"Estimating the Economic Costs of Espionage"

Prepared for CENTRA Technology by the George Bush School of Government and Public Service, Texas A&M University

May 3, 2010

Rich Bell, J. Ethan Bennett, Jillian R. Boles, David M. Goodoien, Jeff W. Irving, Phillip B. Kuhlman, and Amanda K. White

Table of Contents

Executive Summary

Economic espionage is a serious threat to the vitality of the U.S. economy. While this is a widely accepted fact, there is no formal way to measure the damage an incident of economic espionage has on the U.S. economy. The U.S. government would like to know how damaging economic espionage is on the economy. However, the full repercussions of an incident of economic espionage are never known. A stolen trade secret, over the course of many years, could be used in different products and in different industries. The loss of a trade secret is an immeasurable value.

Instead of attempting to measure such an overarching elusive concept, the research team sought to measure the potential consequence of economic espionage. In this study, the research team constructed a model to identify the severity of an incident of economic espionage and its consequences on the U.S. economy. The model was designed for use by federal government employees with the intent that the federal government could apply publically available case information to the model. The model provides a qualitative estimate of "consequence" as it relates to economic loss.

The model generates a severity score between 0 and 1, which corresponds to a 'low', 'moderate', and 'high' consequence. The severity score incorporates the model's four main variables into two primary components: 'Industry' and 'Case Variables'.

'Industry' assesses the significance of where the incident of economic espionage occurred. 'Industry' is derived from a combination of the percentage of GDP in terms of value added for each of the 14 industries and the 'susceptibility' of each of the 14 industries. This process enables the model to be individualized to a specific industry, which allows a different potential consequence to the U.S. economy.

'Case Variables' assess the significance of the incident of economic espionage. 'Case Variables' include the 'Characteristics of the Theft', 'Cost', and 'Beneficiary' variables. The model requires the user to first select the 'Industry' where the incident occurred and then to identify the 'Case Variables'. Therefore, the potential consequence on the U.S. economy from an incident of economic espionage is dependent on the industry.

To greater individualize the model, the research team designed a method whereby questions within the model would matter more when compared to others. As no two incidents of economic espionage are identical, the research team developed a system of weighing the variables and their respective questions. With all the variables measured, standardized, and weighed against each other, the model calculates an overall severity score, which corresponds to the level of consequence for an incident of economic espionage.

Acknowledgements

The Capstone research team was comprised of Rich Bell, J. Ethan Bennett, Jillian R. Boles, David M. Goodoien, Jeff W. Irving, Philip B. Kuhlman, and Amanda K. White. The team would like to express its gratitude and acknowledge the contributions of others who contributed to the success of this project.

The team would like to sincerely express the guidance, leadership, and feedback of Dr. Jeffrey Engel, Associate Professor at the Bush School. Dr. Engel served as the faculty advisor for this Capstone project. His support was integral to the success of this project.

Additionally, the team would like to thank the following Bush School faculty for their assistance in the development of our methodology. Specifically, the team would like to acknowledge Dr. Gina Reinhardt, Assistant Professor; Dr. Kishore Gawande, Professor, and Dr. Joanna Lahey, Assistant Professor, provided guidance on the standardization and statistical modeling used in the development of this project.

The team would also like to thank the International Affairs faculty at the Bush School, the first year International Affairs students at the Bush School, Texas A&M University faculty in the Departments of Economics and Political Science, and outside experts who provided invaluable feedback through their participation in the project's survey.

The team would also like to thank the second year International Affairs students at the Bush School who provided invaluable feedback through their participation in the project's simulation. The team would also like to thank Ms. Janeen Wood, Assistant to the Department Head for International Affairs, and Ms. Rebecca Eaton, Senior Office Associate for International Affairs, who provided administrative and logistical support throughout the duration of the Capstone project.

The team would also like to thank Mr. Mark Kacer, User Services Administrator for the Bush School, for his technological support.

Finally, the Capstone research team would like to express its sincerest gratitude to Centra Technology for providing this project to the Bush School. It was a challenging, but rewarding experience for the research team.

While there are many other individuals not mentioned above, the Capstone research team also thanks them for their support and guidance. To all those that assisted in this project, the Capstone research team sincerely thanks each and every one of you for making this project a success.

Introduction

The objective of this research study is to develop a method to measure the consequence of economic espionage on the U.S. economy. As defined by the 1996 Economic Espionage Act, economic espionage is the misappropriation of trade secrets (including conspiracy to misappropriate) with the knowledge or intent that the theft will benefit a entity, specifically a foreign government, instrumentality, or agent.

In addition to economic espionage, there are other ways in which foreign entities can benefit from U.S. ingenuity, such as industrial espionage and reverse engineering. This study does not measure the consequence of these other means, only the theft or intended theft of trade secrets that benefit or intend to benefit a foreign entity. A trade secret is any form of information in which its value is derived from the information remaining secret.

This study will investigate cases filed under the Economic Espionage Act to determine their consequence on the U.S. economy. The results will measure the consequence of economic espionage on an ordinal scale. For the purposes of this study, consequence is defined as the impact or potential impact an individual incident of economic espionage has or can have on the U.S. economy, in terms of competitiveness and potential impact to GDP. The model calculates consequence and defines it as 'Low,' 'Moderate,' or 'High.'

The study resulted in the development of a user model for the federal government. The purpose of the user model is to measure the level of consequence each incident of economic espionage has on the U.S. economy. The user model generates a value on an ordinal scale with a corresponding level of consequence.

The study hypothesizes that there is a dynamic relationship between the industry, characteristics of the theft, cost, and beneficiary that influences the level of consequence an incident of economic espionage has on the U.S. economy. The study defines the consequence of economic espionage on the U.S. economy as its dependent variable. Furthermore, the study defines the relationship between industry, characteristics of the theft, cost, and beneficiary as the independent variables. It is important to note that many incidents of economic espionage lack perfect information. Therefore, the study incorporates imperfect information into its assessment, and the model was designed to adjust for incidents of imperfect information. Due to the lack of information on the topic of economic espionage, specifically means to measure consequence, this study recommends future research that evaluates the causes and effects of incidents of economic espionage on the U.S. economy.

Literature Review

Overview:
The purpose of this literature review is to provide an overview of the current body of literature on economic espionage and related studies. An examination of existing literature reveals limitations on available information, specifically methods to measure the consequence of economic espionage. Given the available literature, the topic of economic espionage can be divided into two distinct categories. The first section will provide an overview of literature on estimated loss. The second section will examine methodologies that attempt to measure the consequence of economic espionage.

Literature on Estimated Loss
Formal studies measuring the costs of cyber crime share methodological similarities with attempts to measure the consequence of economic espionage. Although reports often cite wide-ranging figures for dollars lost, researchers are hesitant to release their methodologies and sources of data. For example, a 2004 report on the costs of cyber-crime by the Congressional Research Service assessed that the worldwide cost of computer attacks in 2003 ranged from $13 billion to over $226 billion.[1] Likewise, the report noted that shareholder losses in stock prices on the New York Stock Exchange ranged from $50 to $200 billion following the announcement of a cyber-attack.[2]

Many reports, such as the Congressional Research Service's 2004 study on cyber attacks, attempt to quantitatively measure the damage. However, they do not explain the methodology behind the scale. Additionally, while reports, such as the Department of Justice's "Cybercrime against Businesses" and Defense Security Service's "Technical Collection Trends," reference survey respondents from companies and theft reports as their primary source of data, [3,4] but maintain the anonymity of the survey respondents and their affiliated companies. Therefore, it is difficult to apply the available data to subsequent research methodologies because current reports do not establish a relationship between the type of survey response and the type of company.

A separate report by the American Society for Industrial Security (ASIS) estimated U.S. companies lost over $300 billion in 1997 due to espionage targeting proprietary information.[5] Similarly, the White House Office of Science and Technology estimated that economic espionage cost U.S. businesses about $100 billion in 1996.[6] However, no information is provided on how this figure was estimated.

Although these reports represent a relatively small cross-section of the literature, they often lack sufficient information on the process, variables, and data used to estimate cost.

---

[1] U.S. Congressional Research Service. "The Economic Impact of Cyber-Attacks," (RL32331; April 1, 2004) Brian Cashell, et al.
[2] Ibid
[3] Ramona R. Rantala. "Cybercrime Against Businesses 2005." *Bureau of Justice Statistics Special Report, U.S. Department of Justice*. (2008).
[4] Sara Dewitz, Joseph O'Brien, Timothy Deerr, John Parsons, and Erika Souliere. "Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry." *Defense Security Service.* (2008).
[5] F.W. Rustmann Jr. CIA, Inc. Espionage and the Craft of Business Intelligence. Potomac Books Inc., 2002, p. 121.
[6] Luke Bellocchi, "Assessing the Effectiveness of the Economic Espionage Act of 1996." *International Journal of Intelligence and Counterintelligence* 14:3 (July 2001): 366-367.

Methodologies to Measure the Consequence of Economic Espionage:
Few studies measure the cost of economic espionage. Not only are companies' economic losses often undisclosed but even estimations in the literature of total loss "only reflect inventory "snapshots" on the day the audit was performed.[7]

The American Society for Industrial Security (ASIS) report is the most comprehensive report on economic espionage. The data in the report is a compilation of survey responses from private companies that address monetary loss incurred from thefts. The companies were asked to rate the financial impact of thefts. For example, the 1997 report published by ASIS indicated that U.S. companies lost over $300 billion due to espionage targeting proprietary information.[8] The specific methodology of the ASIS report is considered proprietary information, and therefore unavailable. Nonetheless, it stands to reason that the survey results, which concluded a $300 billion loss, are laden with company bias. The report does not focus on an impartial measurement to identify the consequence of economic espionage, but on the common methods of theft and the appropriate risk mitigation strategies. This survey identifies the main threats and determines cost by industry through examining how a company's security policy, propensity to outsource, and type of information assets can all contribute to a company experiencing a higher loss. With this information, ASIS provides a better understanding of "the variety of ways in which information is compromised within the private sector and the effect that these losses have on U.S. corporations."[9] However, ASIS does not reveal the methodology used to establish this relationship and develop the loss estimations.

Likewise, Marc Zwillinger and Christian Genetski, Adjunct Professors of Law at Georgetown University, do not disclose their methodology in their article "Calculating Loss Under the Economic Espionage Act of 1996." However, Zwillinger and Genetski identify variables that could measure cost. This article examines the cost of economic espionage from a civil litigation perspective using a company's damage assessment.[10] Based on past case rulings, Zwillinger and Genetski conclude that courts predominately calculate overall loss by using "lost profits," and not the fair market value of the stolen information.[11] The article explains that another common method of measuring loss is to base the monetary loss on the defendant's financial gain from the theft.[12] This method is commonly applied when the company has not suffered an actual loss or when the loss did not equal the value of the stolen product.[13] The authors also list "reasonable royalty" as a method for determining loss. "Reasonable royalty" calculates damages as an "amount that a willing buyer would have paid a willing seller to license the stolen trade secret."[14] Lastly, courts may use the company's research and development costs to create an appropriate replacement cost.[15] Although this article may examine the consequence of economic espionage

[7] Dave Drab. "Economic Espionage and Trade Secret Theft: Defending Against the Pickpockets of the New Millennium." *The Xerox Corporation*. (2003):4. <http://www.xerox.com/downloads/wpaper/x/xgs_business_insight_economic_espionage.pdf>. (accessed March 13, 2010).
[8] F.W. Rustmann Jr. CIA, Inc. Espionage and the Craft of Business Intelligence. Potomac Books Inc., 2002, p. 121.
[9] ASIS 2007. "Trends in Proprietary Information Loss." *Survey Report, ASIS & National Counterintelligence Executive*, p. 1.
[10] Marc J. Zwillinger and Christian S. Genetski. "Calculating Loss Under the Economic Espionage Act of 1996." *George Mason Law Review* 323, (2001): 1.
[11] Ibid, 4.
[12] Ibid, 5.
[13] Ibid.
[14] Ibid.
[15] Ibid, 7.

from a corporate and legal perspective, its study of past cases and its identification of important variables associated with cost significantly contribute to the literature concerning the consequence of economic espionage.

Although the majority of literature does not provide methodologies, Chris Carr and Larry Gorman of California Polytechnic State University include methodologies in their research. In their study entitled "The re-victimization of companies by the stock market who report trade secret theft under the Economic Espionage Act," Carr and Gorman use statistical event study methodology to determine if "the publicity associated with the reporting of a trade secret theft to the government has a negative impact on the stock price of the victimized firm."[16] Out of the 23 cases that were prosecuted under the EEA by 2001, Carr and Gorman drew their data from 11 companies. Carr and Gorman focused on the percentage change in the stock price and controlled for variables such as "broad stock market moves" and "the effect of all other extraneous firm-specific news."[17] From their statistical test, they conclude that, on average, the public disclosure of a loss from economic espionage is "associated with a negative stock market response that is both statistically and economically significant."[18]

This study not only provides a method for measuring the cost of economic espionage to a company, but its discussion and findings have significant implications for understanding the consequence of economic espionage. By quantifying cost, even within a limited scope, companies and law enforcement agencies have a starting point to report, assess, and protect against loss from economic espionage.[19] However, the results of this study have no bearing on private companies that are not traded on the stock market. For publicly traded companies, the shareholders have the power to influence change within a company. Thus, a loss in shareholder profit from a trade secret theft can potentially lead to significant changes within the infrastructure of the company, and possibly result in more instability. Second, as this study is dependent on the assumption that the theft was reported, companies may be less likely to report future theft, so as to protect jobs within the company. While this study is an important step in quantifying the cost of economic espionage, its implications on the overall consequence are less clear.

Although literature on the topic of economic espionage is available, literature that identifies methods to measure the consequence of economic espionage is limited. Due to these limitations, the research study was unable to modify a previously developed methodology. Rather, the researchers developed a new and unique methodology. Additional research that includes information on how to measure consequence will improve the ability to design methodologies that assess the consequence of an incident of economic espionage on the U.S. economy.

[16] Chris Carr and Larry Gorman. 2001. "The Re-Victimization of Companies by the Stock Market Who Report Trade Secret Theft under the Economic Espionage Act." *The Business Lawyer* 57(1).
[17] Ibid.
[18] Ibid.
[19] Ibid.

Methodology

Overview:
There are inherent limitations with the model that the research team sought to minimize through the methodological process. External validity was difficult to improve because of the small sample of cases with available information and the absence of an independent source to corroborate the model's findings. Therefore, the research team devoted its efforts to improving the internal validity of the model. It was determined that internal validity could be improved by having experts in the field of economic espionage rank the importance of variables and questions designed to help measure these variables. Because the survey population was unresponsive to the survey request, the research team independently ranked the importance of the variables and their associated questions.

The research team developed operational definitions for the variables and the questions within each variable. These definitions were designed to improve the survey participants' understanding, so that the survey participants had sufficient information to rank the variables and their associated questions. These definitions are the same definitions used in the model's user manual. Based on the feedback from the survey participants, the definitions were revised to better clarify each variable and the variable questions.

The survey results provided by the research team were tabulated. The weights for each variable and the variable questions were derived from standardizing the survey results. These standardized scores were then inputted into the model's calculations, so that the model can generate a severity score based on the user's responses.

Operational Definitions of Variables:

Overview:
The research team created a list of potential variables and relevant questions to measure the consequence of economic espionage. During this process, the research team eliminated some variables and questions because of the inability to properly measure these factors.

The research team then narrowed the model's variables and relevant questions. The research team defined four key variables: (1) Industry; (2) Characteristics of the Theft; (3) Cost; and (4) Beneficiary; and questions relevant to each of the four key variables.

Definitions:

(1) Industry:

Industry measures the value added per industry as a percent of Gross Domestic Product (GDP) and Susceptibility to economic espionage. **Industry**, as defined by the U.S. Bureau of Economic Analysis, identifies the following14 key industries: agriculture, mining, utilities, construction, manufacturing, wholesale, retail, transportation, information, finance, professional services, educational services, arts, and other services.

- ***GDP Percent of Value Added*** measures value added per industry as a percentage of GDP. Value added is the difference between a product's sale price and the cost of the materials to produce the product.
- ***Susceptibility*** measures 'Inherent Vulnerability' (how inherently at risk the industry is to economic espionage) and 'Attractiveness' (the likelihood that the industry will be targeted). *Susceptibility = Inherent Vulnerability + Attractiveness*

(2) Characteristics of the Theft:

Characteristics of the Theft measures the impact of the scope of the attack, the network impact, and the characteristics of the thief/thieves on the overall impact of the attack on the company.

- ***Scope of Attack*** examines at the range of the theft in terms of the amount of products and information stolen and the frequency of attacks.
- ***Network Impact*** measures the amount of time a company's server or electronic networks were affected by the incident and any repair costs associated with the incident.
- ***Placement of the thief/thieves*** examines the origin of the theft and the thief's association with the company.

(3) Cost:

Cost measures the monetary loss sustained by a company that was the victim of economic espionage. **Cost** is a conclusive measure of stage of production, time spent in R&D, complete loss, product produced under high security, and restitution paid.

- ***Stage of Production*** measures the three stages under which a product is developed. ***Stage of Production*** can be divided into three key stages: planning, R&D, and production.
- ***Time Spent in R&D*** measures the amount of time a product (or information) stays in the research and development stage with the assumption that there is a positive

correlation between the length of time a product is in the R&D stage and overall production costs.

- ***Complete Loss*** measures the amount of the finished product stolen from the company. ***Complete Loss*** is the total loss the company experiences from an incident of economic espionage with the assumption that if a product or information is in the final stage of production, then it will be a greater loss. A complete loss can be defined as an incident where the total or majority of the product is stolen, irretrievable, and used by the beneficiary.
- ***High Security*** measures the level of security applied by the company during the stages of production to protect the value of the product or information with the assumption that there is a positive correlation between the level of security and the value of the product.
- ***Restitution*** measures the amount of payment the company receives from the thief/thieves or beneficiary. 'Restitution' assesses the total cost incurred by a company by subtracting the restitution payment from the overall loss the company experienced from the incident.

(4) Beneficiary:

Beneficiary measures the ability of the beneficiary to exploit or intend to exploit the stolen product or information. ***Beneficiary*** is a conclusive measure of Human Development Index (HDI), urbanization ratio, and the Global Competitiveness Index (GCI).

- ***HDI*** measures a country's level of development by examining the life expectancy at birth, the knowledge and education (as measured by the adult literacy rate and the combined primary, secondary, and tertiary gross enrollment ratio), and standard of living (as measured by GDP per capita at the purchasing power parity). [20]
- ***Urbanization Ratio*** measures the ratio of a country's urbanized population, or the population living in urban areas, and rural population, or the population living outside of urban areas.
- ***GCI*** level of competitiveness is an aggregation of "the many factors enabling national economies to achieve sustained economic growth and long-term prosperity."[21]

[20] Thapa, Shyam. 1995. "The Human Development Index: A Portrait of the 75 Districts in Nepal." Asia-Pacific Population Journal Volume Number: 10 (2): p3-14. United Nations Website. <http://www.un.org/Depts/escap/pop/journal/v10n2a1.htm>. (Accessed April 1, 2010).

[21] Sala-I-Martin, Xavier, et al. 2009. "The Global Competitiveness Report." World Economic Forum 2009-2010 Report: p3. <http://www.weforum.org/pdf/GCR09/GCR20092010fullreport.pdf>. (Accessed April 1, 2010).

Enhancing Internal Validity:

Overview

During the development of the model, several obstacles inherent with the study of economic espionage were identified. The nature of these obstacles hindered the validity of the model. Among these were the following:

First, a general lack of information about the economic espionage cases coupled with the inability to obtain additional information from individuals involved in the case, either at the federal or company level, inhibited any serious analysis when developing the metric. The dearth of information rendered the researchers unable to achieve a numerical value for "loss of money" or "economic damage to industry." Therefore, at the outset of the project, the researchers operated under the assumption that any metric or measurement applied to the model would be qualitative.

Second, the number of sample sizes (in this instance, case studies) was too few to ascertain quantitative values. In total, twelve case studies were provided to the group. Using the model and its assigned weighing system, the researchers ran the Lockwood, et al. (please see Appendix) case study through the model to produce results. It is important to note that the lack of a sufficient number of case studies rendered an inability to numerically apply the model across an industry as a whole. Therefore, the case study only serves to support the model's qualitative analysis, to demonstrate that an economic espionage case can be run through the model, and to produce a logical result. As a result of these limitations, the researchers had to determine the severity of the loss given the qualitative measures produced by the model.

Third, the length of time that it takes the consumer to receive the case's information further complicated the process of achieving greater validity. This is an extension of the first predicament, lack of information. For example, while a case of economic espionage may receive media attention, this publicity does not equate to the public access of court documents. Rather, in many instances, such as that of the Ye and Zhong case (please see Appendix), court documents remain sealed and unavailable to the public. Additionally, it is highly unlikely that the prosecuting attorney's office will provide any details on the case because of the confidential nature and overall sensitivity of the case and proceedings. Further confounding these issues, are instances where defendants are either going through retrial or assisting the government in additional prosecutions.

Internal Validity

Given the limitations mentioned above, the research team sought internal validity measures to increase the model's strength. Internal validity is the extent to which the model's design is likely to avoid bias. In developing the model, the research team attempted to gain internal validity by pursuing a course of action whereby weights were assigned to the various questions in the model. Due to the limited available information on cases of economic espionage, the inability of government experts in the field to openly discuss cases, and the research team's limited access to economic espionage experts, it was determined that the research team represented the most cohesive sample of individuals with a substantial understanding of past economic espionage cases. A total of 6 members of the research team participated in the internal validation process.

External Experts Survey:

The purpose of the survey was to enhance the internal validity during the process of assigning a weighing scale to the model's key variables. The survey asked respondents to rank the level of importance on a scale of "low, medium, and high" for each variable and subset of variables included in the model.

A ranking process was applied because it allowed the research team to determine the level of importance each variable and subset of variables had on the model. A high level of importance was correlated with a greater weight (severity) than a lower level of importance (not as severe).

The survey population targeted economic espionage experts. The survey population sample identified a group of less than 30 experts from academia, the federal government, and the private sector.

The survey was divided into two sections: industry susceptibility and level of variable importance per industry. The first section "industry susceptibility" was designed to measure the level of susceptibility in each of the industries. Susceptibility was defined as the level of vulnerability and the level of attractiveness present in a given industry. The respondents were asked to rank the level of importance for both inherent vulnerability and attractiveness within each industry. The second section "level of variable importance per industry" identified the other three independent variables: (1) characteristics of the theft; (2) cost; and (3) beneficiary; and their associated variable subsets. For each industry, the respondent was asked to rank the level of importance that each of the three main variables has on that specific industry as well as the level of importance each of the variable subsets has on that specific industry.

The survey resulted in only 12 respondents. Given the variations in the small sample size and direct feedback from the survey sample, it was concluded there was confusion on the terminology "economic espionage." Many academics with a background in intelligence defined "espionage" traditionally and did not see a relationship between espionage and industries. Additionally, some survey respondents noted the length of the survey and the amount of time required to rank the variables and variable subsets.

As a result of the inconclusive responses and comments on confusion and uncertainty from the survey sample, it was determined it would be more accurate for the research team to rank the variables and their associated subsets. Six of the seven members of the research team independently completed the survey. After their results were received, the respondents' answers were averaged together and the weighing scale was created. The survey enabled the researchers to assign a weighing scale to the model's variables while concurrently bolstering internal validity and mitigating bias.

Variable Weights:

Weights

The variables were measured on different numerical scales, which required standardization to weigh the variables. The standardization was conducted using a Z-score for each variable in the model. The Z-score, which shows the number of standard deviations an observation is away from the mean, is calculated by taking each observation in a population of numbers and subtracting each observation from the total population's mean. All of these values are then divided by the population's standard deviation. After calculating the Z-score for each variable, the research team normalized the Z-scores on a scale from 0 to 1. The normal density function produced a cumulative standard normal distribution.

The Process of Applying Weights: An Example

For example, consider the variable 'Industry: Information' and the variable of 'Cost.' The 'Cost' variable consisted of five questions designed to measure 'Cost.' For each observation, the research team calculated the Z-score by using the mean and standard deviation from the five questions within the variable 'Cost.' The user will select a number for the required question (-, 0, 1, 2, 3). In this example, the user selects 'Stage of Production,' and believes the theft occurred during 'finalized product stage.' Thus, the user assigns a rank of '3.' That score is then multiplied by the weight of the calculated standardized Z-score for that individual question. In this example, the weight is '.1424.' That same process is then repeated for every question in the 'Cost' variable. The products of the five numbers, or the answers to the questions referenced under the 'Cost' variable, are summed. The sum of these five numbers is then multiplied by the weight assigned to 'Cost' under the Information industry. In this example, the weight is '.6084.' The same process is repeated for all questions under 'Characteristics of the Theft' variable.

Under the 'Beneficiary' variable, the user is only required to select a country. When the user selects the country, the model performs an internal calculation. The calculation conducted here is similar to the calculation used in the 'Cost' variable. However, the weight for the 'Beneficiary' variable includes a combined weight based on significance of the three variable questions and their predetermined values. The 'Beneficiary' variable' consists of three measurements: Human Development Index (HDI), Urbanization Ratio, and the Global Competitiveness Index (GCI). Because HDI, Urbanization Ratio, and GCI, were all ranked on different scales, they had to be standardized using the Z-score. The weights for the 'Beneficiary' variable's three questions, and the 'Beneficiary' variable itself, were calculated using the same process as 'Cost.'

Model

Overview:

The model is intended to measure the potential consequence on the U.S. economy due to an individual incident of economic espionage. A lofty goal of the research was to develop a metric that would generate a dollar figure representative of the monetary loss from an incident of economic espionage. Initially, a list of variables to measure the impact of cost was developed. However, specific information from the company was needed to incorporate these variables into a model. Because this information is not readily available, it was unfeasible for the research team to develop a metric to generate a dollar figure representative of the monetary loss from an incident of economic espionage. Therefore, the research team chose to create a model that uses ordinal scales to assess consequence. The research team designed an electronic user interface and developed a user manual to accompany the model.

The model consists of four variables that incorporate subjective and objective measurements. The model contains two variables that are self-generated: 'Industry' and 'Beneficiary.' The model operates under the assumption that an EEA indictment was rendered. An EEA indictment requires that a theft or intended theft occurred, which means that the targeted industry and the beneficiary or intended beneficiary is identifiable. Therefore, the user of the model must select which industry and which beneficiary or intended beneficiary is applicable to the incident.

The model includes two variables that are not self-generated, but subjective: 'Cost' and 'Characteristics of the Theft.' Based on his/her judgments and opinions, the user determines severity by identifying key factors important to the variables.

The model provides a value based on the user's ordinal inputs and the generated values from indices. This value represents the level of consequence, in terms of 'Low,' 'Moderate,' and 'High,' that the specific incident of economic espionage had on the U.S. economy.

Assumptions:
An evaluation of different variables was conducted during the initial stages of the model's development. It was determined that the functionality of the model was based on two assumptions. These key assumptions include: an Economic Espionage Act (EEA) indictment and the absence of company cooperation.

Economic Espionage Act (EEA) Indictment
The first assumption is that each case inputted into the model will include at least one EEA indictment issued to the defendant. Issuing an indictment under the EEA is a complex process that requires high coordination and cooperation between the federal government and private companies. The indictment process includes the following steps:[22]

(1) The company is victimized.
(2) The company becomes aware of the incident.
(3) The company conducts an internal investigation.
(4) The company notifies the FBI and/or another federal government office.
(5) FBI determines if the known information is sufficient to pursue an investigation.
(6) FBI contacts the District Attorney's office that has jurisdictional authority where the incident occurred.
(7) FBI launches an investigation to collect evidence.
(8) FBI and the District Attorney's office review the evidence. At this point, they may determine there is insufficient evidence to support an indictment and will drop the case. There are many cases are terminated at this point.
(9) If the FBI and District Attorney's office conclude there is sufficient evidence, the District Attorney's office issues an indictment(s).

It is important that EEA statutes are applicable to each case tested under the model because the EEA represents the official legal guidelines for assessing incidents of economic espionage. An EEA indictment is necessary because it indicates there is sufficient evidence to try a case under the EEA, and it validates the case information inputted into the model.

Incomplete Case Information
The second assumption is that there will be incomplete case information for each case inputted into the model because of a lack of company cooperation. A company will be reluctant to provide full information on an incident of economic espionage because of the negativity associated with the incident. Studies conducted on incidents of security breaches, trade secret theft, and economic espionage indicates that companies tend to provide minimal to no information on an incident. The following two studies are significant examples of this trend:

(1) The 2007 report entitled "Trends in Proprietary Information Loss" produced by ASIS indicated a survey response rate of 10.3%.
(2) The 2009 report entitled "CSI Computer Crime and Security Survey – Executive Summary" produced by CSI indicated a survey response rate of 7.3%.

[22] Matthew A. Parrella, Assistant U.S. Attorney and Chief of Computer Hacking/Intellectual Property (CHIP) Unit Conducted (personal communication via phone interview, March 4, 2010).

This model is intended to be used by a U.S. federal employee with working knowledge of economic espionage. For example, a Department of Homeland Security employee would not be able to access private company information without a subpoena and would not have special access to sealed case information. Therefore, the model was designed with the acknowledgement that there would be incomplete case information. This assumption influenced the identification of the variables and each of their associated questions. The variables and each of their associated questions were included in the model because they would produce a measurable consequence by compensating for the incomplete case information.

Variables:

Overview

The model identified four key variables to measure the consequence of economic espionage. These variables include: (1) Industry; (2) Characteristics of the Theft; (3) Cost; and (4) Beneficiary. Each of these four variables is calculated by a subset of variables.

(1) Industry:

Industry is a conclusive measure of two variables: value added per industry as a percent of Gross Domestic Product (GDP) and Susceptibility to economic espionage. The U.S. Bureau of Economic Analysis identifies 14 key industries in the U.S. economy: agriculture, mining, utilities, construction, manufacturing, wholesale, retail, transportation, information, finance, professional services, educational services, arts, and other services.

Value added is the difference between the sale price of a product and the cost of materials to produce it. Two separate dimensions constitute the second variable, Susceptibility: 'Inherent Vulnerability,' how inherently at risk the industry is to economic espionage and 'Attractiveness,' the likelihood that the industry will be targeted.

Susceptibility = Inherent Vulnerability + Attractiveness

The Inherent Vulnerability of an industry to economic espionage refers to how susceptible it is due to the nature of what is valued within that industry. Inherent Vulnerability can be conceptualized as the difference between tacit, or implicit, knowledge and explicit knowledge. Tacit knowledge is information which is not easily quantified or objectively defined, such as an art form. As a result of its nature, tacit knowledge is difficult to transfer, and thus, is not easily shared, let alone stolen. Explicit knowledge is that which can be expressed mathematically, or verbally as a written set of instructions. Most of the sciences fall into this category. This is a relevant consideration for economic espionage because it is very difficult to transfer tacit knowledge intentionally, let alone for it to be openly shared. For example, information technology or manufacturing process data is explicitly defined and neatly stored, which leaves it more vulnerable to hostile acquisition than an appreciation for supply chain management, which must be uniquely applied to each situation in which it is implemented.

The attractiveness of an industry to economic espionage refers to how likely it is to be targeted due to the industry's general appeal. Attractiveness can be conceptualized by identifying several factors that make the industry appealing, such as the type of products targeted; that which is valued by economic spies; industries that have a competitive advantage; industries that embrace a niche market; and those that claim a high product demand. For example, economic spies desiring a new supply chain management system may find the retail industry very attractive. High product demand industries and those that embrace niche markets can be seen developing highly advanced computer chips or software.

The industry variable is important to the consequence of economic espionage because it incorporates the percent of value added to each industry in terms of GDP and each industry's associated level of susceptibility to an incident of economic espionage. Additionally, the industry variable allows the metric to be personalized for the individual user. Each user identifies the

industry affected by the incident of economic espionage. Because different weights are assigned to the variables, the model will render different results depending upon which industry is selected by the user.

In the model, GDP measures how important the industry is to the U.S. economy as a whole. Susceptibility balances the weight of GDP by measuring each industry's level of attractiveness and defense against economic espionage. The Susceptibility variable permits a particular industry, one whose GDP percentage may not be as great to the entire U.S. economy as other industries, to reflect a greater overall weight (importance), given that it may be a frequent target of economic espionage. The 'Information' industry serves as a relevant example. 'Information' yields a high level of 'Susceptibility,' but only accounts for 4.2% of GDP, well below the ranking of several other industries. Because the level of threat is far greater for 'Information' than other industries, Susceptibility becomes increasing important to the model. Thus, higher Susceptibility rankings add weight to an industry, even if the industry is only a small portion of GDP. Given the GDP and Susceptibility variables, it is expected that the level of importance for insignificant industries, or those with low GDPs and low Susceptibility scores, will pale in comparison to significant industries, or those with high GDPs and high Susceptibility rankings. Additionally, political risk is inherently measured in the Susceptibility variable because particular industries have a greater disposition to public concern (information, manufacturing, etc).

Overview of 14 U.S. Industries:

1. Agriculture:
Farms and Forestry, fishing, hunting, and related activities.
2. Mining:
Oil and gas extraction, Mining (except oil and gas), and Support activities for mining
3. Utilities:
4. Construction:
5. Manufacturing: (divided into two sections: Durable and Nondurable Goods)
A. Durable Goods:
Wood products, Nonmetallic mineral products; Primary metals; Fabricated metal products; Machinery; Computer and electronic products; Electrical equipment; appliances and components; Motor vehicles, bodies and trailers, and parts; Other transportation equipment; Furniture and related products; and Miscellaneous manufacturing
B. Nondurable Goods:
Food and beverage and tobacco products; Textile mills and textile product mills; Apparel and leather and allied products; Paper products; Printing and related support activities; Petroleum and coal products; Chemical products; Plastics and rubber products
6. Wholesale Trade:
7. Retail Trade:
8. Transportation and Warehousing:
Air transportation; Rail transportation; Water transportation; Truck transportation; Transit and ground passenger transportation; Pipeline transportation; Other transportation and support activities; Warehousing and storage
9. Information:
Publishing industries (includes software); Motion picture and sound recording industries; Broadcasting and telecommunications; Information and data processing services
10. Finance, Insurance, Real Estate, Rental, and Leasing:
A. Finance and insurance:
Federal Reserve banks, credit intermediation, and related activities; Securities, commodity contracts, and investments; Insurance carriers and related activities; Funds, trusts, and other financial vehicles
B. Real estate and rental and leasing:
Real estate; Rental and leasing services and lenders of intangible assets
11. Professional and Business Services:
A. Professional, scientific, and technical services:
Legal services; Computer systems design and related services; Miscellaneous professional, scientific, and technical services
B. Management of companies and enterprises.
C. Administrative and waste management services:
Administrative and support services; Waste management and remediation services
12. Educational services, health care, and social assistance:
A. Health care and social assistance, Includes:
Ambulatory health care services; Hospitals and nursing and residential care facilities; Social assistance
13. Arts, entertainment, recreation, accommodation, and food services:
A. Arts, entertainment, and recreation:
Performing arts, spectator sports, museums, and related activities; Amusements, gambling, and recreation industries
B. Accommodation and food services:
Accommodation; Food services and drinking places
14. Other Services: (except government)

(2) Characteristics of the Theft:
'Characteristics of the Theft' is a conclusive measure of the scope of the attack, the network impact, and the placement of the thief/thieves. 'Characteristics of the Theft' identifies key factors that influence the impact of the theft on the company. The scope of the attack can be defined as the range of impact the theft had on the firm in terms of tangible and intangible damages. The network impact can be defined as any theft in which a company's server and/or electronic network system is affected. The placement of the thief/thieves examines if the individual(s) was an internal actor, or employed by the company; an external actor, or a non-employee of the company; or a combination of both internal and external actors.

The scope of attack examines the range of the theft in terms of the amount of products and information stolen and the frequency of attacks. Network impact measures the amount of time a company's server or electronic networks were affected by the incident and any associated repair costs. The placement of the thief/thieves examines the origin of the theft and the thief's association with the company.

An example of an internal theft would be an employee who steals a patent from his company. An example of external theft would be someone who breaks into a company and steals that same patent. Research findings support the conclusion that thieves with 'insider' access cause more damage to the company, which results in a greater company loss.[23]

(3) Cost:
Cost is a conclusive measure of stage of production, time spent in R&D, complete loss, product produced under high security, and restitution paid. The cost variable measures the monetary loss sustained by a company that was the victim of economic espionage. This variable aims to create a comprehensive understanding of the amount lost by assessing the value of the product lost and the company's investment in the production of that product.

The first measure of the Cost variable is 'Stage of Production.' 'Stage of Production' contributes to the measure of cost because a company's investment in developing a trade secret increases with each production stage. Stage of Production evaluates the three stages under which a product is developed. These three stages include: planning, R&D, and production. During the planning stage, the input of factor endowments, namely labor and capital, is limited because the primary purpose of this stage is for a small and controlled group of employees and researchers to formulate ideas and plans. Thus, the likelihood of a product being stolen in the planning stage is extremely low.[24] Additionally, if an incident of economic espionage was detected, the company would have greater flexibility to adjust the development of its product and protect intellectual property during this stage than in subsequent stages of production.

The second measure of the Cost variable is 'Time Spent in R&D'. Time Spent in R&D measures the amount of time a product or information spent in the research and development stage of production. A company invests the greatest amount of capital and labor during the research and

[23] Lisa A. Kramer and Richard J. Heuer Jr. "America's Increased Vulnerability to Insider Espionage." *International Journal of Intelligence and CounterIntelligence* 20, (2007): 50-64.
[24] ASIS 2007. "Trends in Proprietary Information Loss." *Survey Report,* ASIS & National Counterintelligence Executive.

development stage.[25] It is reasonable to assume a positive correlation between the length of time a product is in the R&D stage and the overall production costs. Additionally, knowledge about the total R&D costs is important because there is a precedent in economic espionage cases to use total R&D costs as "an appropriate measure of replacement costs."[26] Thus, information on the length of time associated with the production of a trade secret or trade secret process is important in determining the overall cost of an incident of economic espionage.

The third measure of the Cost variable is 'Complete Loss.' Complete Loss can be defined as the amount of the finished product stolen from the company. Although a product is most vulnerable to economic espionage during the R&D stage,[27] an incident is more likely to occur during the production stage. The production stage is the final stage and includes an evaluation of the total loss incurred by the company. As the product or process develops through the three stages of production, the overall production cost increases. Therefore, the loss of the product or process during the final phase of the production stage is the most expensive. By this point, the company has completed the most costly production stage, which makes the exploitation of the product or process more valuable to the thief because it reduces the overall cost for the beneficiary. An incident of economic espionage during the final phase of the production stage enables the thief/thieves to enter the market as a competitor, which denies the company its expected competitive advantage. Furthermore, detection of an incident of economic espionage during the production stage is limited. However, if a product is stolen during the production stage, it is not necessarily a complete loss as the amount stolen can vary. When a product is stolen, "whatever can be rescued is a net gain and…a disaster control approach is critical."[28] A minor loss can be defined as an incident in which the product or information stolen is insufficient to allow a beneficiary to reproduce the product, or the trade secret never reached its intended beneficiary. . An example of this type of loss is seen in the Ye-Zhong case when the suspects were arrested prior to the information being transported to the beneficiary, in this case China (please see Appendix). A complete loss can be defined as an incident of economic espionage where the total or majority of the product or information is stolen, irretrievable, and used by the beneficiary.

'High Security' is the fourth measure of the Cost variable. High Security is defined by enhanced security measures implemented by the company during the stages of production to protect the value of the product or information. A successful theft under high security in the R&D stage should be considered as a greater loss than a theft under low security. Although companies can incur additional costs by providing increased security during R&D,[29] the existence of increased security minimizes the likelihood of an incident of economic espionage. It is also reasonable to assume that a product under high security has an inherently higher value because the company is willing to increase production costs to better protect the security of the product.

[25] ASIS 2007. "Trends in Proprietary Information Loss." *Survey Report,* ASIS & National Counterintelligence Executive.
[26] Marc J. Zwillinger and Christian S. Genetski. "Calculating Loss Under the Economic Espionage Act of 1996." *George Mason Law Review*, 323, (2001): 7.
[27] ASIS 2007. "Trends in Proprietary Information Loss." *Survey Report,* ASIS & National Counterintelligence Executive.
[28] Samli A Coskun and Laurence Jacobs. "Counteracting Global Industrial Espionage: A Damage Control Strategy." *Business and Society Review*, 108, (2001):1.
[29] ASIS 2007. "Trends in Proprietary Information Loss." *Survey Report,* ASIS & National Counterintelligence Executive.

The fifth measure of the Cost variable is 'Restitution.' Restitution can be defined as any amount of payment the company receives from the thief/thieves or beneficiary. Restitution assesses the total cost incurred by a company by subtracting the restitution payment from the overall loss the company experienced from the incident. The company can file a civil litigation suit against an individual/individuals if the economic espionage case identifies the thief/thieves responsible for the incident. While the restitution payment will not recover the full damages experienced by the company, it can minimize the overall monetary loss experienced by the company.

(4) Beneficiary:
Beneficiary is a conclusive measure of the Human Development Index (HDI), Urbanization Ratio, and the Global Competitiveness Index (GCI). This category measures the ability of the beneficiary to exploit the stolen product or information. Beneficiary can be defined as the foreign entity that is intended to benefit or did benefit from an incident of economic espionage.

The HDI measures a country's level of development by examining the life expectancy at birth, the knowledge and education (as measured by the adult literacy rate and the combined primary, secondary, and tertiary gross enrollment ratio), and standard of living (as measured by GDP per capita at the purchasing power parity). [30] The Urbanization Ratio measures the ratio of a country's urbanized population, or the population living in urban areas. The GCI level of competitiveness is an aggregation of "the many factors enabling national economies to achieve sustained economic growth and long-term prosperity."[31]

The 'Beneficiary' variable is important to the model because it identifies the receptive party of the theft. Beneficiary includes any foreign entity who receives the product. For example, if a product or information was stolen and delivered to China, then the beneficiary would be China. Beneficiary also includes any foreign entity who is the intended recipient of the product or information. For example, if a product or information was stolen and there was an attempted delivery to China, but there was never proof the product and information ever reached China, then the beneficiary would be China. In many cases prosecuted under EEA, the perpetrators are apprehended prior to the product or information reaching the intended beneficiary. Therefore, intended beneficiary is essential because a receptive foreign entity must be identified for a case to be brought under the EEA.

Additionally, it is important to note that the intended beneficiary is important to the model because of the many unknowns in the model, which may impact the final severity score. Although the research team attempted to compensate for many of these unknowns, the research team found it difficult to balance them given the subjective nature of the model. For example, consider an incident of economic espionage in manufacturing design. Rather than successfully deliver the design to their intended beneficiary, the perpetrators were arrested before the product could be delivered to the beneficiary. While the model can be applied to the incident, it cannot gauge some of the unknown consequences: Did anyone else see the design prior to the arrest? Were copies of the design made? All of these are examples of potential "idea diffusion." Thus,

[30] Shyam Thapa. "The Human Development Index: A Portrait of the 75 Districts in Nepal." *Asia-Pacific Population Journal* 10, 2 (1995): 3-14. United Nations Website. <http://www.un.org/Depts/escap/pop/journal/v10n2a1.htm>. (Accessed April 1, 2010).

[31] Xavier Sala-I-Martin, et al. "The Global Competitiveness Report." *World Economic Forum 2009-2010 Report* (2009): 3.<http://www.weforum.org/pdf/GCR09/GCR20092010fullreport.pdf>. (Accessed April 1, 2010).

the concept of “idea diffusion” weighs heavily on the negative implications associated with intended beneficiary. As a result, many cases receive a higher severity score due to the industry impacted and its various unknown consequences. Thus, ‘Beneficiary’ or ‘Intended Beneficiary’ is important to the final severity score.

The Severity Score:
The severity score measures the overall consequence of an incident of economic espionage on the U.S. economy in terms of 'Low,' 'Moderate,' and 'High' severity. The severity score incorporates the model's four main variables into two primary components: 'Industry' and 'Case Variables.' Industry is derived from an equal combination of the percentage of GDP (value added) and 'Susceptibility' of each of the 14 industries. Case Variables include the 'Characteristics of the Theft,' 'Cost,' and 'Beneficiary' variables. The relationship of the values between Industry and Case Variables requires additional justification because of its subjective nature.

Initially, the research team assigned a greater weight to 'Industry' than 'Case Variables.' However, this arbitrary weight was dismissed because the standardization process inherently weighed the variables within 'Industry' greater than the 'Case Variables'. The research team believes this inherent bias toward 'Industry' is acceptable because the industry in which a theft occurs sets a range for how detrimental an individual incident of economic espionage is on the U.S. economy.

The overall severity score corresponds to either a 'Low,' 'Moderate,' or 'High' consequence.

- **Low [less than .3742]:** The impact of the case on the U.S. economy is low. A case that has a low severity score does not have the potential to render severe loss to the U.S. economy.
- **Moderate [greater than or equal to .3742 or less than or equal to .6004]:** The impact of the case on the U.S. economy is moderate. A case that has a moderate severity score has the potential to render significant loss to the U.S. economy.
- **High [greater than .6004]:** The impact of the case on the U.S. economy is high. A case that has a high severity score has the potential to render severe loss to the U.S. economy.

The ranges for 'Low,' 'Moderate,' and 'High' consequence were derived by generating a random selection of model inputs and plotting their corresponding severity scores on a distribution. The researchers conducted 150 random combinations, which were inputted into the model to calculate 150 severity scores. One hundred and fifty severity scores were placed on a distribution from 0 to 1. This distribution reflected the range and density of the model. The severity score distribution has a mean of .4873 and a standard deviation of .1131. By adding the standard deviation of .1131to the mean of .4873 and then subtracting the standard deviation of .1131 from the mean of .4873, the numerical bounds for Moderate consequence are derived. Low consequence is defined as any severity score below .3742. Moderate consequence is defined as any severity score greater than or equal to .3742 and less than or equal to .6004. High consequence is defined as any severity score above .6004. On a normal distribution, 68.2% of the results fall within one standard deviation from the mean. Because the model was constructed under the assumption that the results would adhere to a normal distribution, the vast majority of the results will fall within the Moderate severity score, or within one standard deviation from the mean. Therefore, the significance of this model is its ability to correctly identify extreme incidents of economic espionage.

Overview of the User Interface Model:
The user interface model is designed to be simple and intuitive, with drop-down boxes allowing the user to select his/her responses to each question. Included in the interface are 14 industries, each of which is divided by separate tabs at the bottom of the spreadsheet.

Below is an example of the user interface model. In this particular example, the user chose the "Mining" industry. Based on this choice, a predetermined value from the "Industry" variable was assigned. Given the research team's desire to minimize any user confusion or uncertainty, this value does not appear in the interface. Rather, the value assigned to "Mining" is automatically included in the final calculation of the severity score.

After selecting the industry, the user then answered the questions for the variables 'Characteristic of the Theft' and 'Cost.' Answers to the questions for these variables are dependent on the components of the specific incident of economic espionage. For the variable 'Beneficiary,' the user selected 'Venezuela.' All of these answers produced a severity score of '.3529,' which correlates with a 'Low' consequence on the U.S. economy.

Mining Industry Definition:	Oil and gas extraction, mining (except oil and gas), and support activities for mining.				
Number	Variables	Questions		Instructions	User Inputs
1	Mining Industry:				
2	Characteristics of the Theft Variable:				
		Placement of the thief?		Reference user manual for Definitions.	Internal
		Scope of the theft?		Reference user manual for Definitions.	2
		Information network impact?		Reference user manual for Definitions.	0
3	Cost Variable:				
		Stage of production.		Reference user manual for Definitions.	2
		Complete loss?		Reference user manual for Definitions.	1
		Time spent in research and development?		Reference user manual for Definitions.	2
		Restitution paid?		Reference user manual for Definitions.	0
		Product under high security?		Reference user manual for Definitions.	3
4	Beneficiary Variable:				
		Beneficiary country?		Select Country	Venezuela
				Severity Score	0.3529807

Lockwood, et al. Test Case Simulation:

In an effort to prove the efficacy of the model, the research team conducted a test simulation. The research team selected the Lockwood, et al. case as the sample case due to its plethora of information. The research team randomly selected a sample of graduate students to participate in the simulation.

Selection of the Sample Group

The sample group was randomly selected via a computer randomizing program. The sample group consisted of 12 graduate students selected from a population of second year graduate students enrolled in the International Affairs program at the Bush School. The research team selected the sample from this population because it was representative of individuals with a working knowledge of intelligence and economics, who possess a rudimentary understanding of economic espionage. Additionally, the user interface was designed with the intent of use by government employees. Therefore, the research team concluded the academic background of the selected sample was representative of future users.

Simulation

The simulation group was given a one-page summary of the Lockwood, et al. case. The user manual provided information on how to use the model and explanations of the model's variables. The simulation was conducted one time over a thirty-minute period.

Results

The simulation proved that the model succeeded in its intended purpose: the user could take a selected case of economic espionage and use the model to render an appropriate consequence. There were several trends in the simulation group's responses, as all simulation participants were able to objectively answer questions related to the variables. [32]

Lessons learned

The simulation group provided important feedback about the terms and operational definitions associated with the model's variables. The research team adjusted these terms and definitions to better clarify the model and its intended purpose.

[32] At the time of the simulation, this variable was titled "End User."

Conclusion

The research presented in this paper will contribute to the future analysis of economic espionage. Unlike previous research, this study goes beyond highlighting targeted industries and focuses on the variables that have the greatest impact on the consequence of economic espionage. In addition to expounding on previous research, this study provides a user interface to measure the consequence of economic espionage. The model is designed to serve as a template for federal government agencies. The federal government can apply publically available information about specific incidents of economic espionage to the model, which will then generate a customized consequence. However, it is the opinion of the research team that obtaining more detailed data and employing different measures for each variable would further enhance this model.

Detailed data can be achieved by obtaining information from companies that experienced an incident of economic espionage. Industry specific information would aid the model's developers in more accurately assigning weights to each variable and its measures. Therefore, detailed data would allow the user to narrow the range of severity and the level of consequence experienced from an incident of economic espionage. Additionally, detailed data would improve overall statistical analysis allowing the user to include more complicated measures, such as the change in stock market prices or political consequence.

The concept of internal validity is a gap in the model. Although the research team attempted to achieve internal validity by having external experts provide feedback on the significance of each of the variables and their questions, poor response rates inhibited internal validity. Therefore, the research team acted in the stead of experts in weighing the variables.

To improve internal validity, the research team recommends that experts in the field of economic espionage provide feedback on the level of significance for the four variables and their associated questions. Although the research team provided feedback on the significance levels, the research team concluded that the process enhanced the assignment of weights because of the team's greater understanding of the topic of economic espionage. Thus, it is the strong opinion of the research team that the weights used in this model will remain similar to any weights based on feedback from economic espionage experts.

In moving forward, the current model serves as a template that companies and the government can use to identify the level of consequence on the U.S. economy based on a specific incident of economic espionage. The model's variables, weights, and internal calculations provide a method of identifying the consequence an incident of economic espionage has on the overall U.S. economy. It is the hope of the research team that the methodology developed in this study will contribute greatly to the ongoing analysis of the impact of economic espionage.

Appendix

Common EEA Terminology

Consequence/Impact:
Consequence is the overall damage caused by an event. Along with probability, consequence is an input used to calculate risk.

Economic Espionage Act of 1996:
The act criminalizes economic espionage and industrial espionage. Section 1831 criminalizes the disclosure of a trade secret to a foreign entity. Section 1832 criminalizes the transfer of trade secrets for interstate commerce.

Economic Espionage:
Economic Espionage is the knowing misappropriation of trade secrets with the knowledge or intent that the offense will benefit a foreign government, foreign instrumentality, or foreign agent. Misappropriation includes, but is not limited to, stealing, copying, altering, destroying, transmitting, sending, receiving, buying, possessing, or conspiring to obtain trade secrets without authorization. Section 101(a) of the Economic Espionage Act (EEA) of 1996 criminalizes economic espionage.[33]

Industrial Espionage:
Industrial espionage is the knowing misappropriation of trade secrets related to or included in a product that is produced and/or placed in interstate or foreign commerce for the economic benefit of anyone other than the owner, with the knowledge or intent that the offense will injure the owner of that trade secret. Misappropriation includes, but is not limited to stealing, copying, altering, destroying, transmitting, sending, receiving, buying, possessing, or conspiring to misappropriate trade secrets without authorization. Industrial espionage is also criminalized under the EEA.[34]

Probability:
Probability is the likelihood that an event will occur over time. In this situation, probability, along with consequence, is used to determine risk.

Reverse Engineering:
Reverse engineering is the exploitation of profitable information for the benefit of another company. The information does not have to be acquired clandestinely.

Risk:
Risk is an expression of the impact of an undesired event in terms of the event's severity and likelihood.[35]

[33] Office of the National Counterintelligence Executive. "Annual Report to Congress on the Foreign Economic Collection and Industrial Espionage," FY 2008, July 23, 2009, pg. V.
[34] Ibid.
[35] Department of Transportation, Federal Aviation Association, 8040.4, Appendix 1, June 26, 1998, p. 1. <http://www.faa.gov/library/manuals/aviation/risk_management/ss_handbook/media/app_g_1200.PDF>. (accessed May 1, 2010).

Trade Secret:
The term 'trade secret' means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if the owner thereof has taken reasonable measures to keep such information secret; and the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by the public.[36]

[36] Economic Espionage Act of 1996, 18 U.S.C. 1839 (3).

Economic Espionage Cases

Overview:
An important component of the project was obtaining a thorough understanding of the significant cases tried under the Economic Espionage Act of 1996 (EEA).[37] Since 1996, eight significant cases have been tried under the EEA. These eight cases include:

- Dongfan "Greg" Chung
- Lan Lee and Yuefei Ge
- Anne Lockwood, Fuping Liu, and Michael Haehnel
- Hong Meng
- Xiaodong Sheldon Meng
- Younggang "Gary" Min
- Takashi Okamoto and Hiroaki Serizawa
- Fei Ye and Ming Zhong

Based on low response rates to surveys conducted on trade secret and proprietary information loss,[38] it was concluded that researching the key cases and then interviewing individuals associated with these cases would be the most effective way to obtain additional information. During a two-month period, case-related research was conducted and attempts were made to interview individuals associated with the cases. However, it was discovered that many court documents remain sealed and government and private sector individuals associated with the cases cannot participate in interviews.

In regards to the companies, either the company representatives could not comment or the company would not accept the phone or written request for an interview. In regards to the District Attorney's office, some attorneys were able to discuss the generalities of economic espionage, but only after receiving permission from the Department of Justice. In regards to the Department of Justice and the Federal Bureau of Investigation, protocol prevented representatives from discussing the cases. In regards to the defendants' attorneys, some were willing to discuss economic espionage and general details of the case.

While interviews with individuals associated with these cases proved futile, the available open-source material provides useful insight to the cases brought forth under the EEA. Additional information on these eight cases is available in the executive summaries listed below.

[37] The Economic Espionage Act of 1996 (EEA) criminalized the theft or misappropriation of trade secrets. Section 1831 addresses the misappropriation of trade secrets, including the conspiracy to misappropriate trade secrets, with the intent to benefit a foreign entity. Section 1832 addresses the misappropriation of trade secrets for a product shipped through interstate commerce and with the knowledge or intent to cause injury to the owner of the trade secret.

[38] The 2006 "Trends in Proprietary Information Loss" report produced by ASIS indicated a survey response rate of 10.3%. The 2009 "CSI Computer Crime and Security Survey – Executive Summary" report produced by CSI indicated a survey response rate of 7.3%.
ASIS 2007. "Trends in Proprietary Information Loss." *Survey Report*, ASIS & National Counterintelligence Executive, p. 6, Sarah Peters. "Executive Summary" in *14th Annual CSI Computer Crime and Security Survey*. Computer Security Institute. December 2009, p. 3.

EXECUTIVE SUMMARY: DONGFAN "GREG" CHUNG CASE

Overview:
FBI investigators discovered on March 29, 2007 that Dongfan "Greg" Chung (CHUNG) had accessed and stolen aerospace technology from The Boeing Company. CHUNG's name was found in documents linked to economic espionage at Boeing during a 2005 investigation of Chi Mak, an engineer at Power Paragon in Anaheim, CA.[39]

In 1973, CHUNG began working for Boeing (formerly Rockwell International). In 2002, he retired from Boeing and became a contractor for the company. During his tenure with Boeing, CHUNG held a 'secret' level security clearance.[40]

Beginning in 1979, CHUNG received assignments from Chinese aviation industry representatives. In a letter dated May 2, 1987 from Gu Weihao, an official in the People's Republic of China's (PRC) Ministry of Aviation and the China Aviation Industry Corporation, CHUNG was instructed to visit China with his wife, who was an artist invited by the PRC to visit Chinese art institutions; to use Chi Mak as an intermediary to expedite and secure communications between CHUNG and the PRC; and to provide the PRC with data on Boeing's 150-seat airplanes and shuttle orbiter. In a follow-up letter dated April 12, 1988, CHUNG was instructed to provide the PRC with information on 'advanced technologies' and to target the U.S. aerospace industry.

In response to these requests, CHUNG provided the PRC with information on the following technologies: The Delta IV Rocket (including three space shuttle flight stress analysis manuals from 1979); C-17 transport plane; B-1 bomber (24 manuals); and allegedly U.S. helicopters. [41]

Shortly thereafter, CHUNG began collecting manuals on aircraft fatigue: the F-100, the X-15, and the B-70. In 1985, CHUNG, with ample knowledge of U.S. aerospace technology, traveled to China where he lectured on aircraft and space technology at government institutions, universities, and local aircraft manufacturing companies.

During a 2006 search of his residence, authorities discovered 250,000-300,000 pages of information. Included in the discovery were data on the shuttle's phased-array system (communications technology), the Delta IV rocket and the C-17. The Delta IV technology is estimated to be valued between 17[42] and 50[43] million U.S. dollars (in terms of Boeing's R&D expenditures).

---

[39] Serrano, Richard A. and Reza, H.G. "O.C. Man Accused of Being a Spy." *Los Angeles Times*. February 12, 2008. <http://articles.latimes.com/2008/feb/12/nation/na-espionage12/3>. (accessed May 1, 2010).

[40] U.S. Department of Justice Press Release. "Former Boeing Engineer Charged with Economic Espionage in Theft of Space Shuttle Secrets for China." *U.S. Department of Justice*, February 11, 2008. <http://www.usdoj.gov/criminal/cybercrime/chungCharge.htm>. (accessed April 27, 2010).

[41] Flaccus, Gillian. "Engineer Pleads Not Guilty to Spy Charge." *Oakland Tribune*. February 20, 2008. <http://sfgate.com/cgi-bin/article.cgi?f=/n/a/2008/02/11/state/n183827S86.DTL>. (accessed February 11, 2008).

[42] ---- 2009. First economic espionage trial set in California for Chinese-born engineer Dongfan Chung N. pag. LA Times. (accessed May 31, 2009).

[43] ---- 2009. First US economic espionage trial winds down N. pag. AP Online. <http://www.google.com/hostednews/ap/article/ALeqM5ioiyrNfUPsz4aaQl8lT1URmYuouQD991C7G82>. (accessed June 24, 2009).

On July 16, 2009, CHUNG was convicted of economic espionage against Boeing and of acting as an agent of the PRC. On February 8, 2010, CHUNG was sentenced to over 15 years, or the equivalent of 188 months, in prison.[44]

Timeline:

- 1973: CHUNG began working for Rockwell International.
- 1979: CHUNG is tasked by Chinese aviation officials to target civilian aviation, military aviation, and shuttle data.
- 1979: CHUNG sent three manuals related to Shuttle flight stress analysis via sea freight (it is unknown if these manuals were received).
- 1985-2003: CHUNG traveled to China with the knowledge of Rockwell/Boeing and lectured at universities and aircraft manufacturers on flight stress.
- May 2, 1987: CHUNG is instructed to use Chi Mak as an intermediary
- April 12, 1988: Chinese handlers explicitly request "advanced technologies."
- 1996: Boeing acquires Rockwell. CHUNG's office moves from Downy, CA, to Huntington Beach, CA.
- 2002: CHUNG retired from Boeing, but continues to work as a contractor for the company.
- 2006: CHUNG terminated contract work for Boeing.
- March 29, 2007: FBI arrested CHUNG, who is implicated during the Chi Mak investigation.
- July 16, 2009: CHUNG is convicted of economic espionage on July 16, 2009 and of acting as an agent of China.
- February 8, 2010: CHUNG is sentenced to 188 months in prison.

Company Overview:

<u>The Boeing Company</u>

- Boeing is divided into two sections: Boeing Commercial Airplanes and Boeing Defense, Space & Security.
- Boeing is one of the largest U.S. exporters.
- With employees from 70 countries, 57% of whom hold college degrees or higher, Boeing represents one of the most diverse, talented, and innovative workforces in the world.
- The company has nearly 12,000 commercial jetliners in service worldwide, which is roughly 75 percent of the world fleet.
- Boeing designs, produces, modifies and supports fighters, bombers, transports, rotorcraft, aerial refuelers, missiles, munitions, and spacecraft for military and commercial use.

[44] U.S. Federal Bureau of Investigation. "Former Boeing Engineer Sentenced to Nearly 16 Years in Prison for Stealing Aerospace Secrets for China." *Department of Justice Press Release*, February 8, 2010 <http://losangeles.fbi.gov/dojpressrel/pressrel10/la020810.htm>. (accessed March 24, 2010).

EXECUTIVE SUMMARY: LAN LEE AND YUEFEI GE CASE

Overview:
In 2006, Lan Lee (LEE) and Yuefei Ge (GE) were indicted for trade secret theft.[45] On September 26, 2007, they were indicted for violations to section 1831 and 1832 of the Economic Espionage Act (EEA).[46] LEE and GE were accused of stealing 130 nanometer microchips[47] and a software code[48] from their employer NetLogic in San Jose, California during the period of 2002 to 2003. Additionally, they were charged with illegally downloading information from NetLogic computers.[49]

LEE and GE established SICO Microsystems, Inc. in Delaware to develop and market products created from the stolen trade secrets. LEE and GE received $3.6 million in capital for SICO through China's 863 Program.[50] Liu Baisen was identified as the venture capitalist for SICO.[51] The Beijing Electronic Development Company Limited also provided a portion of the capital.[52]

In 2002, Lily Le, GE's wife, emailed NetLogic CEO Ron Jankov and called the FBI regarding her concerns about SICO Microsystems and LEE's and GE's activities.[53] In 2003, the FBI launched an investigation in which they discovered correspondences between LEE and GE and individuals in China.[54] LEE's computer also contained venture capital information.[55]

Additional evidence used in the LEE and GE case came from a plea bargain made with Fei Ye and Ming Zhong. In exchange for Ye's and Zhong's confession to requesting foreign funds, all charges were dropped against them.[56] The U.S. Attorney General's office believed that the LEE and GE case had more value than the YE and MING case.[57]

---

[45] Dan Levine. "Defense Blames Chinese Espionage Case on Neglected Wife." *Law.Com*. October 22, 2009. <http://www.law.com/jsp/law/international/LawArticleIntl.jsp?id=1202434866919>. (accessed April 27, 2010).
[46] U.S. Department of Justice. "Two Bay Area Men Indicted on Charges of Economic Espionage." *Department of Justice Press Release*. September 26, 2007. < http://www.justice.gov/criminal/cybercrime/liIndict.htm>. (accessed April 27, 2010).
[47] Josh Gerstein. "Spy Charges in High-Stakes Microchip Race." *New York Sun.* June 19, 2006. <http://www.economicespionage.com/NewYorkSun.htm>. (accessed April 27, 2010).
[48] Dan Levine. "DOJ's Economic-Spy Strategy Emerges." *The Recorder*. May 5, 2008. < http://www.law.com/jsp/law/international/LawArticleIntl.jsp?id=1202421126406>. (accessed April 27, 2010).
[49] Ibid.
[50] U.S. Department of Justice. "Two Bay Area Men Indicted on Charges of Economic Espionage." *Department of Justice Press Release*. September 26, 2007. < http://www.justice.gov/criminal/cybercrime/liIndict.htm>. (accessed April 27, 2010).
[51] Jonathan Eric Lewis. "The Economic Espionage Act and the Threat of Chinese Economic Espionage in the U.S." *University of Connecticut, School of Law*. <http://jip.kentlaw.edu/art/volume%208/8%20Chi-Kent%20J%20Intell%20Prop%20189.pdf >. (accessed April 27, 2010).
[52] Josh Gerstein. "Spy Charges in High-Stakes Microchip Race." *New York Sun.* June 19, 2006. <http://www.nysun.com/national/spy charges-in-high-stakes-microchip-race/34620/> (accessed April 27, 2010).
[53] Dan Levine. "Rare Economic Espionage Case Filled with Quirks." *Law.Com.* October 20, 2009. < http://www.law.com/jsp/law/LawArticleFriendly.jsp?id=1202434787775>, (accessed April 27, 2010).
[54] Howard Mintz. "Silicon Valley Espionage Case Only Second of Kind in Nation to go to Trial." *San Mercury News*. October 18, 2009. <http://it.tmcnet.com/news/2009/10/19/4432100.htm>. (accessed April 30, 2010).
[55] Josh Gerstein. "Spy Charges in High-Stakes Microchip Race." *New York Sun.* June 19, 2006. <http://www.nysun.com/national/spy charges-in-high-stakes-microchip-race/34620/>. (accessed April 27, 2010).
[56] Dan Levine. "DOJ's Economic-Spy Strategy Emerges." *The Recorder*. May 5, 2008. < http://www.law.com/jsp/law/international/LawArticleIntl.jsp?id=1202421126406> (accessed April 27, 2010).
[57] Ibid.

The LEE and GE case is the first case to be heard before a jury trial. [58] On November 20, 2009, LEE and GE were acquitted on two charges, but the jury was deadlocked on the other charges. LEE and GE remain eligible for retrial for the counts of conspiracy, economic espionage, and trade secret theft.[59] If convicted under the EEA, the maximum penalty is 60 years with a $1.5 million fine.[60] If convicted for conspiracy, the maximum penalty is 15 years and $500,000 fine plus restitution, as applicable.[61] If convicted, the maximum penalty for substantive counts is 10 years and $250,000 fine plus restitution, as applicable and for each count.[62]

Timeline:

• 2002-2003	LEE and GE stole a software code and 130 nanometer microchips code as well as illegally downloaded information from NetLogic computers
• 2002	NetLogic and FBI informed of LEE's and GE's activities
• 2003	FBI launched investigation
• June 2006	First Indictment (Trade Secret Theft)
• September 26, 2007	Second Indictment (Economic Espionage Act)
• November 20, 2009	LEE and GE were acquitted on two charges and remain eligible for retrial on the counts of conspiracy, economic espionage, and trade secret theft

Company Overview:

NetLogic Microsystems, Inc. [63]

- NetLogic is the worldwide leader in intelligent semiconductor solutions that are used in Internet networks and differentiated network traffic tasks.
- NetLogic's product portfolio includes high-performance Multi-Core Processors, Knowledge-based Processors, Content Processors, Network Search Engines, Low-Power Embedded Processors and high-speed 10/40/100 Gigabit Ethernet PHY solutions.
- Demand for NetLogic products is driven by the following: internet traffic, network security, convergence of voice, video and data traffic, proliferation of internet-connected devices, growth in data center and cloud computing deployments, adoption of IP 3G/4G mobile wireless infrastructure.
- NetLogic has offices in the following locations: Mountain View, California (corporate headquarters); Cupertino, California; Austin, Texas; Raleigh, North Carolina; Canada; France; China, Korea, Japan, and India.

---

[58] Jordan Robertson. "Rare Economic Espionage Case Going to Trail". *USA Today*. October 21, 2009. <http://www.usatoday.com/tech/news/2009-10-21-china-computer-espionage_N.htm>. (accessed April 28, 2010).

[59] Jordan Robertson. "Economic Espionage Case Ends in Jury Deadlock." *USA Today*. November 24, 2009. < http://www.usatoday.com/tech/news/2009-11-24-china-net-logic_N.htm>. (accessed April 27, 2010).

[60] Josh Gerstein. "Spy Charges in High-Stakes Microchip Race." *New York Sun*. June 19, 2006. <http://www.nysun.com/national/spy charges-in-high-stakes-microchip-race/34620/>. (accessed April 27, 2010).

[61] Collen Taylor. "Two Charged with Conspiracy to Commit Economic Espionage." *Electronic News*. September 27, 2007. <http://www.edn.com/article/CA6483922.html?text=> (accessed April 28, 2010).

[62] Ibid.

[63] "Company Profile." *NetLogic Microsystems*, <http://www.netlogicmicro.com/Company/Profile.htm>. (accessed April 27, 2010).

EXECUTIVE SUMMARY: ANNE LOCKWOOD, FUPING LIU, AND MICHAEL HAEHNEL CASE

Overview:
Between February and December 2004, Anne Lockwood (LOCKWOOD), Fuping Liu (LIU), and Michael Haehnel (HAEHNEL), stole secret and proprietary information from Metaldyne, an international auto parts manufacturer, with the intention of assisting Metaldyne's Chinese competitors. LOCKWOOD was a disgruntled employee who, after leaving her job as Vice President of sales at Metaldyne in early 2004, began collaborating with LIU. LIU was a metallurgist for Metaldyne until April 2004, when he resigned and took a position at GKN Sinter Metals' Shanghai office. GKN Sinter Metals' headquarters are located in Michigan. LOCKWOOD and LIU jointly planned to steal Metaldyne's manufacturing process for the powdered metal connecting rod used in truck engines. Metaldyne and GKN Sinter Metals, Inc. are the only two companies that have the ability to successfully produce heavy vehicle components from powdered metal.[64] Additionally, LOCKWOOD's and LIU's activities targeted Metaldyne and GKN's internal business planning, GKN's business plans for China, cost and production information, and their internal cost structure for the connecting rods.[65] To complement LIU's high-level access to Metaldyne's and GKN's trade secrets, LOCKWOOD recruited her husband, Michael Haehnel, a senior engineer at Metaldyne, to collect information on Metaldyne's manufacturing process.[66]

Both LOCKWOOD and LIU passed the information obtained from their activities to GKN's Chinese competitor, Chongqing Huafu Industry Company, Ltd.[67] LIU also provided GKN's information to another Chinese auto parts manufacturer, Liaoning Shuguang Automotive Corporation (SG Auto). Frequent emails between LOCKWOOD and LIU and the two competitors eventually attracted attention and rumors, ultimately resulting in Metaldyne's decision to file a complaint with the FBI.[68]

The FBI's Detroit office investigated this case, which resulted in the 2006 indictments of LOCKWOOD, LIU, and HAEHNEL on 64 counts. The primary count in the indictment was the conspiracy to steal confidential and proprietary information in order to assist a Chinese competitor.[69] HAEHNEL was charged with one count of stealing confidential information valued at over $5,000 in a single-year period. LIU was also charged with the same count as well as three separate counts of transporting stolen goods, mainly electronic files, each valued at over $5,000 in a single-year period.

U.S. Attorney Terrence Berg, with Assistant U.S. Attorney Cynthia Oberg, prosecuted the case. On September 15, 2008, LOCKWOOD and LIU pleaded guilty to the main indictment count

[64] Megan Lampinen. "Former Metaldyne Employees Plead Guilty to Information Theft." *Automotive World* (2008).
[65] U.S. Department of Justice. "Former Metaldyne Employees Sentenced to Prison in Conspiracy to Steal Confidential Business Information to Benefit Chinese Competitor." *U.S. Department of Justice*. February 13, 2009. <http://www.justice.gov/criminal/cybercrime/lockwoodSent2.pdf >. (accessed April 27, 2010).
[66] David J. Lynch. "FBI Goes on Offensive vs. Tech Spies." *USA Today*, July 24, 2007. <http://www.usatoday.com/money/world/2007-07-23-china-spy-2_N.htm>. (accessed May 2, 2010).
[67] Joseph M. Capus . "Theft of Metaldyne Connecting Rod Technology." Powder Metallurgy 48(1) (2005): 1-4.
[68] Richard Felton. "Caught Out!" *Metal Powder Report* 60(3) (2005): 3.
[69] U.S. Department of Justice. "Former Metaldyne Employees Sentenced to Prison in Conspiracy to Steal Confidential Business Information to Benefit Chinese Competitor." *U.S. Department of Justice*. February 13, 2009.

while HAEHNEL pleaded guilty to the misdemeanor of illegally accessing stored electronic records. LOCKWOOD received 30 months in prison with a two year supervised release and a $100 special assessment. LIU was sentenced to 9 months in prison with a two year supervised release. HAEHNEL received 18 months of probation with 6 months in prison and 6 months under house arrest.

Timeline:

• Early 2004	LOCKWOOD resigned as the Vice-President of Sales at Metaldyne.
• February-December 2004	The theft of Metaldyne property and information occurred.
• April 2004	LIU resigned from Metaldyne and relocated to Shanghai to work for GKN.
• May 2004	LOCKWOOD and LIU repeatedly emailed Metaldyne information to Huafu.
• May 28-June 6 2004	LOCKWOOD and HAEHNEL traveled to China.
• Oct. 27-Dec. 20 2004	LIU emailed GKN information to SG Auto.
• June 2006	64 count indictment filed.
• September 15, 2008	All three defendants pled guilty.
• February 2009	All three defendants sentenced.

Company Overview:

Metaldyne

- Metaldyne is a designer and manufacturer of automotive components that focuses on metal-formed products for engine and transmission applications.
- Metaldyne is a global company, and its clients include automakers such as Chrysler, Ford, BMW, Hyundai, GM, and Toyota, and parts suppliers such as Cummins, Delphi, and ArvinMeritor.
- Metaldyne's leading global presence is a result of its focus on designing and supplying its own highly technical products, specifically in forging products and the Powder Metallurgy industry.

EXECUTIVE SUMMARY: HONG MENG CASE

Overview:

Hong Meng (H. MENG) was a senior research chemist for DuPont where he worked on OLED technology, which is technology for a new screen display for televisions and computer monitors. When H. MENG resigned from Dupont USA in 2009 to take a position with DuPont China in Shanghai, he did not inform DuPont that he also accepted a faculty position at the Peking University in Beijing in their College of Engineering's Department of Advanced Materials and Nanotechnology.

During H. MENG's job transfer, he downloaded approximately 595 documents from his work computer to his personal external storage device.[70] Of these documents, almost 550 of them were later found on MENG's personal computer.[71] H. MENG intended to use these trade secrets to start a program at Peking University to commercialize OLED technology for industrial application. However, DuPont officials, during a routine review of MENG's work computer, discovered MENG's activities prior to his transfer to Shanghai. Not only did they discover he downloaded confidential OLED documents, but also that he had accepted a faculty position at Peking University.[72]

Although H. MENG was caught before he successfully implemented his plan, the damage level his activities caused remains unknown. DuPont has filed a civil lawsuit seeking damages, but has not released a monetary amount.[73] Federal authorities filed a criminal complaint in 2009, but the District Attorney's office has yet to issue an indictment[74]. If indicted, the counts will include a maximum fine of $250,000, restitution, and a maximum prison sentence of five years.[75]

[70] Marc Reisch. "Chemist Charged With Crime." *Chemical and Engineering News* 87(41) (2009): 12-22.
[71] U.S. Department of Justice. "Former DuPont Chemist Charged: Dr Hong Meng Accused of Unauthorized Computer Access of OLED Technology." October 2, 2009. <http://www.justice.gov/criminal/cybercrime/mengChar.pdf>. (accessed April 27, 2010).
[72] O'Sullivan, Sean. 2009. "DuPont charges industrial espionage Employee accused of plotting to take secret data to China." *The News Journal*, 7, September 2009.
[73] Sean O'Sullivan. "DuPont Charges Industrial Espionage Employee Accused of Plotting to Take Secret Data to China." *The News Journal*, (2009): <http://www.mainefairtrade.org/pdf/DuPont%20charges%20industrial%20espionage.pdf>. (accessed April 27, 2010).
[74] Marc Reisch. "Chemist Charged With Crime." *Chemical and Engineering News* 87(41) (2009): 12-22.
[75] U.S. Department of Justice. "Former DuPont Chemist Charged: Dr Hong Meng Accused of Unauthorized Computer Access of OLED Technology." October 2, 2009. <http://www.justice.gov/criminal/cybercrime/mengChar.pdf>. (accessed April 27, 2010).

Timeline:

- November 2002 — MENG began employment with DuPont.
- 2007 — MENG is promoted to senior research chemist and co-edited a book on OLED.
- Early 2009 — MENG secretly accepted a position at Peking University.
- August 18-19, 2009 — DuPont security officials interviewed MENG after they search his work computer.
- August 23, 2009 — MENG fired from DuPont.
- Late August — DuPont filed a civil suit against MENG.
- October 2, 2009 — MENG arrested and charged with a one-count criminal complaint.

Company Overview:

E.I. du Pont de Nemours and Company ("DuPont")

- DuPont is a science and manufacturing company.
- DuPont's inventions and manufacturing knowledge sustain the company's competitive advantage and represent a significant component of DuPont's market capitalization.
- Each manufacturing plant requires significant investments, which are depreciated over many years.
- DuPont's growth focus is in high-risk economies.
- DuPont has strong collaboration with external entities.

XIAODONG SHELDON MENG CASE

Overview:
Between 2003 and 2004, Chinese native Xiaodong Sheldon Meng (MENG) violated the Economic Espionage Act (EEA). MENG was employed at Quantum 3D as a systems engineer, computer systems analyst, and 3D graphics application senior engineer. Quantum 3D is a California-based provider of real-time visual simulation and computing systems for commercial and military consumption. When MENG changed employment in early 2004 from Quantum 3D to Orad, a Chinese competitor, he stole Quantum 3D's Mantis 1.5.5 program. For the following year, MENG repeatedly attempted to sell this Quantum 3D property as an Orad product to the Chinese government. MENG also used the Mantis program during Orad presentations and sales pitches to the Malaysian Air Force and the Thai Air Force.

Additionally, MENG stole six segments of source code and at least 100 other software components from Quantum 3D. However, Mantis 1.5.5 is classified as a defense article and cannot be exported without a U.S. export license.[76] Mantis 1.5.5 is a military application trade secret used in military combat simulation software. Specifically, Mantis 1.5.5 military simulation programs employ viXsen and nVsensor, which are exclusively used in precision military training of fighter pilots, who use night vision and thermal equipment.[77] Therefore, MENG not only violated EEA with his intent to benefit a foreign government, but also violated the U.S. Arms Export Control act by exporting classified defense articles listed on the U.S. Munitions List.

Following a joint investigation by the U.S. Attorney's Computer Hacking and Intellectual Property (CHIP) Unit, FBI, DHS, and ICE produced a 36 count indictment. MENG pled guilty to violating the EEA and the Arms Export Control Act, both national security violations. He was sentenced by the Honorable Jeremy Fogel, U.S District Court Judge, to two years imprisonment and a fine of $10,000.[78]

[76] U.S. Department of Justice. "Former Chinese National Charged with Stealing Military Application Trade Secrets from Silicon Valley Firm to Benefit Governments of Thailand, Malaysia, and China." *U.S. Attorney Northern District of California*. December 14, 2006. <http://www.justice.gov/criminal/cybercrime/mengCharge.htm>. (accessed April 27, 2010).
[77] Ibid.
[78] Jaikumar Vijayan. "Trial to Begin in Economic Espionage Case Involving China." *Computerworld*. October 21, 2009. <http://www.computerworld.com.au/article/323000/trial_begin_economic_espionage_case_involving_china/>. (accessed April 27, 2010).

Timeline:[79]

- June 2000 - March 2003 — MENG was employed with Quantum 3D.
- March 26, 2003 — MENG departed the U.S. for Taipei, Taiwan.
- April - December 2003 — MENG served as a consultant for Quantum 3D in Asia.
- June 15, 2003 — MENG attempted to sell the Malaysian Air Force with Quantum 3D products.
- August 17, 2003 — MENG attempted to sell the Malaysian Air Force with Quantum3D products.
- January 2004 — MENG accepted a position with Orad in China and resigned as a consultant with Quantum 3D.
- May - July 2004 — MENG conducted a demonstration for Chinese government agencies with stolen Quantum 3D.
- July - August 2004 — MENG provided a proposal to the Royal Thai Air Force containing stolen Quantum 3D information.
- September 2004 — MENG provided additional demonstrations to the Chinese Navy and Air Force.
- Dec. 2004 - Jan. 2005 — MENG deleted over 900 emails.
- December 2006 — MENG charged in 36 count indictment
- August 1, 2007 — MENG pled guilty.
- June 18, 2008 — MENG sentenced.

Company Overview:

Quantum 3D

- Quantum 3D develops and manufactures real time visual computing hardware and software products.
- Quantum 3D has development centers throughout the U.S. and sales and logistics operations in Europe.
- Quantum 3D's clients include private companies such as Boeing, Lockheed Martin, Raytheon, Rockwell Collins, and Ford Motors. Quantum 3D also works on U.S. military projects such as the Stryker Interim Armored Vehicle, Bradley A3 Test Bed, and M1 Abrams Tank.
- Quantum 3D competes in multiple industries, including Industrial & Military Computer Systems, Computer Hardware, Specialized Computer Systems, Semiconductors, and Graphics, Video Chips, and Boards.
- The company's success depends on developing a strong client base and niche software products.

[79] U.S. Department of Justice. "Former Chinese National Charged with Stealing Military Application Trade Secrets from Silicon Valley Firm to Benefit Governments of Thailand, Malaysia, and China." *U.S. Attorney Northern District of California*. December 14, 2006. http://www.justice.gov/criminal/cybercrime/mengCharge.htm (accessed April 27, 2010).

EXECUTIVE SUMMARY: YOUNGGANG "GARY" MIN CASE

Overview:
Between August and December of 2005, Younggang "Gary" Min (MIN) accessed extremely high numbers of abstracts and full-text pdf documents from E.I. du Pont de Nemours and Company's (DuPont) Electronic Data Library (EDL). The EDL server accessed by MIN is one of Dupont's foremost databases for storing the company's trade secrets. MIN downloaded about 22,000 abstracts from EDL and accessed over 16,000 documents. In total, MIN's downloads represented about 10 percent of information stored on the EDL server. His usage was more than 15 times that of the next highest user during that period. In addition to his downloading activities, MIN also photographed sensitive DuPont notebooks. His EDL searches ranged from DuPont's most significant technologies and product lines to its latest technologies in the R&D stage. The market value of information accessed by MIN exceeded $400 million.[80]

Upon raiding MIN's residence, authorities found DuPont documents on "numerous" computers. One had an external disk drive running a program to erase all of the data on it.[81] An additional 100 documents were found in a storage unit, and more documents were discovered in a one-room apartment rented by MIN.[82]

According to the plea agreement, on November 13, 2006, MIN agreed to plead guilty in the United States District Court for the District of Delaware to Count I of Felony Information. Count I charges MIN with theft of trade secrets. The offense carries a maximum prison sentence of 10 years, a fine of up to $250,000, and restitution. In accordance with the terms of his plea agreement, MIN pled guilty to misappropriating DuPont's trade secrets and agreed to cooperate with the government. [83] MIN was sentenced to 18 months in prison, and was ordered to pay US $14,500 in restitution and a US $30,000 fine.[84]

This case was investigated by the FBI, Wilmington Resident Agency, and the United States Department of Commerce. United States Attorney Colm F. Connolly and Assistant United States Attorney Robert F. Kravetz prosecuted the case.[85]

[80] The U.S. Department of Justice. "Guilty Plea in Trade Secrets Case." *United States Attorney's Office District of Delaware*. February 15, 2007. <http://www.justice.gov/criminal/cybercrime/minPlea.pdf>. (accessed April 27, 2010).
[81] Jaikumar Vijayan. "DuPont Scientist Admits Downloading, Stealing $400M Worth of Trade Secrets." *Computerworld*. February 15, 2007. <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9011367>. (accessed April 27, 2010).
[82] The U.S. Department of Justice. "Guilty Plea in Trade Secrets Case." *United States Attorney's Office District of Delaware*. February 15, 2007. <http://www.justice.gov/criminal/cybercrime/minPlea.pdf>. (accessed April 27, 2010).
[83] Ibid
[84] Chase, Randall. "Former Dupont Scientist Sentenced to 18 months in Prison for Stealing Company's Trade Secrets." *Associated Press.* Nov. 6, 2007. <http://www.msnbc.msn.com/id/21661606>. (accessed May 1, 2010).
[85] Ibid

Timeline:

• November 1995	MIN began working for DuPont as a research chemist.
• July 2005	MIN began discussions with DuPont competitor, Victrex PLC, about possible employment opportunities in Asia.[1]
• October 18, 2005	MIN signed a contract with Victrex (for January 2006 start date).
• December 12, 2005	MIN told DuPont about Victrex employment offer.
• Aug. 2005 – Dec. 12, 2005	MIN accessed EDL and stole information.
• February 2, 2006	MIN uploaded approximately180 DuPont documents, including documents containing confidential trade secret information to his Victrex-assigned laptop computer.
• February 3, 2006	DuPont tells Victrex about the theft.
• February 8, 2006	Victrex seized MIN's computer and turned it over to FBI.
• February 14, 2006	FBI and Department of Commerce raided MIN's home in Ohio.
• November 13, 2006	MIN entered a guilty plea.
• November 6, 2007	MIN sentenced.

Company Overview:

<u>E.I. du Pont de Nemours and Company ("DuPont")</u>

- DuPont is a science and manufacturing company.
- DuPont's inventions and manufacturing knowledge sustain the company's competitive advantage and represent a significant component of DuPont's market capitalization.
- Each manufacturing plant requires significant investments, which are depreciated over many years.
- DuPont's growth focus is in high-risk economies.
- DuPont has strong collaboration with external entities.

EXECUTIVE SUMMARY: TAKASHI OKAMOTO AND HIROAKI SERIZAWA CASE

Overview:
From January 1997 to July 26, 1999, Takashi Okamoto (OKAMOTO) was employed by the Lerner Research Institute (LRI) of the Cleveland Clinic Foundation (CCF) to research causes and treatments for Alzheimer's Disease.[86] The Alzheimer's research was funded under a $2 million research grant funded by the National Institute of Health.

In April 1999, OKAMOTO was offered a position with the Brain Research Institute at the Institute of Physical and Chemical Research (RIKEN) in Japan.[87] RIKEN is 94% funded by Japan's Ministry of Science and Technology.[88]

On July 26, 1999, OKAMOTO resigned from LRI. He began working for RIKEN on August 3, 1999. [89] Between July 8 through 12, 1999, OKAMOTO destroyed and stole Alzheimer's research from LRI that included: DNA, cell line regents, and other scientific materials.[90] During the summer of 1999, OKAMOTO emailed colleagues at RIKEN to request storage space for research materials from LRI.[91]

OKAMOTO returned to the U.S. in August 1999 to retrieve some of the stolen materials and to plant fake DNA test tubes at LRI, all with the assistance of a research colleague, Hiroaki Serizawa (SERIZAWA). [92] Although claiming ignorance to OKAMOTO's intent, SERIZAWA stored the stolen research materials in Kansas City, Kansas, and later transported said research to Japan where OKAMOTO was residing. [93]

An anonymous person within the LRI recorded phone conversations implicating OKAMOTO in the theft.[94] Additionally, researchers at the LRI went to authorities after discovering missing research materials.[95]

---

[86] U.S. Department of Justice. "First Foreign Economic Espionage Indictment; Defendants Steal Trade Secrets from Cleveland Clinic Foundation." *United States Attorney Northern District of Ohio*. May 8, 2001. <http://www.justice.gov/criminal/cybercrime/Okamoto_SerizawaIndict.htm>. (accessed April 27, 2010).
[87] Ibid.
[88] Ibid.
[89] Unknown. "DNA Plea-bargain Brings Probation." *The Daily Yomiuri*. May 30, 2003, <http://www.lexisnexis.com/us/lnacademic/search/homesubmitForm.do>. (accessed April 28, 2010).
[90] U.S. Department of Justice. "First Foreign Economic Espionage Indictment; Defendants Steal Trade Secrets from Cleveland Clinic Foundation." *United States Attorney Northern District of Ohio*. May 8, 2001. <http://www.justice.gov/criminal/cybercrime/Okamoto_SerizawaIndict.htm>. (accessed April 27, 2010).
[91] Unknown. "Internal Report Suggests Gene Samples Lifted from U.S." *The Nikkei Weekly*. June 11, 2001. <http://www.lexisnexis.com/us/lnacademic/search/homesubmitForm.do>. (accessed April 28, 2010).
[92] U.S. Department of Justice. "First Foreign Economic Espionage Indictment; Defendants Steal Trade Secrets from Cleveland Clinic Foundation." *United States Attorney Northern District of Ohio*. May 8, 2001. <http://www.justice.gov/criminal/cybercrime/Okamoto_SerizawaIndict.htm>. (accessed April 27, 2010).
[93] Justin Gillis. "Scientists Accused of Theft; Espionage Alleged Against Japanese." *The Washington Post*. May 10, 2001. < http://www.lexisnexis.com/us/lnacademic/search/homesubmitForm.do>. (accessed April 28, 2010).
[94] Unknown. "Scientist 'Seen Taking Gene Samples'". *The Daily Yomiuri*. July 2, 2001. <http://www.lexisnexis.com/us/lnacademic/search/homesubmitForm.do>. (accessed April 28, 2010).
[95] Ibid.

In May 2001, OKAMOTO and SERIZAWA were indicted on four criminal counts including: two violations under the Economic Espionage Act (EEA), interstate transport of stolen goods, and perjury. [96] The maximum penalty was a $500,000 fine and 15 years imprisonment. [97]

Two investigation teams, one from RIKEN and one from the Ministry of Education, Science, and Technology, investigated the research materials handled by OKAMOTO at RIKEN. [98] They concluded there was insufficient evidence linking the CCF's research materials to RIKEN. [99]
In May 2002, SERIZAWA agreed to a plea bargain in which he admitted to perjury and agreed to testify against OKAMOTO in exchange for the EEA charges against him to be dropped. [100] On May 28, 2003, SERIZAWA was sentenced to three years probation, a $500 fine, and 150 hours of community service. [101]

In March 2002, the U.S. requested the extradition of OKAMOTO under the U.S.-Japan extradition treaty. [102] In 2004, the Tokyo High Court rejected the extradition of OKAMOTO based on the lack of sufficient evidence under the EEA [103] treaty's stipulation that the two countries share similar laws. Japan does not have an equivalent of the EEA.

[96] U.S. Department of Justice. "First Foreign Economic Espionage Indictment; Defendants Steal Trade Secrets from Cleveland Clinic Foundation." *United States Attorney Northern District of Ohio*. May 8, 2001. <http://www.justice.gov/criminal/cybercrime/Okamoto_SerizawaIndict.htm>. (accessed April 27, 2010).
[97] Ibid.
[98] Unknown. "Riken Plans In-house Probe." *The Daily Yomiuri*. May 11, 2001. <http://www.lexisnexis.com/us/lnacademic/search/homesubmitForm.do>. (accessed April 28, 2010).
[99] "Ibid.
[100] Unknown. "DNA Plea-bargain Brings Probation." *The Daily Yomiuri*. May 30, 2003.
[101] Ibid.
[102] Ibid.
[103] Unknown. "Accused Doctor Sues Govt for 43 mil. Yen over Detention." *The Daily Yomiuri*. August 26, 2004. <http://www.lexisnexis.com/us/lnacademic/search/homesubmitForm.do>. (accessed April 28, 2010).

Timeline:

- Jan. 1997 – July 26, 1999 OKAMOTO employed by LRI.
- April 1999 OKAMOTO offered a position with RIKEN.
- July 26, 1999 OKAMOTO resigned from LRI.
- August 3, 1999 OKAMOTO began working for RIKEN.
- July 8-12, 1999 OKAMOTO stole and destroyed Alzheimer's research.
- Summer 1999 OKAMOTO requested storage space at RIKEN for Alzheimer's research.
- August 1999 OKAMOTO returned to the U.S. to retrieve some Alzheimer's research.
- September 1999 SERIZAWA transported stolen research to OKAMOTO in Japan.
- May 2001 OKAMOTO and SERIZAWA were indicted on 4 criminal counts.
- March 2002 U.S. requested extradition of OKAMOTO.
- May 2002 SERIZAWA agreed to plea bargain (plead guilty to perjury and testify against OKAMOTO in exchange for EEA charges to be dropped)
- May 28, 2003 SERIZAWA sentenced to 3 years probation, $500 fine, and 150 hours of community service.
- April 2004 Japan refused to extradite OKAMOTO.

Company Overview:

Lerner Research Institute, Cleveland Clinic Foundation[104]

- LRI is the center for all of the CCF's laboratory, translational, and clinical research.
- LRI's mission is to understand the causes of human diseases and to develop cures and treatments for such diseases.
- In 2009, Cleveland Clinic was ranked as the fourth best hospital in the U.S.
- There are over 200 biomedical researchers and 1,200 scientists and support staff at LRI. In 2008, LRI received an estimated $75 million from the National Institute of Health and its total research budget was $258 million.
- In 2008, investigators submitted 62 invention disclosures to Cleveland Clinic Innovations, which resulted in 12 licenses, 22 patents, and three spin off companies.

[104] "About Us." *Lerner Research Institute, Cleveland Clinic Foundation.* <http://www.lerner.ccf.org/info/>. (accessed April 27, 2010).

EXECUTIVE SUMMARY: FEI YE AND MING ZHONG CASE

Overview:
On November 23, 2001, Fei Ye (YE) and Ming Zhong (ZHONG) were arrested at the San Francisco International Airport while attempting to board an aircraft bound for China with stolen trade secret information in their luggage. YE and ZHONG admitted to possessing stolen trade secrets from Sun Microsystems, Inc. and Transmeta Corporation. They also admitted their intent to utilize the trade secrets to design a computer microprocessor that would benefit the People's Republic of China and would be manufactured and marketed by Supervision, Inc., (a/k/a Hangzhou Zhongtian Microsystems Company Ltd., a/k/a Zhongtian Microsystems Corporation) a company established by YE and ZHONG in 2001.[105]

There were a total of four companies victimized by the YE and ZHONG plot: NEC Electronics Corp., Sun Microsystems Inc., Transmeta Corp. and Trident Microsystems Inc. YE and ZHONG both worked at Transmeta and Trident. YE also worked at NEC and Sun.[106]

In pleading guilty, YE and ZHONG admitted that any share of profits on chips sales would be given to the City of Hangzhou and the Province of Zhejiang in China because this city provided the capital to establish Supervision. YE and ZHONG further admitted applying for funding from the National High Technology Research and Development Program of China, commonly known as the "863 Program." Furthermore, papers seized from the men allegedly show their solicitation to the Chinese government for funding to assist with their startup costs and processes. According to prosecutors, the documents show YE and ZHONG marketed Supervision as a company that would elevate China's chip-making know-how and improve Chinese competition in the micro-electronics market. However, it is unknown if YE and ZHONG were successful in obtaining any Chinese funding. Additionally, the indictments did not charge any representative of the Chinese government as a co-conspirator.[107]

The YE and ZHONG case was the first conviction under the Foreign Espionage Act of 1996. YE and ZHONG were indicted by a federal grand jury on December 4, 2002. YE and ZHONG were charged with a total of ten counts, including: one count of conspiracy in violation of 18 U.S.C. 371, 1831(a)(5) and 1832(a)(5); two counts of economic espionage in violation of 18 U.S.C. 1831(a)(3); five counts of possession of stolen trade secrets in violation of 18 U.S.C. 1832(a)(3); and two counts of foreign transportation of stolen property in violation of 18 U.S.C. 2314. The maximum statutory penalty for each count in violation of 18 U.S.C. 1831 is 15 years and a fine

[105] U.S. Department of Justice. "Two Men Plead Guilty to Stealing Trade Secrets from Silicon Valley Companies to Benefit China." *U.S. Attorney Northern District of California*. December 14, 2006. <http://www.usdoj.gov/criminal/cybercrime/yePlea.htm> (accessed April 27, 2010).

[106] U.S. Department of Justice. "Pair from Cupertino and San Jose, California, Indicted for Economic Espionage and Theft of Trade Secrets From Silicon Valley Companies." *U.S. Attorney Northern District of California*. December 4, 2002. <http://www.justice.gov/criminal/cybercrime/yeIndict.htm>. (accessed April 27, 2010).

[107] U.S. Department of Justice. "Pair from Cupertino and San Jose, California, Indicted for Economic Espionage and Theft of Trade Secrets From Silicon Valley Companies." *U.S. Attorney Northern District of California*. December 4, 2002. <http://www.justice.gov/criminal/cybercrime/yeIndict.htm>. (accessed April 27, 2010).

of $500,000, plus restitution if appropriate. YE and ZHONG each pled guilty to two counts of economic espionage.[108]

Kyle F. Waldinger and Richard C. Cheng, Assistant U.S. Attorneys in the Computer Hacking and Intellectual Property Unit, prosecuted the case, with the assistance of legal technicians Ponly Tu and Kathy Huynh.

The government highly valued YE's and ZHONG's cooperation. While Assistant U.S. Attorney Kyle Waldinger calculated their prison sentences to extend beyond three years, the government recommended only 12 months in prison.

Timeline:

• 2001	YE and ZHONG established Supervision, Inc.
• November 23, 2001	YE and ZHONG arrested at San Francisco International Airport.
• November 23-24, 2001	Allegations are brought against YE for the possession at his residence of a feasibility report review regarding Hangzhou Zhongtian Microsystems Corporation at his house. The report suggested that the project receive the support of the Chinese government.
• November 23, 2001	Allegations are brought against ZHONG for the possession at his residence of a project application form for the National Special Foundation for Importing Knowledge of Software and Integrated Circuits printed by the National Bureau of Foreign Experts. The application stated that the project is of tremendous significance to the Chinese integrated circuitry industry and should receive the support of the government.
• December 4, 2002	Indictments filed on YE and ZHONG for 10 counts.
• December 14, 2006	YE and ZHONG pled guilty.
• November 21, 2008	YE and ZHONG are each sentenced to one year in prison.

Company Overview:

Sun Microsystems, Inc.

- Founded on February 24, 1982.
- A wholly owned subsidiary of Oracle Corporation, selling computers, computer components, computer software, and information technology services.
- On January 27, 2010, Sun was acquired by Oracle Corporation.

Transmeta Corporation

- Founded in 1995, Transmeta was a former U.S.-based corporation that licensed low power semiconductor intellectual property.
- Transmeta originally produced very long instruction word code morphing (micro-coded)

[108] U.S. Department of Justice. "Two Men Plead Guilty to Stealing Trade Secrets from Silicon Valley Companies to Benefit China." *U.S. Attorney Northern District of California.* December 14, 2006. <http://www.usdoj.gov/criminal/cybercrime/yePlea.htm>. (accessed April 27, 2010).

microprocessors, with a focus on reducing power consumption in electronic devices.

- In January 2009, Transmeta was acquired by Novafora, which ceased operations in August 2009.

NEC Corporation

- Japanese multinational IT company headquartered in Minato, Tokyo, Japan.
- Provides information technology (IT) and network solutions to business enterprises, communications services providers and government.
- Part of the Sumitomo Group[109]

Trident Microsystems

- Established in 1987.
- Supplier of display-processors for flat panel displays (plasma, LCD, etc.).
- A former supplier of PC graphics chipsets and sound controllers.

[109] A large *keiretsu* in Japan.

Omitted Variables

Investor Confidence:

The variable "Investor Confidence" can be defined as the level of risk and expected decrease in investment returns identified by an investor following an incident of economic espionage. Common investor confidence measures include the Barron's Confidence Index[110] and the Standard and Poor's Confidence Indicator.[111] Finance theorists explain that stock prices for publically traded firms represent the firm's fair value and can be used to measure the monetary impacts of economic espionage.[112] The introduction of new information affecting stock prices is quickly reflected in stock price fluctuations.[113] Therefore, finance theorists contend that the affects of a negative event, such as an act of economic espionage, can be measured through the difference between the expected earnings[114] of a firm's stocks on a given day and the actual earnings of the firm's stocks on that same day.[115] "Investor Confidence" is important to the consequence of economic espionage because incidents of economic espionage are likely to decrease investor confidence, which negatively impacts future investment and growth rates in U.S. industries. The variable "Investor Confidence" can be measured by examining the following: the amount of publicity, the length of resolution, and the quantity of company-investor communication.

The amount of publicity is defined as the information made public by the Department of Justice, the company, the defendant (defendant's spokesperson), or any other entity. The assumption is that an increased exposure to publicity causes the investor's perceived risk to increase. A higher perceived risk lowers overall investor confidence because it creates a negative and uncertain investment environment. The amount of publicity is measured by the number of news releases on the economic espionage incident produced by nationally accredited media sources. The amount of publicity can be measured by examining the following: the number of news releases on the economic espionage incident, the distribution of news releases by sources, and the frequency of news releases given major milestones in the case.

---

[110] Barron's Confidence Index is an indicator used to gauge investors' confidence based on how much investors are investing in a speculative grade of bonds. When investors are optimistic about the market, they tend to invest in high-quality bonds, but when they are worried about the market they invest in lower-quality bonds. This indicator is calculated by dividing the average yield on 10 high-grade bonds by the average yield on 10 intermediate-grade bonds. The difference between the two is used to determine investors' confidence.
InvestorWords. <http://www.investorwords.com/7494/Barrons_Confidence_Index.html>. (accessed April 17, 2010).

[111] Standard & Poor's Confidence Indicator is used in the securities markets and is calculated by constructing an index of low-priced to high-grade common stock. A rising index indicates increased investor willingness to assume risk, which indicates increased investor confidence.
The Free Dictionary <http://financial-dictionary.freedictionary.com/Standard+&+Poor's+500.>.
(accessed April 17, 2010).

[112] Chris Carr and Larry Gorman. 2001. "The Re-Victimization of Companies by the Stock Market Who Report Trade Secret Theft under the Economic Espionage Act." *The Business Lawyer* 57(1).

[113] Ibid.

[114] The expected stock return on a specific day is determined through a statistical comparison between the historical values of pre-event stock returns and an established benchmark for returns, usually determined by Standard & Poor's 500 stock index.
Chris Carr and Larry Gorman. 2001. "The Re-Victimization of Companies by the Stock Market Who Report Trade Secret Theft under the Economic Espionage Act." *The Business Lawyer* 57(1).2001. "The Revictimization of Companies by the Stock Market who Report Trade Secret Theft Under the Economic Espionage Act." The Business Lawyer 57:1.

The length of resolution is defined as the amount of time between when the incident is made public by the Department of Justice and when the case is closed by the federal court system. The assumption is that a longer amount of time before a resolution is reached causes an investor's perceived risk to increase. A higher perceived risk lowers overall investor confidence because it increases the level of uncertainty for investors.

The quantity of company-investor communication is defined as the company's ability to mitigate the incident by providing investors with symmetrical information on the economic espionage incident. The assumption is that the less information directly provided to investors by the company causes an investor's perceived risk to increase. A higher perceived risk lowers overall investor confidence because it decreases trust between investors and the company as well as increases the level of uncertainty for investors. The quantity of company-investor communication is measured by the frequency of communication, as related to the economic espionage incident, between the company and investors. The quantity of company-investor communication can be measured by examining the length of time between the company learning of the incident and informing investors of the incident and the number of formal communications (letters, memos, conference calls, emails, reports, and others) made by the company with investors.

The inability to talk to private companies that are not traded on the stock market precluded the researchers from linking a decrease in investor confidence with an incident of economic espionage. The relationship is not provable, as it contains many immeasurable variables.

Company Rationale:
The variable "Company Rationale" can be defined as a company's decision to report an incident of economic espionage to the FBI. It is assumed that companies would be less inclined to notify the FBI of an incident of economic espionage because public knowledge of an incident is likely to harm investor confidence.

Following a company becoming aware of an economic espionage incident, an in-house damage assessment of the theft is typically conducted. During the damage assessment, the company will determine the probability of the incident leaking to the public without the company's consent. If the theft becomes public without the company's consent, the firm could suffer a damaged reputation because it implies an attempted "cover-up" of the incident. The damage to a company's reputation and subsequent consequence to the company's investor confidence will need to be weighed against the likelihood of the theft leaking to the public. However, this relationship is not measurable because there are too many externalities to conclude the existence of a causal relationship between the variables.

Additionally, an incident of economic espionage may be investigated by the FBI without the company's consent. An instance like this is likely to occur when the incident is reported to the FBI by a third party, or an individual who is neither an employee of the company nor the thief of the trade secret.

Furthermore, a company's rationale differs depending on whether the company is publically traded or private. A publically traded company, or a company that is traded on the stock market,

is more sensitive to its public image because the public image influences levels of investment. Therefore, a public company would be more inclined to maintain the confidentiality of an incident of economic espionage. On the other hand, a private company would be more likely to make the incident public. A private company, or one that is not traded on the stock market, has a smaller pool of investors. Therefore, it is much easier for the company to inform investors of the incident. Both public and private companies may also desire restitution as a product of a civil trial, incentivizing the company to make the incident known.

While the characteristics of the company are important, the frequency of incidents of economic espionage will be more influential in a company's decision to inform FBI. It can be assumed that a company's decision to declare a theft would demonstrate the severity of an incident, and the associated publicity of the incident would deter future thefts. Past experiences with incidents of economic espionage may make it more difficult for a company to maintain the confidentiality of the incident. Also, it could be necessary for the company to improve security measures and prevent similar incidents from occurring by allowing a federal investigation and prosecution of the incident, or by consulting with a private security company.

Introduction:
This model calculates the economic consequence of espionage based upon four key variables, which indicate the magnitude of loss. These four key variables include: the industry in which the theft occurred, the characteristics of the theft, the cost, and the characteristics of the beneficiary country.

Overview of Variables:

(1) Industry

The 'Industry' variable consists of measurements that represent 14 sectors of the U.S. economy, excluding the government and public sector. Depending upon the nature of the company targeted and the specifics of the espionage incident, several economic sectors may be impacted. However, the user of this model should indicate the single industry that would receive the greatest impact from the incident.

(2) Characteristics of the Theft

The 'Characteristics of the Theft' variable is a conclusive measure of the scope of the attack, the network impact, and the placement of the thief/thieves. The Characteristics of the Theft identify key factors that influenced the impact of the theft on the company including scope of attack, network impact, and placement of the thief/thieves.

(3) Cost

The 'Cost' variable includes measurements that consider the resources and monetary commitment the company previously invested into the stolen material. This variable also considers factors that could improve or worsen the direct costs of the espionage incident. The Cost variable is measured by examining stage of production, time spent in R&D, complete loss, product produced under high security, and restitution paid.

(4) Beneficiary

The 'Beneficiary' variable includes measurements that consider the foreign entity, the destination of the stolen materials, and the impact the beneficiary has on the overall costs of the incident. Using values from independent sources and country characteristics, an estimate of a country's production potential is produced. This category recognizes that certain countries, regardless of the value of the stolen material they may acquire, are incapable of utilizing certain materials in a way that would compete with the U.S. economy.

User Manual Instructions:

Scale for Assigning Values

The process of assigning values consists of the user identifying the key industry affected by the incident and then assigning values to each of the subset variables applicable to the given case. A value of unknown/non-applicable, 0, 1, 2, or 3 should be assigned to each applicable variable within the subset. Irrelevant or indeterminate variables within the subset should be assigned a value of 0. Unknown or non-applicable should be assigned to variables where the information is either unknown or non-applicable to the case. The valuation of the scale should be based upon the following criteria:

(1) Industry

Select the industry affected by the espionage incident. In the event that several industries were affected, select the industry which suffered the greatest economic loss.

1. Agriculture:
Farms and Forestry, fishing, hunting, and related activities.
2. Mining:
Oil and gas extraction, Mining (except oil and gas), and Support activities for mining
3. Utilities:
4. Construction:
5. Manufacturing: (divided into two sections: Durable and Nondurable Goods)
A. Durable Goods:
Wood products, Nonmetallic mineral products; Primary metals; Fabricated metal products; Machinery; Computer and electronic products; Electrical equipment; appliances and components; Motor vehicles, bodies and trailers, and parts; Other transportation equipment; Furniture and related products; and Miscellaneous manufacturing
B. Nondurable Goods:
Food and beverage and tobacco products; Textile mills and textile product mills; Apparel and leather and allied products; Paper products; Printing and related support activities; Petroleum and coal products; Chemical products; Plastics and rubber products
6. Wholesale Trade:
7. Retail Trade:
8. Transportation and Warehousing:
Air transportation; Rail transportation; Water transportation; Truck transportation; Transit and ground passenger transportation; Pipeline transportation; Other transportation and support activities; Warehousing and storage
9. Information:
Publishing industries (includes software); Motion picture and sound recording industries; Broadcasting and telecommunications; Information and data processing services
10. Finance, Insurance, Real Estate, Rental, and Leasing:
A. Finance and insurance:
Federal Reserve banks, credit intermediation, and related activities; Securities, commodity contracts, and investments; Insurance carriers and related activities; Funds, trusts, and other financial vehicles
B. Real estate and rental and leasing:
Real estate; Rental and leasing services and lenders of intangible assets
11. Professional and Business Services:
A. Professional, scientific, and technical services:
Legal services; Computer systems design and related services; Miscellaneous professional, scientific, and technical services
B. Management of companies and enterprises.
C. Administrative and waste management services:
Administrative and support services; Waste management and remediation services
12. Educational services, health care, and social assistance:
A. Health care and social assistance, Includes:
Ambulatory health care services; Hospitals and nursing and residential care facilities; Social assistance
13. Arts, entertainment, recreation, accommodation, and food services:
A. Arts, entertainment, and recreation:
Performing arts, spectator sports, museums, and related activities; Amusements, gambling, and recreation industries
B. Accommodation and food services:
Accommodation; Food services and drinking places
14. Other Services: (except government)

(2) Characteristics of the Theft

Rank the following factors' relevance to the incident of economic espionage.

Scope of the theft?

Scope can be defined as the range of impact the theft had on the firm in terms of tangible and intangible damages.

- The scope of the theft is unknown or not applicable.
0. There was an attempted theft, which was unsuccessful.
1. There was a theft, which had limited targeting. The theft may have caused minimal damage.
2. The theft targeted a moderate level of information. The theft may have caused significant damage to the company.
3. The theft targeted a large quantity of information. The degree of compromise may be catastrophic.

Information Network impact?

Information Network impact can be defined as any theft in which a company's server and/or electronic network system is affected.

- The level of information network impact is unknown or not applicable.
0. The theft did not impact the information network.
1. The theft had a minimal impact on the information network. Other users were either unaffected or only minimally inconvenienced.
2. The theft had a moderate level of impact. A larger number of users may be affected and repair costs may be significant.
3. The theft had a high level of impact. The information network was severely damaged, affecting a large number of users and repair costs were extremely high.

Placement of the Thief/Thieves?

Placement of the Thief/Thieves can be defined as an internal actor, external actor, or both internal and external. An internal actor is an individual who is employed by the company. An external actor is a non-employee of the company. A combination of both an internal and external actor includes at least one individual who is an employee of the company and at least one individual who is a non-employee of the company.

1. The placement of the thief/thieves constitutes an external actor.
2. The placement of the thief/thieves constitutes an internal actor.
3. The placement of the thieves constitutes a combination of an internal actor(s) and an external actor(s).

(3) Cost

Rank the following factors relevance to the incident of economic espionage.

Stage of Production.

Stage of Production can be defined by the three key stages: planning, R&D, and production, under which a product is developed. The planning stage allows a small and controlled group of employees and researches to formulate ideas and plans. The R&D stage consists of the research and development of a product or information. The production phase is the manufacturing of a product or information.

- The specific stage of production is unknown or not applicable.

1. The process/product was stolen during the planning stage.
2. The process/product was stolen during the research and development stage.
3. The process/product was stolen during the finalized production stage.

Time Spent in Research and Development (R&D)?

Time Spent in R&D can be defined as the amount of time a product or information spent in the research and development stage of production. It is reasonable to assume a positive correlation between the length of time a product is in the R&D stage and the overall production costs.

- Time spent in R&D is unknown or not applicable

0. There was no time spent in R&D.
1. The time spent in R&D is less than 1 year.
2. The time spent in R&D is between 1 and 10 years.
3. The time spent in R&D is more than 10 years.

Complete Loss?

Complete Loss can be defined as the amount of the product stolen from the company. A **Complete Loss** is an incident of economic espionage where the total or majority of the product or information is stolen, irretrievable, and used by the beneficiary. A **Minor Loss** can be defined as an incident of economic espionage in which the product or information stolen or compromised is insufficient to allow a beneficiary to reproduce the production or as an incident where the product or information stolen is returned to the company.

- The amount of loss is unknown or not applicable.

0. There was no loss.
1. A negligible portion of the product was stolen and/or the amount stolen is inadequate for the product to be reproduced by a competitor. Or, the majority of the product was recovered.
2. A partial amount of the product was stolen and/or the production cannot be quickly reproduced by a competitor. Or, a partial amount of the product was recovered.
3. A significant majority or the entirety of the product was stolen. The amount stolen is so great that a competitor will be able to reproduce the product quickly.

Product Under High Security?

High Security can be defined as enhanced security measures implemented by the company during the stages of production to protect the value of the product or information.

- It is unknown if the product was produced under high security or not applicable.

0. The product was not under security during its development process.
1. The product had low security during its development process.
2. The product had moderate security during its development process.
3. The product had high security during its development process.

Restitution Paid?

Restitution Paid can be defined as any amount of payment the company receives from the thief/thieves or beneficiary. 'Restitution' assesses the total cost incurred by a company by subtracting the restitution payment from the overall loss the company experienced from the incident.

- It is unknown if restitution was paid or not applicable

1. A high restitution was paid.
2. A moderate restitution was paid.
3. Little restitution was paid.

(4) Intended Beneficiary

Please select the name of the country (or countries) that benefitted or were intended to benefit from the theft.

Bibliography

"About Us." *Lerner Research Institute, Cleveland Clinic Foundation.* <http://www.lerner.ccf.org/info/>. (accessed April 27, 2010).

ASIS 2007. "Trends in Proprietary Information Loss." *Survey Report,* ASIS & National Counterintelligence Executive.

Barkoviak, Michael. "Two Silicon Valley Engineers Receive One-Year Prison Sentences." *Daily Tech.* November 24, 2008. <http://www.dailytech.com/Two+Silicon+Valley+Engineers+Receive+One+Year+Prison+Sentences/article13503.htm>. (accessed April 27, 2010).

"Barron's Confidence Index." *InvestorWords.com.* <http://www.investorwords.com/7494/Barrons_Confidence_Index.html>. (accessed April 17, 2010).

Bellocchi, Luke "Assessing the Effectiveness of the Economic Espionage Act of 1996. *International Journal of Intelligence and Counterintelligence* 14: (July 2001).

Freedom House. "Freedom in the World: Methodology." *Freedom House Online* (2008) n. p. <http://www.freedomhouse.org/template.cfm?page=351&ana_page=341&year=2008>. (accessed April 1, 2010).

Capus, Joseph M.. "Theft of Metaldyne Connecting Rod Technology." Powder Metallurgy 48(1) (2005).

Carr, Chris and Gorman Larry. "The Re-Victimization of Companies by the Stock Market Who Report Trade Secret Theft under the Economic Espionage Act." *The Business Lawyer* 57 (2001).

"Company Profile." *NetLogic Microsystems,* <http://www.netlogicmicro.com/Company/Profile.htm>. (accessed April 27, 2010).

Coskun, Samli A. And Jacobs, Laurence. "Counteracting Global Industrial Espionage: A Damage Control Strategy." *Business and Society Review,* 108, (2001).

Dewitz, Sara, Joseph O'Brien, Timothy Deerr, John Parsons, and Erika Souliere. "Targeting U.S. Technologies: A Trend Analysis of reporting From Defense Industry." *Defense Security Service.* (2008).

"Economic Espionage Act of 1996." 18 U.S.C. 1831-39, 1996.

Felton, Richard. "Caught Out!" *Metal Powder Report* 60(3) (2005).

Freedom House. "Freedom in the World: Methodology." *Freedom House Online* (2008) n. p. <http://www.freedomhouse.org/template.cfm?page=351&ana_page=341&year=2008>. Accessed April 1, 2010.

Flaccus, Gillian. "Engineer Pleads Not Guilty to Spy Charge." *Oakland Tribune*. February 20, 2008.

Gerstein, Josh. "Spy Charges in High-Stakes Microchip Race." *New York Sun*. June 19, 2006. < http://www.nysun.com/national/spy charges-in-high-stakes-microchip-race/34620/>. (accessed April 27, 2010).

Gillis, Justin. "Scientists Accused of Theft; Espionage Alleged Against Japanese." *The Washington Post*. May 10, 2001. < http://www.lexisnexis.com/us/lnacademic/search/homesubmitForm.do>. (accessed April 28, 2010).

Kramer, Lisa A. And Heuer, Richard J. Jr. "America's Increased Vulnerability to Insider Espionage." *International Journal of Intelligence and CounterIntelligence* 20, (2007).

Lampinen, Megan. "Former Metaldyne Employees Plead Guilty to Information Theft." *Automotive World* (2008).

Levine, Dan. "Defense Blames Chinese Espionage Case on Neglected Wife." *Law.Com*. October 22, 2009. <http://www.law.com/jsp/law/international/LawArticleIntl.jsp?id=1202434866919> (accessed April 27, 2010).

Levine, Dan. "DOJ's Economic-Spy Strategy Emerges." *The Recorder*. May 5, 2008. < http://www.law.com/jsp/law/international/LawArticleIntl.jsp?id=1202421126406> (accessed April 27, 2010).

Levine, Dan. "Rare Economic Espionage Case Filled with Quirks." *Law.Com*. October 20, 2009. < http://www.law.com/jsp/law/LawArticleFriendly.jsp?id=1202434787775>, (accessed April 27, 2010).

Lewis, Jonathan Eric. "The Economic Espionage Act and the Threat of Chinese Economic Espionage in the U.S." University of Connecticut, School of Law.

Lynch David J. "FBI Goes on Offensive vs. Tech Spies." *USA Today*, July 24, 2007. <http://www.usatoday.com/money/world/2007-07-23-china-spy-2_N.htm>. (accessed May 1, 2010).

Memorandum of Plea Agreement, United States District Court, District of Delaware. November 13, 2006. <http://www.usatoday.com/money/world/min-plea-agreement.pdf>. (accessed April 27, 2010).

Mintz, Howard. "Silicon Valley Espionage Case Only Second of Kind in Nation to go to Trial." *San Mercury News*. October 18, 2009. <http://it.tmcnet.com/news/2009/10/19/4432100.htm>. (accessed April 30, 2010).

Office of the National Counterintelligence Executive. "Annual Report to Congress on the Foreign Economic Collection and Industrial Espionage," FY 2008, July 23, 2009.

O'Sullivan, Sean. "DuPont Charges Industrial Espionage Employee Accused of Plotting to Take Secret Data to China." *The News Journal*, (2009). <http://www.mainefairtrade.org/pdf/DuPont%20charges%20industrial%20espionage.pdf> .(accessed April 27, 2010).

O'Sullivan, Sean. "Industrial Espionage Case Reads Like Spy Thriller." *The News Journal*. February 16, 2007. <http://66.84.23.86/node/4640>.

Parrella, Matthew A. Assistant U.S. Attorney and Chief of Computer Hacking/Intellectual Property (CHIP) Unit Conducted (personal communication via phone interview, March 4, 2010).

Rantala, Ramona R. "Cybercrime Against Businesses 2005." *Bureau of Justice Statistics Special Report, U.S. Department of Justice*. (2008).

Reisch, Marc. "Chemist Charged With Crime." *Chemical and Engineering News* 87(41) (2009).

Robertson, Jordan. "Economic Espionage Case Ends in Jury Deadlock." *USA Today*. November 24, 2009. < http://www.usatoday.com/tech/news/2009-11-24-china-net-logic_N.htm>.

Robertson, Jordan. "Rare Economic Espionage Case Going to Trail". *USA Today*. October 21, 2009.

Roberston, Jordan. "Engineers sentenced to 1 year for espionage case." *Associated Press.* November 21, 2008. <http://www.google.com/hostednews/ap/article/ALeqM5jlbm2BCyrbel-HLKe2lO_Mo48-PQD94JI3A00>.

Rustmann Jr., F.W. *CIA, Inc. Espionage and the Craft of Business Intelligence*. Potomac Books Inc., 2002.

Sala-I-Martin, Xavier, et al. "The Global Competitiveness Report." *World Economic Forum 2009-2010 Report* (2009): 3. <http://www.weforum.org/pdf/GCR09/GCR20092010fullreport.pdf>. (accessed April 1, 2010).

Serrano, Richard A. and Reza, H.G. "O.C. Man Accused of Being a Spy." *Los Angeles Times*. February 12, 2008. http://articles.latimes.com/2008/feb/12/nation/na-espionage12/3 (accessed May 1, 2010).

"Standard and Poor's 500 Index." *TheFreeDictionary.com*. <http://financial-dictionary.thefreedictionary.com/Standard+&+Poor's+500>. (accessed April 17, 2010).

Taylor, Collen. "Two Charged with Conspiracy to Commit Economic Espionage." *Electronic News*. September 27, 2007. <http://www.edn.com/article/CA6483922.html?text=>. (accessed April 28, 2010).

Thapa, Shyam. "The Human Development Index: A Portrait of the 75 Districts in Nepal." *Asia-Pacific Population Journal* 10, 2 (1995): 3-14. United Nations Website. <http://www.un.org/Depts/escap/pop/journal/v10n2a1.htm>. (accessed April 1, 2010).

Unknown. "Accused Doctor Sues Govt for 43 mil. Yen over Detention." *The Daily Yomiuri*. August 26, 2004. <http://www.lexisnexis.com/us/lnacademic/search/homesubmitForm.do>. (accessed April 28, 2010).

Unknown. "DNA Plea-bargain Brings Probation." *The Daily Yomiuri*. May 30, 2003, <http://www.lexisnexis.com/us/lnacademic/search/homesubmitForm.do>. (accessed April 28, 2010).

Unknown. "Internal Report Suggests Gene Samples Lifted from U.S." *The Nikkei Weekly*. June 11, 2001.

Unknown. "Riken Plans In-house Probe." *The Daily Yomiuri*. May 11, 2001. <http://www.lexisnexis.com/us/lnacademic/search/homesubmitForm.do>. (accessed April 28, 2010).

Unknown. "Scientist 'Seen Taking Gene Samples'". *The Daily Yomiuri*. July 2, 2001. <http://www.lexisnexis.com/us/lnacademic/search/homesubmitForm.do>. (accessed April 28, 2010).

U.S. Attorney General's Office. "Economic Espionage and Trade Secret Theft: Defending Against the Pickpockets of the New Millennium." *The 2002 Annual Report to Congress on Foreign Economic Espionage and Industrial Espionage,* (2002).

U.S. Congressional Research Service. "The Economic Impact of Cyber-Attacks," (RL32331; April 1, 2004) Brian Cashell, et al.

U.S. Department of Justice. "First Foreign Economic Espionage Indictment; Defendants Steal Trade Secrets from Cleveland Clinic Foundation." *United States Attorney Northern District of Ohio.* May 8, 2001. <http://www.justice.gov/criminal/cybercrime/Okamoto_SerizawaIndict.htm>. (accessed April 27, 2010).

U.S. Department of Justice Press Release. "Former Boeing Engineer Charged with Economic Espionage in Theft of Space Shuttle Secrets for China." *U.S. Department of Justice*, February 11, 2008. <http://www.usdoj.gov/criminal/cybercrime/chungCharge.htm>. (accessed April 27, 2010).

U.S. Federal Bureau of Investigation. "Former Boeing Engineer Sentenced to Nearly 16 Years in Prison for Stealing Aerospace Secrets for China." *Department of Justice Press Release*, February 8, 2010 (accessed March 24, 2010). <http://losangeles.fbi.gov/dojpressrel/pressrel10/la020810.htm>.

U.S. Department of Justice. "Former Chinese National Charged with Stealing Military Application Trade Secrets from Silicon Valley Firm to Benefit Governments of Thailand, Malaysia, and China." *U.S. Attorney Northern District of California.* December 14, 2006. <http://www.justice.gov/criminal/cybercrime/mengCharge.htm>. (accessed April 27, 2010).

U.S. Department of Justice. "Former DuPont Chemist Charged: Dr Hong Meng Accused of Unauthorized Computer Access of OLED Technology." October 2, 2009. <http://www.justice.gov/criminal/cybercrime/mengChar.pdf>. (accessed April 27, 2010).

U.S. Department of Justice. "Former Metaldyne Employees Sentenced to Prison in Conspiracy to Steal Confidential Business Information to Benefit Chinese Competitor." *U.S. Department of Justice*. February 13, 2009. <http://www.justice.gov/criminal/cybercrime/lockwoodSent2.pdf>. (accessed April 27, 2010).

U.S. Department of Justice, "Guilty Plea in Trade Secrets Case." *United States Attorney's Office District of Delaware*. February 15, 2007. <http://www.justice.gov/criminal/cybercrime/minPlea.pdf>. (accessed April 27, 2010).

U.S. Federal Bureau of Investigation, *Investigative Program Counterintelligence Division: Focus on Economic Espionage*. <http://www.fbi.gov/hq/ci/economic.htm>. (accessed April 27, 2010).

U.S. Department of Justice. "Pair from Cupertino and San Jose, California, Indicted for Economic Espionage and Theft of Trade Secrets From Silicon Valley Companies." *U.S. Attorney Northern District of California*. December 4, 2002. <http://www.justice.gov/criminal/cybercrime/yeIndict.htm >. (accessed April 27, 2010).

U.S. Department of Justice. "Two Bay Area Men Indicted on Charges of Economic Espionage." *Department of Justice Press Release*. September 26, 2007. < http://www.justice.gov/criminal/cybercrime/liIndict.htm>. (accessed April 27, 2010).

Department of Transportation, Federal Aviation Association, 8040.4, Appendix 1, June 26, 1998. <http://www.faa.gov/library/manuals/aviation/risk_management/ss_handbook/media/app_g_1200.PDF>. (accessed May 1, 2010).

Vijayan, Jaikumar. "DuPont Scientist Admits Downloading, Stealing $400M Worth of Trade Secrets." *Computerworld*. February 15, 2007. <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9011367>. (accessed April 27, 2010).

Vijayan, Jaikumar. "Trial to Begin in Economic Espionage Case Involving China." *Computerworld*. October 21, 2009. <http://www.computerworld.com.au/article/323000/trial_begin_economic_espionage_case_involving_china/>. (accessed April 27, 2010).

Zwillinger, Marc J. and Genetski, Christian S. "Calculating Loss Under the Economic Espionage Act of 1996." *George Mason Law Review* 323, (2001).