

Cyber Defense Resources & Vulnerabilities



Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University



Josephine Wolff, PhD Candidate

Start: September 2010

Research Group: Advanced Network Architecture Group in CSAIL; Explorations in Cyber International Relations, MIT-Harvard

Thesis Advisor: Dr. D. Clark, Senior Research Scientist at CSAIL

Workshop on

Who Controls Cyberspace?

MIT, November 6 and 7, 2012

Problem	Proposed Research	Expected Contributions
<p>Investment in security is aimed at reducing losses due to security breaches and typically determined by calculating annualized loss expectancy (ALE) metrics. However, in the cybersecurity space there is inadequate data on the frequency of breaches, the costs associated with those breaches, and the effectiveness of countermeasures, for organizations to be able to perform meaningful ALE calculations. With rising rates of both IT security spending and online attacks, surveys indicate that many business and government executives are unsure of how to allocate resources for defense and whether their investments in security measures are making any</p>	<h3 style="text-align: center;">Investment in Cyber Defense Measures</h3> <div style="text-align: center;"> </div> <p style="font-size: small;">Source: Rowe, B. & Gallaher, M. (2006) "Private Sector Cyber Security Investment Strategies: An Empirical Analysis." Film Workshop on the Economics of Information Security.</p>	<ul style="list-style-type: none"> • Comparative analysis of the processes by which different private companies and government agencies decide how to allocate resources for defense against cyber attacks and information security breaches and methods used to assess the effectiveness of those allocations • Characterization of the different elements involved in defense against cyber attacks • Assessment of where and how different types of organizations ultimately end up spending their resources for defense • Mapping of defense resource allocations onto a taxonomy for distinguishing between different types of attacks by understanding how well they have been defended against
<h3>Key Questions</h3>	<p>Qualitative case studies enable analysis of <i>how</i> organizations make decisions about whether or not to invest in specific cyber defenses — what drives these decisions, who makes them, and how budgets are determined — as well as <i>what</i> the final defense outcomes of these decisions are and what defense measures are ultimately implemented.</p>	<h3>Literature Review</h3>
<ul style="list-style-type: none"> • How do private and public organizations make decisions about allocating resources for defense against cyber attacks, malware and online abuse and how do they assess whether those decisions were worthwhile or successful? • Where do private organizations and government agencies ultimately end up allocating these resources? • How can a deeper understanding of the different factors that contribute to defense decisions map onto a new understanding of different categories of attacks and vulnerabilities? 	<h3 style="text-align: center;">Defense-Based Taxonomy of Attacks</h3>	<p>Gordon & Loeb (2006) found that less than 25% of firms reported using economic analysis to inform investments in information security, while an earlier survey found that many firms employ a “wait-and-see” approach, deferring investments in online security until after their systems are breached (Gordon et al., 2003). Rowe & Gallaher (2006) identified several factors driving firms’ investment in information security, but little work has been done to understand how these decisions are made or characterize the resulting cyber defense landscape.</p>
<h3>Methods</h3>	<p>Cyber attacks have been classified according to a variety of different elements, including:</p> <ul style="list-style-type: none"> • Motivation • Technique • Target <div style="display: flex; justify-content: space-around;"> <div data-bbox="869 1727 1342 1992"> </div> <div data-bbox="1342 1573 1693 1992"> </div> <div data-bbox="1693 1492 2136 1727"> </div> </div> <p>However, a crucial determinant of an attack’s success is the extent to which it has been anticipated and protected against, factors that are not incorporated into most existing attack taxonomies.</p>	<h3>Funding Acknowledgment</h3>
<p><u>Comparative Case Studies & Interviews:</u></p> <ul style="list-style-type: none"> • Case studies of defense resources allocated by private companies in different sectors and government agencies, including U.S. Cyber Command and the Department of Homeland Security <p><u>Process Tracing:</u></p> <ul style="list-style-type: none"> • Analysis of decision-making processes for implementing defense measures <p><u>Document Analysis:</u></p> <ul style="list-style-type: none"> • Assessment of formal documents used for outlining defense strategies and metrics 	<p>This work is funded by the Office of Naval Research under award number N00014-09-1-0597. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author and do not necessarily reflect the views of the Office of Naval Research.</p>	