12-10-2014

China-Based Industrial Espionage

Joel Savary
Chapman University, savar100@mail.chapman.edu

China-Based Industrial Espionage 间谍

Joel Savary
MAIS, Chapman University; Orange, California

Abstract

"On Oct 8, 2014 China has surpassed the United States as the world's largest economy in terms of Purchasing Power Parity (PPP)" (IMF). My paper explores one of the instances of unfair business practices that has contributed to China's new world position. China based espionage undercuts American businesses and U.S. foreign policy directly, causing catastrophic economic implications for America, its businesses, and its allies. The U.S. government is grappling with the means and methods China uses to disseminate information stolen from U.S. businesses to support China based industries. Due to the lack of transparency in China, it has been difficult to gather this information. However, by conducting a regression analysis between the numbers of cyber-attacks on American companies by industry in relation to industry growth in China, this paper is able to find China's main industry targets of espionage. This research shows a positive relationship between the number of cyber-attacks and industry growth. The results in this paper highlight the importance of recognizing industrial espionage as a major issue of national security. In order to address this issue, new financial policies, regulatory amendments, and mandatory self-reporting is needed to better study, respond, and abate the long lasting negative effects of these attacks.

Industrial Espionage Trends

- China targets specific industries more often than others.
- Some of these targets may be viewed as unlikely because they are smaller and has less capital than larger financial firms.
- However, these smaller targets are often subcontracted to larger firms allowing for easer infiltration

Industries	Detail
New Energy	Nuclear, wind and solar power
Energy conservation and environmental protection	Energy reduction targets
Biotechnology	Drugs and medical devices
New materials	Rare earths and high – end semiconductors
New IT	Broadband networks, internet security infrastructure, network convergence
High-end equipment manufacturing	Aerospace and telecom equipment
Clean energy vehicles	

This table lists China's priority areas.

(Table 1, created from information on China's Five- Year plan)

How is the U.S. currently dealing with Industrial Espionage?

These approaches are written as a collaborative effort between U.S. intelligence and defense agencies in the 'Administration Strategy on Mitigating the theft of U.S. Trade Secrets,' and the main points are highlighted below:

- Convey concerns to countries with many incidents
- Press governments on protection and enforcement
- Give private sector warnings and threat assessments
- Increase public awareness of threats and risks

The 'create awareness' approach to these strategies does not press businesses or individuals to curtail or respond effectively to these attacks. These attacks should be responded to with greater urgency than they are now as the implications are immense.

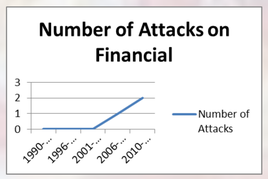
How should the U.S. deal with Industrial Espionage?

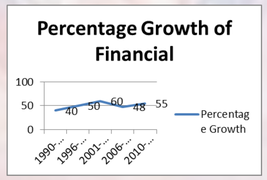
The U.S. should view industrial espionage in the same vein as other terrorist activities.

Mandatory self-reporting of espionage activity to the Securities and Exchange Commission (SEC) on financial filings.

Stronger collaboration of intelligence community (ex. FBI, CIA) with financial agencies (SEC, SBA)

State sponsored business defense in collaboration with businesses to counter the large, state- sponsored espionage programs as seen in China.





Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.886[a]	.784	.687	16.72174

a. Predictors: (Constant), Industry recoded (tech =1), Fifth Period of time (2005 - now), Industry recoded (Ent = 1), Industry recoded (Manufactoring =1), Industry recoded (health =1), First period of time (1992-1995 = 1), Industry recoded (financial =1), Industry recoded (Education = 1), Number of Attack per Industry

Methodologies

I investigate which U.S. companies are being targeted for cyber espionage by international countries, specifically China. To answer these questions, I study a unique, hand-collected dataset of 52 U.S. based companies that have been purported as hacked by an international entity, focusing specifically on hacking originating from China. I gather the number of firms that have been attacked and group them by industry type (Entertainment, Retail, Technology, Education, Manufacturing, Health, Financial). I also gathered 5 periods of 5-Year increments to measure growth from 1990- Present (This measure also correlates with China's 5-Year plan). My research suggest that if Chinese industries finds growth in similar American industries that was a victim of a Chinese based cyber-attack or cyber espionage then it can be implied that the infiltration allowed Chinese based firms to gain an unfair advantage. It is likely that Chinese are using data or information collected from American companies for industry growth.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	20687.833	11	1880.712	6.471	.000[b]
	Residual	5231.127	18	290.618		
	Total	25918.960	29			

a. Dependent Variable: Percentage of Chinese Growth
b. Predictors: (Constant), FourthPeriodDummied, Industry recoded (tech =1), Industry recoded (Ent = 1), Industry recoded (Manufactoring =1), Third Period Dummied, Industry recoded (retail =1), Number of Attack per Industry, Industry recoded (financial =1), SecondPeriod_Dummied, Industry recoded (Education = 1), Fifth Period of time (2005 -now)

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-12.030	9.952		-1.209	.242
	Number of Attack per Industry	-.586	1.270	-.086	-.462	.650
	Industry recoded (Education = 1)	74.772	11.077	.948	6.750	.000
	Industry recoded (Ent = 1)	12.030	19.740	.073	.609	.550
	Fifth Period of time (2005 -now)	24.452	14.297	.333	1.710	.104
	Industry recoded (financial =1)	40.717	10.785	.516	3.775	.001
	Industry recoded (Manufactoring =1)	5.159	11.822	.060	.436	.668
	Industry recoded (retail =1)	19.980	10.782	.253	1.853	.080
	Industry recoded (tech =1)	20.724	11.918	.263	1.739	.099
	SecondPeriod_Dummied	10.191	10.443	.129	.976	.342
	Third Period Dummied	21.814	9.845	.297	2.216	.040
	FourthPeriodDummied	16.036	9.924	.218	1.616	.124

Acknowledgements
I would like to thank the faculty and staff at Chapman University's International Studies program and the Business School for affording me the resources needed to be successful and competitive after graduation. I would like to send the sincerest thanks to my Thesis advisor Lynn R. Horton, Ph.D who has helped focus my degree on my educational and professional interests. I also want to give a great thanks to two professors who has sparked my interest in National Security through their passion and expertise on the subject: Nubar Hovsepian Ph.D and Jean Tomphie Ph.D. I would like to send my sincerest thanks to Andrea Molle, Ph.D, and the Social Science Resaerch Department for the tools and guidance in the statistical analysis. I also want to thank my colleague Steve Zbichorski, while I interned in the federal service he has been a great mentor for me in the field of national security. Finally, I would like to thank my parents that have inspired me to never give up even through adversity.

Conclusions
This paper sheds light on the importance of distinguishing heterogeneity in industrial espionage in order to better discern China's industry targets. More so, it allows for greater understanding of how and why China may be disseminating trade secrets information. Like many previous studies, we find that there is an increase in industrial espionage attacks on American businesses. However, there is no direct correlation between the number of attacks and an increase in China industry growth. Consistent with the argument that China targets certain industries that are of more political and economic importance, this research finds that China's growth is correlated and dependent on both Industry and number of attacks. This research also finds that once there is industrial infiltration of any sort it may take years for that information to be made materially useful to China. Thus, this study's highlights the importance of American policy changes that will allow for further research, defense of all foreign-based industrial espionage.

Future Research

Industrial espionage studies on the heterogeneities of American industries and its impact on China based industries has not been explored before and is in need of more analytical research. This is an exploratory research and uses limited data due to the lack of mandatory reporting of industrial espionage as well as the business stigma behind reporting these attacks to the media. As such, this research features an exploratory database of reported western businesses that have become victim of industrial espionage or other cyber attacks. It is important for additional research to study a more robust catalog of American industries that have fallen victim to espionage so that greater defensive measures catered to industry type and size can be put in place. Further research may include the following:

- Viewing the dates that espionage activities have taken place in relation to mergers and acquisitions.
- Analyze whether the companies targeted is a contractor to a major firm. Size of firm affected.
- Analyze American business competitors that have seen growth.
- Analyze American industry growth in comparison with number of China-based espionage.