2012-12

Offense-defense balance in cyberspace: a proposed model

Malone, Patrick J.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

OFFENSE-DEFENSE BALANCE IN CYBERSPACE: A PROPOSED MODEL

by

Patrick J. Malone

December 2012

Thesis Advisor: Dorothy Denning
Second Reader: Leo Blanken

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2012	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE OFFENSE-DEFENSE BALANCE IN CYBERSPACE: A PROPOSED MODEL		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Patrick J. Malone			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

The offense-defense balance is an indicator of the conflict dynamic in a system. Cyberspace is a domain where offense-defense costs are clearer than in the physical world. While there have been numerous comments about the current balance there has not been a study conducted. In this thesis, I use a heuristic model to show what the current theoretical balance point is, and what it was for two different case studies, Estonia in 2007 and Stuxnet.

Based on the data, the cost of one dollar by the attacker spent on offense, the defender spends $1.32. When looked at from an aggregate perspective, using the data from the model, attackers to defenders, the disparity is significantly larger, with a one dollar to $131 cost ratio. The Estonia case study had a one dollar to $424 cost ratio, and Stuxnet had a one dollar to seven dollar ratio.

This proposed model may provide a glimpse of what the current balance is for a specific system. Using this model, it may be possible to provide measures of effectiveness for modifications made to the system, which could help mitigate costs for cyber defenders.

14. SUBJECT TERMS Offense, Defense, Cyberspace, Cyberattack, Cyberdefense, Estonia, Stuxnet, offense-defense balance,			**15. NUMBER OF PAGES** 101
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

OFFENSE-DEFENSE BALANCE IN CYBERSPACE: A PROPOSED MODEL

Patrick J. Malone
Major, United States Army
B.S., University of Arizona, 1998

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
December 2012

Author: Patrick J. Malone

Approved by: Dr. Dorothy Denning
Thesis Advisor

Dr. Leo Blanken
Second Reader

Dr. John Arquilla
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The offense-defense balance is an indicator of the conflict dynamic in a system. Cyberspace is a domain where offense-defense costs are clearer than in the physical world. While there have been numerous comments about the current balance there has not been a study conducted. In this thesis, I use a heuristic model to show what the current theoretical balance point is, and what it was for two different case studies, Estonia in 2007 and Stuxnet.

Based on the data, the cost of one dollar by the attacker spent on offense, the defender spends $1.32. When looked at from an aggregate perspective, using the data from the model, attackers to defenders, the disparity is significantly larger, with a one dollar to $131 cost ratio. The Estonia case study had a one dollar to $424 cost ratio, and Stuxnet had a one dollar to seven dollar ratio.

This proposed model may provide a glimpse of what the current balance is for a specific system. Using this model, it may be possible to provide measures of effectiveness for modifications made to the system, which could help mitigate costs for cyber defenders.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACL	Access Control List
CPU	Central Processing Unit
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoD	United States Department of Defense
DoE	United States Department of Energy
DoJ	United States Department of Justice
DMZ	Demilitarized Zone
€	Euro (Currency)
FBI	United States Federal Bureau of Investigation
FCC	United States Federal Communications Commission
GDP	Gross Domestic Product
GHz	GigaHertz
GUI	Graphical User Interface
IC3	Internet Crime Complaint Center
IP	Internet Protocol
IPEC	Intellectual Property Enforcement Coordinator
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
ISP	Internet Service Provider
IT	Information Technology
ITSR	Internet Threat Security Report
KR	Estonian Kroon (Currency)
Mbps	Mega Bits Per Second
NASA	United States National Aeronautics and Space Administration
NNSA	United States National Nuclear Security Administration
OBI	Omnibus Broadband Initiative
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition

SEB	As SEB Pank
SQL	Structured Query Language
SSL	Secure Socket Layer
SYN	Synchronization
USD	United States Dollars
UTM	Unified Threat Management System
VPN	Virtual Private Network

ACKNOWLEDGMENTS

To my wife and family for their love, support and understanding during this process

Brandy and Alex Malone

To my advisors for their guidance, mentoring and patience

Dr. Dorothy Denning

Dr. Leo Blanken

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

In July of 2011, the United States Department of Defense (DoD) published an unclassified cyber strategy, the purpose of which was to explain how the U.S. military's vision of cyberspace opportunities and threats would be met. The strategy outlines 5 steps that would be taken to allow the DoD to "effectively operate in cyberspace."

It is interesting to note that of the five DoD proposed steps, three of them are focused entirely on cyber security or defense. In a 2012 executive report by the Cyber Conflict Studies Association discussing the research it has conducted on cyberspace, it is noted that cyberspace is currently unstable and dangerous and that there is no good solution to reducing conflict in cyberspace.[1] Martin Libicki, a noted authority on technology and national security, argues that cyber warfare is too uncertain and that a highly technological society should attempt to avoid becoming embroiled in it in order to minimize its own risk.[2] While this is an ideal solution, the question arises whether it is even possible to avoid the conflict in cyberspace.

The United States is focusing immense efforts on defending their military networks. Although numerous experts voice concerns over the conflict, what is left out of the discussion is to what degree it is a problem. One method to determine the degree of conflict in the system is offense-defense balance theory.

George Quester, in 1977, proposed the offense-defense theory which states that the number of conflicts in the international system will increase when offense is cheaper than defense.[3] This theory has several critics, with the primary argument focusing on the

1 Dr. James C. Mulvenon, and Dr. Rattray J. Gregory, Addressing Cyber Instability: Executive Summary, Executive Summary, Washington, DC: Cyber Conflict Studies Association, 2012.

2 Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009).

3 George H. Quester, *Offense and Defense in the International System*, (New York, N.Y.: John Wiley and Sons, 1977).

difficulty of operationalizing the theories implications for testing, because in the physical world it is extremely difficult to discern what an offensive weapon is and what a defensive weapon is.

In cyberspace, the problems with identification of offensive and defensive weapons are reduced. This paper proposes a cost model to analyze the offense-defense balance in cyberspace. This proposed balance point would indicate the extent of the problem of conflict in the system. It would also provide a possible measure of effectiveness to various attempted conflict resolutions in cyberspace, giving a means to judge the success of attempted solutions.

B. OBJECTIVES

The objective of this thesis is to build an effective model of the cyber offense-defense balance in order to provide a means to discern the conflict balance point in cyberspace at a given time. The proposed model framework is designed to provide a snapshot in time based on current costs. The model uses current high, low, and average costs for personnel, hardware and software systems in order to provide a range as well as an average midpoint solution.

Using the theoretical model, data from two case studies will be analyzed in order to provide a real world perspective. Specifically, the proposed methodology will be used to discern the offense-defense balance for each of the two conflicts.

C. METHODOLOGY

Overall methodology uses a heuristic method combining empirical data and specific case studies. From the proposed model a theoretical range of offense-defense balance costs are derived as well as a specific balance point for the case studies. From the offense-defense balance points some analysis is made both on what the data shows as well as further research necessary.

The heuristic model will use empirical data gained from current costs of various cyber sub-systems. The focus is on specific offense and defense hardware and software, as well as the personnel who conduct attack and defense. The model is designed to

provide a look at current specific costs by sub-system in order to provide a range of high and low cost options. Using the range of high and low costs, a midpoint cost can be derived for offense and defense. By analyzing the cost ratio between offense and defense, a balance point can be determined. This balance point is an indicator of the theoretical current offense-defense balance in cyberspace.

Using the model, two case studies, one involving the 2007 cyber-attacks against Estonia and the other Stuxnet, will be analyzed to determine their offense-defense ratios. Both case studies will estimate the actual costs for both the attackers and defenders in order to determine their offense-defense ratios and compare them to the theoretical model.

There are several limitations to using this proposed methodology. It can be argued that the data feeding the model is inaccurate. Personnel costs, system management costs, and physical security costs have all been assumed, further data would make these areas more accurate. There are several examples of prices and costs in both case studies, that are estimations which might with further information provide a more accurate offense-defense ratio. Additionally, the methodology assumes specific offensive and defensive system setups in order to compare costs, however allowing for and researching more types of system configurations might provide more accuracy in the model.

Chapter II of the thesis gives background on offense-defense balance theory. Chapter III describes the theoretical framework introduced in this thesis for computing the offense-defense cost ratio for cyber-attacks, while Chapter IV discusses specific case studies. Chapter V concludes.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

A. OFFENSE-DEFENSE BALANCE THEORY

Offense-defense balance theory is a proposition that the onset of international conflicts can be explained and predicted by comparing the relationship of the cost balance between offensive and defensive operations. Robert Jervis proposed that states that had less risk of being exploited were more likely to be at peace and less likely to threaten their neighbors.[4]

Put in the simplest possible terms, conflicts will tend to increase when the costs of offensive operations are less than the cost of defending against them. Put another way, if defensive operations are dominant (or easier to apply), it is less costly to defend than to attack, and according to the theory, countries are more likely to be at peace, if all other factors are close to being equal.

Offense-defense theory remains extremely controversial today, with, successful critical attacks on several levels. However, these critiques usually center around two primary axes, first, the difficulty of categorizing weapons or systems as offensive or defensive, and second, the historical argument for the pre-eminence of defense over offense.

The first, and primary, critique of the theory is based on the difficulty of determining whether a weapon, system, or other hardware should be considered offensive or defensive in application. Depending on use, it appears that any weapon could be either.[5]

Obviously, designing a weapon for one side of the balance does not limit the use of that weapon. For example, in WWII the Germans had an anti-aircraft gun (thus primarily defensive), the 88 mm, that for a number of reasons became a good anti-tank

4 Robert Jervis, "Cooperation under the Security Dilemma," *World Politics* 30, no. 2 (1978): 167–214.

5 Jack S. Levy, "The Offensive/Defensive Balance of Military Technology: A Theoretical and Historical Analysis," *International Studies Quarterly* 28, no. 2 (1984): 219–238.

and anti-infantry weapon, which enabled it to be used on the offensive in major operations. In spite of its initial design purpose, the system became an outstanding weapon on both sides of the balance.

Based on examples such as this, and many more throughout military history, this critical argument then becomes that it is impossible, or at least extremely difficult, to decide when, where, and in which direction the balance will tilt, leaving the theory limited in application and difficult to analyze.

The second powerful argument opposing the theory revolves around a central tenet of military analysis that history clearly shows, and military studies clearly state, that all other things being equal defense is always favored over offense. As Clausewitz said, "Defense is the stronger form of war."[6]

This argument is much weaker, in my opinion, for a number of reasons. First, without getting into enormous detail, it has become a firmly held military belief that the attackers should 'outnumber' defenders at the ratio of three to one.[7]Although historical and theoretical studies have set this rule of thumb almost in concrete, this assumes similarity in the unit types (ground attacks) in the physical world, and therefore does not invalidate the theory.

Essentially, although the 3 to 1 argument has validity in many situations, it does not follow that this is always the case. Mainly the argument simply is a good planning factor when attacking prepared defensive positions. Many factors can outweigh this argument, including surprise, maneuver, and superior personnel or equipment. Additionally, this argument primarily applies specifically to ground force operations.

However, even with weakness of the defense over offense argument, it still leaves the theory, with limited application in any real world situation. As a matter of fact, the arguments for the theory have tended to be applied only in vague international arenas and not in any useful fashion. Despite its shortcomings, offense-defense theory remains a

6 Carl V. Clausewitz, *On War*. 1984. Edited by Michael Howard and Peter Paret, Translated by Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 69.

7 John J. Mearsheimer, "Assessing the Conventional Balance: The 3:1 Rule and Its Critics," *International Security* 13, no. 4 (1989): 54–89.

useful heuristic tool for examining conflict and, in particular, may provide a conceptual tool for analysis of emerging arenas of conflict.

B. CYBERSPACE APPLICATION

In the last 30 years, a new area of conflict has emerged. Computer technology used for communication, calculation and direct military operations (cyberspace) seems to provide the possibility of insight into and clarification of the offense-defense balance theory, with some possibility of real world applications.

First, the confusion between the application of offense or defense to weapons systems is greatly reduced within the Cyberspace realm. Programs are specifically developed for particular purposes, and, barring unintended consequences (or poorly written code), it is easy to determine the offense/defense nature of the program. The written code describes exactly what it will do and what it is to accomplish. A program code written to attack or exploit another system cannot be used to defend itself or another system.

This clarity of purpose is somewhat reduced by the concept of reconnaissance tools in cyberspace and the use of those tools for both offense and defense. However, reconnaissance tools are just that, reconnaissance and are not themselves an attack or defense. It is possible for a reconnaissance tool, such as packet sniffer, to get a password transmitted in the clear. This password would then allow an attacker into the network. It is clear that the possibility of damage exists from “reconnaissance.” However, the reconnaissance itself is not an attack.

Second, in cyberspace, any ratio of necessary attack versus defense forces has yet to be, and may be impossible to be, defined. It may be that offense is actually more powerful (easier to apply, or cheaper to apply) than defense. Gary McKinnon, an individual using the Internet and his personal computer, “hacked” into NASA, and Department of Defense systems, in the process shutting down U.S. Naval munitions

supply shipments and an entire network of U.S. Army computers.[8] The estimated cost of this attack to the U.S. was in the multi-millions.

This anecdotal evidence suggests that individual hackers working in a basement with personal computers have done damage to Department of Defense systems, necessitating billions of dollars for cyber security every year, and establishes strong evidence that any balance may not favor defense in cyberspace.

It is possible that by analyzing systems in the cyberspace domain, a domain that seems to simplify or remove the confusions inherent in the offense-defense balance Theory, a clearer model might emerge, providing insight into how to apply, how to analyze, and even whether to apply, this theory.

As an example, during my analysis of offense-defense balance theory, the balance seems heavily in favor of offense. This analysis might actually help explain why there is so much conflict within cyberspace. Given the reduced cost of offense in comparison to defense, the Theory indicates that conflict would increase—the greater the "imbalance," the greater the increase in conflict.

To clarify this, although arguments could be made against various elements of the proposed model and the associated costs, it seems that it is equally difficult to measure offense and defense within cyberspace. Because of this as a practical application within cyberspace, the argument against the input data may not matter quite so much. It could be argued that the perception of imbalance as seen by the various participants is more important than the actual balance solution.

If offense is seen as cheaper, and defense is seen as expensive, actors within the system may remain more likely to strike out against others for both gain and as a preemptive measure. Even if states or actors do not perceive the balance accurately, Lynn-Jones notes that it still affects their behavior, because their behavior is based on their perception of the balance.[9]

---

8 Clark Boyd, "Profile: Gary McKinnon." *BBC News*, July 30, 2008.

9 Sean M. Lynn-Jones, "Offense Defense Theory and its Critics," Security Studies 4, no. 4 (1995): 660–691.

In cyberspace this problem remains, but is compounded by the fact that there is currently little perceived risk in cyber-attacks. Added to the balance misunderstanding, there is also little risk if an attack fails making the potential "cost" of offense even lower.

In 2011, the U.S. Department of Justice investigated 387 people for Intellectual Property and Computer Crimes, and prosecuted and charged 215.[10] The U.S. Federal Bureau of Investigation in coordination with the U.S National White Collar Crime Center has put together a reporting database that aims to help facilitate cybercrime reports and push them to the proper level. The Internet Crime Complaint Center (IC3) 2010 report annotated that the center received over 303,000 complaints of Internet crime. Of those complaints 121,000 were referred to local, state or federal law enforcement. The percentages of referred cybercrime cases were 9.3% credit card, 6.1% computer crimes, and 16.6% identity theft, which totals out to 32% or 38,947.

This sounds relatively good until other parts of the report come to light. Of the 121,710 referred reports, IC3 analysts prepared 1,420 cases (representing 42,808 complaints). Law enforcement prepared 698 cases (representing 4,015 complaints). In addition, law enforcement requested FBI assistance on 598 Internet crime matters. Of the referrals prepared by the FBI analysts, 122 open investigations were reported, which resulted in 31 arrests, 6 convictions, 17 grand jury subpoenas, and 55 search/seizure warrants.[11] So of the 121,710 reports, in reality only 47,421 were actually put into cases.

It is interesting to note as well that neither the U.S. Federal Bureau of Investigation (FBI) nor the U.S. Department of Justice (DoJ) track statistics on cybercrime. They do however lump cybercrime with intellectual property and produce a report, the Intellectual Property Enforcement Coordinator (IPEC) report. In 2011, they prosecuted 215 people for either intellectual property violations or cybercrime.[12] Based

10 Internet Crime Complaint Center, 2010 IC3 Internet Crime Report, Annual, Washington, DC: National White Collar Crime Center, 2010.

11 Ibid.

12 U.S Intellectual Property Enforcement Coordinator, 2011 Annual Report on Intellectual Property Enforcement. Annual, (Washington, DC: GPO, 2011).

on the report itself, it is unknown how many of the cases were prosecuted, but at a minimum less than half of the crimes were even referred.

This breakdown of cyber-crime statistics enumerates some of the issues, providing an indication of the level of risk a cyber-attacker runs inside of the U.S. Outside of the U.S., some countries are working on stopping this problem while others ignore it. Because of this many cyber-attackers can attack for the most part with little to no repercussion. In addition to cyber-attacks identified, many attacks are not reported or not identified. Additionally none of these statistics track the number of incidents done for reasons of international power or espionage, merely crime.

Based on this, the perception seems to be that cybercrime is less risky than other crimes, and offense within cyberspace greatly reduced in "cost" at least with regard to risk. It is also interesting to note that there are no repercussions to attacks that do not succeed. Symantec and other cyber security companies track the attacks that did not succeed; Symantec itself tracked over 5.5 billion blocked attacks in 2011.[13]

One other significant influence on the cyberspace argument for offense-defense theory is that the "weapons" used in attack or defense are never actually expended as they are in conventional military operations. An attack within cyberspace succeeds or fails without physical damage to the attacker. Any program used can simply be shelved for use at some future time or improved for further operations.

The risk is to data, and an attack may succeed so that real world assets are disrupted or destroyed, which is the point of the attack or the defense, but the cyberspace offense/defense assets remain. Not only that, but computer operations can be executed automatically. This allows for continuous attacks/defenses without additional effort. This further reduces the "cost" of cyberspace operations and distorts the attempt to decide on the relationship between offense and defense within cyberspace.

Given the nature of cyberspace, I argue that offense-defense theory can actually explain/analyze why there is so much conflict in cyberspace, and that the major

13 "Internet Security Threat Report 2011 Trends," Threat Report, Symantec Corporation, 2012.

arguments against the theory are minimized or even removed by the simple fact that offense and defense are more obvious within the cyberspace domain. This seems to allow cyberspace to provide a clearer arena for the application of offense-defense balance theory.

With the identification of offensive versus defensive weapons, the balance not seeming to favor the defense, and the perception of cost for offense the most prominent arguments are reduced and cyberspace can be seen as a microcosm for offense defense theory in the international system.

THIS PAGE INTENTIONALLY LEFT BLANK

III. PROPOSED COST ANALYSIS SYSTEM

A. PROPOSED OFFENSE-DEFENSE MODEL FRAMEWORK

In order to analyze the offense-defense balance theory for conflicts within cyberspace, it is necessary to build a comprehensible framework. This proposed framework must be designed to help define costs so that offense and defensive spending can be compared and contrasted. However, when comparing offense and defense costs, there are some difficulties. Problems with multiple use, hidden costs and balancing costs create issues within any framework capable of determining relationships between offense and defense with any fidelity and reliability.

First, very little spending on computers is specifically designated for offense or defense, even within software purchases. The purchase of a firewall within a specific software program certainly does not inherently imply that the program was purchased for defensive purposes. And while defensive aspects of specific software may be considered in the purchase of a program, i.e., a program may be more protected or less vulnerable, determining the portion of the cost that can be considered defensive in nature is very hard to discern.

In addition to these multiple use problems, specific aspects of offense abound with hidden costs that are equally difficult to determine. For example, how many hours were spent conducting reconnaissance of a target, was it necessary, and did it require physical presence (human intelligence) to determine vulnerability of the target? How much time was spent developing an attack program and what systems were used? Each aspect of the problem adds to the difficulty in determining specific attack costs.

A balancing act in estimating costs then becomes a central feature of offense and defense. Reviewing the available information made it obvious that, in cyberspace conflicts, the primary determination to the cost of an attack is the specific defenses in place at the target. For example, it is obviously significantly cheaper to conduct an attack against antiquated, unaltered protective software, particularly if it has multiple previously identified vulnerabilities. That scenario could make it possible that the only cost of an

offensive attack would be a short reconnaissance, to determining what software the target was using, since it is very likely that a freeware script to exploit those old vulnerabilities is already available at no cost.

Based on these issues the framework must be flexible and allow for significant variation. The framework needs to look at the personnel and their capabilities, along with the hardware and the software in place for offense and defense. In addition to this inherent variation, the framework must also use several assumptions to develop any useful analysis.

1. Initial Assumptions

1. People: Personnel training for offensive and defensive operations, though an extremely expensive aspect of both sides of the conflict are assumed to be equal between the two sides. The skills necessary to defend a network are similar enough to the skills necessary to attack it that these costs negate each other and are considered balanced. This includes such things as certifications as well as any other more generalized training.
2. Hardware: Hardware costs are determined by those systems within a network that were bought for the sole purpose of defending the system. Systems such as Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Virtual Private Network (VPN) servers, and/or Computer Locks.
3. Software: Software costs are determined by those systems within a network that were bought for the sole purpose of defending the system. Software such as a firewall, IDS, IPS, VPN, Anti-virus, Data Security, Network Analyzer, Proxy Software, and/or Encryption software.
4. Software Services: For purpose of this model, services such as security, data storage or even sub-contracting of the information security systems will be entered under software.
5. Timing: Defense systems are set in place. For purposes of the framework, in order to prevent a recursive loop, defensive systems will be considered set at the moment of conflict with no immediate upgrades in software or hardware available for that point in time. Obviously, if defense can make immediate successful adjustments, offense will have to upgrade, making determination of the balance point impossible. In real conflicts, this aspect becomes important, but for purposes of study, the framework will use a flash point aspect, with defensive system costs unchanging.

B. FRAMEWORK

Offense : Defense
Offense (People + Hardware + Software) : Defense (People + Hardware + Software)

People = Training + Wages
Hardware = Specific Hardware purchased specifically for attack or defense
Software = Specific Software purchased for attack or defense

Again, while the referenced hardware and software do not comprise the entire system or suite operating in a cyberspace conflict, the equipment and software that does not pertain specifically to defense or offense may be obstacles /vulnerabilities but will not be considered as costs for purposes of this model.

This model is the proposed basis for cost analysis for offense and defense in the cyber domain when in conflict. However, in order to get a specific answer from the equation there is some additional simplification necessary.

Assumption one considers the subset of training for people to be the same for both sides of the equation. It is necessary in order to remove redundancy and simplify the equation. Both Computer Security Personnel and Computer Attackers (Hackers) require roughly the same level of training (includes such things as certifications for specific systems) and understanding of the system. Because of this it will be assumed for purposes of this paper that they are the same and pulled from the equation.

Assumption two and assumption three are necessary to simplify cost analysis because while a nation or company may purchase computers or hardware for use, not all computers or physical items purchased that operate in cyberspace are defensive hardware/software. For purposes of this theoretical framework, only those systems that are purchased specifically for defense will be considered. An example of this would be a printer on a network. While the printer is a system that must be defended; it is not a defensive system and is rarely bought as such.

Using these assumptions, the final analysis equation then becomes:

Offense (Wages + Hardware + Software) : Defense (Wages + Hardware + Software)

In addition to the balance between offense and defense, there are additional factors when using this framework. The offensive costs necessary to successfully attack a system are determined by the defenses in place. Therefore, in the equation offensive costs are dependent on defensive costs. In order to determine any specific offense-defense balance, the equation must start from the defensive side.

C. A NOTE ON RISK ASSESSMENT

In order to reduce the variability within the analysis, risk is not considered within the analytical framework.

The purpose of a risk assessment is to look at vulnerabilities, threats and solutions in order to determine what a company should do in order to mitigate identified problems to an acceptable level. A typical risk assessment analysis would determine how much a company should spend to bring the risk to a level that the company can tolerate. The key, then, is “acceptable level.”

The need for defenses can be determined by assessment, but the cost of the defenses themselves is the critical factor for the study of the Theory, not a range of costs to reduce risk. This offense-defense balance analysis framework determines how much is spent on offense and defense as a more general application of costs.

Additionally, risk assessment has to consider the value of what is being protected. More money/time may be spent on more valuable data. The proposed offense defense framework is designed to determine a more general analysis from a specific instance, whereas risk assessment is designed for use for that specific system for a specific problem. Risk assessment is looking at possible threats in relation to assets at risk and determining if the value of the asset is worth the protection necessary to defend it. The offense-defense balance analysis framework is not at all concerned with the possible assets at risk and, therefore, it is designed to determine how much offensive operations cost in relationship to defensive operations.

D. COSTS BY FUNCTION

Specific hardware and software costs for the theoretical model were derived using two low cost options and two high cost options for each system, based on current costs.[14] The specified sub-systems are listed with their specific costs and additional variables that influence price. The average or midpoint number is computed using all four data points. The low cost price point is determined by the lowest cost of the data points; the highest costs price point is determined the same way, unless otherwise specified.

The overall cost numbers for hardware and software are computed assuming that every attacker and defender uses each system. The numbers are computed and a range of costs are provided, one high, one low and one average. It can be argued that this method, to determine theoretical costs, places a higher burden on defense since there are more defensive systems and they may not all be used. For example a number of companies may only use anti-virus software. This method of defense notwithstanding, for purposes of the theoretical model, defenders and attackers will use all systems available with the only variable being cost.

1. Defensive Hardware Costs

Cyber security hardware includes a number of standard systems of protection. Usually, these include a Firewall, a Virtual Private Network (VPN), and an Intrusion Detection Systems (IDS) and/or an Intrusion Protection System (IDP). In addition to those specific systems, the second most common architecture is what is known as a demilitarized zone (DMZ) concept which doubles the number of Firewalls, VPN or IDS/IDP in order to secure the company public side from the outside as well as secure the companies public side from its own private side.[15] Beyond that for costs savings purposes some of the hardware may be integrated into an all in one hardware systems, called a unified threat management system (UTM), which incorporates some or all of the

14 Costs computed using Google shopping, accessed between November 1–5, 2012, http://www.google.com/shopping?ie=UTF-8&hl=en&tab=wf, to gather price data, specific product websites provided further specification data.

15 U.S. Computer Emergency Response Team, Control Systems Security Program (CSSP), 2012, accessed November 7, 2012, 2012. http://www.us-cert.gov/control_systems/csvuls.html.

previously mentioned features. Physical security measures can include computer locks, and secured locations, with other basic physical security measures.

UTM systems provide significant costs savings for companies looking to defend their systems, especially if there are enough security risks to require a DMZ structure, which effectively doubles the actual number of hardware security systems. However, like any all-in-one product it makes sacrifices in order to package it all in one system.

For purposes of the analysis framework these UTM, "all-in-one" systems, will not be priced. There is such wide disparity in actual value, possible cost savings, and actual protection, that there is no way to reliably determine a valid cost range for comparative purposes.

Additionally physical security features also will not be used as a cost within hardware for purposes of the offense-defense framework. It is possible to incorporate these features and determine a price range, however for the most part physical security is focused more on the corporation as a whole and less on data security. There are possible scenarios where physical security is a feature of cyber security, but for purposes of the theoretical offense-defense balance analysis it will not be incorporated. Essentially, the analysis will use the essential security measures of the Firewall, VPN and IDS/IDP standard protective suite.

a. Firewall: Hardware

A firewall provides security for the link between the World Wide Web, the Internet, and the intra-net of the organization. The firewall filters incoming packets of data and information to prevent damage, invasion or data theft.

The cost of firewall solutions vary widely, from small, personal computer protections that can range from $200 to $1,000, to huge systems that incorporate training, personnel, hardware software and services, with costs ranging well into six figures or above.

At this higher level, an enterprise[16] hardware firewall, can have features to include training and support packages, protection for all levels of communication, and specific protections for different systems, along with licensing costs for the number of units, and can vary in cost from $10,000 to $100,000. Table 1 contains the specific costs for two low cost and two high cost firewalls.

However, at the $100,000 price range the firewalls that were examined were more of a unified threat management system (UTM) which contains such integrated features as Firewall, IDS / IDP, VPN services, and even load balancing in order to maximize throughput. In addition to all of that, they included training, software, and support for the system for at least a year. Costs for further support were not examined.

FIREWALLS	COST	PORTS	SPEED (Mbps)
CISCO Small Business RV110W	$ 79.81	4	90
NETGEAR FVS318 ProSafe VPN Firewall	$ 90.00	8	95
JUNIPER NetScreen ISG 1000	$ 12,073.00	4	2000
CISCO ASA 5585-X Firewall Appliance	$ 34,317.00	8	4000

Table 1. Defensive Hardware Firewall Price Range

b. Virtual Private Network (VPN): Hardware

A virtual private network is designed to encrypt traffic between a network and a remote host. VPN hardware consists of two different types. The first and oldest is Internet protocol security (IPSEC) which builds a secure tunnel through the Internet. The IPSEC tunnel is encrypted, but it requires similar third party hardware on both ends in order to operate. However, a more recent addition is secure socket layer (SSL), which is designed to operate at a higher application layer and tends to be more configurable.

There are pros and cons to each and it depends on a number of factors on which would be the best for a company to deploy. That being said, most of the higher end VPN systems at this time are SSL. The cost of VPN hardware also depends on a number of factors. The focus of cost is the number of simultaneous users and the licensing fees

16 Enterprise is the common use term which refers to a large, complex computer system such as a corporation, school, or government network with usually more than 2500 hosts operating on it.

associated with the hardware. Most products involve a significant service price component. VPNs range in price from $1200–$51,000, again depending on licensing fees and product support, which can increase the price significantly. Table 2 contains the specific costs for two low cost and two high cost VPN systems.

VPN	COST	PORTS	TUNNELS	LICENSE
ZyXEL VFG6005N	$ 80.95	4	32 (IPSEC)	N/A
D-Link DIR-130 Broadband VPN Router	$ 87.27	8	25 (IPSEC)	N/A
Barracuda SSL VPN 880	$ 39,993.00	6	500	N/A
Dell SonicWALL Aventail E-Class SRA EX7000	$ 65,695.50	6	5,000	1000

Table 2. Defensive Hardware VPN Price Range

c. Intrusion Detection System / Intrusion Prevention System: Hardware

Intrusion detection systems (IDS) and intrusion protection systems (IPS) are newer security developments which are designed to look more closely than traditional firewalls at the risk potential of inbound packets.

IDS and IPS hardware tend to be an addition to firewalls and VPN systems, and tend not to be standalone hardware systems. While the terms IDS and IPS tend to be used interchangeably, they are in some respects separate functions.

An IPS works similarly to a firewall; it stops packets from entering the network completely. An IDS is designed to look at traffic within a network and provide analysis of various points in order to see if the system is acting outside of “normal” parameters. The primary difference is that an IPS that can take action, while an IDS is designed to monitor and notify.

That being said, a number of systems integrate these functions in order to minimize costs to the organization. Costs for IDS/IPS range between $5000–$40,000, with the primary cost difference focused on throughput and monitoring interfaces. Table 3 contains the specific costs for two low cost and two high cost IDS/IPS systems.

IDS / IPS	COST	PORTS	THROUHPUT (Mbps)
CISCO IPS 4240	$ 5,517.00	N/A	250
JUNIPER IDP 75	$ 5,763.00	N/A	150
MCAFEE NSP M-4050	$ 48,546.00	N/A	10000
CISCO IPS 4520	$ 91,032.00	N/A	10000

Table 3. Defensive Hardware IDS/IPS Price Range

Tables 1–3 show that overall hardware costs vary widely depending on the size of the network to be protected, along with how much homogenous hardware is desired. Thus, at the low end, a company which uses a complete suite of defensive hardware can spend less than $6000 to defend a small network, where a larger company could need to spend upward of $191,000 to defend a more complex system. The mid-point ("average") for low and high costs systems priced for the analysis framework is almost $76,000. Figure 1 charts a comparison of low high and average hardware costs.

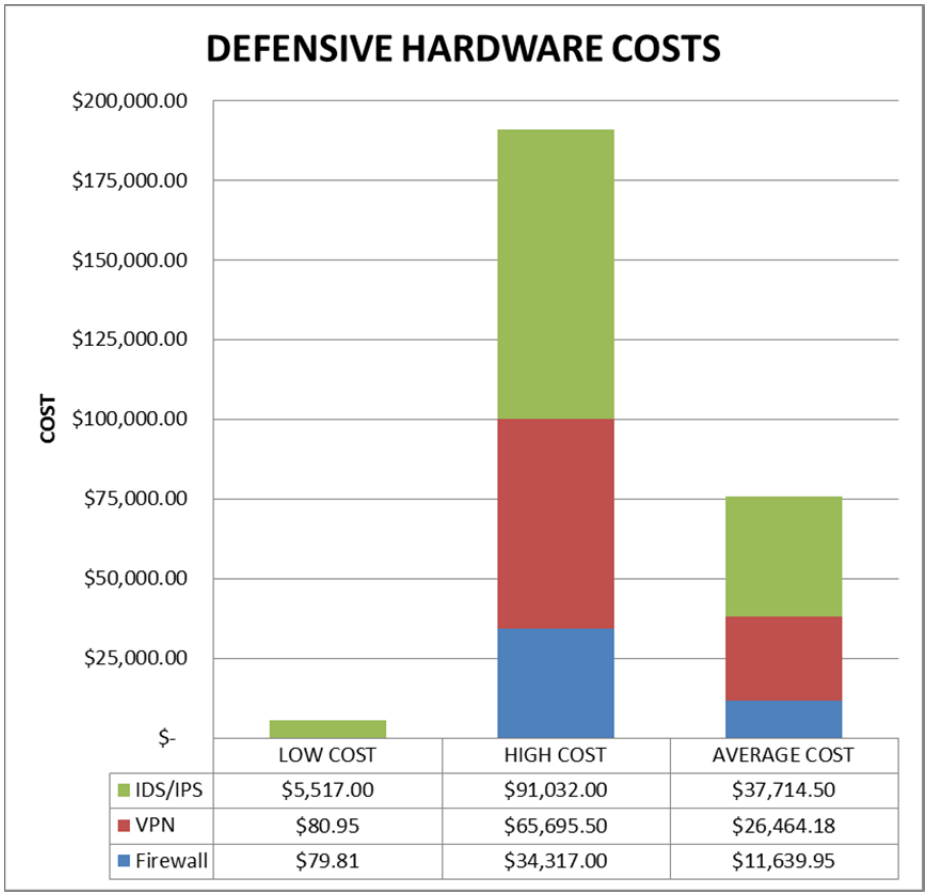


Figure 1. Defensive Hardware Costs by Price Range

2. Defensive Software Costs

Cyber Security software is also complicated by a number of factors. With regard to specific vendor software, it tends to be bundled systems that are designed to work with other same vendor systems. Attempting to build a functioning security software suite with multiple vendors' products may increase the risk of security holes and possible functionality issues. Rather like hardware there are many software manufactures willing to sell security products. In addition to software, many of those same vendors provide support packages up to and including onsite technical assistance and monitoring, with of course a significant increase in cost.

Software security systems are in some respects the same as hardware security in that the similar systems do the same task, albeit it in a different manner. Security software includes firewalls, VPNs, and IDS/IPS. In addition to these, there is also software for proxy servers, encryption, data security, network analyzers, and anti-virus. The primary cost feature for software tends to be licensing fees, depending on a number of factors.

a. Anti-Viral: Software

Anti-viral software is probably the most ubiquitous software defense. For most individual users it is the primary software defense on their computer. Anti-viral software is designed to scan programs operating on or being downloaded by a computer and run them against a filter. This filter is updated by the various service providers and contains signatures for known threats. Most anti-viral software is not designed to stop computer viruses that are not yet known.

As for any other piece of software, the costs of security software vary; however, they all tend to be based on number of hosts the software licenses. And costs stay relatively similar, providing even a cost discount for large license purchases. At the low end, anti-viral software freeware is available; at the high end, the price is less than $100 for a 10 pack license. Table 4 contains the specific costs for two low cost and two high cost anti-virus software.

ANTI-VIRUS	COST	LICENSE (Units)
Freeware	$ -	N/A
Symantec Norton Internet Security 2012	$ 12.00	1
KasperskyInternet Security 2012	$ 88.77	5
Symantec Norton Internet Security 2012	$ 99.49	10

Table 4. Defensive Software Anti-Virus Price Range

b. Virtual Private Network (VPN): Software

Virtual private network software or VPN ware is designed to provide a software solution for encrypting data between two computers or within a network. However, VPN software is much less robust than hardware and for the most part is not designed for large business networks.

Within the small to medium business range, however, it is a viable alternative to expensive hardware, with many software systems running as little as $19.99 a month. However, that cost is per user, not machine. Some VPN software systems are designed as an application running on a specific system, while others are designed to connect through a third party system. Each system has pluses and minus depending on what needs to be secure and the needs of the particular individuals using it. There is even VPN freeware for individual users; however these products have significant limitations.

Software of this type runs between $8–$20 per month per user on the low end and up to around $1000 a year on the high end for around 100 users.[17] Table 5 contains the specific costs for two low cost and two high cost VPN software.

17 "Order: Personal / Corporate," PureVPN, November 1, 2006, accessed October 24, 2012, http://www.purevpn.com.

VPN	COST	LICENSE (Units)
Cisco VPN Client	$ 32.00	1
D-Link VPN Client	$ 45.00	1
WatchGuard VPN Manager	$ 6,264.00	N/A
Check Point VPN-1 Power VSX	$ 73,922.00	50

Table 5. Defensive Software VPN Price Range

c. Intrusion Detection System / Intrusion Prevention System: Software

IDS and IPS systems are designed to identify intrusion into a network. The IDS is an application software system that operates at the edges of a system, like a firewall. However, its job is not usually to stop an attack so much as to identify one occurring. IPS is also an application software package, but one that can be deployed inside a network to look for patterns of behavior that do not correspond to "designated" normal traffic or operations. IDS tends to be more passive than IPS, with IPS able to modify firewalls in order to reduce "abnormal" traffic.

IPS software systems in some respects act as an extra layer behind a firewall, and tend to be priced as such. A software firewall is a software application that is designed to intercept or control packets to and from a computer. This is done either at the host or server level depending on the size of the company. The firewall filters packets according to an Access Control List (ACL), which is a set of rules specifying which packets are allowed to pass and which are dropped. An IPS takes this a step further and looks for patterns of traffic entering a network that match known attack signatures.

The cost of IDS / IPS software again depends on the number of systems it will deploy on and some of the features that it provides. For purposes of clarification of this data there was no difference made between IDS and IPS software. When purchasing this software the terms tend to be used synonymously, and without more detailed specifications from the vendors it is impossible to know if the software is IDS or IPS, or some hybrid version.

The costs for software IDS/IPS range between around $100 at the low end to as much as $63,000 for an IDS/IPS system. However, at the higher end, for systems

such as integrated Cisco ASA platforms, the IDS/IPS software is very hardware specific and prices vary greatly depending on the number of nodes, the length of the contract and the various support services that are provided. At the highest cost, above what is priced for the theoretical model, dedicated Information Technology defense companies can even provide an on-site support team for system monitoring and integration. Table 6 contains the specific costs for two low cost and two high cost IDS/IPS software.

IDS/IPS	COST	LICENSE (Years Service)	LICENSE (Node)
Symantec Managed Security Service v.1.0	$ 107.22	3	1
Kaspersky Business Space Security	$ 155.05	1	5
Cisco IPS Service Agreement (ASA 5585)	$ 38,526.00	1	1
Dell SonicWALL Intrusion Prevention (E10800 Systems)	$ 62,062.00	1	1

Table 6. Defensive Software IDS/IPS Price Range

d. Proxy: Software

Proxy software acts as a buffer for a network, however, unlike a firewall, it is designed to hide the IP addresses in use behind it, providing a common IP address in order to prevent attackers from seeing into a network.

Costs for this type of software again run the gamut depending on what it will be used for and what level of support is needed to run it. For example at the lowest cost, there are proxy freeware services, which in theory provide proxy services for free. However, from most companies' perspective, there is a significant trust issue with this method. At the high end, proxy services can run upward of $24,000 depending on how much throughput needs to flow and how the proxy is set up. Again at the high end the proxy systems tend to be coordinated with hardware and get very specific Table 7 contains the specific costs for two low cost and two high cost proxy software.

PROXY	COST	LICENSE (Years Service)
Freeware	$ -	N/A
IBM Sterling Secure Proxy - Unix, PC	$ 135.00	1
Cisco ASA 5500 Series UC Proxy License	$ 21,579.03	1
Novell LDAP Proxy - Unix	$ 24,283.65	1

Table 7. Defensive Software Proxy Price Range

e. Encryption: Software

Encryption software is not necessary in all cases. For purposes of cost, it has been analyzed, but most software includes encryption for data transmission. Most encryption software available for purchase is to protect data that resides in storage inside a network, either on an individual host computer or data that resides in a data warehouse server somewhere. Encryption software also has a large cost differential depending on the use and its application within a network.

Costs for encryption software run from freeware to over $10,000 for an encryption system that is designed to protect data on storage media unobtrusively inside a network. Encryption costs for low and high software can be seen in Table 8.

ENCRYPTION	COST	LICENSE (Licenses)
Freeware	$ -	N/A
Trend Micro Endpoint Encryption	$ 6.06	1
Symantec Endpoint Encryption	$ 115.46	1
Cisco MDS 9000 Family Storage Media Encryption package	$ 10,562.00	1

Table 8. Defensive Software Encryption Price Range

f. Network Analyzers: Software

Network Analyzers are a software system designed to provide clear pattern recognition based on various logs, making event logs more readable and easy to scan for network problems. They can be used as an IDS as well, depending on the system administrator.

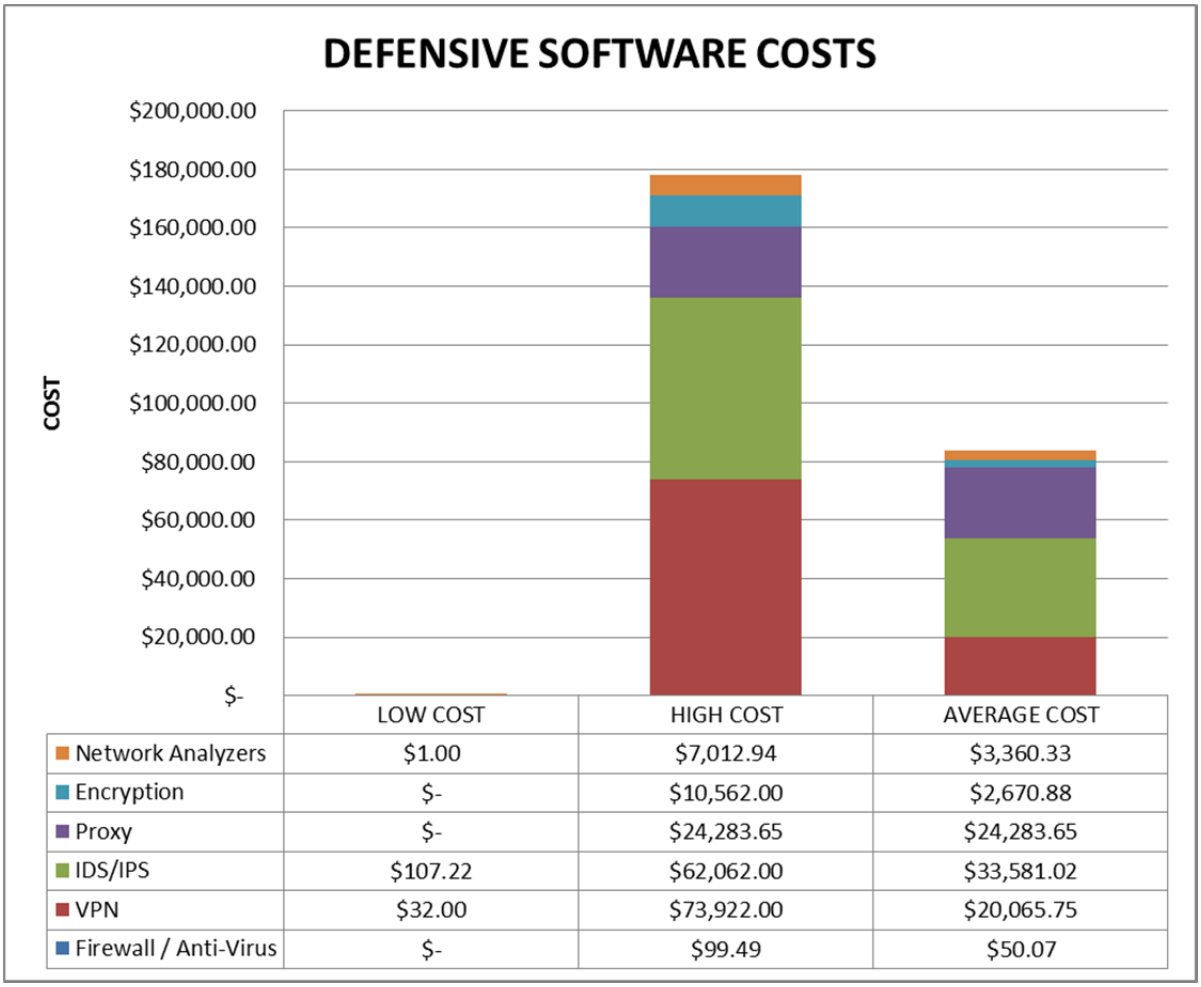
Costs for this type of software again depend on a number of factors; however, the factor that seems to influence cost most is how well the analyzer works with the network. Low cost options can run as low as a $1. Higher costs options can run around $7,000 for an analyzer that is integrated with the hardware and has proprietary graphical user interfaces (GUIs) that make seeing the network "easier." Table 9 contains the specific costs for two low cost and two high cost network analyzers.

NETWORK ANALYZIERS	COST	LICENSE (Years Service)
Dorado Redcell Traffic Flow Analyzer - Unix, PC	$ 1.00	1
Dell SonicWALL Analyzer (SRA 1200)	$ 97.38	1
Intelligent Management Center Network Traffic Analyzer (NTA) -	$ 6,330.00	1
Orion NetFlow Traffic Analyzer Module (SL2000)	$ 7,012.94	1

Table 9. Defensive Software Network Analyzers Price Range

Overall software costs can be seen to vary widely depending on what a company needs as well as the size of the company. It could be argued that most small businesses depend on their anti-virus and eschew other software. This model is not designed to determine the wisdom of such a decision.

However, for purposes of the offense-defense analytical framework, it will be assumed that all software protections are necessary and used. See Appendix A for full calculations. On that basis, as can be seen in Figure 2, a low cost network software system would cost around $140. At the high end, software could cost upward of $178,000. The average (mid-point) cost of software for the offense defense analysis framework is $84,000.



	LOW COST	HIGH COST	AVERAGE COST
Network Analyzers	$1.00	$7,012.94	$3,360.33
Encryption	$-	$10,562.00	$2,670.88
Proxy	$-	$24,283.65	$24,283.65
IDS/IPS	$107.22	$62,062.00	$33,581.02
VPN	$32.00	$73,922.00	$20,065.75
Firewall / Anti-Virus	$-	$99.49	$50.07

Figure 2. Defensive Software Costs by Price

3. Defensive Personnel

Applying costs to personnel providing defense will vary widely based on company considerations. For many companies there is only one person, or possibly an outsourced service, working all information technology for the business. Some part of these services will include security.

At the higher end, major corporations have teams of personnel in various functions—including maintenance and defense of the network.

Companies that outsource their information technology make determining specific defensive personnel costs difficult. Even dedicated personnel will vary widely in cost,

because salaries can depend on the cost of living, the training/education levels of the individuals, and other direct factors in employment.

For our purposes here, cost of living and training have been removed to allow use of the proposed cost framework. Average cost by IT function, annual and hourly, in Table 10 was derived from the Robert Half Information Technology 2013 salary guide.[18] It may be possible in some cases for there not to be any dedicated computer personnel; however for the initial theoretical base line, it will be assumed that there is at least some part time capacity.

PERSONNEL	AVERAGE SALARY	HOURLY*
ADMINISTRATIVE	$ 148,600	$ 59.44
APPLICATIONS DEVELOPMENT	$ 93,589	$ 37.44
CONSULTING AND SYSTEMS INTEGRATION	$ 106,854	$ 42.74
DATA/DATABASE ADMINISTRATION	$ 102,688	$ 41.08
QUALITY ASSURANCE AND TESTING	$ 82,000	$ 32.80
INTERNET AND E-COMMERCE	$ 81,554	$ 32.62
NETWORKING / TELECOMMUNICATIONS	$ 89,422	$ 35.77
OPERATIONS	$ 59,292	$ 23.72
SECURITY	$ 106,750	$ 42.70
SOFTWARE DEVELOPMENT	$ 99,042	$ 39.62
TECHNICAL SERVICES, HELP DESK AND TECHN	$ 63,025	$ 25.21
*Hourly wage is based on a 50 hour week, for a 50 week year subdivision of salary		

Table 10. Personnel Wage Range (Offense & Defense)

The personnel assumption for the offense-defense analysis framework will include one Networking Telecommunications person with an average IT salary employed at the lowest cost level. To allow for other information technology needs, only 1/3 of the salary will be added to the framework at the lowest cost level. At the highest cost level, a team cyber security cost will be applied to include one administrative person, two data/database administration persons, one Internet and e-commerce person, two networking and telecommunications persons, two security persons, one operations person

18 "Robert Half® Technology 2013 Salary Guide." Robert Half International. 2012, accessed October 24, 2012, http://www.rhi.com/SalaryGuides

and one software development person. This develops a low cost estimate of $29,807 and a high cost team total of $989,938, with the average (mid-point) of $539,680, shown in Figure 3.

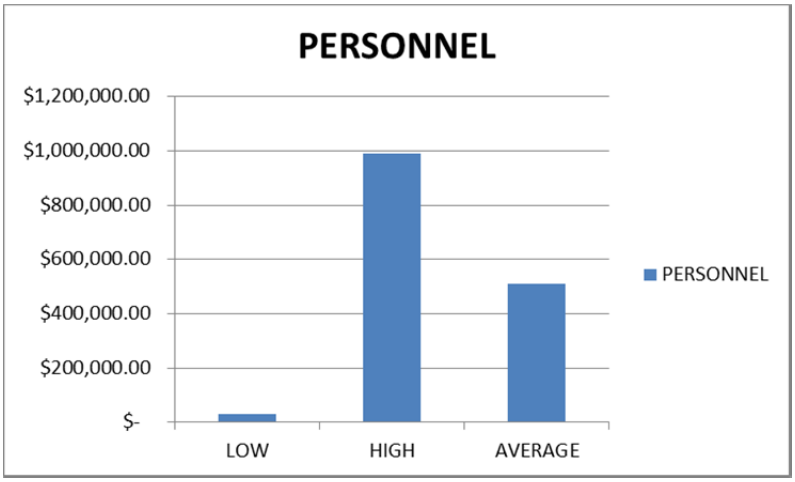


Figure 3. Defensive Personnel Wages Cost by Price

4. Total Defensive Costs

Applying the assumptions from the framework above and costs by system for defensive hardware, software, and personnel, it can be seen that the cost for defense runs the gamut (see Appendix A for Defensive Cost Overview). The lowest cost for cyber defense is $35,625 and the highest cost for $1,358,926. Using this framework, an average (midpoint) cost for cyber defense is $669,275. It can be seen from Figure 4 below, that the greatest portion of costs, for any level of defense, comes from the personnel wage costs.

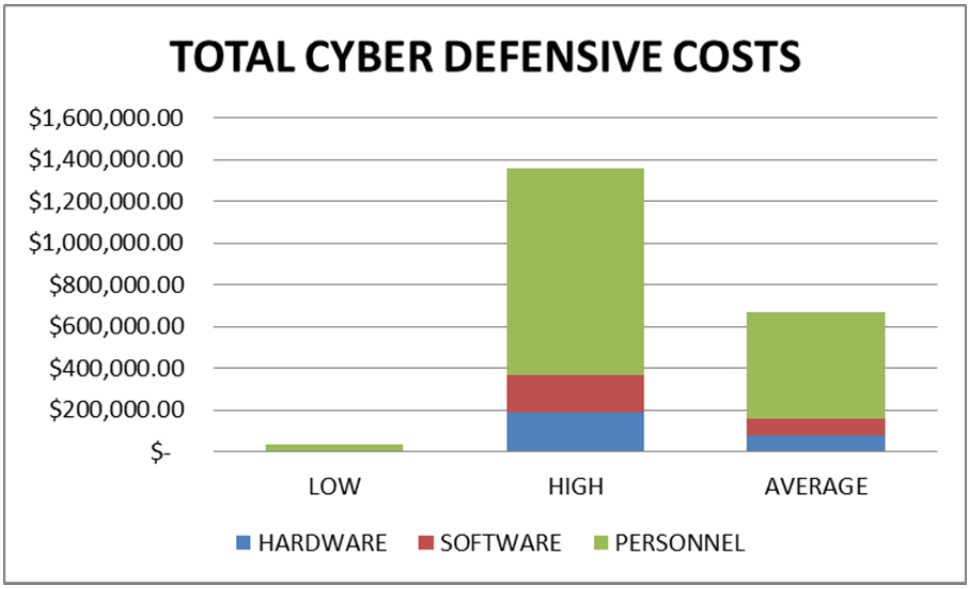


Figure 4. Total Defensive Costs by Price Range

5. Offensive Hardware Costs

For effective cyber offense there is really only one hardware item necessary, the actual computer. While it may be useful for attackers to use other purchased hardware such as a proxy, for purposes of this study those extra pieces of hardware will not be added as a cost. However, distributed denial of service (DDoS) attacks or botnets will be added to hardware as a cost for purposes of this analysis framework.

It is possible to argue that botnets tend to be software and attackers often purchase that software in order to build their own botnet. However, because some attackers will build their own botnet and some will rent one, both rental and build costs will be priced. However, for purposes of the analysis framework, only one system will be used, for the overall costs the lowest cost botnet will be used, either hardware or software and vice versa at the highest cost level. Rented Botnets will be priced as hardware. Software to build a botnet will be priced with software.

Certainly, an attacker might use both, but only one cost will be built into the final offensive attack analysis. The lowest cost botnet either hardware or software will be used, the other will be ignored for purposes of the model, the high cost botnet will be treated the same.

a. Computer: Hardware

The cyber attacker's computer can be any functioning computer; however there are some specific features that distinguish it from other more standard computers. Most important to a cyber-attacker is the need for multiple processors in order to increase the number of computations a second.

Many offensive pieces of software require massive number crunching in order to crack encryptions and passwords. The faster a processor can run combined with the number of cores, which enable faster multitasking, the more computations per second can be accomplished. Increased processing speed will allow an attacker to send attacks faster, and enter more systems.

Prices for computers run between around $300 at the low end for an entire computer system with a dual core processor to around $10,000 for systems with 16 cores. In addition to number of cores, which is an indicator, the systems were also rated by their benchmark speed, with the lowest cost system running 671 to the highest costs system running a benchmark of over 30,000.[19] Benchmark numbers are a means to quantitatively judge a systems performance based on a series of CPU tests applied to all tested computers. For purposes of this model hardware system, it provides a means to assess the performance of identified systems without further specifications. Table 11 contains the specific costs for two low cost and two high cost computer systems.

COMPUTERS	COST	CORE	BENCHMARK SPEED
Emachine EL1360G Desktop PC	$ 279.99	2	671
HP - Desktop (P2-1334)	$ 289.99	2	688
HP Desktop (H8-1440T)	$3,130.98	6	12637
DELL Precision T7600	$9,039.00	16	30179

Table 11. Offensive Hardware Computers by Price Range

19 "CPU Benchmarks," Passmark Software, November 1, 2012. http://www.cpubenchmark.net/ (accessed November 1, 2012).

b. DDoS/Botnets: Hardware

Botnets are large distributed networks of computers that are controlled by a remote host. These computers can be used as more processing power to crack passwords. They can also be used as a distributed denial of service (DDoS) network of attackers which can flood a company's website with traffic from multiple IP addresses in order to overwhelm the available bandwidth, thus locking out legitimate users.

Due to the illegality of botnets which compromise a host, renting costs are hard to determine. In 2010, VeriSign iDefense researchers produced a report that claimed the average cost to rent a botnet was $67 for 24 hours.[20] According to Trend Micro, costs for Botnets depend on what spam or DDoS needs to be accomplished with prices ranging from $30-$70 a day for DDoS to $10 for 1 million spam emails.[21] For purposes of the framework model, Botnet costs over a period of 30 days will be used. Table 12 contains the specific costs for two low cost and two high cost botnet rental costs.

BOTNET	COST	Days
Call Flooding*	$ 600	30
ICQ Flooding*	$ 900	30
DDoS*	$ 900	30
DDoS	$ 1,200	30
*Numbers Adjusted for 30 days of service		

Table 12. Offensive Hardware Botnet by Price Range

In Figure 5 overall hardware costs can be seen to vary widely depending on the type of attack and the resources the attacker devotes to the process. However, at the low end, the costs for a cheap attack can be less than $1000. For more well-funded attacks it can cost upward of $10,000 in hardware. Be aware that that is for a single attacker's hardware; for teams the costs go up. See Appendix B for full calculations.

20 Dancho Danchev, "Study Finds the Average Price for Renting a Botnet," ZD Net.com. May 26, 2010. accessed November 7, 2012, http://www.zdnet.com/blog/security/study-finds-the-average-price-for-renting-a-botnet/6528.

21 Max Goncharov, Russian Underground 101, Research Paper, Cupertino, CA: Trend Micro International, 2012.

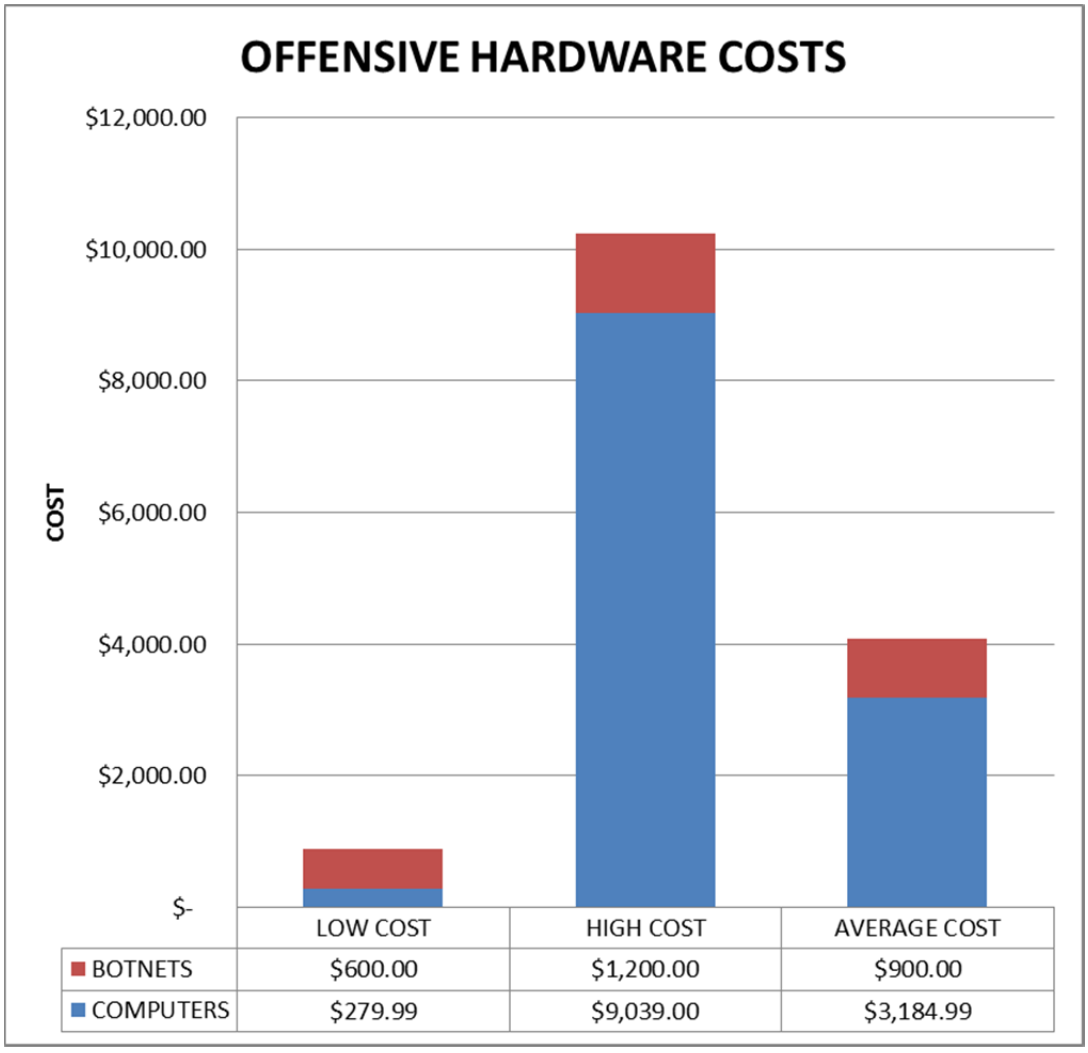


Figure 5. Overall Offensive Hardware by Price Range

6. Offensive Software Costs

Offensive Cyber Software is especially difficult to price for the simple reason that most of it is individually developed and probably illegal to use.

For the most part, offensive software tends to be either freeware posted on various hacker websites, or extremely expensive proprietary software that is sold to anyone willing to pay for the latest zero-day exploit. For zero-day prices, Forbes published a range of $5000 to $250,000.[22] However, there is no other published data for this claim

22 Andy Greenberg, "Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits," *Forbes*, March 3, 2012.

and for purposes of this framework, it will be assumed that attackers are using either freeware or self-developed software, since this is far and away the most common source of attacks.

a. Botnet: Software

According to Trend Micro most attackers do not rent botnets, but rather purchase the software for building a botnet. For purposes of this framework it will be assumed that the attack cost is to purchase a ZeuS toolkit to build a botnet. Using Trend Micro numbers, the cost to purchase ZeuS runs between $100 and $500.[23] Again for purposes of the framework it will be assumed that attackers on the cheap will use the lowest cost method for botnets, either renting time, or building their own, and vice versa at the high cost level. Table 13 contains the software costs for two low and two high cost botnet toolkits.

BOTNET	COST
Socks	$100
Smoke DDoS	$300
Optima DDoS	$350
ZeuS	$500

Table 13. Offensive Software Botnet by Price Range

b. Proxy: Software

Proxy software provides anonymity for an attacker. It is possible to use either freeware proxy services or purchase proxy software for as much as $20 for a single proxy IP.[24] Table 14 contains the specific costs for two low cost and two high cost offensive proxy software kits.

23 Goncherov,"Russian Underground 101."

24 Ibid.

PROXY	COST	DAYS	SERVERS
SOCKS 4/5	$ 3.00		100
HTTP	$ 3.50	N/A	1000
SOCKS	$ 25.00	21	1500
HTTP/S, SOCKS 4/5	$ 55.00	90	1

Table 14. Offensive Software Proxy by Price Range

In Figure 6 overall software costs can be seen to vary widely depending on the type of attack program desired and the specific services desired. It is not necessary that an attacker use a proxy service. However, because it helps increase anonymity and reduce chances of getting caught conducting illegal activities, it will be assumed that attackers do so. Based on this the software for an attack at the low end costs around $100 and at the high end may cost over $500. This does not price software that an attacker develops themselves; that cost is assumed as part of the salary. It can be argued that with zero-day exploit costs between $5,000 and $250,000 the price of attack goes up significantly. However, this model assumes that every software and hardware system is used by each attacker and that is not the case with zero-day exploits. While zero-day exploits attacks are a desired attack vector, they are extremely rare in comparison to other more well-known exploits and for purposes of the model will not be added to cost. See Appendix B for full calculations.

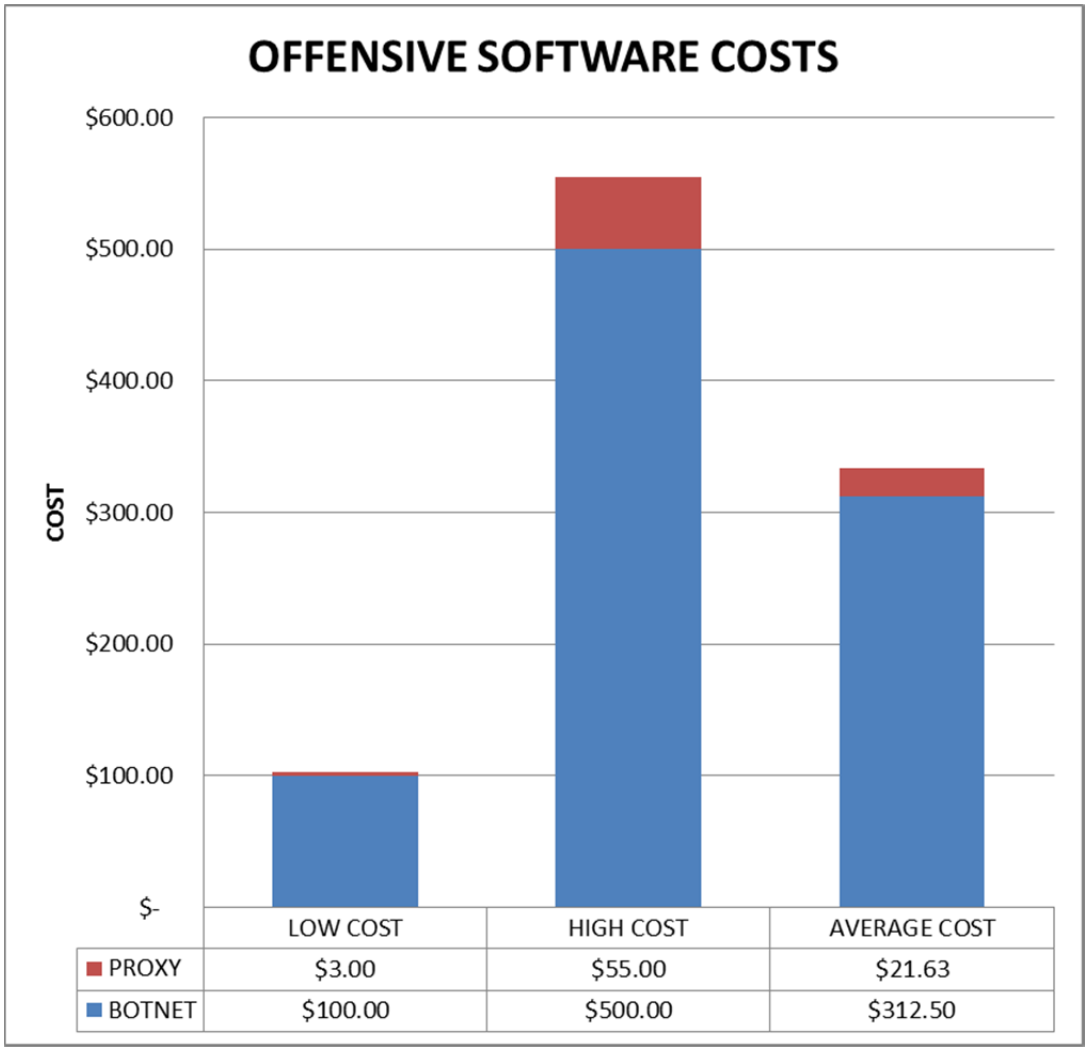


Figure 6. Overall Offensive Software Costs by Price Range

7. Adjusted Botnet Price

As noted earlier Botnets can be either hardware or software, depending on the control the attacker wants and the costs an attacker is will to incur. A rented botnet costs more, however there is no time cost to build the botnet or manage it. A software botnet costs less than a rental, however it requires some specialized knowledge and time to build a botnet that will accomplish the attacker's objectives. Time costs for setup and building a network were not analyzed for this cost point. Using this subdivision the lowest cost is software botnets at $100 and the highest cost Botnet is renting at around $1200, seen in Table 15.

*ADJUSTED BOTNET COSTS	LOW COST	LOW COST 2	HIGH COST 2	HIGH COST	AVERAGE COST
BOTNET: HARDWARE	$ 600	$ 900	$ 900	$ 1,200	$ 900.00
BOTNET: SOFTWARE	$ 100	$ 300	$ 350	$ 500	$ 312.50
*As specified in the model, Botnets will cost from hardware or software, depending on which is higher or lower, for each category					
TOTAL BOTNET ADJUSTED COSTS	$ 100	$ 300	$ 900	$ 1,200	$ 625.00

Table 15. Adjusted Botnet Cost for Hardware and Software by Price

8. Offensive Personnel

Again, because of the illegality of most attack operations, personnel costs are difficult to pin down. Is the attack a full-time occupation, and is there teamwork involved? The legend of multiple home-based "hackers" bringing down huge corporations is pervasive, and there is some literature to support cyber-crime networks.[25] Along with this, there is evidence that hackers attack other networks for "fun" and there is no salary involved, but for purposes of the analysis framework, the costs will be applied as if they worked in the IT field, by using the salary guide above.

Because hacking can be conducted with scripts and freeware, the amount of time spent on offense at the lowest cost level will be assumed to be less than the amount of time a defender will spend. Again, the cost of personnel for the offense defense framework removes cost of living or training. Average cost by IT function, annual and hourly, was derived from the Robert Half Information Technology 2013 salary guide.[26] See Table 10 for wage costs.

For purposes of the offense-defense analytic framework, it will be assumed that attackers will need significant security focus, with some networking skills. For the low end attacks, a single attacker will be assumed to be using 1/4 of his time at the cost of an average security salary. The highest cost level will include a team of as many as five

25 Nelson D. Schwartz, "F.B.I. Says 24 Are Arrested in Credit Card Theft Plan," New York Times, June 26, 2012

26 "Robert Half® Technology 2013 Salary Guide."

attackers; one network person, three security persons, and one software development person. This is reasonable, with reports of some cyber-attack supply chains, not networks, having more than seven individuals.[27]

The cost structure, seen in Figure 7, then becomes low cost personnel with a total of $26, 687 and the highest cost calculated at $508,713. The average (mid-point) cost is then $267,700.

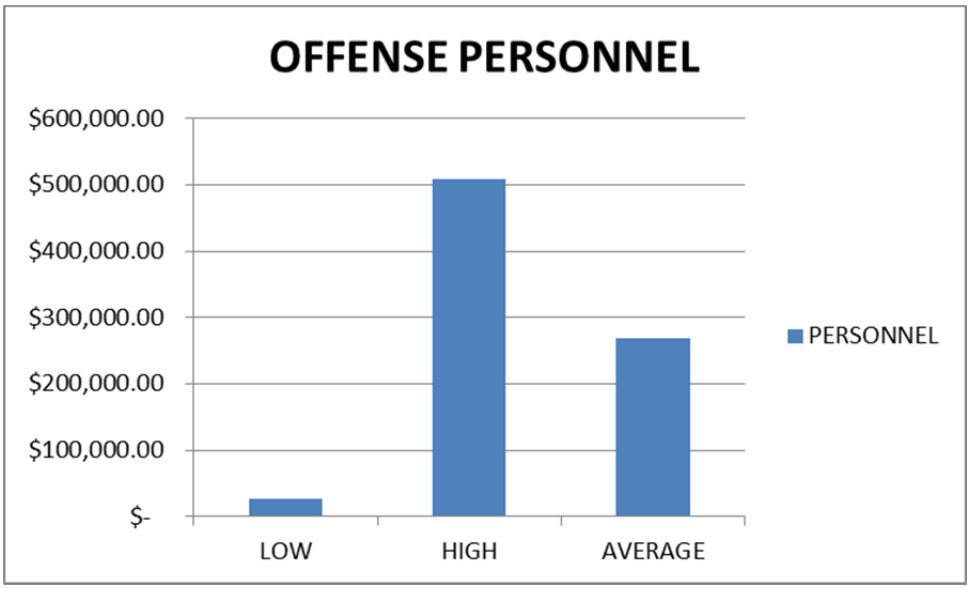


Figure 7. Overall Offensive Personnel Wages by Price Range

9. Total Offensive Costs

Totaling the offensive costs will depend on the resources and "enthusiasm" the attacker can muster. For purposes of the model, the lowest cost for a cyber-attack is $27,070. The highest cost for a team attack is $519,007. The average (midpoint) then becomes $273,039. Figure 8 charts the comparison; see Appendix B for full calculations.

27 "Life in the FAAS Track," EMC Corporation, 2012, accessed November 19, 2012, http://www.rsa.com/products/consumer/whitepapers/11794_120612_Life_in_The_FaaS_Track.pdf.

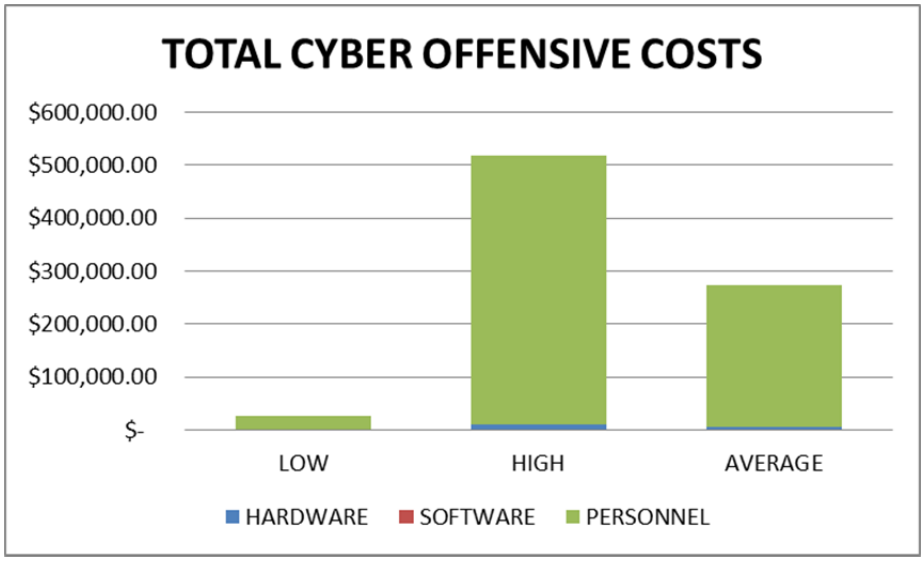


Figure 8. Overall Offensive Costs by Price Range

E. OFFENSE-DEFENSE THEORETICAL BALANCE

Based on the costs developed, it is obvious that the range of costs is enormous, and depends completely on the effort and resources applied to each individual situation. In addition, it needs to be highlighted that while these numbers provide theoretical price points for low and high cost systems, they do not comprise the most expensive defenses or attacks, nor do they show the cheapest.

Defensive systems may cost more if a company chooses to build DMZ architecture, integrating multiple defensive hardware and software systems for additional security. It is also certainly possible, and even probable, that there are companies that choose to use no security beyond what comes with the systems and products they acquire. The analysis framework here assumes that all companies will do their best to defend their systems, within the limits of resources.

This analysis is given as a means to determine a theoretical Offense-defense balance point in cyberspace based on current "weapon" values. Further study could be done using this model to determine what numbers of companies employ what types of defenses, and then pricing the specific hardware and software. Further study could also be made into cyber-attack costs to determine actual costs of conducting an attack to gain more fidelity and improve the initial data into the model.

F. THEORETICAL ESTIMATE

Using the analysis framework, the theoretical balance between offense and defense at the low end is around $27,000 (Offense) to just over $35,000 (Defense) or 1:1.3, while at the other end of the scale, more heavily weighted to the attacker with a ratio of $519,507 to $1.359 million, or more than double the cost for the defender 1:2.62; see Table 16. It is also possible for a low cost attacker to attack a high cost defender, which would have roughly a 1 to 50.2 ratio. The average costs ratio is 1:2.55. For clarification purposes the ratio is brought out 2 decimal places (highlighting that the average is lower than the high cost), but it can be argued that the data does not support such accuracy.

THEORETICAL MODEL OFFENSE-DEFENSE RATIO			
	OFFENSE	DEFENSE	RATIO
LOW COST RATIO	$ 27,070	$ 35,625	1.32
HIGH COST RATIO	$ 519,008	$ 1,358,926	2.62
AVE COST RATIO	$ 273,039	$ 697,275	2.55
LOW TO HIGH RATIO	$ 27,070	$ 1,358,926	50.20

Table 16. Offense Compared to Defense Costs with Associated Ratio

The above ratios fail to take into account several important issues between offense and defense. The first is that while costs were functionally determined, they do not take into account scaling sizes for companies.

According to the specification data for the defensive hardware, the largest throughput numbers that the defensive IDS/IPS high cost systems provide is 10,000 Mbps; however at the highest cost, the firewall is only running a throughput of 4,000 Mbps. The system cannot run faster than the slowest throughput.

The U.S. Federal Communications Commission omnibus broadband initiative (OBI) in 2010 estimates that the average user requires 4Mbps, with variance running

between .5Mbps and 7Mbps and 80% falling in the range .5Mbps– 4Mbps.[28] Using this estimate, it will be assumed that 3 Mbps is a reasonable bandwidth per user. While for some companies this is high, for others it is low, especially for those companies or users who upload large amounts of data or use intensive video conferencing. If 3Mbps is the norm then it can be assumed that a 4000 Mbps system would contain around 1300 users.

Based on Internet world statistics, in the United States alone there are 273 million Internet users as of December 2011. There are 2.4 billion Internet users worldwide.[29] Using these numbers, combined with the U.S. census data on business employment numbers, Table 17, it can be seen that 5.7 million firms employ around 112 million people. This is not to say that all firms use computers; however, it gives an estimate of employment size which indicates how large companies are. Using these statistics, only .3% of businesses have more than 500 people, which would need the highest cost cyber defense based on bandwidth. And 79% of businesses are less than 10 people, needing close to the lowest costs defense.[30]

NAICS CODE	NAICS DESCRIPTION	ENTERPRISE EMPLOYMENT SIZE	NUMBER OF FIRMS	EMPLOYMENT	ANNUAL PAYROLL ($1,000)
--	Total	2: 0-4	3,575,240	5,926,452	226,541,056
--	Total	3: 5-9	968,075	6,358,931	212,039,611
--	Total	4: 10-19	617,089	8,288,385	283,246,473
--	Total	5: <20	5,160,404	20,573,768	721,827,140
--	Total	6: 20-99	475,125	18,554,372	719,061,251
--	Total	7: 100-499	81,773	15,868,540	665,644,629
--	Total	8: <500	5,717,302	54,996,680	2,106,533,020
--	Total	9: 500+	17,236	56,973,415	2,834,450,349
--	Total	1: Total	5,734,538	111,970,095	4,940,983,369

Table 17. 2010 U.S. Census Employment Business Data

[28] Federal Communications Commission, *Broadband Performance, OBI Technical Paper NO. 4*, Technical Paper, Washington, DC: GPO, 2010.

[29] Miniwatts Marketing Group. *Internet World Stats: Usage and Population Statistics*. June 30, 2012, accessed November 7, 2012, http://www.internetworldstats.com/stats.htm.

[30] U.S. Census Bureau, *U.S. Department of Commerce. U.S., all industries [xls, 2.8 MB]*, October 25, 2012, accessed November 7 2012, http://www.census.gov/econ/susb/index.html.

Besides businesses, there are 273 million individual users in the U.S. that could be the target of a cyber-attack. However, because the defensive costs for home computing tend to be low, involving only an anti-virus and a router, we will only consider attacks against the 5.7 million U.S. companies.

Because of computer automation, it is not unreasonable to assume that any given attacker may attack hundreds or thousands of computers a day. Using such tools as Nmap (a scanning tool), it is possible to scan thousands of IP addresses a day in order to look for possible targets. There is no current statistic for how many attackers are operating. In addition, attackers can operate across borders, so the number of attackers in China or Nairobi can affect the number of attacks in the U.S. Thus, the number of attackers is probably a moving number at the best.

According to Symantec, there were on average 82 targeted attacks on companies per day in 2011.[31] This number does not take into account the number of SQL injection attacks attempted or other various means to gain access into a site. However, applying just the number 82 to 5.7 million companies, we get an extraordinary number of attacks (470 million) per day. It is extremely unlikely that with 2+ billion Internet users there are 470 million cyber attackers out there, indicating that some attackers are conducting multiple attacks per day.

Currently, there is no reliable study of the amount of time an attacker needs to conduct an attack. However, we can make an estimate from the amount of time it takes to conduct a scan using Nmap. Based on a standard Nmap scan, scanning 1000 ports per computer for 10 IP addresses took an average 78.668 sec. See Appendix C Nmap scanning data for further clarification. The scan also showed that the more ports that were open or even identified as closed, the more time the scan took. For example, a 10 IP address scan from Monterey, CA to Sao Paulo, Brazil with several filtered ports and 2 closed ports took upward of 267 sec. In addition, this was a regular Nmap SYN

31 “Internet Security Threat Report 2011 Trends.”

(synchronization) scan. There are much more intensive scans available. Those more intensive scans are designed to be more intrusive with a correspondingly lower scanning rate, due to both the depth of the scan and in order to reduce detection to IDS hardware and software.[32]

Using the average of 79 sec to scan 10 IP addresses, it is possible for an attacker to scan 7.6 IP addresses a minute or 457 an hour. In an 8-hour period, it is possible to scan around 3660 IP addresses; in a 24 hour period it is possible to scan just under 11,000. Using these numbers, shown in Table 18, in order to attack 5.7 million companies 427 million times in a day through a scan, there would need to be between 42,815 and 128,445 attackers. Considering this is a worldwide problem, it is not inconceivable that there are as many as 128,000 or more attackers in a 2+ billion Internet user population.[33]

SINGLE ATTACKER			
Hours	**Sec**	**IP**	
	7.87	1	
	60	7.6	
	78.67	10	
1	360	458	
8	2880	3661	
24	69120	10983	
Total Hours	**Total Sec**	**Total IP**	
16604	59774256	470232116	Scanning
Total Number of Attackers		42815	24 Hours a Day
		128445	8 Hours a Day

Table 18. Attacker IP Attacks Over Time

Taking the average number of attackers from Table 18 (85630) and using it with the low and high defense cost, it is possible to get an estimate of costs for all attackers conducting attacks. Attackers are likely to be more heavily weighted toward low cost

32 See Appendix C for complete Nmap Scan Report

33 Miniwatts, Internet World Stats: Usage and Population Statistics.

than high cost, so using a similar cost skew, to that of U.S. companies, of 79% low cost attackers and 21% high cost attackers will be used. Therefore, with an average of over 85,000 attackers and allowing for the 79% cost skew toward low cost attack, there are 67,648 low cost attackers. As can be seen in Table 19, the total cost for attackers is just over $11 billion. Using this estimated cost for attack, according to the model the estimated overall cost ratio is 1:131.7, or almost 132 times more expensive.

				LOW COST	HIGH COST
			OFFENSE	$ 27,070.49	$ 519,007.54
		# Low Cost	DEFENSE	$ 35,625.27	$ 1,358,925.57
AVE # ATTACKERS	85630.14	67648	=	$ 1,831,259,362	$ 9,332,964,480
# OF COMPANIES	5734538	4530285	=	$ 161,392,634,565	$ 1,636,490,164,977
Assumption 79% Low Cost (Attackers and Defenders)					
			Offense-Defense Cost Ratio	88.1	175.3
			Average Offense-Defense Cost Ratio =		131.7

Table 19. Average Offense to Defense Cost Ratio

The model indicates that of the 5.7 million U.S. businesses, there is on the order of $1.7 trillion being spent on defense. While this number seems high based on any current corporate cyber security spending analysis,[34] this is a theoretical model which is designed to give an estimate of the balance between the two expenditures. It is not particularly likely that of the 85,000 plus attackers estimated they are spending over $10 billion on attacks either.

Overall the model has done simplifying in order to be usable based on available data. It is certainly possible that the amount spent on personnel is too high, and, it can be argued that the amount spent at the lowest tier of businesses is actually far lower than the number used in the model. For example, many small companies use nothing but anti-virus software as a cyber-defense and have no IT personnel on staff. A further example of cost problems is that while costs are high for personnel defense, it seems unlikely that

34 Eduard Kovacs, "Gartner: Security to Remain a Priority, Spending Might Reach $86 Billion in 2016," Softpedia. September 14, 2012, accessed November 7, 2012, http://news.softpedia.com/news/Gartner-Security-to-Remain-a-Priority-Spending-Might-Reach-86-Billion-in-2016–292307.shtml.

cyber criminals are all being paid on par with the U.S. information technology pay scale. Further research may improve and refine this model as better data with regards to graduations of defense costs and pay become available.

IV. CASE STUDIES

A. ESTONIA

1. Background

In early 2007, Estonia was hit by a major distributed denial of service attack that crippled the country. The most obvious reason for this attack was movement of a Soviet Statue commemorating the defeat of the Nazis in WWII. After World War II, as part of the USSR, Estonia was a reluctant member of the Soviet Union, and, now having achieved independence, the Estonian public felt the statue was a symbol of oppression. Ignoring Russian threats and governmental statements, Estonia moved the stature from its central location. There were street protests and riots by the Russian minority within Estonia, and the government was forced to move the statue in secrecy, eventually settling in a nearby cemetery. However, this did not end the protests and Russian "patriots" began an online protest against Estonia.[35]

The online protest took the form of distributed denial of service (DDoS) attacks using ping floods, synchronize (SYN) floods, and other general data floods. In addition to DDoS attacks on webservers, there were web defacements (using various tools such as SQL injections) and email flooding. The attacks heavily affected the communications infrastructure of Estonia, altered routing tables, overloaded DNS servers, and caused email server mainframes to overload.[36]

Beyond the structure of the attacks, it was the scope that was significant. The attacks literally made the following sites inoperable: the Estonian presidency and its parliament, almost all of the country's government ministries, political parties, three news organizations, two of the biggest banks and communication's firms, governmental

35 Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," Wired.com. August 21, 2007. Accessed August 5, 2012,http://www.wired.com/politics/security/magazine/15–09/ff_estonia?currentPage=all.

36 "Estonia Cyber Attacks Latest 2007," (November 23, 2009, Dakar, Senegal) accessed October 24, 2012, http://meeting.afrinic.net/afrinic-11/slides/aaf/Estonia_cyber_attacks_2007_latest.pdf.

Internet service providers, and most telecom companies. This attack did not go on for one day but went on for weeks, with sites going up and down during that entire time.[37]

The largest attacks came around 9 May and lasted until 11 May 2007. However, attacks were conducted from 26 April through 23 May.[38] According to ArborSert, which published an Estonian DDoS summary on 17 May 2007, there were 128 unique DDoS attacks. Most of the attacks were split between 9 different IP addresses. The attacks varied in length with 17 under a minute, 78 between 1–60 minutes, 16 between 1 and 5 hours, and 7 lasting more than 10 hours. Measured bandwidths varied, but 12 attacks were between 70 and 95 Mbps. The ArborSert analysis indicated at least one major botnet attacked Estonia.[39]

2. Offense

According to Digital Protection, "The New Frontier: Estonia under Cyber Assault," a botnet costs between $5000 and $7000 for around 50,000–70,000 bot-hosts. If each zombie bot is connected to a broadband network at 1Mbps, it is possible for 100 bots to push out the 100Mbps attack that Estonia saw. However, because bots tend to be older machines without updates, and ISPs will tend to quarantine anything putting out that much traffic, the number of bots needs to be much higher in order to produce 100 Mbps.

Based on this assumption, it seems reasonable that the attacking bot nets were around 10,000 computers. Bot machines as explained earlier are machines that are being remotely controlled, all or in part. Bots can be used to add to processor speed for calculations or to distribute the load for transmitted packets as in DDoS attacks.

37 "Estonia Cyber Attacks Latest 2007," 5.

38 Ibid., 5.

39 Jose Nazario, "DDoS and Security Reports: The Arbor Networks Security Blog," ArborSert. May 17, 2007, accessed October 24, 2012, http://ddos.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/.

Karim Hijazi, CEO of Unveillance the Wilmington, DE botnet-tracking firm, estimates that currently of the 4 billion IP addresses, 6% are bot machines.[40] This would be around 360 million machines. 2006 prices to rent a botnet were $500 a day for a 10,000 host system.[41]

The easiest way to distinguish attacks is by bandwidth. Of the attacks against Estonia 52 were 10–30 Mbps, 22 were 30–70 Mbps, and 12 were 70–95 Mbps. By making the assumption that the 12 70–95 Mbps attacks were 10,000 machine botnets at $500 each as per the previous discussion, the 22 30–70 Mbps attacks were done by 5,000 machine botnets at $250 each and the 52 10–30 Mbps attacks were done by 2,500 machine botnets at $125, this comes to $6000 for the 70–95 Mbps, $5500 for the 30–70 Mbps attack, and $6500 for the 10–30 Mbps attack. The entire series of attacks, shown in Table 20, cost $18,000 for the time period that ArborSert tracked the attacks between 3 May and 11 May. According to official records the attacks took place over an entire month, thus multiply $18,000 by 4 and the attack cost roughly $72,000 give or take.

OFFENSE			
52 (10-30 Mbps)	$ 125.00	=	$ 6,500
22 (30-70 Mbps)	$ 250.00	=	$ 5,500
12 (70-95 Mbps)	$ 500.00	=	$ 6,000
	TOTAL		$ 18,000
$ 18,000.00	4 Weeks	=	$ 72,000

Table 20. Estonia Offense Cost Calculations

This does not take into account that some of the attacks were conducted by the same botnet, nor that there might have been discounts based on rental length or Russian

40 Mark Clayton, "Biggest-ever criminal botnet links computers in more than 172 countries." *The Christian Science Monitor*. (2011). accessed October 24, 2012, http://www.csmonitor.com/USA/2011/0629/Biggest-ever-criminal-botnet-links-computers-in-more-than-172-countries.

41 Andrea M. Matwyshyn, "Penetrating the Zombie Collective: Spam as an International Security Issue," *SCRIPT 3*, no. 4 (2006).

patriotic fervor. This also does not take into account website hacking with SQL injections, which would increase the cost, if only for man hours expended.

3. Defense

Estonian defense spending is much more difficult to determine. Based on the websites attacked the entire Estonian government, government ISP servers, all political parties, all telecom systems, 2 banks, and 3 news services were all under attack.

Estonian government spending for 2007 was 76,036,666,000 Kroons (kr).[42] According to FXtop.com, the conversion rate at the time was $1 USD to 10.628 kr. Thus, 76 billion kr becomes $7.153 billion USD.[43] Current U.S. government cyber security spending is about 18% of its information technology (IT) budget.[44] Assuming that Estonia was spending as much as the current U.S. percentage may be a stretch, however it is an average of all departments to include Department of Defense (DoD) at 29% and National Aeronautics and Space Administration (NASA) at 3%. Better data is unavailable at this time.

42 Estonia Ministry of Finance. State Budget 2006–2009, Budget, Talinn, Estonia: Ministry of Finance for the Government of Estonia, 2011.

43 FXTOP Sarl, Historic Currency Conversion rates @ http://fxtop.com/en/historates.php?MA=1

44 U.S. Office of Management and Budget. Fiscal Year 2011 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002, Congressional Report, (Washington, DC: GPO, 2012), 63.

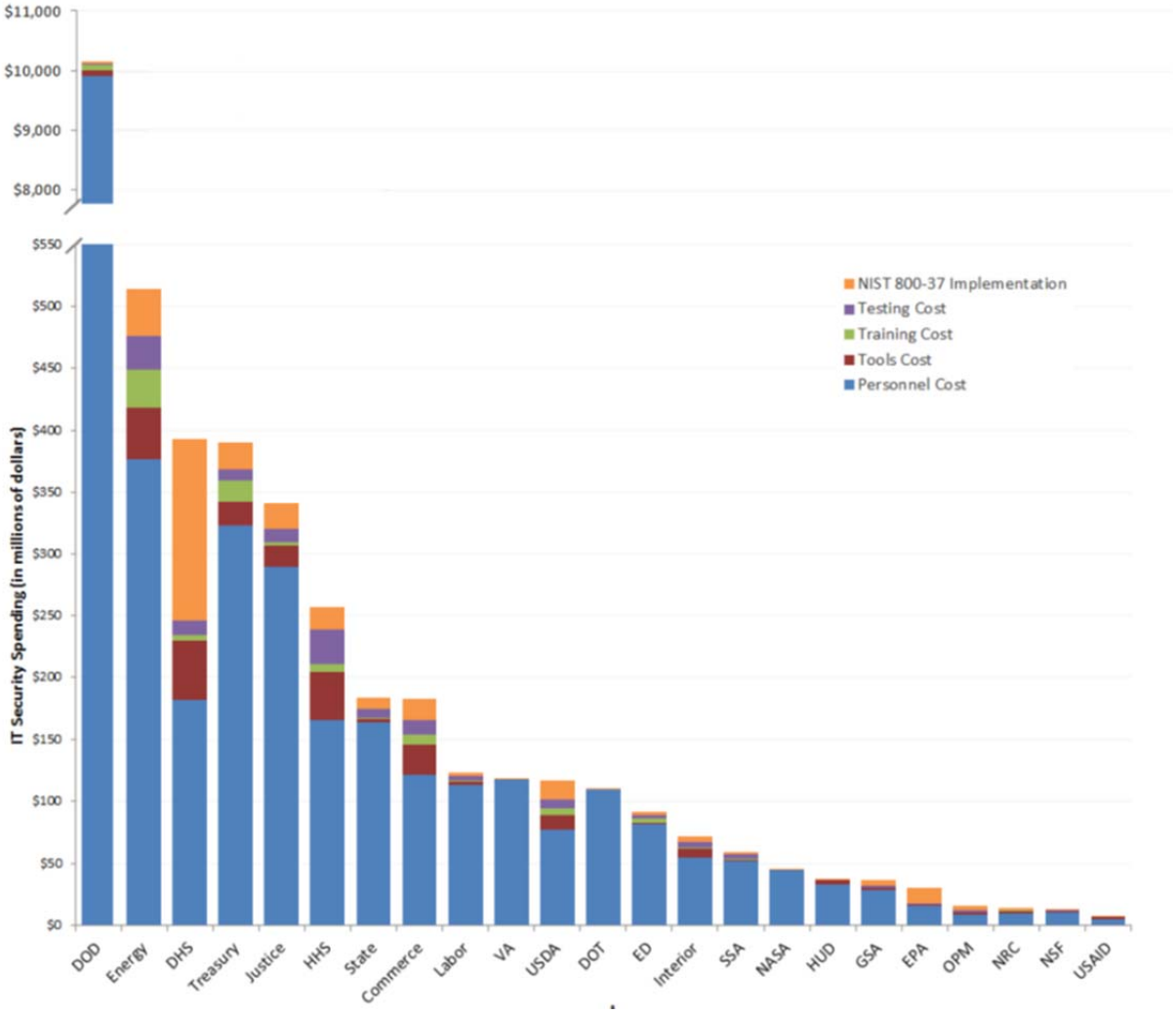


Figure 9. Total U.S. Government IT Security Spending by Department (From OMB 2011)[45]

In 2011 the U.S. government spent $74.106 billion on IT. Using that number, $13.339 billion was spent in the U.S. on IT Security (see Figure 9). Total 2011 U.S. spending was $3,834 billion,[46] making IT spending about 2% of the total spending. Assuming this percentage is about the same for most governments, 2% of Estonia's budget was $143 million. From this with 18% spent on IT Security, it can be estimated that $25.750 million were spent on cyber security by Estonia in 2007. This number does not include the amounts spent by the banks, the telecom systems, or the various political parties.

45 OMB, Fiscal Year 2011 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002, 63.

46 Ibid.

For corporations the running figure for IT spending is around 4% of operating expenses. According to Victor Wheatman, IT security should make up about 5.6% of that number.[47] Using that figure as an example, for a company like the Postimees (2nd Largest Estonian Newspaper in the country, a wholly owned subsidiary of the Norwegian company Schibsted) with $16.189 million in operating costs for 2011,[48] it can be shown that at a minimum they were probably spending about $36,000 USD for cyber security.[49], [50] This is based on data from Estonia GDP growth and current operating expenses for 2011.

In addition to news services, three separate corporate banks were hit. According to Art Gillis, who authors "Automation in Banking," an annual report by his consulting company, large banks spend around 20% of operating expenses on IT.[51] Using that as a reference point and assuming that their security costs increase linearly with IT expenditures, around 28% of that would be on security.

AS SEB Pank, or SEB as it is now known, one of the leading banks in Estonia was one of the banks attacked. According to its 2007 financials it spent around $8.3 million USD in IT costs.[52] Using the estimate of 28% from above, it means that SEB was spending around $2.3 million USD in IT Security.

---

47 Victor Wheatman, "Corporate spending on IT Security." FT.com, November 8, 2011, accessed October 24, 2012, http://www.ft.com/intl/cms/s/0/83f39434–0a23–11e1–92b5–00144feabdc0.html#axzz2ARJsgE5T.

48 Estonian Ministry of Foreign Affairs, "Revenues of Estonian Daily Postimees grow 11 pct in 2011," *Estonian Review*. April 16, 2012, accessed November 7, 2012, http://www.vm.ee/?q=en/node/14229.

49 Statistics Estonia. *Real GDP per Capita, Growth Rate and Totals*. Tallinn, Estonia 2012, accessed November 7, 2012, http://www.stat.ee/29958.

50 2007 costs were derived using national economic growth data percentage change per year (2007, 7.7, 2008–4, 2009–14, 2010 3.4, and 2011 8.3). By this measure estimated operating expenses in 2007 were 10.997 million euro or $16.18 million USD. Using the 4% IT expense ($647,000) and taking 5.6% of that it is estimated that Postimees was spending around $36,000 in IT security.

51 Art Gillis, "Large Banks Blew the Lid off IT Expense in 2010," Bank Systems and Technology. April 05, 2011, accessed October 24, 2012, http://www.banktech.com/core-systems/large-banks-blew-the-lid-off-it-expense/229400900.

52 As SEB Pank, *Annual Report 2007*, Annual Financial Report, (Talinn, Estonia: AS SEB Pank, 2007).

4. Framework Estimate

If you take this data, for the number of companies that were hit, 3 news services and 2 banks, the corporations spent around $4.7 million on cyber security. That number added to the estimated $25 million spent by the government, means that for the $72,000 spent by the attackers the defenders spent $30.5 million. Based on the proposed offense defense framework that would mean the attack to defense ratio is 1 to 423. Tables 21 and 22 show the calculations for the Estonia case.

DEFENSE				
ESTONIAN GOVERNMENT				
2%	$ 7,153,000,000	=	$ 143,060,000	Government IT Spending
0.18	$ 143,060,000	=	$ 25,750,800	Security as a % of IT Spending
ESTONIAN CORPORATION				
Postimees				
€ 10,950,000.00				2011 Operating Costs
in 2007	2007 Exchange Rate			
€ 10,997,140	1.4721		$ 16,188,889	See Appendix 2: GDP Rate Change adjusted for Operating costs
€ 16,188,889	4%	=	$ 647,556	4% IT Costs
€ 647,556	5.6%	=	$ 36,263	5.6% IT Costs are security
SEB				
88,300,000 kr	0.094084	=	$ 8,307,617	2007 IT Costs, as per 2007 Financial Statements
$ 8,307,617	28%	=	$ 2,326,133	20% IT costs are security
TOTAL ESTONIAN CORPORATIONS				
3 News (Postimees)				
$ 36,263	3	=	$ 108,789	
2 Banks (SEB)				
$ 2,326,133	2	=	$ 4,652,266	
TOTAL DEFENSE SPENDING				
Government	Corporations	=	Estonian Total	
$ 25,750,800	$ 4,761,055	=	$ 30,511,855	

Table 21. Estonian Cyber Defense Calculations [53][54]

ESTONIA OFFENSE-DEFENSE COST RATIO			
OFFENSE	**DEFENSE**		**RATIO**
$ 72,000	$ 30,511,855	=	424

Table 22. Estonia Estimated Offense-Defense Cost Ratio

[53] For most corporations or government spending, numbers are determined without breaking it down into the model constituent parts of Personnel, Hardware and Software

[54] Refer to Footnote 50 above.

This scenario cost for offense is lower than the theoretical model using U.S. prices. There are some obvious reasons for this. The primary reason is that the only attack costs are Botnet rental prices, without any other attack costs added. However, it can be argued that the lack of data for other Estonian companies or political parties makes up for the lack of further attack costs. Additionally, it can also be argued that DDoS attacks, focused on flooding bandwidth, are an extremely cheap attack and can be conducted by the lowest cost of attacker.

Using the proposed offense-defense model, for the Estonian scenario, the offense-defense balance breaks down to Offense 72,000 : Defense 30,511,854 or for every 1 dollar spent on offense, around $424 was spent on defense; see Table 22.

B. STUXNET CASE STUDY

1. Background

Between June and July 2010 a virus now commonly known as Stuxnet was discovered. Stuxnet is a term derived by anti-virus experts who studied the worm from part of the code. The virus was spread through a number of Microsoft Windows vulnerabilities, several of which were zero-day vulnerabilities.

Unlike many previous computer viruses, this one specifically targeted industrial systems with the intent to cause catastrophic failure to the system. Specifically it focused on what are known as supervisory control and data acquisition (SCADA) systems and the programmable logic controllers (PLCs) that control physical devices, in this case centrifuges used to enrich uranium.[55] Another of the other innovations that was unique to Stuxnet, at the time, was that while it spread indiscriminately, it specifically targeted Siemens control systems. If those systems did not exist on the system, the virus did nothing but reproduce itself.[56]

---

[55] Nicolas Falliere, Liam O. Murchu, and Eric Chien, *W32.Stuxnet Dossier (Version 1.4)*, White Paper, Cupertino, CA: Symantec Corporation, 2011.

[56] Viyat Ghandhi, "Stuxnet : The Most Amazing Computer Virus Of All Time— Know all about it," TechnoGrafy. December 24, 2011, accessed November 7, 2012, http://technografy.blogspot.com/2011/12/stuxnet-most-amazing-computer-virus-of.html.

It is also interesting to note that initial discovery and evaluation determined that Stuxnet was a program to conduct cyber espionage, stealing sensitive industrial control data. It was only later that further analysis revealed that the program was designed to subvert specific control systems for Siemens industrial systems.[57]

Further research and investigation by David Sanger, provided in his book "Confront and Conceal," revealed that the Stuxnet virus was created by a joint U.S. and Israeli team in order to disrupt Iranian nuclear enrichment operations. The system was designed the way it was in order to spread throughout Iran and jump an airgap, through removable media, between wired Iranian networks and the secure systems inside Iranian nuclear plants.[58]

However, it is the time and resources for this particular computer attack that are the most interesting from an Offense-defense balance perspective. This attack took significant time to plan, develop intelligence, build, and then execute. Additionally while the attack was extremely resource intensive, the cyber defenses in place to defend against it were more physical than cyber.

2. Defense

Iranian nuclear cyber security costs are not easily available. However, some details are known. According to David Sanger, the focus of the attack was against the uranium enrichment plant Natanz. Based on reports this facility was air-gapped, which means that it was not wired to the rest of the Internet. However, it has been estimated that the Natanz plant cost an estimated $270 million USD to build, with an estimated

[57] Eric Chien, "W32.Stuxnet Dossier," Symantec. February 4, 2011, accessed November 7, 2012, http://www.symantec.com/connect/blogs/w32stuxnet-dossier

[58] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, June 1, 2012: A1.

$20,000 USD per centrifuge.[59] This number is extremely rough; however, it gives a baseline in order to determine the size of the facility, in comparison to other nation's nuclear facilities.

For clarification the budget of the U.S. National Nuclear Security Administration (NNSA), a department within the U.S. Department of Energy, was $9.9 billion in 2010. Of that, defense of nuclear security was $769.8 million (7.7% of U.S. DoE Budget), with $25.3 million of that specifically going to information security.[60]

Estimated Iranian GDP for 2010 was $331.015 billion. U.S. GDP for 2010 was $14,582 billion USD.[61] Based on this Iran's GDP is 2.3% of that of the United States. U.S. total spending on energy was $26.425 billion; of that $9.873 billion was spent on the U.S. NNSA for nuclear energy (or the nuclear program is .0677% of GDP).[62] For purposes of the model an estimate of Iranian nuclear spending could be said to be the same, thus giving a ballpark figure of $224.1 million USD for nuclear power.

Another method is to estimate what Iran is spending on nuclear weapons development as a percentage of defense. This method assumes that nuclear development is tied to defense as it is for the other countries that have developed nuclear weapons, including the U.S., India, Pakistan, and China to name a few. According to Global Zero's Nuclear Weapons Cost Study, the average amount nuclear countries spend on defense is

---

59 Geoffrey Forden, "What Does Natanz Cost?" Arms Control Wonk, June 27, 2009, accessed November 7, 2012 http://forden.armscontrolwonk.com/archive/2363/what-does-natanz-cost.

60 Chief Financial Officer, U.S. National Nuclear Security Administration, *Department of Energy FY2012 Congressional Budget Request National Nuclear Security Administration. Budget Request,* Washington, DC: GPO, 2011.

61 "Data GDP (2007–2011)," The World Bank. 2012, accessed November 7, 2012, http://data.worldbank.org/indicator/NY.GDP.MKTP.CD.

62 CFO, NNSA, *Department of Energy FY2012 Congressional Budget Request National Nuclear Security Administration. Budget Request.*

9%.[63] Iranian defense spending in 2008, was estimated at $9.174 billion, of which 9% is $825.7 million (Data from 2010 was not available).[64]

In addition to these methods, President Ahmadinejad said in a speech, "the U.S. has recently added $81 billion to its current budget on nuclear weapons, some 300 times the entire Iranian nuclear budget," which would provide an estimated $270 million for Iran's nuclear budget.

Using the average from the three estimates above provides an estimated Iranian Nuclear budget of $371.045 million USD. Assuming 7.7% goes to defense of the nuclear program, Iranian nuclear defense spending can be roughly estimated to be $33.85 million. Because both cyber and physical defenses were important to this attack the entire defense budget is used. See Table 23 for calculations of Iranian nuclear defense spending.

[63] Matthew A. Brown, and Bruce G. Blair, "Nuclear Weapons Cost Study | June 2011," White Paper, Washington, DC: Global Zero, 2011.

[64] Carina Solmirano, and Pieter D. Wezeman, "Military Spending and Arms Procurement in the Gulf States," Fact Sheet, (Solna, Sweden: Stockholm International Peace Research Institute, 2012.

DEFENSE				
US GDP	**IRAN GDP**		**Iran GDP as a % of US GDP**	
$ 14,582,000,000,000.00	331,015,000,000	=	2.27%	
IRAN NUCLEAR COMPARED TO U.S. NNSA				
	U.S. NNSA Total		**NNSA Defense**	**NNSA IT Security**
	$ 9,873,000,000.00		$ 769,823,000.00	$ 25,300,000.00
% of US GDP	0.06771%		0.005279%	0.0001735%
IRAN NUCLEAR ENERGY SPENDING AS A PERENTAGE OF GDP		=	$ 224,119,537.44	
IRAN NUCLEAR SPENDING AS % OF DEFENSE				
	TOTAL SPENDING		**9% of TOTAL**	
Iran Defense Spending (2008)	$ 9,174,000,000.00	=	$ 825,660,000.00	
Nuclear Spending on average 9%				
PRESIDENT AHMADINEJAD ESTIMATE				
300% of U.S. SPENDING	**US**		**IRAN**	
	81,000,000,000	=	$ 270,000,000.00	
AVERAGE OF IRANIAN SPENDING ESTIMATES				
% OF GDP			**$ 224,119,537.44**	
% OF DEFENSE SPENDING			$ 825,660,000.00	
% of US SPENDING			$ 270,000,000.00	
	AVERAGE	=	$ 439,926,512	
IRANIAN NUCLEAR DEFENSE AS % OF NUCLEAR BUDGET				
NNSA TOTAL BUDGET	**NUCLEAR DEFENSE**		**IRANIAN NUCLEAR**	
$ 9,873,000,000.00	$ 769,823,000.00		**DEFENSE**	
% of NNSA BUDGET	7.797%	=	$ 34,302,193	

Table 23. Iranian Nuclear Defense Estimate

3. Offense

The Stuxnet software itself is extremely complex. Internal code describes numerous sub-systems which were developed separately. Additionally, the Stuxnet software itself has three distinct versions, with compile times of June 2009, March 2010, and April 2010.[65] Symantec experts estimate what it would have required to build the system;

> The code is sophisticated, incredibly large, required numerous experts in different fields, and mostly bug-free, which is rare for your average piece

65 Nicolas Falliere, et al., W32.Stuxnet Dossier

> of malware. Stuxnet is clearly not average. We estimate the core team was five to ten people and they developed Stuxnet over six months. The development was in all likelihood highly organized and thus this estimate doesn't include the quality assurance and management resources needed to organize the development as well as a probable host of other resources required, such as people to setup test systems to mirror the target environment and maintain the command and control server.[66]

David Sanger suggests that not only was the code developed between two different countries over a period of several years, with extensive reconnaissance of the target system network, but that the code was tested on live centrifuge systems to ensure that it would cause catastrophic failure as planned.[67] This adds, in addition to the coding requirements, extensive reconnaissance and a live systems test with Siemens centrifuges to the costs of development. Beyond development costs there is also a cost to secrecy. Ben Rich and Leo James estimated in, "Skunk Works: A Personal Memoir My Years at Lockheed" that at least 25% more cost was added to a secret project for security requirements and overhead.[68]

4. Framework Estimate

Using these numbers as a baseline, a very rough estimate can be generated for Offense cost. A ten-man team working for 4 years, 2006–2010, can be estimated from advertised U.S government pay rates for information security between, $45,771–$129,517 per year.[69,70] The average of those salaries would be $87,644 a year or $3.505 million for the team over a four-year period. Cost for a functioning centrifuge is

66 Ibid.

67 Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," A1.

68 Leo Janos, and Ben R. Rich. *Skunk Works: A Personal Memoir of My Years at Lockheed* . (Boston, MA: Back Bay, 1996).

69 U.S. Office of Personnel Management, 2010 Salary Tables and Related Information, Washington, DC, GPO, 2012, accessed November 7, 2012, http://www.opm.gov/oca/10tables/.

70 U.S. Office of Personnel Management, USA Jobs (Information Technology). November 1, 2012, accessed November 7, 2012, https://www.usajobs.gov/JobSearch/Search/GetResults?Keyword=Information+Technology&Location=&search.x=24&search.y=11.

$20,000.[71] According to U.S. NNSA data there are 33,000 employees, both government and civilian contractors,[72] and a cyber-infrastructure budget of $99.838 million, meaning on average $3,025 a year is spent per employee. Because the team would have been dedicated IT personnel, with extensive computing needs, the average IT infrastructure cost will be doubled for each person on the team. Over a four year period, the team's share of the infrastructure costs would thus be $242 thousand dollars. Adding this to the personnel and centrifuge costs, and then an additional 25% across the board for secrecy, it took $4.709 million to execute Stuxnet. See Table 24 for calculations.

OFFENSE						
	LOW		HIGH	AVERAGE	10 People	TOTAL BUDGET (4 Years)
WAGES FOR 10 PERSON TEAM	$ 45,771		$ 129,517	$ 87,644	$ 876,440	$ 3,505,760
CENTRIFUGE			$ 20,000			$ 20,000
	PERSONNEL		BUDGET	COST PER PERSON PER YEAR	IT PEOPLE (x2)	
INFRASTRUCTURE	33000		$ 99,838,000	$ 3,025	$ 6,051	$ 242,032
TOTAL						$ 3,767,792
SECRECY FACTOR (+25%)						$ 4,709,739

Table 24. Estimated Stuxnet Offense Costs

STUXNET OFFENSE DEFENSE COST RATIO			
DEFENSE*	OFFENSE		RATIO
$ 34,302,193	$ 4,709,739	=	7.3

Table 25. STUXNET Estimated Offense-Defense Cost Ratio

Table 25 shows that based on the proposed model the offense-defense balance in this scenario is $4.7 million of offense spent against $34.3 million of defense, or for every $1 dollar spent on offense $7.30 was spent on defense.

71 Forden, "What Does Natanz Cost?"

72 National Nuclear Security Administration, "Our Jobs, NNSA Federal Employment," NNSA November 7, 2012, accessed November 7, 2012, http://nnsa.energy.gov/federalemployment/ourjobs.

For this scenario the cost for offense is much higher than the theoretical model. There are some obvious reasons for this. The primary reason is that it was a massive project, with U.S. costs and salaries over a multiyear life cycle. This project was secret and David Sanger's book notwithstanding, the budget for this project is still highly classified. Other reasons include the fact that it is a single attacker against a single defender, which should bring the number closer to the 1 to 2 ratio, rather than the ratio of total number of attackers to defenders at 1:132. In addition to attack costs estimations, there are a large number of assumptions made on Iranian nuclear defense spending, which may also be slanting the ratio. However, it seems likely that while the cost may not be 1 to 7, it is almost certainly at the extreme edge of attack spending to defense. Further research might provide greater clarity on the input data, which would refine the balance numbers.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

Offense-defense balance theory is an interesting, though controversial, concept. It postulates that conflict will increase in the international system if the cost of offense is less than the cost to defend. In the physical world, this theory is complicated by a number of factors such as multiuse technology and the tendency that all other things being equal, defense is stronger than offense. However, in the cyber domain these issues are reduced and the offense-defense balance can more clearly be seen.

Cyber-attacks have increased by leaps and bound between 2010 and 2011. According to Symantec global threat report, in almost all areas cyber threats have increased, some by as much as 81%. The only reduction seen was in spam, and that reduction was only seen with pharmaceutical spam.

According to the Symantec report there were 5.5 billion attacks blocked in 2011, up from 3 billion in 2010.[73] This global span of attacks indicates that conflict in cyberspace is a growing problem. Even with billions of dollars spent globally on computer defense, the attacks are increasing. According to offense-defense balance theory this is because the cost of offense is less than the cost of defense.

It can be seen through a quick scan of news articles on cyber space that hacking and cyber-attacks are perceived as a major problem. Using a quick Google news search will bring hundreds if not thousands of hits for “cyber-attack” every day. While this is not an accurate measurement, it does indicate how pervasive the threat has become.

When looked at through the proposed framework, it can be seen that the costs of attack are significantly lower than the costs to defend. In fact, the only time when an attack nears the costs of a defense is at the lowest level with a single attacker compared to a single low cost defender. And as it was shown in the theoretical estimate, the cost of that offensive act is still 80% of the cost of defense. Based on the theoretical model at the high levels, it is around 2.5 times more expensive to defend against an attacker. In

73 “Internet Security Threat Report 2011 Trends,” 15.

addition, even at the high cost level, the model does not take into account the need to scale defenses for larger companies that employ more than 1400 employees. For example, a company such as Wal-Mart which employs over 2.2 million people, has exponentially higher costs for cyber defense than a small company.[74]

From the single attack numbers, the picture is not particularly bad. While a ratio of one to two should indicate some conflict, 5.5 billion attacks blocked by Symantec alone indicate much more than "some." If you look at the estimated number of attacks against the number of companies, the numbers become much different. It can be seen that using a calculation based on the number of attacks possible, from an average computer over a 24 hour period, with 427 million attacks in the U.S. a day there are around 85,000 attackers. With that many attackers compared to the 5.7 million U.S. firms defending against them, the ratio of attackers to firms becomes 1:130 which is much more disconcerting than the initial estimate, between a single attacker and a single defender of a one to two ratio.

The case studies examined present an even more interesting set of numbers. Using the proposed model gives a very high defense cost ratio in the case of Estonia and a very low one in the case of Stuxnet. However, the offense-defense balance model, while hampered by very rough data, clearly showed the balance was in favor of the attack in both cases.

The Stuxnet case shows that even an extremely costly attack, using massive amounts of resources and time, using the available data, was still 7 times less expensive than the cost of the defenses in place.

And in the case of the cyber-attack on Estonia, a lower cost attack focused on a relatively small geographic area and a finite number of defenders, the attack costs were shows 400 times less than was spent on defense. The Estonia attacks were an automatic bandwidth flooding system and were not particularly sophisticated, which lowered the costs. However, in both case studies, the attackers succeeded on every level.

---

74 "FORTUNE 500 annual ranking of America's largest corporations," CNN Money. May 21, 2012, accessed November 7, 2012, http://money.cnn.com/magazines/fortune/fortune500/2012/performers/companies/biggest//.

There are several limitations to the methodology in this thesis. Each of the It is assumed that for offense and defense that at least one of every system is purchased. This is not true in all cases; it is especially not true when it comes to defensive software and hardware where the functions are so similar. The size of the corporations and their respective security measures are not adequately differentiated which could affect costs, drastically in some cases. Additionally offensive costs were assumed to be computers, botnets and proxies with the assumption that the rest of the attackers' costs are either freeware or can be incorporated into wages; this assumption too adds to the limitations.

In addition to limits of cost and scale, the methodology also assumes the price ranges are accurate, which considering the differences in services offered with high end products may add a significant margin of error. Cost of system management and system monitoring in addition to personnel wages was not discussed, and probably requires more clarification for more accuracy.

Security costs are also an issue, because while physical security measures are discussed, for purposes of the model they are not incorporated into anything but the Stuxnet case study. It was determined that for purposes of the model that physical security costs could not be separated betweenwhat is needed to keep out physical threats and cyber threats. However, with further research it may be possible to reduce this issue and provide a clearer model with regard to physical security.

Probably the key limitation for the methodology is personnel costs. The model assumed that all personnel wages are the same, for both the attacker and defender. This is not even true for the defender. For large organizations there are set pay systems, smaller companies are less similar in wages, with significantly more variation. In the initial assumptions, the methodology assumed that both offensive and defensive personnel cost for training was similar enough that it could be removed; with additional resources and time that could be examined which may help refine personnel costs as well. However, the biggest limitation for personnel is the wage cost of a cyber-attacker. For some cyber attackers it is true they operate on a pay scale, such as government cyber forces. However, at the other end of the cyber attacker spectrum are criminals and hobbyists whose wages without further data adds some significant error to the model.

The application of the proposed offense defense model in cyberspace provides an estimate of the current balance point. It provides an indication, of where cyberspace currently rests. With an estimated 1:132 offense-defense ratio of attackers to defenders, it seems inevitable that conflict will occur. Jervis's theory, that conflict increases the cheaper offense is to defense, seems exceptionally clear in cyberspace.

This current balance point is not a final answer. It can be argued that unlike physical weapon systems infrastructure, the cost to adjust software is minuscule. In a number of respects, it is significantly cheaper to make changes in cyberspace. These changes may provide an opportunity to adjust the balance more in favor of defense. Costs change every day, and the data provided herein is a snapshot in time. The model's estimated balance should not be viewed as a negative indicator, but should be viewed as a base line to determine methods to adjust it more in favor of defense. In addition to technological adjustments, some scholars talk of working toward adjusting societal norms which would reduce cyber-attacks through self-policing.[75] In the end, the proposed model is not good or bad. It is an estimate of where cyberspace currently sits.

[75] Libiciki, *Cyberdeterrence and Cyberwar.*

APPENDIX A: CONSOLIDATED DEFENSE THEORETICAL MODEL CALCULATIONS

DEFENSIVE COSTS					
HARDWARE	LOW COST	LOW COST 2	HIGH COST 2	HIGH COST	AVERAGE COST
Firewall	$ 79.81	$ 90.00	$ 12,073.00	$ 34,317.00	$ 11,639.95
VPN	$ 80.95	$ 87.27	$ 39,993.00	$ 65,695.50	$ 26,464.18
IDS/IPS	$ 5,517.00	$ 5,763.00	$ 48,546.00	$ 91,032.00	$ 37,714.50
TOTAL HARDWARE	$ 5,677.76			$ 191,044.50	$ 75,818.63
SOFTWARE	LOW COST	LOW COST 2	HIGH COST 2	HIGH COST	AVERAGE COST
Anti-Virus	$ -	$ 12.00	$ 88.77	$ 99.49	$ 50.07
VPN	$ 32.00	$ 45.00	$ 6,264.00	$ 73,922.00	$ 20,065.75
IDS/IPS	$ 107.22	$ 155.05	$ 38,526.00	$ 62,062.00	$ 33,581.02
Proxy	$ -	$ 135.00	$ 21,579.03	$ 24,283.65	$ 24,283.65
Encryption	$ -	$ 6.06	$ 115.46	$ 10,562.00	$ 2,670.88
Network Analyzers	$ 1.00	$ 97.38	$ 6,330.00	$ 7,012.94	$ 3,360.33
TOTAL SOFTWARE	$ 140.22			$ 177,942.08	$ 84,011.69
PERSONNEL	AVERAGE SALARY	HOURLY*			
ADMINISTRATIVE	$ 148,600	$ 59.44			
APPLICATIONS DEVELOPMENT	$ 93,589	$ 37.44			
CONSULTING AND SYSTEMS INTEGRATION	$ 106,854	$ 42.74			
DATA/DATABASE ADMINISTRATION	$ 102,688	$ 41.08			
QUALITY ASSURANCE AND TESTING	$ 82,000	$ 32.80			
INTERNET AND E-COMMERCE	$ 81,554	$ 32.62			
NETWORKING / TELECOMMUNICATIONS	$ 89,422	$ 35.77			
OPERATIONS	$ 59,292	$ 23.72			
SECURITY	$ 106,750	$ 42.70			
SOFTWARE DEVELOPMENT	$ 99,042	$ 39.62			
TECHNICAL SERVICES, HELP DESK AND TECHN	$ 63,025	$ 25.21			
*Hourly wage is based on a 50 hour week, for a 50 week year subdivision of salary					
	LOW	HIGH	AVERAGE		
PERSONNEL	$ 29,807	$ 989,939	$ 509,873		
TOTAL DEFENSIVE	LOW	HIGH	AVERAGE		
HARDWARE	$ 5,678	$ 191,045	$ 75,819		
SOFTWARE	$ 140	$ 177,942	$ 84,012		
PERSONNEL	$ 29,807	$ 989,939	$ 509,873		
TOTAL	$ 35,625	$ 1,358,926	$ 697,275		
Costs are pulled from top 2 and bottom two costs, as per November 2012 online sales data					
Items are delineated based on a single identifier, such as number of sessions on a VPN hardware					
Primary cost was pulled from www.google.com (Google Shopping), confirmed through individual website specifications					

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B: CONSOLIDATED OFFENSE THEORETICAL MODEL CALCULATIONS

OFFENSIVE COSTS					
HARDWARE	LOW COST	LOW COST 2	HIGH COST 2	HIGH COST	AVERAGE COST
COMPUTERS	$ 279.99	$ 289.99	$ 3,130.98	$ 9,039.00	$ 3,185
BOTNETS*	$ 600.00	$ 900.00	$ 900.00	$ 1,200.00	$ 900
TOTAL HARDWARE	$ 280			$ 10,239	$ 5,259
SOFTWARE	LOW COST	LOW COST 2	HIGH COST 2	HIGH COST	AVERAGE COST
BOTNET*	$ 100.00	$ 300.00	$ 350.00	$ 500.00	$ 312.50
PROXY	$ 3.00	$ 3.50	$ 25.00	$ 55.00	$ 21.63
TOTAL SOFTWARE	$ 103.00			$ 55.00	$ 79.00
***ADJUSTED BOTNET COSTS**	LOW COST	LOW COST 2	HIGH COST 2	HIGH COST	AVERAGE COST
BOTNET: HARDWARE	$ 600	$ 900	$ 900	$ 1,200	$ 900.00
BOTNET: SOFTWARE	$ 100	$ 300	$ 350	$ 500	$ 312.50
*As specified in the model, Botnets will cost from hardware or software, depending on which is higher or lower, for each category					
TOTAL BOTNET ADJUSTED COSTS	$ 100	$ 300	$ 900	$ 1,200	$ 625.00
PERSONNEL	AVERAGE SALARY	HOURLY*			
ADMINISTRATIVE	$ 148,600	$ 59.44			
APPLICATIONS DEVELOPMENT	$ 93,589	$ 37.44			
CONSULTING AND SYSTEMS INTEGRATION	$ 106,854	$ 42.74			
DATA/DATABASE ADMINISTRATION	$ 102,688	$ 41.08			
QUALITY ASSURANCE AND TESTING	$ 82,000	$ 32.80			
INTERNET AND E-COMMERCE	$ 81,554	$ 32.62			
NETWORKING / TELECOMMUNICATIONS	$ 89,422	$ 35.77			
OPERATIONS	$ 59,292	$ 23.72			
SECURITY	$ 106,750	$ 42.70			
SOFTWARE DEVELOPMENT	$ 99,042	$ 39.62			
TECHNICAL SERVICES, HELP DESK AND TECHNICAL SUPPORT	$ 63,025	$ 25.21			
*Hourly wage is based on a 50 hour week, for a 50 week year subdivision of salary					
	LOW	HIGH	AVERAGE		
PERSONNEL	$ 26,688	$ 508,714	$ 267,701		
TOTAL OFFESIVE	LOW	HIGH	AVERAGE		
HARDWARE	$ 280	$ 10,239	$ 5,259		
SOFTWARE	$ 103	$ 55	$ 79		
PERSONNEL	$ 26,688	$ 508,714	$ 267,701		
TOTAL	$ 27,070	$ 519,008	$ 273,039		

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C: NMAP SCAN DATA

A. SCAN COMPUTER CONFIGURATION

Processor: Intel i7, 3.5 Ghz

Broadband Speed: 10.2 Mbps Download; 3 Mbps Upload [76]

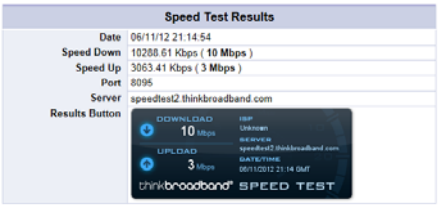


Figure 10. Broadband Speed Test Results

B. SCAN METHODOLOGY

IP Scan Addresses, using 5 different series of IP geolocated through www.nirsoft.net for each specific location. Figures 11-15 show the specific Nmap scan data.

C. SCAN RESULTS

1. East Cost

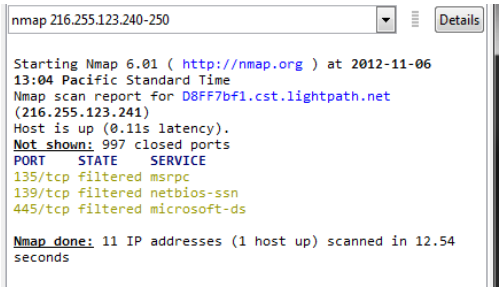


Figure 11. Nmap Results Vicinity NY, NY (216.255.123.240–250)

Speed 12.54 Sec (10 IP addresses) 1 Host up (3 Filtered Ports)

[76] Broadband speed discerned through thinkbroadband.com

2. Europe

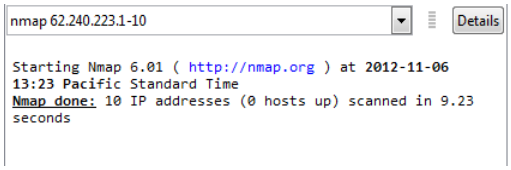


Figure 12. Nmap Results Vicinity Zurich, Switzerland (62.240.223.1–10)

Speed 9.23 Sec (10 IP addresses) 0 Hosts up

3. Africa

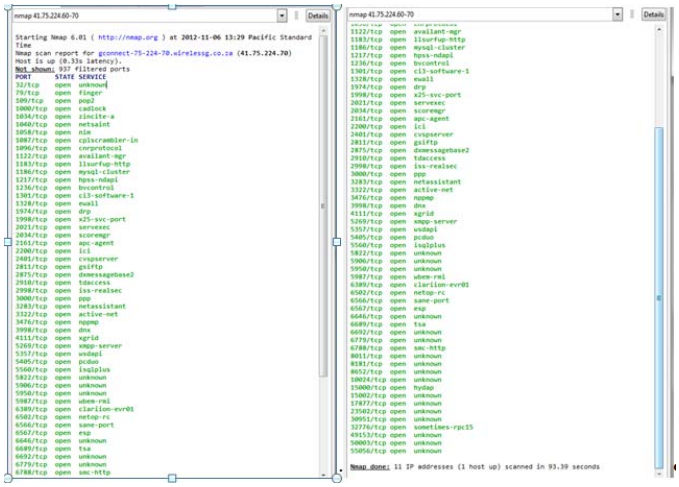


Figure 13. Nmap Results Vicinity Durban, South Africa (41.75.224.60–70)

Speed 93.39 Sec (10 IP addresses) 1 Hosts up (63 open ports)

4. China

Figure 14. Nmap Results Vicinity Jinan, China (58.15.1.70–80)

Speed 10.32 Sec (10 IP addresses) 0 Hosts up

5. South America

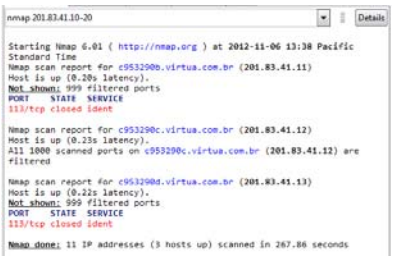


Figure 15. Nmap Results Vicinity Sao Paulo, Brazil (201.83.41.10–20)

Speed 267.86 Sec (10 IP addresses) 3 Hosts up (2 Closed Ports)

D. SCAN CONCLUSION

Table 26 shows the summary of geolocated IP addresses and times. Table 27 shows the scan time calculations for 470 million IP addresses.

LOCATION	IP RANGE (START)	IP RANGE (END)	SPEED (SEC)	HOSTS	PORTS (OPEN/FILTERED /CLOSED)
New York, NY	216.255.123.240	216.255.123.250	12.54	1	3 FILTERED
Zurich, Switzerland	62.240.223.1	62.240.223.10	9.23	0	N/A
Durban, South Africa	41.75.224.60	41.75.224.70	93.39	1	63 OPEN
Jinan, China	58.15.1.70	58.15.1.80	10.32	0	N/A
Sao Paulo, Brazil	201.83.41.10	201.83.41.20	267.86	3	2 CLOSED

Table 26. Nmap Standard Scan Results

SINGLE ATTACKER			
Hours	**Sec**	**IP**	
	7.87	1	
	60	7.6	
	78.67	10	
1	360	458	
8	2880	3661	
24	69120	10983	
Total Hours	**Total Sec**	**Total IP**	
16604	59774256	470232116	Scanning
Total Number of Attackers		42815	24 Hours a Day
		128445	8 Hours a Day

Table 27. Nmap Based Time to Scan Calculations for 470 million IP Addresses

APPENDIX D: CONSOLIDATED ESTONIA CASE STUDY CALCULATIONS

DEFENSE				
ESTONIAN GOVERNMENT				
2%	$ 7,153,000,000	=	$ 143,060,000	Government IT Spending
0.18	$ 143,060,000	=	$ 25,750,800	Security as a % of IT Spending
ESTONIAN CORPORATION				
Postimees				
€ 10,950,000.00				2011 Operating Costs
in 2007	2007 Exchange Rate			
€ 10,997,140	1.4721		$ 16,188,889	See Appendix 2: GDP Rate Change adjusted for Operating costs
€ 16,188,889	4%	=	$ 647,556	4% IT Costs
€ 647,556	5.6%	=	$ 36,263	5.6% IT Costs are security
SEB				
88,300,000 kr	0.094084	=	$ 8,307,617	2007 IT Costs, as per 2007 Financial Statements
$ 8,307,617	28%	=	$ 2,326,133	20% IT costs are security
TOTAL ESTONIAN CORPORATIONS				
3 News (Postimees)				
$ 36,263	3	=	$ 108,789	
2 Banks (SEB)				
$ 2,326,133	2	=	$ 4,652,266	
TOTAL DEFENSE SPENDING				
Government	Corporations	=	Estonian Total	
$ 25,750,800	$ 4,761,055	=	$ 30,511,855	

OFFENSE			
52 (10-30 Mbps)	$ 125.00	=	$ 6,500
22 (30-70 Mbps)	$ 250.00	=	$ 5,500
12 (70-95 Mbps)	$ 500.00	=	$ 6,000
	TOTAL		$ 18,000
$ 18,000.00	4 Weeks	=	$ 72,000

ESTONIA OFFENSE-DEFENSE COST RATIO			
OFFENSE	**DEFENSE**		**RATIO**
$ 72,000	$ 30,511,855	=	424

ESTONIAN GDP RATE WITH REGARD TO POSTIMEES OPERATING EXPENSES					
	8.30%	3.40%	-14%	-4%	7.70%
€ 10,950,000	€ 10,110,803	€ 9,778,340	€ 11,370,163	€ 11,843,919	€ 10,997,140
2011	2010	2009	2008	2007	

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E: CONSOLIDATED STUXNET CASE STUDY CALCULATIONS

.

DEFENSE					
US GDP	IRAN GDP		Iran GDP as a % of US GDP		
$ 14,582,000,000,000.00	331,015,000,000	=	2.27%		
IRAN NUCLEAR COMPARED TO U.S. NNSA					
	U.S. NNSA Total		NNSA Defense	NNSA IT Security	
	$ 9,873,000,000.00		$ 769,823,000.00	$ 25,300,000.00	
% of US GDP	0.06771%		0.005279%	0.0001735%	
IRAN NUCLEAR ENERGY SPENDING AS A PERENTAGE OF GDP		=	$ 224,119,537.44		
IRAN NUCLEAR SPENDING AS % OF DEFENSE					
	TOTAL SPENDING		9% of TOTAL		
Iran Defense Spending (2008)	$ 9,174,000,000.00	=	$ 825,660,000.00		
*Nuclear Spending on average 9%					
PRESIDENT AHMADINEJAD ESTIMATE					
300% of U.S. SPENDING	US		IRAN		
	81,000,000,000	=	$ 270,000,000.00		
AVERAGE OF IRANIAN SPENDING ESTIMATES					
% OF GDP			$ 224,119,537.44		
% OF DEFENSE SPENDING			$ 825,660,000.00		
% of US SPENDING			$ 270,000,000.00		
	AVERAGE	=	$ 439,926,512		
IRANIAN NUCLEAR DEFENSE AS % OF NUCLEAR BUDGET					
NNSA TOTAL BUDGET	NUCLEAR DEFENSE		IRANIAN NUCLEAR DEFENSE		
$ 9,873,000,000.00	$ 769,823,000.00				
% of NNSA BUDGET	7.797%	=	$ 34,302,193		

OFFENSE						
	LOW		HIGH	AVERAGE	10 People	TOTAL BUDGET (4 Years)
WAGES FOR 10 PERSON TEAM	$ 45,771		$ 129,517	$ 87,644	$ 876,440	$ 3,505,760
CENTRIFUGE			$ 20,000			$ 20,000
	PERSONNEL		BUDGET	COST PER PERSON PER YEAR	IT PEOPLE (x2)	
INFRASTRUCTURE	33000		$ 99,838,000	$ 3,025	$ 6,051	$ 242,032
TOTAL						$ 3,767,792
SECRECY FACTOR (+25%)						$ 4,709,739

STUXNET OFFENSE DEFENSE COST RATIO			
DEFENSE*	OFFENSE		RATIO
$ 34,302,193	$ 4,709,739	=	7.3
* Estimated costs include both cyber and physical			

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

As SEB Pank. *Annual Report 2007*. Annual Financial Report, Talinn, Estonia: As SEB Pank, 2007.

Boyd, Clark. "Profile: Gary McKinnon." BBC News, July 30, 2008.

Brown, Matthew A., and Bruce G. Blair. "Nuclear Weapons Cost Study | June 2011." White Paper, Washington, DC: Global Zero, 2011.

Chief Financial Officer, U.S. National Nuclear Security Administration. *Department of Energy FY2012 Congressional Budget Request National Nuclear Security Administration*. Budget Request, Washington, DC: GPO, 2011.

Chien, Eric. "W32.Stuxnet Dossier." Symantec. February 4, 2011. http://www.symantec.com/connect/blogs/w32stuxnet-dossier (accessed November 7, 2012).

Clausewitz, Carl V. On War. 1984. Edited by Michael Howard and Peter Paret. Translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.

Clayton, Mark. "Biggest-ever criminal botnet links computers in more than 172 countries." *The Christian Science Monitor*. June 29, 2011. http://www.csmonitor.com/USA/2011/0629/Biggest-ever-criminal-botnet-links-computers-in-more-than-172-countries (accessed October 24, 2012).

"CPU Benchmarks." PassMark Software , November 1, 2012. http://www.cpubenchmark.net/ (accessed November 1, 2012).

Danchev, Dancho. "Study finds the average price for renting a botnet." ZD Net.com. May 26, 2010. http://www.zdnet.com/blog/security/study-finds-the-average-price-for-renting-a-botnet/6528 (accessed November 7, 2012).

"Data GDP (2007–2011)" World Bank. 2012. http://data.worldbank.org/indicator/NY.GDP.MKTP.CD (accessed November 7, 2012).

Davis, Joshua. "Hackers Take Down the Most Wired Country in Europe." *Wired.com*. August 21, 2007. http://www.wired.com/politics/security/magazine/15–09/ff_estonia?currentPage=all (accessed August 5, 2012).

EMC Corporation. *Life in the FAAS Track*. Webcast, Bedford, MA: RSA, Security Division of EMC, 2012. http://www.rsa.com/products/consumer/whitepapers/11794_120612_Life_in_The_FaaS_Track.pdf. (accessed November 19, 2012).

"Estonia Cyber Attacks Latest 2007." (November 23, 2009, Dakar, Senegal), http://meeting.afrinic.net/afrinic-11/slides/aaf/Estonia_cyber_attacks_2007_latest.pdf (accessed October 24, 2012).

Estonia Ministry of Finance. *State Budget 2006–2009*. Budget, Talinn, Estonia, 2011.

Falliere, Nicolas, Liam O. Murchu, and Eric Chien. W32.Stuxnet Dossier (Version 1.4). White Paper, Cupertino, CA: Symantec Corporation, 2011.

Federal Communications Commission, *Broadband Performance, OBI Technical Paper NO. 4*. Technical Paper, Washington, DC: GPO, 2010.

Forden, Geoffery. "What Does Natanz Cost?" Arms Control Wonk. June 27, 2009. http://forden.armscontrolwonk.com/archive/2363/what-does-natanz-cost (accessed November 7, 2012).

"FORTUNE 500 annual ranking of America's largest corporations." CNN Money. May 21, 2012. http://money.cnn.com/magazines/fortune/fortune500/2012/performers/companies/biggest// (accessed November 7, 2012).

Ghandhi, Viyat. "Stuxnet : The Most Amazing Computer Virus Of All Time— Know all about it." TechnoGrafy. December 24, 2011. http://technografy.blogspot.com/2011/12/stuxnet-most-amazing-computer-virus-of.html (accessed November 7, 2012).

Gillis, Art. "Large Banks Blew the Lid off IT Expense in 2010." Bank Systems and Technology. April 05, 2011. http://www.banktech.com/core-systems/large-banks-blew-the-lid-off-it-expense/229400900 (accessed October 24, 2012).

Goncharov, Max. *Russian Underground 101*. Research Paper, Cupertino, CA: Trend Micro International, 2012.

Greenberg, Andy. "Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits." *Forbes,* March 3, 2012: 2.

Internet Crime Complaint Center. *2010 IC3 Internet Crime Report.* Annual, Washington, DC: National White Collar Crime Center, 2010.

"Internet Security Threat Report 2011 Trends." Threat Report, Symantec Corporation, 2012.

Janos, Leo, and Ben R. Rich. *Skunk Works: A Personal Memoir of My Years at Lockheed*. Boston, MA: Back Bay, 1996.

Jervis, Robert. "Cooperation under the Security Dilemma." *World Politics* 30, no. 2 (1978): 167–214.

Kovacs, Eduard. “Gartner: Security to Remain a Priority, Spending Might Reach $86 Billion in 2016.” Softpedia. September 14, 2012. http://news.softpedia.com/news/Gartner-Security-to-Remain-a-Priority-Spending-Might-Reach-86-Billion-in-2016–292307.shtml (accessed November 7, 2012).

Libicki, Martin. Cyberdeterrence and Cyberwar. Santa Monica, CA Rand Corporation, 2009.

Levy, Jack S. “The Offensive/Defensive Balance of Military Technology: A Theoretical and Historical Analysis.” *International Studies Quarterly* 28, no. 2 (1984): 219–238.

Lynn-Jones, Sean M. “Offense Defense Theory and its Critics.” *Security Studies* 4, no. 4 (1995): 660–691.

Matwyshyn, Andrea M. “Penetrating the Zombie Collective: Spam as an International Security Issue.” *SCRIPT-ed* 3, no. 4 (2006).

Mearsheimer, John J. “Assessing the Conventional Balance: The 3:1 Rule and Its Critics.” *International Security* 13, no. 4 (1989): 54–89.

Ministry of Foreign Affairs, Estonia. “Revenues of Estonian daily Postimees grow 11 pct in 2011.” *Estonian Review*. April 16, 2012. http://www.vm.ee/?q=en/node/14229 (accessed November 7, 2012).

Miniwatts Marketing Group. *Internet World Stats: Usage and Population Statistics*. June 30, 2012. http://www.internetworldstats.com/stats.htm (accessed November 7, 2012).

Mulvenon, James C., and Gregory J. Rattray. *Addressing Cyber Instability: Executive Summary*. Executive Summary, Washington, DC: Cyber Conflict Studies Association, 2012.

National Nuclear Security Administration. NNSA Federal Employment “Our Jobs.” November 7, 2012. http://nnsa.energy.gov/federalemployment/ourjobs (accessed November 7, 2012).

Nazario, Jose. “DDoS and Security Reports: The Arbor Networks Security Blog.” ArborSert. May 17, 2007. http://ddos.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/ (accessed October 24, 2012).

“Order: Personal / Corporate.” PureVPN. November 1, 2006. http://www.purevpn.com (accessed October 24, 2012).

Quester, George H. *Offense and Defense in the International System*. John Wiley and Sons, 1977)

"Robert Half® Technology 2013 Salary Guide." Robert Half International. 2012. http://www.rhi.com/SalaryGuides (accessed October 24, 2012).

Sanger, David E. "Obama Order Sped Up Wave of Cyberattacks Against Iran." New York Times, June 1, 2012: A1.

Schwartz, Nelson D. "F.B.I. Says 24 Are Arrested in Credit Card Theft Plan." New York Times, June 26, 2012.

Solmirano, Carina, and Pieter D. Wezeman. Military Spending and Arms Procurement in the Gulf States. Fact Sheet, Solna, Sweden: Stockholm International Peace Research Institute, 2012.

Statistics Estonia. *Real GDP per capita, growth rate and totals*. Tallinn, Estonia 2012. http://www.stat.ee/29958 (accessed November 7, 2012).

U.S. Computer Emergency Response Team. *Control Systems Security Program (CSSP)*. 2012. http://www.us-cert.gov/control_systems/csvuls.html (accessed November 12, 2012).

U.S. Census Bureau. *U.S. Department of Commerce, U.S., all industries [xls, 2.8 MB]*. Washington D.C., October 25, 2012. http://www.census.gov/econ/susb/index.html (accessed November 7, 2012).

U.S Intellectual Property Enforcement Coordinator. *2011 Annual Report on Intellectual Property Enforcement*. Annual, Washington, D.C.: GPO, 2011.

U.S. Office of Management and Budget. *Fiscal Year 2011 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002*, Congressional Report, Washington D.C., GPO, 2012.

U.S. Office of Personnel Management. *2010 Salary Tables and Related Information.* Washington D.C.. 2012. http://www.opm.gov/oca/10tables/ (accessed November 7, 2012).

———. *USA Jobs (Information Technology)*. Washington D.C.: November 1, 2012. https://www.usajobs.gov/JobSearch/Search/GetResults?Keyword=Information+Technology&Location=&search.x=24&search.y=11 (accessed November 7, 2012).

Wheatman, Victor. "Corporate spending on IT security." FT.com. November 8, 2011. http://www.ft.com/intl/cms/s/0/83f39434–0a23–11e1–92b5–00144feabdc0.html#axzz2ARJsgE5T (accessed October 24, 2012).

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Information Proponent Office
   Fort Leavenworth, Kansas

4. 1st IO Command
   Fort Belvoir, Virginia

5. Marine Corps Information Operations Center
   Quantico, Virginia

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu