 7

Distinguishing between traditional national security espionage and industrial espionage: they’re not the same thing 7

OPENING QUOTES / AFFIRMATIVE PHILOSOPHY 7

We must take action against cyber espionage: Bad behavior has to have consequences 7

INHERENCY 7

A/T “2015 US/China cyber agreement solves” – Just a temporary shift in China’s tactics, not really solving 7

A/T “2015 US/China cyber agreement solves” – China hasn’t actually done anything to implement the agreement 8

No WTO cases have been filed yet on commercial cyber espionage 8

The US has not pursued any WTO action against China for cyber espionage 8

China’s not following WTO rules on intellectual property 8

Justice Department action alone is unlikely to have measurable impact 9

Justice Department prosecutions of Chinese military hackers won’t have much impact 9

The Chinese hackers will never really face trial in the US: China will refuse to hand them over 9

China admits that their government does cyber espionage 9

Chinese Army participates in cyber industrial espionage 10

Chinese government has a fully organized system of cyber industrial espionage 10

A/T “China is improving, let’s give them time” – We can’t afford to wait, we need to act now 10

China can’t solve IP violations internally 11

A/T “UN / International Telecom Union will solve” – It’s being run by the biggest violators: China and Russia 11

Status Quo international efforts won’t solve for Chinese economic cyber espionage 11

Markets won’t solve for cybersecurity 11

Private sector can’t solve – businesses can’t defend themselves against foreign government attacks 12

HARMS / SIGNIFICANCE 12

A/T “US does the same thing, ask Ed Snowden” – NSA was not doing economic espionage 12

Important data was stolen by Chinese government agents from US companies 12

Chinese cyber espionage is the greatest transfer of wealth in history 12

Intellectual Property theft hurts world economic growth, and it’s an urgent issue now 13

Cyber industrial espionage is NOT the same as, and should NOT be accepted as, military/national security spying 13

SOLVENCY / ADVOCACY 14

Criminal indictment isn’t enough, we need the WTO. It would deal a blow to Chinese cyber piracy 14

WTO complaints would be effective at curbing cyber espionage violations 14

WTO is the right forum to address Chinese cyber industrial espionage, and it would be effective at stopping it 14

China would comply with WTO ruling on a US complaint about economic cyber espionage 15

WTO complaint would have an immediate effect on Chinese decision-making 15

Best approach is a WTO complaint before doing sanctions: China has a good record of following WTO dispute system 15

Fidler is wrong: WTO is the right forum to dispute Chinese cyber industrial espionage 16

Fidler is wrong: WTO rules can and should apply to international cyber espionage 16

WTO’s “TRIPS” [Trade-Related Aspects of Intellectual Property Rights] agreement can and should cover cyber piracy 16

DISADVANTAGE RESPONSES 17

A/T “Starting a trade war” – We’re already in a trade war 17

A/T “WTO sanctions will start trade war with China” – Didn’t happen the last time we filed complaints, in ’07. WTO process doesn’t lead to trade wars 17

A/T “US / China War Risk” – Won’t happen; everyone knows it would be too catastrophic 17

A/T “US / China War Risk” – No brink. China is not aggressive and not even close to considering acts of war 18

A/T “Hurts US/China relations” – Non-unique. China has already given up on meaningful relationship with the US 18

Works Cited: Chinese Cyber-Piracy Retaliation 19

Arrgh: The Case for WTO Retaliation for Chinese Cyber-Piracy

The United States has warned China about the dangers of its practice of using computer hacking, or “cyber espionage,” to steal technology from American companies. Wayne Morrison with Congressional Research Service in 2015 said QUOTE:

“Following a meeting with Chinese President Xi Jinping in June 2013, President Obama warned that if cyber security issues are not addressed and if there continues to be direct theft of United States property, then “this was going to 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]](#footnote-1)

END QUOTE. Unfortunately, China’s responses are inadequate, and we must escalate. We need to affirm that: The United States Federal Government should substantially reform its policies toward the People’s Republic of China.

OBSERVATION 1. We offer the following DEFINITIONS.

Substantial:

“large in amount, size, or number” (*Merriam Webster Online Dict. 2016* <http://www.merriam-webster.com/dictionary/substantial)>

Reform:

“to improve (someone or something) by removing or correcting faults, problems, etc.” (*Merriam Webster Online Dict. 2016* [*http://www.merriam-webster.com/dictionary/reform*](http://www.merriam-webster.com/dictionary/reform)*)*

Policy:

“a high-level overall plan embracing the general goals and acceptable procedures especially of a governmental body” (*Merriam Webster Online Dict. 2016* [*http://www.merriam-webster.com/dictionary/policy)*](http://www.merriam-webster.com/dictionary/policy))

**WTO**: The World Trade Organization

OBSERVATION 2. INHERENCY, or the structure of the Status Quo. We offer 2 key FACTS

FACT 1. Criminal indictments. The Justice Dept. is prosecuting members of the Chinese Army for cyber espionage. And China won’t cooperate.

Wayne M. Morrison 2015 (Specialist in Asian Trade and Finance, Congressional Research Service) March 17, 2015 China-U.S. Trade Issues <https://www.google.fr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=37&cad=rja&uact=8&ved=0CEYQFjAGOB4&url=https%3A%2F%2Ffas.org%2Fsgp%2Fcrs%2Frow%2FRL33536.pdf&ei=3wRqVaG5D8rkUfDZgNAG&usg=AFQjCNEn_j9n5J08-uopqlFBfNEcUnGjhQ&sig2=MWYX9j8fJDWPfzJaaMI9UA>

On May 19, 2014, the U.S. Department of Justice issued a 31-count indictment against five members of the Chinese People’s Liberation Army (PLA) for cyber espionage and other offenses that allegedly targeted five U.S. firms and a labor union for commercial advantage, the first time the Federal government has initiated such action against state actors. The named U.S. victims were Westinghouse Electric Co. (Westinghouse); U.S. subsidiaries of SolarWorld AG (SolarWorld); United States Steel Corp. (U.S. Steel); Allegheny Technologies Inc. (ATI); the United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Service Workers International Union (USW); and Alcoa Inc. The indictment appears to indicate a high level of U.S. government concern about the extent of Chinese state-sponsored cyber commercial theft against U.S. firms. It is not clear how the U.S. indictment will impact U.S.-China relations. China strongly condemned the U.S. indictment and announced that it would suspend its participation in the U.S.-China Cyber Working Group, established in 2013.

FACT 2. Not enough. The Justice Department isn’t enough, we need the WTO.

Sen. Chuck Schumer 2014. (D-NY) quoted by journalists James Politi and Shawn Donnan in “US claims victory over China in WTO car dispute” 23 May 2014 <http://www.ft.com/intl/cms/s/0/25c785ee-e222-11e3-915b-00144feabdc0.html> (Brackets in original)

“Cyber attacks from China and other nations could prove crippling to American businesses in the years to come, so we need real teeth in our response,” said Mr Schumer. “[The Department of Justice] did the right thing in filing these indictments, but the only way to really punish China for these outrageous attacks is through the WTO.”

OBSERVATION 3. The HARM. Chinese cyber industrial espionage harms the US and global economies.

Subpoint A. Thousands of companies hacked. Thousands of American companies are victims of Chinese economic cyber espionage

James Lewis 2014. (cyber security expert at the Center for International and Strategic Studies) 19 May 2014 The Obama administration has put China on notice — with indictments for cyber espionage <http://www.pri.org/stories/2014-05-19/obama-administration-has-put-china-notice-indictments-cyber-espionage>

China is the leading source of economic espionage against the US. An internal study from the Department of Defense showed that Chinese economic espionage dwarfed that of all other countries, including Russia. Last year, the FBI notified 3,000 American companies that they'd been hacked. (That works out to more than eight per day.) It's simply amazing. We're talking huge numbers of incidents and significant economic harm to the US.

Subpoint B. Massive job losses. Chinese industrial espionage costs the US 100,000 to 200,000 jobs

James Lewis 2014. (cyber security expert at the Center for International and Strategic Studies) 19 May 2014 The Obama administration has put China on notice — with indictments for cyber espionage <http://www.pri.org/stories/2014-05-19/obama-administration-has-put-china-notice-indictments-cyber-espionage>

I find that a really useful argument, because this kind of commercial espionage probably costs the US between 100,000 and 200,000 jobs. It's not that these people are out on the street, although that does happen. It means they go from a high paying job in manufacturing to a low paying job in some kind of service industry. This hurts our economy. China is not playing by the WTO rules. If China wants to be a major power and be a global economic leader, it has to play by the rules.

Subpoint C: Loss of technological innovation. Chinese theft of intellectual property does long-term damage to the US and global economy by destroying business incentives for innovation.

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” published by the National Bureau of Asian Research <http://www.ipcommission.org/report/ip_commission_report_052213.pdf>

The scale of international theft of American intellectual property (IP) is unprecedented—hundreds of billions of dollars per year, on the order of the size of U.S. exports to Asia. The effects of this theft are twofold. The first is the tremendous loss of revenue and reward for those who made the inventions or who have purchased licenses to provide goods and services based on them, as well as of the jobs associated with those losses. American companies of all sizes are victimized. The second and even more pernicious effect is that illegal theft of intellectual property is undermining both the means and the incentive for entrepreneurs to innovate, which will slow the development of new inventions and industries that can further expand the world economy and continue to raise the prosperity and quality of life for everyone. Unless current trends are reversed, there is a risk of stifling innovation, with adverse consequences for both developed and still developing countries. The American response to date of hectoring governments and prosecuting individuals has been utterly inadequate to deal with the problem. China has been the principal focus of U.S. intellectual property rights (IPR) policy for many years. As its economy developed, China built a sophisticated body of law that includes IPR protection. It has a vibrant, although flawed, patent system. For a variety of historical reasons, however, as well as because of economic and commercial practices and official policies aimed to favor Chinese entities and spur economic growth and technological advancement, China is the world’s largest source of IP theft.

OBSERVATION 4. The PLAN, implemented by the Congress, the President and the US Trade Representative

1. The US trade representative files a formal complaint against China with the WTO over the existing case of 5 PLA officers caught doing industrial cyber espionage  
2. The US trade representative files a new complaint with WTO for every additional Chinese cyber industrial espionage event discovered in the future  
3. Congress votes to impose any retaliatory trade sanctions authorized by WTO  
Funding through existing budgets of existing agencies  
Enforcement through the Justice Department and all existing agencies that enforce existing trade sanctions.  
Plan takes effect 3 days after an Affirmative ballot.  
And all Affirmative speeches may clarify.

OBSERVATION 5. SOLVENCY. WTO sanctions are the solution. We see this in 2 sub-points

A. We can win. The US can win the WTO complaint

[James P. Farwell](http://nationalinterest.org/profile/james-p-farwell) & [Darby Arakelian](http://nationalinterest.org/profile/darby-arakelian) 2014. (*Farwell is an attorney and expert in cyber who has advised the Department of Defense and the U.S. SPECIAL OPERATIONS COMMAND. Arakelian is a former CIA Officer and a national security expert* ) 20 May 2014 THE NATIONAL INTEREST “China Cyber Charges: Take Beijing to the WTO Instead“ <http://nationalinterest.org/blog/the-buzz/china-cyber-charges-take-beijing-the-wto-instead-10496>

Finally the burden of proof in a WTO proceeding is far easier to sustain than a criminal indictment in U.S. District Courts. Some WTO decision indicate that once a prima facie case is made, the burden shifts to the party against whom the claim is made. One might argue whether that is the correct standard rather than preponderance of evidence, but clearly WTO proceedings entail a burden of proof that is far less onerous that proving guilty beyond a reasonable doubt. If the U.S. believes it can prove the latter, it clearly must feel the evidence exists to make the far more difficult case required for a criminal conviction.

B. The right solution. A WTO complaint will make China stop piracy

[James P. Farwell](http://nationalinterest.org/profile/james-p-farwell) & [Darby Arakelian](http://nationalinterest.org/profile/darby-arakelian) 2014. (*Farwell is an attorney and expert in cyber who has advised the Department of Defense and the U.S. SPECIAL OPERATIONS COMMAND. Arakelian is a former CIA Officer and a national security expert* ) 20 May 2014 THE NATIONAL INTEREST “China Cyber Charges: Take Beijing to the WTO Instead“ <http://nationalinterest.org/blog/the-buzz/china-cyber-charges-take-beijing-the-wto-instead-10496>

China may dislike the idea of criminal convictions against PLA members in a U.S. court. That’s nothing compared to being branded a pirate in a forum of internationally sanctioned justice for theft of intellectual property. If we’re going after the Chinese, we need to be hard-nosed and give no quarter. A WTO victory would be substantive and for the Chinese, it would hurt. China won’t refrain from piracy because that’s the right thing to do. It will act only when it perceives the cost of piracy exceeds the benefits. This is the way to achieve that result.

2A EVIDENCE: WTO RETALIATION FOR CHINESE CYBER PIRACY

DEFINITIONS & BACKGROUND

Distinguishing between traditional national security espionage and industrial espionage: they’re not the same thing

**Analysis: “Traditional” espionage consists of things like spying to find out how big your opponent’s army is or where it’s moving. Countries have been doing that since the dawn of time and it’s not unusual. Economic espionage is different and should be condemned – it means the government is getting economic information and giving it to businesses within their country.**

Christina Skinner 2014 (law degree from Yale Law School) “An International Law Response to Economic Cyber Espionage” CONNECTICUT LAW REVIEW May 2014 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2305326>

Part III addresses the anormativity surrounding economic cyber espionage. It argues that economic cyber espionage violates well-established norms of customary international law, such as sovereignty, non-intervention, and state responsibility. It discusses how the existing principle of state sovereignty also provides a derivative right to economic sovereignty, which is directly violated by economic cyber espionage. Moreover, to the extent states sponsor the economic cyber-intervention of non-state actors—i.e., cyberspies—those states can be held accountable under the doctrines of state responsibility or non-intervention. In short, Part III argues that economic cyber espionage is illegal under customary principles of international law, even if traditional espionage is not.

OPENING QUOTES / AFFIRMATIVE PHILOSOPHY

We must take action against cyber espionage: Bad behavior has to have consequences

James Lewis 2013. (cyber security expert at the Center for International and Strategic Studies) Feb 2013 Conflict and Negotiation in Cyberspace <https://csis.org/publication/conflict-and-negotiation-cyberspace>

The key to greater security is to establish consequences for hostile action in cyberspace. The greatest weakness in American cybersecurity policy has been the failure to respond to repeated hostile action by foreign powers. This signals that Americans are either indifferent or inept. The issue is to identify the policies and actions that will reduce the incentives for cyberattack and cyber espionage and to build international support for a more stable and secure cyberspace. Hostile actions in cyberspace must have political and military consequences.

INHERENCY

A/T “2015 US/China cyber agreement solves” – Just a temporary shift in China’s tactics, not really solving

Scott Warren Harold 2016 (Associate Director, Center for Asia Pacific Policy; Political Scientist; Faculty Member, Pardee RAND Graduate School ) August 2016 “The U.S.-China Cyber Agreement: A Good First Step” <http://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html>

None of these explanations suggest that China changed its behavior because it concluded that private sector firms are illegitimate targets. China's assertions about cyberspace norms focus on the right of states to censor access to online information. Moreover, China's economy, the commanding heights of which are controlled by the state, differs dramatically from a market economy, where the private sector and the government are cleanly separated, making the U.S. argument that private sector actors are illegitimate targets an alien one to Chinese leaders. Many observers suspect that China's apparent compliance with the cyber agreement represents little more than a shift in tactics that is probably temporary. Such analysts note that China did not lay down a costly marker, since it did not admit to having previously engaged in cyber espionage. Because it seems unlikely that China has suddenly changed its view of economically motivated cyber espionage wholesale, it is important for U.S. policymakers to keep focused on this issue.

A/T “2015 US/China cyber agreement solves” – China hasn’t actually done anything to implement the agreement

Aisha Chowdhry 2016 (journalist) 16 Mar 2016 “U.S.-China still at odds on cybersecurity issues” <https://fcw.com/articles/2016/03/31/obama-xi-cyber.aspx>

"It doesn’t seem like much has really happened since the agreement in September," Sarah Granger, a fellow at the Truman National Security Project, told FCW. "I haven’t seen any evidence of increased arrests in China for 'cyber-enabled theft of intellectual property' outlined in the agreement, even though the idea was for more cooperation on investigating crimes. The number of incidents reported in recent months looks to be similar to those before the agreement, so we have no real evidence of any changes yet."

No WTO cases have been filed yet on commercial cyber espionage

Prof. Stewart S. Malawer 2014. (Professor of Law and International Trade at George Mason University ) 23 Dec 2014 “Confronting Chinese Economic Cyber Espionage With WTO Litigation” NEW YORK LAW JOURNAL <http://www.newyorklawjournal.com/id=1202712784205/Confronting-Chinese-Economic-Cyber-Espionage-With-WTO-Litigation?slreturn=20150431145551>

It is clear that TRIPS, adopted in 1994 and effective in 1995, does not explicitly address economic cyber espionage for commercial or trade gain. Of course, it doesn't. The agreement preceded the great changes brought about by the revolution in information and communications technologies in the last 20 years or so. But one needs to see how the general and specific provisions of that agreement, as a multilateral agreement that is intended to govern intellectual property rights, apply to newer events in the future. As of today, no WTO cases have addressed this issue.

The US has not pursued any WTO action against China for cyber espionage

Christina Skinner 2014 (law degree from Yale Law School) “An International Law Response to Economic Cyber Espionage” CONNECTICUT LAW REVIEW May 2014 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2305326>

At first blush, the WTO thus appears an obvious forum for asserting complaints about economic cyber espionage. Indeed, some experts already “have argued that the United States should use international trade law’s protections for intellectual property against countries engaged in economic cyber espionage.” However, WTO members have apparently “shown no interest” in pursuing this path, “despite mounting worries about this practice.” And the United States has not yet pursued any claim against China for economic cyber espionage through the WTO.

China’s not following WTO rules on intellectual property

James Lewis 2014. (cyber security expert at the Center for International and Strategic Studies) 19 May 2014 The Obama administration has put China on notice — with indictments for cyber espionage <http://www.pri.org/stories/2014-05-19/obama-administration-has-put-china-notice-indictments-cyber-espionage>

It's a hard problem for China. It links to the People's Liberation Army and military modernization. It links to economic growth. And it links to corruption. That's a really tough basket for any government to deal with. This is only the first step in trying to get the Chinese to realize that they've got a problem here. On the US side, nobody forced China to join the World Trade Organization. And when they joined the WTO, they promised to abide by rules, including protection of intellectual property. They haven't abided by those rules. The US is saying, 'China is a country that we want to see grow, but you need to play by the rules.'

Justice Department action alone is unlikely to have measurable impact

Robert Westervelt 2014 (journalist) 20 May 2014 Chinese Cyberespionage Crackdown Prompts Look At Intellectual Property Theft <http://www.crn.com/news/security/300072881/chinese-cyberespionage-crackdown-prompts-look-at-intellectual-property-theft.htm>

[Intellectual property theft](http://www.crn.com/news/security/240148798/chinese-group-tied-to-massive-ongoing-cyberattacks-in-u-s.htm) was at the heart of a report issued last year by Alexandria, Va.-based Mandiant (acquired by FireEye) on a Chinese group linked to sustained [cyberespionage activity](http://www.crn.com/news/security/240155458/mandiant-report-sending-chinese-cyberattackers-back-to-the-drawing-board.htm). The move by the Justice Department is not likely to have a measurable impact on global espionage, said Jon Heimerl, a senior security strategist at Solutionary, an Omaha, Neb.-based managed service provider and subsidiary of the NTT Group. Private and government-backed espionage will continue regardless of how this particular case progresses, Heimerl said.

Justice Department prosecutions of Chinese military hackers won’t have much impact

Christina Skinner 2014 (law degree from Yale Law School) “An International Law Response to Economic Cyber Espionage” CONNECTICUT LAW REVIEW May 2014 (brackets in original) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2305326>

The covert theft of U.S. intellectual property and industrial secrets is well covered by domestic criminal law. For one, the Economic Espionage Act of 1996 directly criminalizes this behavior. The statute provides that economic espionage occurs when an actor knowingly or intentionally commits an offense that “will benefit any foreign government, foreign instrumentality, or foreign agent,” and “knowingly”: (1) steals or obtains a trade secret by “fraud, artifice, or deception” or by other unauthorized means; (2) “conveys a trade secret” by various methods of copying (without authorization); or (3) “receives, buys, or possesses a trade secret knowing” it was stolen or otherwise taken without authorization. Given the breadth of this statute, it is surely intended to capture economic espionage that is perpetrated in cyberspace and with cybertools. In fact, the United States has recently used this statute to charge five Chinese military hackers for acts of economic cyber espionage, among other crimes, against U.S. companies. In reality, however, a U.S. prosecution for economic cyber espionage likely does not loom large for foreign actors such as these. It has been noted that “[e]spionage is nothing but the violation of someone else’s laws.”

The Chinese hackers will never really face trial in the US: China will refuse to hand them over

Christina Skinner 2014 (law degree from Yale Law School) “An International Law Response to Economic Cyber Espionage” CONNECTICUT LAW REVIEW May 2014 (brackets in original) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2305326>

Yet, as a practical matter, cyberspies can indefinitely evade prosecution if their host state refuses to cooperate. In the case of China, for example, under the terms of the U.S.-Hong Kong Extradition Treaty, China can refuse to extradite a person within its borders if “surrender implicates the ‘defense, foreign affairs or essential public interest or policy’ of the People’s Republic of China.” Thus the efficacy of the United States’ criminal action will depend on China’s cooperation and the “hope[] that Beijing will ‘respect our criminal justice system and let justice take its course.’” But given Chinese officials’ denials of economic cyber espionage activities, it seems unlikely that its government will submit the accused to U.S. courts.

China admits that their government does cyber espionage

Robert Hackett 2015 (journalist) Gasp! China admits to having cyber warriors, FORTUNE 26 Mar 2015 <https://fortune.com/2015/03/26/china-admits-cyber-warriors/>

So China has at last admitted, albeit obliquely, that it sponsors offensive hacker units—martial cyber corps, if you will. It’s an unprecedented confession for the state, whose persistent denials have been met for years with the diplomatic equivalent of, “Yeah, right.” China’s admission, however unsurprising, is a rare ray of light piercing the murky fathoms of international cyber warfare. The news arrived in the most recent edition of The Science of Military Strategy, a much pored-over document produced by China’s Academy of Military Sciences, the top research institute of the country’s military.

Chinese Army participates in cyber industrial espionage

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> (ellipses in original)

While traditional industrial espionage techniques have been used extensively, cyber methods for stealing IP have become especially pernicious. In a March 2012 report to Congress, the People’s Liberation Army (PLA) was identified as a key player, and was noted as often acting in concert with commercial entities. The report suggests that “rather than isolate certain state owned IT firms as exclusively ‘defense’ in orientation, the PLA…alternately collaborates with China’s civilian IT companies and universities.” The report concludes that “computer network operations have assumed a strategic significance for the Chinese leadership that moves beyond solely military applications and is being broadly applied to assist with long term strategies for China’s national development.”

Chinese government has a fully organized system of cyber industrial espionage

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> (brackets in original)

Similarly, Mandiant Corporation’s February 2013 study, entitled “Exposing One of China’s Cyber Espionage Units,” traces Chinese government sponsorship for cyberattacks on IP. All the industries targeted by the PLA unit studied by Mandiant fall into those considered strategic by the PRC, “including four of the seven strategic emerging industries that China identified in its 12th Five-Year Plan.” The PLA unit began operations in 2006, the year that the indigenous innovation policy was approved. The purposes of the cyberattacks were found to be straightforward: to commit espionage and steal data. The unit was judged to access networks over months or even years to “steal broad categories of intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, and emails and contact lists from victim organization’s leadership.” In the words of the report, “the cyber command is fully institutionalized within the CPC [Communist Party of China] and able to draw upon the resources of China’s state-owned enterprises to support its operations.”

A/T “China is improving, let’s give them time” – We can’t afford to wait, we need to act now

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>

The Commission has also reviewed the current actions being taken by the U.S. government and international organizations like the World Trade Organization (WTO) and the recommendations of official and private studies of the problem. Both current and proposed actions generally emphasize more intensive government-to-government communication requesting foreign governments to rein in their companies and other actors. The Commission judges that the scope of the problem requires stronger action, involving swifter and more stringent penalties for IP theft. The Commission believes that over the long term, as their companies mature and have trade secrets to protect, China and other leading infringers will develop adequate legal regimes to protect the intellectual property of international companies as well as domestic companies. The United States cannot afford to wait for that process, however, and needs to take action in the near term to protect its own economic interests.

China can’t solve IP violations internally

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>

In China, for example, the courts are overwhelmed with cases, and judges in the IP courts are spread thinly. Barriers to discovery in China also remain a vexing problem for U.S. parties seeking redress both there and in U.S. courts. Despite improvements in some sectors following China’s 2010 Special IPR Enforcement Campaign, the country remained on the “priority watch list” published by the United States Trade Representative (USTR) in 2012 and 2013. The USTR notes that IP protection and enforcement remain a significant challenge.

A/T “UN / International Telecom Union will solve” – It’s being run by the biggest violators: China and Russia

Richard Clarke 2013 (chairman of Good Harbor Security Risk Management. He was special adviser to the president for cybersecurity in the George W. Bush administration. ) A global cyber-crisis in waiting 7 Feb 2013 WASHINGTON POST <http://www.washingtonpost.com/opinions/a-global-cyber-crisis-in-waiting/2013/02/07/812e024c-6fd6-11e2-ac36-3d8d9dcaa2e2_story.html>

At the [World Conference on International Telecommunications](http://www.itu.int/en/wcit-12/Pages/default.aspx) in Dubai last year, global regulations concerning cyberspace were also discussed, but the two major culprits of malicious cyber-activity were at the table dominating the meeting. The conference largely turned out to be an attempt by China and Russia to establish more control of cyberspace through the United Nations-sponsored [International Telecommunications Union](http://www.itu.int/en/Pages/default.aspx). Yet it is the Chinese and, to a lesser extent, the Russians who are behind much of the pandemic of online espionage and crime that costs Americans and Europeans hundreds of billions of dollars a year.

Status Quo international efforts won’t solve for Chinese economic cyber espionage

Christina Skinner 2014 (law degree from Yale Law School) “An International Law Response to Economic Cyber Espionage” CONNECTICUT LAW REVIEW May 2014 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2305326>

This anormativity and lack of institutional arrangements for enforcing norms on the international level has created a moral hazard and legal vacuum. In this landscape, economic cyber espionage is arguably perceived by some states, like China and others that are similarly motivated, as a rational strategy for advancing an upward economic trajectory.

Markets won’t solve for cybersecurity

James Lewis 2013. (cyber security expert at the Center for International and Strategic Studies) Feb 2013 Conflict and Negotiation in Cyberspace <https://csis.org/publication/conflict-and-negotiation-cyberspace>

The United States cannot be said to have a strategy to deal with cybersecurity, although several documents bearing the title “Strategy” have been issued by various administrations. There are several reasons for this, the most important being that the United States is hampered by a seductive idea that has dominated American politics for the last 30 years—that the role of government should shrink and that the private sector and market are best placed to solve public problems (thus eliminating the need for taxes). This may have been true in the 18th century, but it is not true now in an interconnected, high-technology security environment.

Private sector can’t solve – businesses can’t defend themselves against foreign government attacks

James Lewis 2013. (cyber security expert at the Center for International and Strategic Studies) Feb 2013 Conflict and Negotiation in Cyberspace <https://csis.org/publication/conflict-and-negotiation-cyberspace>

More than a decade of experience illuminates the requirements for strategy. A “homeland defense approach is inadequate because securing a global network is a problem for international security. Voluntary private action, where the disaggregated and uncoordinated actions of companies are pitted against powerful and unscrupulous state actors, is also inadequate. The many successful attacks against companies highlight the difficulties for any private-sector actor to successfully defend against foreign military and intelligence services.

HARMS / SIGNIFICANCE

A/T “US does the same thing, ask Ed Snowden” – NSA was not doing economic espionage

James Lewis 2014. (cyber security expert at the Center for International and Strategic Studies) 19 May 2014 The Obama administration has put China on notice — with indictments for cyber espionage <http://www.pri.org/stories/2014-05-19/obama-administration-has-put-china-notice-indictments-cyber-espionage>

First, if there was evidence that the NSA stole information to help US companies, don't you think it would have been leaked by now? There is no such evidence. Second, the US has always been really open with China. Espionage is a two-way street. We know great powers engage in espionage. What we object to is commercial espionage.

Important data was stolen by Chinese government agents from US companies

Robert Westervelt 2014 (journalist) 20 May 2014 Chinese Cyberespionage Crackdown Prompts Look At Intellectual Property Theft <http://www.crn.com/news/security/300072881/chinese-cyberespionage-crackdown-prompts-look-at-intellectual-property-theft.htm>

“The indictment alleges that these PLA [People’s Liberation Army, the Chinese Army] officers maintained unauthorized access to victim computers to steal information from those entities that would be useful to their competitors in China, including state-owned enterprises," Holder said. "In some cases, they stole trade secrets that would have been particularly beneficial to Chinese companies at the time they were stolen. In others, they stole sensitive, internal communications that would provide a competitor, or adversary in litigation, with insight into the strategy and vulnerabilities of the American entity.” At Westinghouse, the intruders allegedly stole design specifications for pipes, pipe supports and pipe routing designed for nuclear power plant buildings. At aluminum producer Alcoa, one of the hackers allegedly stole thousands of email messages and attachments from the company's systems regarding a partnership between Alcoa and a Chinese state-owned company.

Chinese cyber espionage is the greatest transfer of wealth in history

Christina Skinner 2014 (law degree from Yale Law School) “An International Law Response to Economic Cyber Espionage” CONNECTICUT LAW REVIEW May 2014 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2305326>

Though there are no doubt other actors who have resorted to economic cyber espionage, Chinese actors appear to be at least one significant source of this activity. In the past few years, China has reportedly attacked many sectors of the U.S. economy and agencies critical to our national security, penetrating the online systems of the U.S. Departments of Homeland Security and State, Coca-Cola, Lockheed Martin, Dow Chemical, Adobe, Yahoo!, and Google, to name just a few. According to General Keith B. Alexander, head of the United States Cyber Command and director of the National Security Agency, these cyber “attacks have resulted in the ‘greatest transfer of wealth in history.’”

Intellectual Property theft hurts world economic growth, and it’s an urgent issue now

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>

Because IP theft is not a new phenomenon, it is important to understand why it is an urgent issue now. Compared with prior eras, today’s economic world is far more interconnected and operates at a far higher speed, with product cycles measured in months rather than years. Companies in the developing world that steal intellectual property from those in the developed world become instant international competitors without becoming innovators themselves. Bypassing the difficult work of developing over decades the human talent, the business processes, and the incentive systems to become innovators, these companies simply drive more inventive companies in the developed world out of markets or out of business entirely. If more and more companies compete for the same amount of business using the same technology and processes, growth stagnates. It is only through innovation that world economic growth can be sustained.

Cyber industrial espionage is NOT the same as, and should NOT be accepted as, military/national security spying

Christina Skinner 2014 (law degree from Yale Law School) “An International Law Response to Economic Cyber Espionage” CONNECTICUT LAW REVIEW May 2014 (brackets in original) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2305326>

As one scholar has argued, in this way states “preserve[] the practice [of espionage] as a tool by which to facilitate international cooperation.” On this view, the “rules” of espionage are not prescribed by law, but rather “are situational.” However, it would be a mistake to afford the same legal treatment to economic cyber espionage. For one, unlike traditional espionage, economic cyber espionage takes place on a much larger scale. The volume of information stolen via cyberspace, using cybertools, is much more significant and happens at a quicker pace than traditional human or technical intelligence gathering. Moreover, the penetration of computer systems and databases is far more difficult to detect and stop than traditional human espionage. Finally, with economic espionage, there is no custom of reciprocity or cooperation that states should be concerned about preserving. With traditional espionage, which focuses on state strategy and military capacity, one can assume that state spying ensures the collective security of all nations. A state’s knowledge about its neighbors’ military capabilities allows it to hedge against or prevent a threat. This, in turn, might decrease the likelihood of any successful or surprise attack. In this way, traditional espionage functions as a structural constraint against open conflict and preserves global stability. Yet there is no such corresponding benefit to global security that accrues from economic cyberespionage. In the most likely scenario, the states that perpetrate this economic spying are motivated to do so because they are still developing and lack desirable technology, innovation, or best practices. Therefore, no state would be incentivized to preserve its option to return the favor. The spying state merely harms the victim state’s incentive to innovate, natural comparative advantages, and robustness as a trading partner. For these reasons, it is a mistake not to draw any legal distinction between traditional espionage and economic cyber espionage.

SOLVENCY / ADVOCACY

Criminal indictment isn’t enough, we need the WTO. It would deal a blow to Chinese cyber piracy

[James P. Farwell](http://nationalinterest.org/profile/james-p-farwell) & [Darby Arakelian](http://nationalinterest.org/profile/darby-arakelian) 2014. (*Farwell is an attorney and expert in cyber who has advised the Department of Defense and the U.S. SPECIAL OPERATIONS COMMAND. Arakelian is a former CIA Officer and a national security expert* ) 20 May 2014 THE NATIONAL INTEREST “China Cyber Charges: Take Beijing to the WTO Instead“ <http://nationalinterest.org/blog/the-buzz/china-cyber-charges-take-beijing-the-wto-instead-10496>

The criminal indictment of five People Liberation Army officers for hacking into the computers of six U.S. companies for economic espionage to steal trade secrets and sensitive information sends a message but the bite has no teeth. The better way to hold China accountable is to take them to a World Trade Organization panel, which could issue a ruling that deals Chinese cyber piracy a telling blow. The TRIPS Agreement (Trade Related-Aspects of Intellectual Property Rights) provides specific protection against theft of intellectual property. It would enable the U.S. to accomplish confluent goals more effectively than a criminal prosecution that the U.S. will never be able to enforce.

WTO complaints would be effective at curbing cyber espionage violations

Christina Skinner 2014 (law degree from Yale Law School) “An International Law Response to Economic Cyber Espionage” CONNECTICUT LAW REVIEW May 2014 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2305326>

This Article urges the international community to respond to the normative and institutional gap in the law in order to treat the problem of economic cyber espionage. In so doing, the Article explains how certain norms of public international law can be said to apply to cyber espionage and should be incorporated into the existing treaty-based framework of the World Trade Organization (WTO). The Article also explains why pressing claims in the WTO would be effective against perpetrators of economic cyber espionage. Namely, this approach would both solidify customary norms against economic cyber espionage and leverage a credible source of authority to curb cyber-violations.

WTO is the right forum to address Chinese cyber industrial espionage, and it would be effective at stopping it

Christina Skinner 2014 (law degree from Yale Law School) “An International Law Response to Economic Cyber Espionage” CONNECTICUT LAW REVIEW May 2014 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2305326>

This Part argues that an international economic institution like the WTO is the most appropriate and effective forum for regulating economic cyber espionage, particularly when perpetrated by states motivated by the simultaneous desire for economic expansion and economic integration, such as China. The WTO provides a legal framework already dedicated to fair trade and competition, and it has the power and authority necessary to ensure compliance with its judgments. This Part first considers how the WTO rules of law fit together with the customary principles developed in Part III. It argues that certain WTO rules, when considered through the lens of a contemporary right to economic sovereignty, protect member states against economic cyber espionage. This Part also argues that the right to economic sovereignty— and a state’s corresponding obligation to refrain from economic cyber espionage—can be asserted within the WTO’s existing dispute settlement framework. Finally, this Part details how a trade-based system would be effective in halting and deterring illegal cyber conduct in the case of China.

China would comply with WTO ruling on a US complaint about economic cyber espionage

Christina Skinner 2014 (law degree from Yale Law School) “An International Law Response to Economic Cyber Espionage” CONNECTICUT LAW REVIEW May 2014 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2305326>

By interpreting the WTO treaty rules in the context of the lex generalis of economic sovereignty and non-economic intervention, member states may arguably assert a claim under the WTO’s Dispute Settlement Understanding (“DSU”) against any member state that engages in or sponsors economic cyber espionage. On that basis, Part IV urges the United States to assert a claim in the WTO against member states that violate its economic sovereignty through economic cyber espionage. In the specific case of China, Part IV argues that the WTO—as the anchor of the international economic order and thus a necessary role-player in China’s plan to obtain superpower status—has the ability to ensure Chinese compliance. And given the procedures of the WTO dispute resolution mechanism, China would be likely to engage cooperatively with the process, avoiding unnecessary confrontation between the United States and China or a deterioration in U.S.-Sino relations.

WTO complaint would have an immediate effect on Chinese decision-making

James Lewis 2013. (cyber security expert at the Center for International and Strategic Studies) Feb 2013 Conflict and Negotiation in Cyberspace <https://csis.org/publication/conflict-and-negotiation-cyberspace>

One area of consequence that the United States has never pursued is in the WTO. The explanation for this is that the WTO processes themselves are very legalistic and that the United States for many years has lacked a strategic vision for international trade. Trade lawyers will tell you that in the absence of compelling evidence, there is no way to take cyber espionage and the theft of IP before the WTO. This is far too timid. A state always has the right to exercise “force majeure,” to go to a body and say that it agreed to procedures and concession on the grounds that other parties would similarly honor their commitments, and since they are not, the agreement no longer holds. This is a major step, but even to discuss it would raise the stakes for China and others to continue their camping of espionage and the theft of IP. The United States could probably also find major economic partners that would be willing to join it in this effort. Some would say that this would risk the collapse of the WTO, but a carefully managed discussion of repercussions for economic espionage could mitigate this risk. China and others might threaten to withdraw, but they are unlikely to do so as they benefit the most from the agreement. An astute diplomatic strategy would first pose the issues before taking any formal action. Even a credible hint that the United States is considering this would have an immediate effect on Chinese decisionmaking.

Best approach is a WTO complaint before doing sanctions: China has a good record of following WTO dispute system

Prof. Stewart S. Malawer 2014. (Professor of Law and International Trade at George Mason University ) 23 Dec 2014 “Confronting Chinese Economic Cyber Espionage With WTO Litigation” NEW YORK LAW JOURNAL <http://www.newyorklawjournal.com/id=1202712784205/Confronting-Chinese-Economic-Cyber-Espionage-With-WTO-Litigation?slreturn=20150431145551>

It is interesting to point out that in a recent corporate filing with the U.S. Department of Commerce (International Trade Administration) concerning the import of solar panels from China, a U.S. firm is asking for higher tariffs to counter the Chinese government's hacking and theft of trade secrets from it.  This case could give the Obama administration another statutory means of imposing unilateral restrictions. This would be via the actions of the two agencies (the U.S. Department of Commerce and the U.S. International Trade Commission) charged with administering trade remedy laws.  
Conclusion  
The best approach is for the United States to file an action in the WTO to receive the blessings of the WTO before imposing sanctions. This would garner the most international support for U.S. actions. The fact of the matter is that China has a pretty good record of observing recommendations of the WTO's dispute resolution system. It has found it to be in its national interest.

Fidler is wrong: WTO is the right forum to dispute Chinese cyber industrial espionage

Prof. Stewart S. Malawer 2014. (Professor of Law and International Trade at George Mason University ) 23 Dec 2014 “Confronting Chinese Economic Cyber Espionage With WTO Litigation” NEW YORK LAW JOURNAL <http://www.newyorklawjournal.com/id=1202712784205/Confronting-Chinese-Economic-Cyber-Espionage-With-WTO-Litigation?slreturn=20150431145551>

Two pieces published by David Fidler from Indiana Law School last year argued that the WTO is not an appropriate venue for addressing economic cyber espionage by China. His three arguments can be summed up as making the following points: that intellectual property rights are granted and protected by TRIPS on a territorial basis, burden of proof is difficult to carry in the dispute resolution system, and there is a lack of public international law on economic espionage. My response is that cyber actions by China outside of its territory but with effects and benefits within its territory, as to its own firms, are reasonably included within the language of the National Treatment Principle of TRIPS. The burden of proof in WTO's trade and commercial proceedings is much less stringent than in criminal proceedings against Chinese officials in the United States. The WTO proceedings are not criminal but typical trade disputes. We are not talking about public international law and 'economic' espionage generally but only the more properly termed 'commercial' espionage against specific firms in the context of particular WTO obligations.

Fidler is wrong: WTO rules can and should apply to international cyber espionage

Christina Skinner 2014 (law degree from Yale Law School) “An International Law Response to Economic Cyber Espionage” CONNECTICUT LAW REVIEW May 2014 (brackets and ellipses in original) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2305326>

As David Fidler points out, WTO members would likely agree that to “covertly obtain intellectual property of nationals of other WTO members operating in their territories could violate WTO obligations to protect such property.” But whether members would also consider WTO rules violated where a member state obtained such “information from private sector entities located outside their territories” remains an open question. Member states may thus assume that there is no basis for claiming economic cyber espionage violates the TRIPS Agreement because WTO rules create obligations for WTO members to fulfill within their territories and do not generally impose duties that apply outside those limits.” This assumption may prove too much. If a member state’s actions taken from within its territory infringe on another member state’s intellectual property rights, should not the WTO rules apply? That the harm is done in cyber space seems a poor reason to limit application of the TRIPS Agreement, which was, in any event, negotiated before the rise of cyber threats to trade and intellectual property rights. After all, the general goals of the TRIPS Agreement, found in its preamble, are to “reduce distortions and impediments to international trade . . . [and] promote effective and adequate protection of intellectual property rights.” In short, to remain relevant, the WTO Agreements must consider the possibility of cyber violations.

WTO’s “TRIPS” [Trade-Related Aspects of Intellectual Property Rights] agreement can and should cover cyber piracy

Christina Skinner 2014 (law degree from Yale Law School) “An International Law Response to Economic Cyber Espionage” CONNECTICUT LAW REVIEW May 2014 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2305326>

No TRIPS provision has explicitly (and entirely) contracted out of the fundamental tenants of state sovereignty and state responsibility. Nor is TRIPS inconsistent with these general principles. The economic corollaries of sovereignty and non-intervention—in addition to the well-recognized requirement to comply with one’s treaty obligations in good faith—should therefore give rise to a cognizable claim that economic cyber espionage violates TRIPS. On this view, the WTO agreements would not exclude a claim of economic cyber espionage simply because the conduct “involves governments obtaining information from private-sector companies located outside their territories.” Arguably, it would be contrary to both the letter and spirit of the WTO agreements to fail to recognize such a claim.

DISADVANTAGE RESPONSES

A/T “Starting a trade war” – We’re already in a trade war

*Prof. Peter Navarro 2012 (professor at the Paul Merage School of Business, University of California-Irvine )* China’s Currency Manipulation: A Policy Debate, FOREIGN AFFAIRS Sept/Oct 2012 <http://www.worldaffairsjournal.org/article/china%E2%80%99s-currency-manipulation-policy-debate>

Richard McCormack, the editor and publisher of Manufacturing & Technology News, gets to the heart of the mercantilist matter by observing, “For China to sell something at one tenth the price of what it would cost in the United States to produce, they are cheating monumentally, in a major, massive sort of way.” According to Dan Slane, head of the US-China Economic and Security Review Commission, “We are in a trade war and stealing, lying, and cheating on the part of the Chinese are all part of it.”

A/T “WTO sanctions will start trade war with China” – Didn’t happen the last time we filed complaints, in ’07. WTO process doesn’t lead to trade wars

Daniel J. Ikenson 2007. (director of Cato Institute's Herbert A. Stiefel Center for Trade Policy Studies; former director of international trade planning for an international accounting and business advisory firm; co-founded the Library of International Trade Resources (LITR), a consulting firm providing interactive information access and international trade consulting. M.A. in economics from George Washington University ) Growing Pains: The Evolving U.S.-China Trade Relationship 7 May 2007 <http://www.cato.org/publications/free-trade-bulletin/growing-pains-evolving-us-china-trade-relationship>

Although some suggest that recent U.S. actions will spark a trade war with China, such an outcome is unlikely. For starters, tit-for-tat trade wars between WTO members are unheard of. The WTO was created, in part, so that trade wars would be relegated to history. Under the rules-based system of trade, members can retaliate in response to an action or inaction of another member only when such a course has been authorized by the Dispute Settlement Body, and only in measured proportions.

A/T “US / China War Risk” – Won’t happen; everyone knows it would be too catastrophic

**Zack Beauchamp 2014** (masters degree in International Relations from the London School of Economics) 7 Feb 2014 [Why Everyone Needs To Stop Freaking Out About War With China](http://thinkprogress.org/world/2014/02/07/3222021/china-japan-war/) <http://thinkprogress.org/world/2014/02/07/3222021/china-japan-war/>

But there’s one big factor shaping the balance of power in East Asia that means the talk is likely to remain just that: nuclear weapons. The tagline for World War I in 1914 — “The War To End All Wars” — would have a decidedly different meaning in 2014, as war’s end would be accomplished by the world’s end. So whereas, in 1914, all of the European powers thought they could win the war decisively, East Asia’s great powers recognize the risk of a nuclear exchange between the United States and China to be catastrophic. Carleton University’s Stephen Saideman calls this the end of the “[preemption temptation](http://saideman.blogspot.com/2014/01/pre-empting-preemption.html);” nobody thinks they can win by striking first anymore.

A/T “US / China War Risk” – No brink. China is not aggressive and not even close to considering acts of war

**Zack Beauchamp 2014** (masters degree in International Relations from the London School of Economics) 7 Feb 2014 [Why Everyone Needs To Stop Freaking Out About War With China](http://thinkprogress.org/world/2014/02/07/3222021/china-japan-war/) <http://thinkprogress.org/world/2014/02/07/3222021/china-japan-war/>

First, while it’s easy to see China as an aggressive expansionist power bent on retaking its “rightful place” in East Asia by force, that’s simply inconsistent with China’s track record to date. In [an influential 2003 article](http://belfercenter.hks.harvard.edu/files/johnston_spring_2003.pdf), Iain Alasdair Johnston, a professor of “China in World Affairs” at Harvard, argued that there’s overwhelming evidence China is more-or-less happy with the current international order. Johnston tested various measures of Chinese interest in upending the global order — like its willingness to work inside the U.N. and internal dialogues within PRC strategists about overtaking the United States — and found very little evidence of China seeking to overturn the global structure, including the U.S.–Japan–Korea alliance system that sets the terms in East Asia. “The regime appears to be unwilling,” according to Johnston, “to bear the economic and social costs of mobilizing the economy and militarizing society to balance seriously against American power and influence in the region, let alone globally.”

A/T “Hurts US/China relations” – Non-unique. China has already given up on meaningful relationship with the US

Stephen Harner 2015. (worked in Japan for more than 12 years in the eighties and nineties with the U. S. State Department, Citibank and Merrill Lynch. After many more years in China in banking (Deutsche Bank and Ping An Bank) and consulting, now works in Tokyo for Yangtze Century Ltd. (Hong Kong/Shanghai) ) 18 Feb 2015 FORBES magazine Has China Given Up On The U.S.? Short Answer: Yes <http://www.forbes.com/sites/stephenharner/2015/02/18/has-china-given-up-on-the-u-s-short-answer-yes/>

Of course, it is easy for those of a Panglossian mentality—i.e., most of the mainstream commentariat toward the policies of the Obama administration–to be misled or encouraged to think that all is–or soon will be—right with the world, to view any development in China-U.S. relations in a positive light, as a signal of steadily and inevitably improving relations, if not systematic convergence.” Such has been the general reception of Chinese President [Xi Jinping](http://www.forbes.com/profile/xi-jinping/)’s acceptance of Obama’s invitation to make a “state visit” to [Washington](http://www.forbes.com/washington/), D.C. in September. A more objective and sober assessment would question whether the Obama administration extended the invitation at the state visit level as a needed inducement to a China reluctant to accept it. Why might China be reluctant? It is because, after four years of sincere and painstaking, but fruitless, unreciprocated Chinese efforts to initiate a “new type of great power relations” with the United States—rather, meeting only the seemingly unstoppable bureaucratic momentum of the administration’s bellicose political/military power “pivot (or “rebalance”) to [Asia](http://www.forbes.com/asia/)”–China has largely given up on beginning a meaningful, positive reset of China-U.S. strategic relations. Now, instead, China has embarked on what is being termed by some its own “pivot to Asia”–redirecting its foreign policy and strategic emphasis to its regional neighbors, and to the regions and countries along its New Maritime Silk Road and New Silk Road.

Works Cited: Chinese Cyber-Piracy Retaliation

1. Aisha Chowdhry 2016 (journalist) 16 Mar 2016 “U.S.-China still at odds on cybersecurity issues” <https://fcw.com/articles/2016/03/31/obama-xi-cyber.aspx>
2. Christina Skinner 2014 (law degree from Yale Law School) “An International Law Response to Economic Cyber Espionage” CONNECTICUT LAW REVIEW May 2014 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2305326>
3. Daniel J. Ikenson 2007. (director of Cato Institute's Herbert A. Stiefel Center for Trade Policy Studies; former director of international trade planning for an international accounting and business advisory firm; co-founded the Library of International Trade Resources (LITR), a consulting firm providing interactive information access and international trade consulting. M.A. in economics from George Washington University ) Growing Pains: The Evolving U.S.-China Trade Relationship 7 May 2007 <http://www.cato.org/publications/free-trade-bulletin/growing-pains-evolving-us-china-trade-relationship>
4. James Lewis 2013. (cyber security expert at the Center for International and Strategic Studies) Feb 2013 Conflict and Negotiation in Cyberspace <https://csis.org/publication/conflict-and-negotiation-cyberspace>
5. James P. Farwell & Darby Arakelian 2014. (Farwell is an attorney and expert in cyber who has advised the Department of Defense and the U.S. SPECIAL OPERATIONS COMMAND. Arakelian is a former CIA Officer and a national security expert ) 20 May 2014 THE NATIONAL INTEREST “China Cyber Charges: Take Beijing to the WTO Instead“ <http://nationalinterest.org/blog/the-buzz/china-cyber-charges-take-beijing-the-wto-instead-10496>
6. Prof. Peter Navarro 2012 (professor at the Paul Merage School of Business, University of California-Irvine ) China’s Currency Manipulation: A Policy Debate, FOREIGN AFFAIRS Sept/Oct 2012 <http://www.worldaffairsjournal.org/article/china%E2%80%99s-currency-manipulation-policy-debate>
7. Prof. Stewart S. Malawer 2014. (Professor of Law and International Trade at George Mason University ) 23 Dec 2014 “Confronting Chinese Economic Cyber Espionage With WTO Litigation” NEW YORK LAW JOURNAL <http://www.newyorklawjournal.com/id=1202712784205/Confronting-Chinese-Economic-Cyber-Espionage-With-WTO-Litigation?slreturn=20150431145551>
8. Richard Clarke 2013 (chairman of Good Harbor Security Risk Management. He was special adviser to the president for cybersecurity in the George W. Bush administration. ) A global cyber-crisis in waiting 7 Feb 2013 WASHINGTON POST <http://www.washingtonpost.com/opinions/a-global-cyber-crisis-in-waiting/2013/02/07/812e024c-6fd6-11e2-ac36-3d8d9dcaa2e2_story.html>
9. Robert Hackett 2015 (journalist) Gasp! China admits to having cyber warriors, FORTUNE 26 Mar 2015 <https://fortune.com/2015/03/26/china-admits-cyber-warriors/>
10. Robert Westervelt 2014 (journalist) 20 May 2014 Chinese Cyberespionage Crackdown Prompts Look At Intellectual Property Theft <http://www.crn.com/news/security/300072881/chinese-cyberespionage-crackdown-prompts-look-at-intellectual-property-theft.htm>
11. Scott Warren Harold 2016 (Associate Director, Center for Asia Pacific Policy; Political Scientist; Faculty Member, Pardee RAND Graduate School ) August 2016 “The U.S.-China Cyber Agreement: A Good First Step” <http://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html>
12. Sen. Chuck Schumer 2014. (D-NY) quoted by journalists James Politi and Shawn Donnan in “US claims victory over China in WTO car dispute” 23 May 2014 <http://www.ft.com/intl/cms/s/0/25c785ee-e222-11e3-915b-00144feabdc0.html>
13. Stephen Harner 2015. (worked in Japan for more than 12 years in the eighties and nineties with the U. S. State Department, Citibank and Merrill Lynch. After many more years in China in banking (Deutsche Bank and Ping An Bank) and consulting, now works in Tokyo for Yangtze Century Ltd. (Hong Kong/Shanghai) ) 18 Feb 2015 FORBES magazine Has China Given Up On The U.S.? Short Answer: Yes <http://www.forbes.com/sites/stephenharner/2015/02/18/has-china-given-up-on-the-u-s-short-answer-yes/>
14. 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>
15. Wayne M. Morrison 2015 (Specialist in Asian Trade and Finance, Congressional Research Service) March 17, 2015 China-U.S. Trade Issues <https://www.google.fr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=37&cad=rja&uact=8&ved=0CEYQFjAGOB4&url=https%3A%2F%2Ffas.org%2Fsgp%2Fcrs%2Frow%2FRL33536.pdf&ei=3wRqVaG5D8rkUfDZgNAG&usg=AFQjCNEn_j9n5J08-uopqlFBfNEcUnGjhQ&sig2=MWYX9j8fJDWPfzJaaMI9UA>
16. Zack Beauchamp 2014 (masters degree in International Relations from the London School of Economics) 7 Feb 2014 Why Everyone Needs To Stop Freaking Out About War With China <http://thinkprogress.org/world/2014/02/07/3222021/china-japan-war/>

1. Wayne M. Morrison 2015 (Specialist in Asian Trade and Finance, Congressional Research Service) March 17, 2015 China-U.S. Trade Issues https://www.google.fr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=37&cad=rja&uact=8&ved=0CEYQFjAGOB4&url=https%3A%2F%2Ffas.org%2Fsgp%2Fcrs%2Frow%2FRL33536.pdf&ei=3wRqVaG5D8rkUfDZgNAG&usg=AFQjCNEn\_j9n5J08-uopqlFBfNEcUnGjhQ&sig2=MWYX9j8fJDWPfzJaaMI9UA [↑](#footnote-ref-1)