

THE DECISION TO ATTACK:
MILITARY AND INTELLIGENCE CYBER DECISION-MAKING

by

AARON FRANKLIN BRANTLY

(Under the Direction of Loch K. Johnson)

ABSTRACT

The debate over the importance of cyber has resulted in the consideration of a new domain of operation vital to national security. States find themselves in an increasingly interconnected world with a diverse threat spectrum and little understanding of how decisions are made within this amorphous domain. Much of the literature on cyber has focused on defining what cyber is. This dissertation examines how states decide to employ cyber in military and intelligence operations against other states. The research question this work seeks to answer is: do states rationally decide to employ cyber in military and intelligence operations against other states? This work contextualizes broader cyber decision-making processes into a systematic expected utility - rational choice approach to provide a mathematical understanding behind the use of cyber weapons at the state level.

INDEX WORDS: Cyber, Intelligence, National Security, Decision-Making

THE DECISION TO ATTACK:
MILITARY AND INTELLIGENCE CYBER DECISION-MAKING

by

AARON FRANKLIN BRANTLY

B.A., Queens University of Charlotte, 2004

M.P.P., The American University, 2008

A Dissertation Submitted to the Graduate Faculty of the University of Georgia in Partial

Fulfillment of the Requirements for the Degree

DOCTOR OF PHILOSOPHY

ATHENS, GEORGIA

2012

© 2012

AARON FRANKLIN BRANTLY

All Rights Reserved

THE DECISION TO ATTACK:
MILITARY AND INTELLIGENCE CYBER DECISION-MAKING

by

AARON FRANKLIN BRANTLY

Major Professor:	Loch K. Johnson
Committee:	Jeffrey Berejikian
	Han S. Park
	Michael Warner
	Christopher Bronk

Electronic Version Approved:

Maureen Grasso
Dean of the Graduate School
The University of Georgia
December 2012

DEDICATION

I dedicate this work to my wife and best friend Nataliya. She has stood by me and waited for more than 5 years while I finished my formal academic education. She has read, commented on, and reread more of my words than anyone. It is her patient and enduring support, which have enabled me to make it as far as I have.

ACKNOWLEDGEMENTS

This work would not have been possible without the support and dedication of the diverse committee standing behind me and pushing me forward. In particular, I would like to thank Dr. Loch K. Johnson for his constant feedback and assistance in helping me to develop the ideas presented in this work. Dr. Johnson has inspired me both as a professor and as a mentor. I would also like to thank Dr. Jeffrey Berejikian, Dr. Han S. Park, Dr. Michael Warner, and Dr. Christopher Bronk each of whom have given enormous amounts of time to help me with my academic and professional pursuits.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS	v
LIST OF TABLES	x
LIST OF FIGURES & CHARTS	xi
GLOSSARY	xii
INTRODUCTION	1
CHAPTER 1 Introduction to Cyber Decision-making	2
What is cyber and why is it important?	3
Cyber and International Relations	15
Understanding decisions of states: the logic of rational choice modeling	18
How this work is organized	35
CHAPTER 2	37
The Key Concepts of Cyber	37
Why is cyber important to national security?	38
Why is cyber an inherently asymmetric domain?	53
CHAPTER 3	62
The Motivation and Utility for Covert Action	62
The motivation and rationality for conflict	64
Political utility and the literature	73
The use of covert action for political utility	75

Afghanistan 1980s.....	82
Italy 1948.....	83
Estonia 2007.....	84
Syria 2007.....	86
Stuxnet 2009.....	87
The Utility of Covert Action	89
Section II - The foundations of a rational decision	90
CHAPTER 4.....	91
Digital Power	91
Defining the components of digital hard power.....	94
Cyber and its vulnerabilities.....	106
Conceptualizing cyber power.....	110
CHAPTER 5.....	113
Anonymity and Attribution in Cyberspace.....	113
The importance of anonymity	114
Political action and anonymity	119
The value of anonymity.....	120
Anonymity, attribution, and decisions	124
Summarizing the debate	126
CHAPTER 6.....	128
Cyber and Conventional: The Dynamics of Conflict	128
The language of conflict.....	129
Combinatory attacks.....	134
Stand-alone conflict.....	139
Cyber and conventional tools a tale of objectives.....	141

CHAPTER 7.....	144
Defining the Role of Intelligence in Cyber	144
Defining Intelligence.....	150
Intelligence and the cyber battlespace.....	158
Policy considerations.....	164
CNE - Network Mapping, Systemic Dependencies, and Historical Records	166
HUMINT and Cyber	175
Time to Attack Recognition, Completion, and Attribution.....	176
IPB and its impact on cyber	178
Utility and Cyber Intelligence	181
Summarizing the role of intelligence within the cyber domain	182
Part III	184
A formal decision-making model for actions within the cyber domain.....	184
CHAPTER 8.....	185
How actors decide to use cyber - a rational choice approach.....	185
Uncertainty & Risk.....	189
Utility Theory of (Cyber) Conflict	191
Next Steps.....	204
CHAPTER 9.....	206
Applying the Expected Utility Theory of International Cyber Conflict.....	206
The expected utility of states across incidents	209
Examining the propositions.....	214
Data in context.....	221
Part IV.....	224

Conclusion	224
CHAPTER 10.....	225
Finding meaning in the expected utility of international cyber conflict.....	225
Take away lessons	225
Failings and areas for improvement	229
The implications of the expected utility theory of international cyber conflict	232
APPENDIX A: POWER SCORE COMPONENTS & SCORE	236
APPENDIX B: MODIFIED ECONOMIST INTELLIGENCE UNIT COMPONENT VALUES	237
APPENDIX C: AFFINITY SCORES	253
WORKS CITED	254

LIST OF TABLES

	Page
Table 1.1: Sampling of cyber controlled instruments pertinent to national security	8
Table 1.2: Presidential Directives/Decisions Pertaining to IT and Cyber 1993-2009	12
Table 1.3: Typologies of computer network operations	22
Table 4.1: Components of Power	105
Table 4.2: Power Scores by Country	111
Table 5.1: Probability of Maintaining Anonymity by Attack	123
Table 7.1: Intelligence collection methods	153
Table 7.2: Components of cyber DBA & DBK.....	163
Table 7.3: Cyber threat spectrum.....	171
Table 9.1: Expected Utilities Across Incidents	211
Table 9.2: Results of t-Tests of utilities	216
Table 9.3: t-Tests of affinity of state likelihood of conflict.....	217
Table 9.4: t-Test of state affinity in year prior to conflict	219

LIST OF FIGURES & CHARTS

	Page
Figure 1.1: Understanding state policy positions.....	20
Figure 2.1: The modern structure of national security.....	40
Figure 2.2: Graphical representation of information diffusion in the new public square.....	42
Chart 2.1: E-commerce as % of total wholesale trade	49
Chart 2.2: E-Commerce total value of sales (million dollars)	49
Figure 2.3: Percentage of individuals using the Internet	60
Figure 3.1: Fearon's bargaining range	68
Figure 3.2: Bi-lateral state policy interaction possibilities	72
Figure 3.3: Covert Action Ladder	81
Figure 4.1: Percentage of individuals using the Internet within countries in the sample	108
Figure 6.1: Objective, Scale and Tools of Conflict	142
Figure 7.1: The Intelligence Cycle.....	160
Figure 7.2: Detailed Network Map	168
Figure 7.3: Timeline for attack implementation	177
Figure 7.4: The influence of intelligence on cyber operations	179
Figure 9.1: State Cyber Power Scores	207
Figure 9.2: Expected Utilities Boxplot	215
Figure 9.3: Distribution of changes in affinity over time	218
Figure 9.4: Distribution of state affinities in year prior to hostilities	219

GLOSSARY

CENTCOM	Central Command
CERT	Computer Emergency Response Team
CINC	Composite Index of National Capabilities
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Computer Network Operations
COW	Correlates of War Project
CYBERINT	Cyber Intelligence
DBA	Dominant Battlespace Awareness
DBK	Dominant Battlespace Knowledge
DDOS	Distributed Denial of Service
DOS	Denial of Service
GEOINT	Geo-Spatial Intelligence
HUMINT	Human Intelligence
ICT	Information Communications Technology
INTs	Intelligence Collection Categories
IPB	Intelligence Preparation of the Battlefield
ISP	Internet Service Provider
MASINT	Measurement and Signatures intelligence

OSINT	Open Source Intelligence
PLC	Programmable Logic Controller
REDEU	Rank Dependent Expected Utility
SAM	Surface to Air Missile
SCADA	Supervisory Control and Data Acquisition
SIGINT	Signals Intelligence
TCP/IP	Transmission Control Protocol/Internet Protocol

INTRODUCTION

CHAPTER 1

Introduction to Cyber Decision-making

The debate over the importance of cyber has resulted in the consideration of a new domain of operation vital to national security. States find themselves in an increasingly interconnected world with a diverse threat spectrum and little understanding of how decisions are made within this amorphous domain. Much of the literature on cyber has focused on defining what cyber is. This work asks the research question: do states rationally decide to employ cyber in military and intelligence operations against other states? This dissertation examines how states decide to employ cyber in military and intelligence operations against other states. This work contextualizes broader cyber decision-making processes into a systematic expected utility - rational choice approach to provide a mathematical understanding behind the use of cyber weapons at the state level.

Is it really necessary to create an entirely new decision-making model for the cyber domain? Illustrated in the coming chapters are examples from the literature, scholars, and policy-makers the clear fact that the cyber domain is distinct from more conventional domains of military and intelligence interaction such as land, sea, air and space. What differentiates cyber from these other domains are four primary attributes. First, the cyber domain is a man-made domain. Second, military capabilities across the other domains are managed through the cyber domain. Third, military and civilian aspects of the cyber domain are often intertwined and difficult to differentiate. Fourth, attribution within the cyber domain is difficult to assign. These attributes combine to create an entirely novel domain of interaction necessitating a different decision-making model.

This work explicitly focuses on a rational choice decision-making model based on Bruce Bueno de Mesquita's development of a utility theory of international conflict in which he maps out values of characteristics associated with the instigation of international conflict. This work builds a rational actor model predicated on the assumption that nation-state cyber actors seek to achieve a positive policy outcomes through the engagement of hostile action with cyber weapons.

This introductory chapter has two main tasks. The first task is to outline what cyber is, and why it is important. This will provide the reader with a framework in which to understand the topic for discussion in this work. The second task is to examine what conventional decision-making models have done, and why they fail to account for the uniqueness of the cyber domain.

What is cyber and why is it important?

It is unlikely there is or has ever been anyone alive who can credibly claim to be the father of land, sea, air, or space. The creation of these other domains is referred to as the product of a cosmic accident or the will of God. Any contemporary individual coming forward taking credit for the creation of one of these conventional domains would surely be subject to the strictest psychological evaluation.

The same could not be said of the creators of cyberspace. Cyberspace can be traced back to a single point and perhaps two original creators, Vinton Cerf¹ and Bob Kahn². These two pioneers in networking and TCP/IP were the precursors of the modern information renaissance.³ Whereas land is defined by its terrestrial nature, sea by vast amounts of water, and air by its fluid properties, cyberspace is defined by the linking of computers.

¹ Vinton G. Cerf, "The day the Internet age began," *Nature* 461, no. 7268 (2009).

² Katie Hafner, "Laurels for Giving the Internet Its Language," *New York Times* 2005.

³ Transmission Control Protocol/Internet Protocol

Computers, the basic unit of the cyber domain, run on simple coding forms constructed of 1's and 0's indicating the on and off of electrical impulses. Long chains of electrical impulses form commands. These commands are written in long blocks called code. Historically coding was time consuming and difficult, often done on punch cards fed into machines. The difficulty of coding eventually gave rise to programming languages. These languages provided a simplified means of writing code. Coding languages are written in logical if - then statements that interact with one another. These statements are then built on top of one another into ever more complicated combinations forming firmware⁴ and software.⁵

Conceptually firmware and software are directions or recipes for action all returning back to the distribution of electrical impulses within hardware.⁶ These impulses are incredibly fast and provide end users with a virtually seamless functional experience. However, without these impulses and the commands and the logical statements defining the commands, the computer, the fundamental particle of the cyber domain, is nothing more than a box of plastic and metal. The device is then similar to a rock, it cannot be given a verbal command or told what to do or have any existential meaning beyond its atomic structure, geo-position, mass, and volume.

The value of the cyber domain lies in its ability to create a virtual world from trillions of commands hopscotching around the world and interacting with one another in logically defined environments, and the ability of commands within digital environments to control devices. A computer is incapable of irrationality. Giving a computer competing logical statements can test

⁴ Firmware is a term often used to denote the fixed, usually rather small, programs and/or data structures that internally control various electronic devices

⁵ Software, is a collection of computer programs and related data that provides the instructions for telling a computer what to do and how to do it.

⁶ Hardware are component devices which are typically installed into or peripheral to a computer case to create a computer upon which system software is installed including a firmware interface such as a BIOS and an operating system supporting application software that performs the operator's desired functions.

the rationality of a computer. Most computer users have had this happen to them. Their computer freezes, or the mouse icon spins. The logical routine is stuck and cannot proceed.

Value in cyber is a reflection of connections to the systems of systems of logic and contained in its ability to store, interact, connect, and control. The power and danger in cyber is the relationship that information has with the world around it. Computers monitor the emergency systems of a nuclear power plant and alerts operators and other systems connected to it whether core temperature is too high or too low. Cyber technologies facilitate the safe and efficient operation of these plants. Similarly the computers that monitor where trains are within a subway system to prevent trains from getting too close to one another, or alerts them that a section of track is out. When this code fails, as was the case in Metro collision in Washington, D.C. in 2009,⁷ the digital failure yields real world pain. Cyber is valuable because it connects, and controls, and interacts with aspects of our everyday lives. It is the interaction and the increasing dependence on cyber that influences its value.

Increasing connections cause the cyber domain to expand and increase its value. Whereas the value of land increases as it becomes scarcer or the content of that land is found to have items contained within it of value to the market, the value of cyberspace increases along in a dynamic relationship with its connections. The growth in value is neither linear nor exponential, however, the value is inherent and can be easily understood.

Our lives, our hopes, and our existence in modern society are directly tied to the cyber world. We depend upon magnetic strips on credit cards to feed and cloth us. We tote mobile lifelines, send e-mails, receive phone calls, and conduct commerce on these devices. Our bank accounts are numbers stored in computers, and the value of our life savings can be wiped away

⁷ Christopher Conkey, Elizabeth Williamson, and Cam Simpson, "Washington Metro Delayed Upgrades," *The Wall Street Journal*, 24 June 2009.

with a stroke of a keyboard. But beyond these modern inventions we are dependent on the electromagnetic spectrum to manage our power grids, the ordering systems that ensure our gas stations have fuel, and our grocery stores have food. We don't have to plug ourselves into the matrix; we already live in it.

The domain is remarkably fragile when compared to conventional domains in that a disruption in the connections that link us to the domain can have a profound effect on our lives. It is very difficult to remove a person from land without killing them, detaining them and forcibly moving them. Land is static. The person using the land must be moved to deny them access. The same is not true of cyber. To deny an individual access it is only necessary to turn off the power, cut the cord, or shut down an Internet Service Provider (ISP). Anyone who has ever tried to buy groceries during a blackout has found it extremely difficult unless they were in possession of hard currency prior to the outage and even then most stores cannot conduct business without electricity, as their sales and inventory systems are dependent on digital connections. Not only can an individual not withdraw hard currency when the power is down, he or she cannot use their credit cards to purchase goods. These connections sustain modern society and undergird the fabric of our everyday lives.

Much as the general public has become increasingly dependent on cyber and its increases in communications, efficiency, and general facilitation of activities in modern life, information technology has also dramatically altered the landscape of national security and created a revolution in military affairs.⁸

Conceptually we comprehend cyber is important and dramatically affects our lives, but what is cyber? Kramer, Starr, and Wentz acknowledge more than 19 different definitions of

⁸ *The national strategy to secure cyberspace*, ([Washington, D.C.]: President's Critical Infrastructure Protection Board, 2003); Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, *Cyberpower and National Security*, 1st ed. (Washington, D.C.: National Defense University Press : Potomac Books, 2009). See Page 193.

cyber,⁹ giving a moving target, difficult to pin down. This work has settled on Kuehl's definition as the most encompassing of various agencies and author positions. Kuehl defines cyber as:

*"A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify exchange, and exploit information via interdependent and interconnected networks using information-communication technologies."*¹⁰

The above definition is formal and difficult to fully digest. So before moving on it is necessary to deconstruct its component parts.

Electronics:¹¹ the branch of physics and technology concerned with the design of circuits using transistors and microchips, and with the behavior and movement of electrons in a semiconductor, conductor, vacuum, or gas.

Electromagnetic Spectrum:¹² the range of wavelengths or frequencies over which electromagnetic radiation extends

More simply these two define the physical characteristics of the domain. The operational characteristics of this domain are defined by the creation, storage, modification, and exploitation of data (information). The target of operations or the asset within domain is information. This information can be used to influence both intra-domain operations, for example how information

⁹ Kramer, Starr, and Wentz, *Cyberpower and National Security*.

¹⁰ Ibid. See Kuehl p28.

¹¹ J. A. Simpson, E. S. C. Weiner, and Press Oxford University, *The Oxford English dictionary* (Oxford; Oxford; New York: Clarendon Press ; Oxford University Press, 1989).

¹² Ibid.

is displayed or shared on a network, and/or extra-domain operations, manipulating the output of an information process such as how a robot in a car manufacturing plant operates to place pieces together.

What is information? Information is a very broad concept best summarized for cyber as:

Information: Computing data as processed, stored, or transmitted by a computer.¹³

This definition hides the value the word itself contains. Data can be programs designed to operate factories, devices, power stations, and much more. But data can also be facts and figures about people, places, and things. Both types of data have value and often both can be interoperable. One type is proactive in affecting digital processes; the other is static in that its value is to the user or consumer.

Despite defining the component parts of the domain it remains difficult to fully understand what the domain constitutes. Table 1.1 is a list of a small sampling of those aspects of national security connected to cyber.

Table 1.1: Sampling of cyber controlled instruments pertinent to national security¹⁴

Satellites	Radio transmissions
Drones	GPS
Heads up displays for pilots	Most modern avionics
Communications technologies	Logistical coordination systems
Intellipedia	Smart projectiles
Electric grids	Power plants
Banks	Stock exchanges

All of the above items in some way make use of cyber for their operation.

Cyber is amorphous and evolving. Tangible boundaries between countries within cyber are difficult to identify and easy to overcome.¹⁵ While the conventional domains of land, sea, and

¹³ Ibid.

¹⁴ This table does not distinguish between public and private cyber domains.

air, are bounded, the cyber domain increases in size and value with every new connection, and every advance in computing power. Although cyber has been defined above, its importance to everyday life and national security are integral to understanding cyber from a military and intelligence perspective.

For military commanders and their men on the battlefield, communication always has been important. Communication technologies have evolved significantly since the use of tools such as the Semaphore, a system of flags could send up to 196 different signals more than 200 years ago.¹⁶ The digital revolution for communication technology can be traced back to the Crimean War and the extension of European telegraph lines.¹⁷ The Crimean War was the first conflict in which policy-makers at home could quickly and efficiently receive and transmit information on operations in the field hundreds, if not thousands of miles away. The 1899 invention of the wireless further advanced the information revolution.¹⁸ Each of these advances played a dramatic role not only in the conduct of warfare from an organizational perspective, but also from a policy perspective. Battlefield information could be transmitted back to populations and greatly affect popular perceptions of conflict.

These early technologies were limited and often had drawbacks. Telegraph lines could be cut, preventing critical information from reaching its destination, or worse telegraph lines could be tapped and provide an enemy with information on troop movements, positions, logistics, and strategy. Radios contained many of the same problems of their telegraph cousins. The signals could be intercepted and read. Worse still for aviators or to the benefit of their targets,

¹⁵ Sean S. Costigan and Jake Perry, *Cyberspaces and global affairs* (Farnham, Surrey; Burlington, VT: Ashgate, 2012). See Chapter 1.

¹⁶ Jeremy Black, *War and the world : military power and the fate of continents, 1450-2000* (New Haven, Conn.: Yale University Press, 1998).

¹⁷ Ibid.

¹⁸ Ibid.

information technology had not caught up with the needs of aviators. Radio transmissions during World War I from Luftwaffe aircraft and zeppelins could provide reliably accurate time and target information and allow for defensive actions over Great Britain.¹⁹ Later in World War II the use of radar allowed for early warning on incoming aircraft with a greater degree of accuracy than radio triangulation, but because it was a new technology and its operators relatively inexperienced, the information it provided was critically ignored/misinterpreted in the bombing of Pearl Harbor.²⁰

Each new development in information communication technology has advanced the conduct of modern warfare from both a military strategic and tactical, as well as an intelligence collection and operations perspective. Information technology is not new. It has, as the two previous paragraphs illustrate, been used for more than a century. Information transference has evolved since its infancy gaining in prominence in multiple ways. The importance of information really took off with the invention of computers.

Computers, which had been around since just prior to World War II, were massive, difficult to use, and had limited functionality. Enormous progress was made on computers throughout the post war period. The most dramatic stride in computing occurred with the invention of ARPANET, a Defense Advanced Research Project on 29 October 1969.²¹ Whereas previously computers were independently functioning machines, ARPANET linked these machines enabling them to communicate with one another. The dramatic strides of ARPANET and progress on computer processing power were of immense value and influenced modern society in everything from commerce and banking to national security and defense. The next

¹⁹ See Chapter 2 in M. L. Dockrill and David French, *Strategy and intelligence : British policy during the First World War* (London; Rio Grande, Ohio: Hambledon Press, 1996).

²⁰ David Kahn, "The Intelligence Failure of Pearl Harbor," *Foreign Affairs*, 1 December 1991.

²¹ Jessica Savio, "Browsing history: A heritage site is being set up in Boelter Hall 3420, the room the first Internet message originated in," *Daily Bruin*, 1 April 2011.

great leap forward in the information revolution occurred with the development of the World Wide Web.

John Arquilla and David Ronfeldt early on contended that information has risen from a tool in support of strategic and tactical advantage to a “fourth dimension of national power.”²² This view, is however, somewhat ignorant of the role of information in the conduct of state and international relations over time and places a newness of emphasis on an aspect of national power that has been of significance for millennia. Information has been a vital aspect of national and international political power since before Sun Tzu in the sixth century B.C. and Kautilya in the 350 B.C.²³ Joseph Nye, widely known for his writings on power and its relationship to states in international relations, finds that cyber is part of an information revolution.²⁴ The value of information has always been inherent in the development of power; however, the tools to quickly access information are quite modern.

Cyber is a domain through which information transference has flourished. While the advent of the Guttenberg press spread the written word and enhanced information transference, information was still limited to those who could afford it. Whereas for centuries information was kept mainly by the few, in the last 30 years the diffusion of information has increased in pace. In the 1970's and even in the 1980's a scholar had to go to library to find articles written by his or her peers, now the library quite literally can go where the author is. The July 2011 DoD Strategy for Operating in Cyberspace makes note that in the last 10 years alone the number of internet

²² See chapter 18 in John Arquilla and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: Rand Corporation, 1997).

²³ See particularly the introduction on the role of information in warfare in Edward Waltz, *Information warfare : principles and operations* (Boston: Artech House, 1998).; See book I and Book XII on the spying and knowledge/information and the benefits they bring to a leader in Kautilya and L. N. Rangarajan, *The Arthashastra* (New Delhi; New York, N.Y., USA: Penguin Books India, 1992).

²⁴ Joseph S. Nye, *The future of power* (New York: PublicAffairs, 2011).

users has risen from approximately 360 million to more than 2 billion.²⁵ Google announced in 2010 that it had scanned over 12 million books and later that same year established the goal of scanning the remaining known 118 million volumes by the end of the next decade.²⁶ These efforts effectively place the equivalent of the collective knowledge of humanity within a few mouse clicks. Yet the ability to store information is in and of itself not the only important aspect of the cyber domain.

There are numerous departmental, congressional committee, executive reports, and analyses on the value of information technology and cyber. Table 1.2 highlights the importance of the cyber domain by referencing presidential directives directly relating to information technology and cyber. The table provides just a small snapshot of the broader governmental efforts to understand, safeguard, and employ the cyber domain.

Table 1.2 Presidential Directives/Decisions Pertaining to IT and Cyber 1993-2009²⁷

Directive	Title	Date
PDD/NSC 3	Public Encryption Management	15 Apr 1993
PRD/NSC 27	Advanced Telecommunications and Encryption	16 Apr 1993
PRD/NSC 48	International Market for Software Products Containing Encryption	1994
PRD/NSC ??	Information Assurance	14 Mar 1996
PDD/NSC ??	Encryption Export Policy	15 Nov 1996
PDD/NEC ?	Electronic Commerce	1 Jul 1997
PDD/NSC 63	Critical Infrastructure Protection	22 May 1998
PDD/NSC 66	Encryption Policy	16 Nov 1998
PDD/NEC ?	Further Work on Electronic Commerce	30 Nov 1998
PDD/NSC 68	U.S. International Information Policy	30 Apr 1999
NPSD 16	To Develop Guidelines for Offensive Cyber-warfare	Jul 2002
HSPD	Critical Infrastructure Identification, Prioritization, and Protection	17 Dec 2003
NSPD 38	National Strategy to Secure Cyberspace	2004
NSPD 54	Cyber Security and Monitoring	8 Jan 2008
HSPD 23	Cyber Security and Monitoring	8 Jan 2008

? represent directive numbers that are unavailable.

²⁵ "Department of Defense Strategy for Operating in Cyberspace," ed. Department of Defense (Washington, D.C.: Department of Defense, 2011).

²⁶ Joab Jackson, "Google: 129 Million Different Books Have Been Published," *PCWorld*(2010), http://www.pcworld.com/article/202803/google_129_million_different_books_have_been_published.html.

²⁷ Information derived from "Presidential Directives and Executive Orders," Federation of American Scientists, <http://www.fas.org/irp/offdocs/direct.htm>.

Within the large-scale governmental emphasis on the cyber domain, nowhere has the information revolution had more of an impact than on the U.S. Department of Defense. While the information revolution can be traced back well before the rise of the internet, the clear turning point in the information revolution of military affairs came during the first Gulf War.²⁸ The first Gulf War is often regarded as the first successful use of Command and Control Warfare (C2W). C2W rendered the majority of Iraqi forces impotent as U.S. forces entered the country in 1990.²⁹ Information technology, cyber, used in the conduct of this war created a revolution in military affairs (RMA).³⁰ The evolution of U.S. military dependence has only increased since the first Gulf War. The changes in the information connectedness of war have resulted in a change in the function of command.³¹ At present the U.S. Military relies on network-centric warfare to conduct its operations around the world, and the U.S. intelligence community relies on a plethora of cyber tools for collection and dissemination of intelligence.³²

The value of cyber for national security has grown if not exponentially, then close to it over the previous two decades. Beneath the collaboration of the military and intelligence communities is the storage of the country's modern crown jewels, schematics for future weapons systems, current logistical operations, and petabytes of information needing to be kept private. If the recent Wiki-leaks scandal has exposed anything, it is that the desire to break down the

²⁸ Alan D. Campen, *The first information war : the story of communications, computers, and intelligence systems in the Persian Gulf War* (Fairfax, Va.: AFCEA International Press, 1992).

²⁹ Martin C. Libicki, *What is information warfare?* (Washington, DC: Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University : For sale by the U.S. G.P.O. Supt. of Docs., 1995).

³⁰ Edward F. Halpin, *Cyberwar, netwar and the revolution in military affairs* (Basingstoke England ; New York: Palgrave Macmillan, 2006).

³¹ David J. Lonsdale, *The nature of war in the Information Age : Clausewitzian future* (London; New York: Frank Cass, 2004).

³² William A. Owens et al., *Technology, policy, law, and ethics regarding U.S. acquisition and use of cyberattack capabilities* (Washington, DC: National Academies Press, 2009).

stovepipes between agencies in the intelligence community and the military has increased the vulnerability of secrets.

The U.S. Military and Intelligence Communities are dependent on the efficient exchange and maintenance of data and as a nation we are in desperate need of a decision-making theory able to confront this new digital reality. It is important to consider why traditional models of decision-making are not applicable in the context of the evolution of technology. Before progressing in this chapter it is necessary to outline what this work does and does not claim with regards to cyber.

All of the information in the preceding paragraphs indicates a growing and inherent value associated with information communications technologies (ICT). The importance of information for every aspect of modern society has grown significantly over the last thirty years. This work does not address the definitional grey area between what constitutes cyber war or pretend to assess the full offensive, defensive, or deterrent capabilities associated with actions taken within this domain. This is immensely important moving forward. While many of the references in subsequent chapters will include the topics of conflict and warfare this work does not explicitly define information operations as acts of war.

This work stands between the linguistic and severity debates and asks how states make rational decisions regarding the conduct of offensive hostile actions within cyberspace. As Jean-Loup Samaan notes there are those who refer to cyber attacks as the equivalent of nuclear warfare and there are those that refer to them as annoyances.³³ This work does not take an official position on the range of debates and seeks rather to present unbiased evidence to further progress towards understanding the domain from a nation state orientation. But before focusing

³³ Jean-Loup Samaan, "Cyber Command," *RUSI Journal* 155, no. 6 (2010).

specifically on cyber decision-making models it is important to understand where cyber fits within the broader international relations literature.

Cyber and International Relations

Starting at the macro-theory level there are only a few works that have ever taken into consideration cyber within the broader theoretical framework of international relations. Johan Eriksson and Giampiero Giacomello uniquely approach the domain from a purely IR perspective.³⁴ They conclude that realism is of little help in fully understanding the intricacies of the domain because it fails to understand the interdependent nature of cyber. They contend that neo-liberalism sans its realist rigidity is the most applicable for a theoretical foundation. Additionally, they find the constructivist paradigm is more applicable to “symbolic, rhetorical, and identity-based aspects of digital-age security.”³⁵ Their discussion is largely helpful contextualizing a theoretical framework and does not necessarily limit the applicability of rational choice modeling of the cyber domain. The theoretical framework will become increasingly important in chapter 3’s analysis of motivation and conceptualization of political utility.

Cyber, in truth, epitomizes the concepts developed by Keohane and Nye in their classic work.³⁶ While many of the economic and societal interdependencies over the last 30 years have been greatly influenced by cyber, their interdependence has in turn created vulnerabilities. These vulnerabilities are systemic in nature. The problem with conceptualizing cyber within IR theory lies in its diffusion and complexity.

³⁴ Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: (IR) relevant Theory?," *International Political Science Review* 27, no. 3 (2006).

³⁵ Ibid.

³⁶ Robert O. Keohane and Joseph S. Nye, *Power and interdependence*, 4th ed. (Boston: Longman, 2012).

When Kenneth Waltz wrote, *Theory of International Politics*, he wasn't imagining a world where the effective borders of civilian interaction were torn down.³⁷ In 1979 the Iron Curtain was still firmly in place and the transfer of information from one nation to another still took time. While ARPANET was in existence, the World Wide Web was not. Computers were beginning to grow in importance, but their value was still somewhat limited. Interdependence occurred in fairly rigid economic transactions and even the rise of multi-nationals was still largely in its developmental phase. Power stations, and banks were becoming increasingly computerized, but they were largely stand-alone entities. The realist world of non-interdependence predicated on issues isolated to security was at its strongest moment. As network connections increased and computerized systems made their way into everything from cars to coke machines the value of those newly networked and digitized tools began to increase the value and interdependence of the international system.

It is possible to philosophically take a step back and still claim, as Mearsheimer does, that we are still in a great power politics struggle, yet this struggle is defined by an information environment very different from the one in which neo-realism was conceptualized.³⁸ Security is still pre-eminent in the eyes of most scholars and still consumes a basic need status, but security is no longer walled off behind borders. Economic systems that support the military capabilities of states no longer have limited contact with their external counterparts. Everything from food security to economic security, to nuclear security is now constantly connected to the world around us.

While it might be beneficial to take into consideration Wendt's constructivist arguments as a theory for framing the new security paradigm, it is less than helpful in managing the

³⁷ Kenneth Neal Waltz, *Theory of international politics* (Reading, Mass.: Addison-Wesley Pub. Co., 1979).

³⁸ John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: Norton, 2001).

complexity. We are therefore caught on a scale between simplicity and complexity.³⁹ Realist theories oversimplify the security situation posed by the development of cyberspace, and constructivist theories look too deeply into the inner workings of a system that is so complex that even those who designed it cannot fully comprehend it. Neo-liberalism is for the purposes of understanding decisions in international relations relating to cyber the most logical theoretical framework.

Neo-liberalism allows for a rational decision-making model to develop without getting lost in the milieu of perceptions. The ontological foundations of Neo-liberalism that alter the realist notions on relative gains matter for security and are of critical importance. Security issues within an interdependent environment with an ever-growing absolute value cannot and should not be conceptualized within a purely relative gains framework. Therefore moving forward in the discussion of where decisions in cyber exist, it is best to locate them somewhere between the constructivist norm development and the realist simplicity. The concept of interdependence and absolute value are of critical importance particularly when considered in the context of the interconnected nature of modern security, economic, social, and political concerns.

Moving forward in this chapter, it is vital to understand that cyber is a something upon which national security depends not only for its Command and Control Warfare (C2W) capabilities. Cyber interacts with national security in the context of its systemic interconnection with every aspect national security from economics, to food production, and beyond. The next step is to outline why an interconnected system, which can be used offensively, does not fit within the current conceptual framework of rational choice theories for conflict.

³⁹ Alexander Wendt, "Constructing International Politics," *International Security* 20, no. 1 (1995).

Understanding decisions of states: the logic of rational choice modeling

Cyber, as the above characteristics indicate, is a domain unlike any of the others. It is a domain that has far reaching implications across domains and has come to shape the modern world and play a role in the U.S. strategy of “full-spectrum dominance.”⁴⁰ Because the domain crosses so many layers of national security, and because of difficulties regarding accurate attribution within the domain pose so many problems for conventionally oriented security studies theorists, cyber seriously challenges traditional decision-making models.⁴¹

Most securities studies works addressing cyber fall somewhere between ambivalence and alarmist. Any policy-maker attempting to make a decision regarding the use of offensive tools in cyberspace beyond their role as facilitators of other aspects of national security, with the expressed goal of achieving political results would rightly be confused. The domain itself is not easily conceptualized. Whereas a policy maker can easily understand the implications of launching a missile to hit an intended target, a cyber attack that might achieve the same result is difficult to comprehend. That the same political utility of a missile attack on a target can be caused by a thumb drive with a virus sounds more reminiscent of science fiction than science fact. A solid and accurate understanding of how to decide to use a cyber weapon is unavailable to the policy maker in a clearly formatted and logical structure.

Moving forward acknowledging the cyber domain is unique from other more conventional domains and is of critical importance to the functioning of the national security of modern states, there needs to be a way to logically conceptualize how a state decides to use cyber as a tool to influence the policy actions of other states. The power and interdependence created by cyber forces it largely into a new domain of decision-making.

⁴⁰ Halpin, *Cyberwar, netwar and the revolution in military affairs*.

⁴¹ Ibid.

There is to a large degree a consensus on the ability of cyber to be used an instrument of soft power. The U.S. State Department frequently makes reference to cyber and implicitly soft power.⁴² The State Department has even used its influence to provide tools or maintain services for the communication and organization of popular uprisings.⁴³ Unlike soft power, an executive of a state must approve hard applications of power, whereas applications of soft power are institutionalized and part of an ongoing policy process.

To create a rational-decision-making model it is necessary to focus on decisions as points in time rather than an institutionalized decision-making process or a functional system for the expansion soft power as an instrument of the state. Because most applications of soft power typically do not require a single decision-maker's approval and because the spectrum of soft power is so vast, ranging from the provision of tools, to the creation of targeted media, it is for the purposes of the subsequent arguments largely ignored. This should not be taken to mean that cyber soft power is not of importance, but rather there are actions within cyber that require a unitary decision and clearly constitute an application of hard power.

Hard and soft power exist on a spectrum. Nye defines hard power on one end of the spectrum as the ability to command, threaten, or sanction.⁴⁴ More simply he defines the difference between hard and soft power as the difference between "push" and "pull."⁴⁵ The decision to use the stick rather than the carrot is typically an executive one requiring a rational decision that weighs the utility of action versus inaction or actions that do not make use of the constitutive aspects of hard power.

⁴² Hillary Rodham Clinton, "Conference on Internet Freedom" (paper presented at the Conference on Internet Freedom, The Hague, Netherlands, 2011).

⁴³ Sue Pleming, "U.S. State Department speaks to Twitter over Iran," *Reuters*(2009), <http://www.reuters.com/article/2009/06/16/us-iran-election-twitter-usa-idUSWBT01137420090616>.

⁴⁴ Nye, *The future of power*: p19.

⁴⁵ Ibid.

Considering the logic of the application of power from a state perspective, it has an large amount of value added. As figure 1.1 illustrates on particular policy positions, states fall along a spectrum. State A can have a preference P_x on a particular policy, while state B can have preference P_y . State preferences are not static and can and often do change over time. The process of change can lead states to move either closer or further apart on the spectrum of a particular policy decision. Figure 1.1 is a simplified example of the policy spectrum and often both states in diplomatic relations will mutually influence one another, possibly moving both their positions either closer or further away from one another.

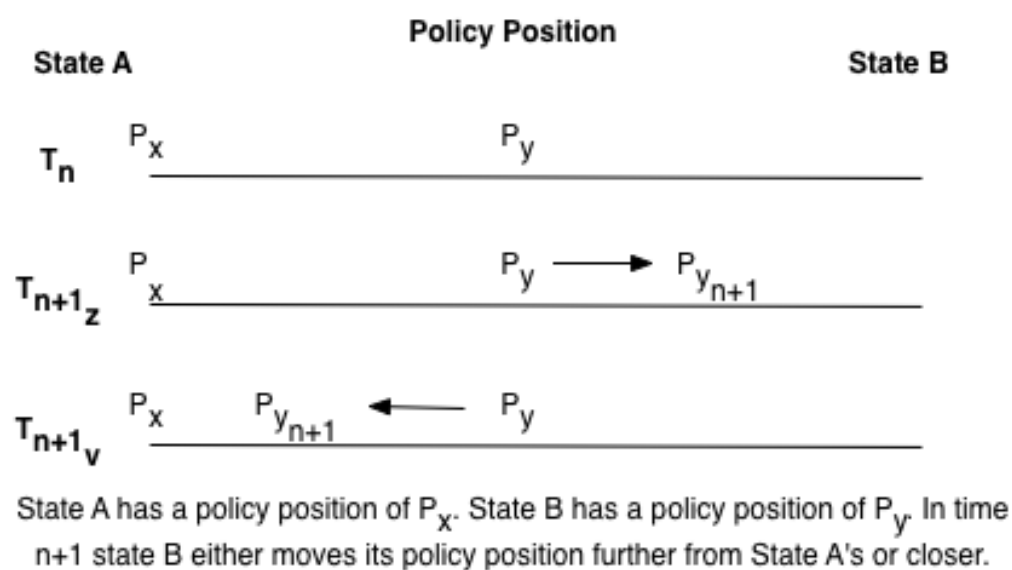


Figure 1.1 Understanding state policy positions

The objectives of hard or soft power are complicated from State A's perspective. State A would like to have State B move closer to its policy position as this would likely lead to improved relations between the two states. If movement towards state A's policy position is not possible or state B has indicated a desire to move further away from A's policy position, then

state A prefers to either slow the movement of state B from its policy decision or to maintain the status quo. Either form of power can be used to accommodate this objective.

How then can we differentiate between the logic of which type of power to use and why is it that hard power necessitates a decision-making model, while it is often unnecessary for soft power? The answer lies in definition of what constitutes hostility. All applications of hard power can reasonably assumed to constitute hostile acts against another state meant to influence their policy position.

Iran likely thought the maintenance of the Twitter networks during their Green uprisings following the 2009 election of Mahmoud Ahmadinejad constituted a hostile action, the act itself was done with little to no aggression and no objective policy goal other than to facilitate an event already in progress. The same could not be said of the recent push by the United States to Sanction Iranian Oil Supplies.⁴⁶ Sanctioning is a clear political signal designed to force the Iranian's to relinquish their nuclear ambitions. The action is hostile and has an expected (desired) outcome, the cessation of Iran's nuclear weapons program.

Building the argument for a decision-making model predicated on the use of hard power has inadvertently created a logical shortcut around an area of major concern for many cyber theorists. Often scholars discussing the use of cyber in the context of national security offense and defense get stuck when it comes time to define what constitutes a hostile action from cyberspace. Most scholars contend that there are three definable types of computer network operations (CNO): computer network attack (CNA), computer network exploitation (CNE), and computer network defense (CND). There is a significant amount of disagreement in this particular area of cyber security studies, because the actions taken to exploit a network are often very similar if not identical to those necessary to attack it. All authors agree that the only form of

⁴⁶ Benoit Faucon, "New Sanctions Target Iran Oil Sales," *Wall Street Journal* 2012.

CND constituting a hostile action arises from retaliation in which case it is less pure CND than a form of CNA.

The distinction between CNA and CNE after the discussion on hard and soft power should be fairly evident. To facilitate the discussion the definitions of the three categories are listed below in Table 1.3.

Table 1.3: Typologies of computer network operations⁴⁷

CNE	Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.
CNA	Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.
CND	Actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks.

Actions taken in cyberspace to exploit information, digital espionage, constitute CNE and do not fulfill the requirement for altering the policy positions of other states. The process of exploiting networks can significantly influence the ability to conduct CNA operations as will be examined in detail in chapter 7, but CNE activities do not warrant a decision by a single executive decision-maker. CNE operations occur with regularity, and while they are a major vulnerability, they do not constitute an application of hard power. This distinction is made particularly within the field of cyber legal studies.⁴⁸

⁴⁷ "What are Information Operations," Cyberspace and information operations study center, <http://www.au.af.mil/info-ops/what.htm>.

⁴⁸ See two articles both dealing with aspects of espionage in the context of legal issues: Neal Kumar Katyal, "Criminal Law in Cyberspace," *University of Pennsylvania Law Review* 149, no. 4 (2001); Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law " *Berkeley Journal of International Law* 27, no. 1 (2008).

Patterns emerge when examining political action around the world. States in the international arena engage in various forms of political action to influence other states. This coercive action can take many forms. The literature in international relations is replete with studies on sanctioning, threat politics, military actions and a host of other tangible activities designed to influence the policy structures of opponents.

Much of the security studies literature focuses on those actions that lead to war or conflict. There are a plethora of works on the causes of war ranging from Blainey to Van Evera and beyond. Each of these studies looks at tangible real world aspects of war and attempts to define a pattern over the long history of conflict.⁴⁹ Within this pattern they hope to explain, not just what causes war, but how to prevent wars as well.

After reading even a small sampling of these works a reader will be quick to recognize the common threads between them diverge and each takes a different stance on the variable factors that lead to conflict. The study of security and conflict between states in most studies is quite odd when one considers the most common variables are material capabilities, power status of states, borders, and beyond. These works gloss over the need for a decision to be made, leading irrevocably towards war.

Conventional paradigm theorists such as Waltz, Mearshimer, Keohane, Moravcsik, Levy, and others indicate ontological foundations, or norm developments as the basis for the conflict trap.⁵⁰ States either form institutions to mitigate information asymmetries, engage in conflict due to power struggles, or conform to norms discouraging or encouraging conflict in various

⁴⁹ Geoffrey Blainey, *The causes of war*, 3rd ed. (New York: Free Press, 1988).; Stephen Van Evera, *Causes of war* (Ithaca (N.Y.): Cornell University press, 1999).

⁵⁰ Waltz, *Theory of international politics*. Mearshimer, *The Tragedy of Great Power Politics*; Robert O. Keohane, *After hegemony : cooperation and discord in the world political economy* (Princeton, N.J.: Princeton University Press, 2005).; Andrew Moravcsik, "Taking Preferences Seriously: A Liberal Theory of International Politics," *International Organization* 51, no. 04 (1997).; Jack S. Levy, "Misperception and the Causes of War: Theoretical Linkages and Analytical Problems," *World Politics* 36, no. 1 (1983).

situations. But why do states decide to take that first shot in any form of conflict? As the previous section on the connection of cyber to international relations indicates the answer lies somewhere in the complexity of the power and interdependence argument developed by Keohane and Nye,⁵¹ but this only gives a theoretical frame within which to understand the broader issues of cyber in international politics. To understand the application of force in cyber it is necessary to drill down to the *casus belli*.

Carl Von Clausewitz is famous for his phrase "War is politics by other means."⁵² This phrase indicates war and conflict are, to a large extent, political acts. Politics is a zone of bargaining designed to influence others to change their policy positions to fit more closely with one's own policy platforms. The process of politicking can be accomplished in many ways. In any given situation there is a range of tools available to individuals to manipulate conditions to their advantage. International politics is not immune to attempts by states to influence the policy positions of one another to their advantage. Often this occurs in explicit bargaining and diplomacy. States sit down and discuss options and attempt to come to a mutually satisfying agreement. There is a range of international institutions facilitating diplomacy. The United Nations, the World Trade Organization, and Mercursor, to name but a few, all play a role in enhancing communication and political interaction between states. Very often these institutions provide the outlet necessary to shift policy decisions among states to an agreeable middle ground. In the world of international politics this is best assumed to be a positive sum game. All parties to a certain degree can walk away from the negotiating table winners.

Security issues often force states into a zero-sum bargaining range. It is in this area that states are apt to resort to hostile tactics. Traditional security studies literature indicates threats

⁵¹ Keohane and Nye, *Power and interdependence*.

⁵² Carl von Clausewitz, Michael Howard, and Peter Paret, *On war* (Princeton, N.J.: Princeton University Press, 1976), 39

and implementation of sanctioning or military action are tools in the toolbox of political leaders to influence the policy positions of other states. As indicated above these actions largely occur in the physical world and are overt actions. The threat of implementation of covert sanctions is likely to have little or no effect as the sanctioned party will not know what policy course it needs to take in order to reduce or eliminate sanctions. The same holds largely true with conventional military action. The objective is to provide a visible and tangible coercive strategy designed to alter the policy position of another state.

The use of means other than non-hostile diplomacy to influence the policy decisions of other states requires a decision to be made. This decision is dependent on a multitude of considerations. However, the decision itself is broadly constrained by three qualifiers: (1) What is the utility of action? (2) What is the uncertainty that such an action will not work? (3) What risk is associated with this type of action? These constraints weigh heavily on the decision to forgo non-hostile methods of political action in favor of actions likely to be construed as hostile.

It is not complicated to deconstruct the above qualifiers. If a state engages in an action and it is successful, what is the expected gain? Will the target of the action shift its policy adequately in the desired direction? How certain is it that this action will be successful? If a state is highly uncertain its action will result in the desired change this weighs greatly on the utility of such an action. Lastly, what risks are associated with such an action? Is there a possibility for retaliation? Will this damage the instigator's reputation? Will this impair future attempts with other states? There are numerous sub-questions to be asked regarding the development of the decision, however, the broad decision matrix is constituted through utility, conditioned by uncertainty, and risk.

There is an understanding that security issues often shift from non-hostile diplomatic negotiating to alternative more overt coercive forms of political action designed to influence the policy positions of states. But, this view of political action as being explicitly overt as considered by most theorists in security studies is largely misplaced. It is misplaced because for millennia the boldest forms of hostile action and often the ones bearing the best political results are those occurring without the knowledge of the intended target. The conflict over political utility and covert action will be examined in exhaustive detail in chapter three.

Breaking down the policy process into three categories, there are three broad categorizations: (1) overt non-hostile bargaining, (2) overt hostile bargaining, and (3) covert hostile manipulation. Most of the international relations literature focuses on the first two. It is, however, the third that has gone largely unnoticed in modern theorizing that has the largest independent political value and is most applicable to the cyber domain.

Whereas in overt non-hostile bargaining both sides are required to sacrifice to reach a mutual decision, and in overt hostile bargaining one or both sides lose to achieve a political goal, covert political action offers a third path, one that influences the intended target to achieve a political result to alter their policy position without their knowledge. As in chess, it is best to have the opponent think they are making their best move, when in reality they are positioning themselves in checkmate.

The broad tenets of the decision to use any of the three types of action are the same. A state engaging in political action will attempt to define its utility for each type of action and from there it will chose the best path.

Utility is not a complicated concept; rather it is something human beings do every day without even realizing it. Utility modeling is a mathematical modeling of aspects of a decision.

Rational Choice utility modeling largely developed by John Von Neumann and Morgenstern in 1944⁵³ was a means to understand economic decisions. Utility theory essentially states that a rational individual given a series of alternatives will weigh the values of each and create a *complete, transitive*, preference ordering. Based on this preference ordering it is possible to quickly and easily discern which alternative an individual will choose.

It is important to note the model works only with individual decisions. This is due to Kenneth Arrow's impossibility theorem, which states that a group of three or more individuals given a set of three or more alternatives cannot rationally order the alternatives.⁵⁴ Arrow illustrates that the simple ordering of the alternatives will greatly influence the ultimate decision, thereby negating the relative value of each of the alternatives and possibly lead to a sub-optimal outcome. Fortunately, for acts of a hostile or covert nature, the ultimate decision to employ such actions is typically relegated to a single decision maker or head of state.⁵⁵

There is little difficulty in comprehending that autocracies and other forms of non-democratic societies have a single decision-maker. This is often why powerful states seek regime change. They hope to influence the ultimate decision-maker within a state. But why do democracies shy away from their democratic principles when issues of hostilities and war arise? As mentioned briefly above, Kenneth Arrow's impossibility theorem essentially lays out the breakdown of the decision-making process in groups. What he finds is of critical importance in situations where the utility of the various policy options being vetted can be subsumed in a mathematical maze of sorts, leading to inefficient outcomes.

⁵³ John Von Neumann and Oskar Morgenstern, *Theory of games and economic behavior* (Princeton, NJ: Princeton University Press, 1944).

⁵⁴ Kenneth Arrow, "A Difficulty in the Concept of Social Welfare," *The Journal of Political Economy* 58, no. 4 (1950).

⁵⁵ Ellen Nakashima, "List of cyber-weapons developed by Pentagon to streamline computer warfare," *The Washington Post* (2011). This article indicates that the DoD is establishing a decision-making chain of command for cyber actions with hostile intent need Presidential authorization.

Groups attempting to derive a decision from different options must consider that each member of the group has a unique preference ordering. If all the preference orderings are weighed equally then the decisions within the group cannot be transitive, or fixed (complete). This leads to a situation in which the utilities of each of the possible options conflicts with the utilities of the other options leading to a circuitous or unsolvable decision process.

Bueno de Mesquita uses the Cuban missile crisis as a hypothetical example of such a decision process.⁵⁶ There was a deep division among the administration's leadership over the appropriate response to the placement of nuclear warheads on Cuba. The decision-makers were presented with three primary options: invasion(i), blockade(b), and surgical air strike(s). Bueno de Mesquita asks the reader to assume that an executive committee rather than the President is tasked with determining what the best course of action to take should be. He denotes three groups. Each of the groups has a preference structure: (a)sPiPb, (b)iPbPs, (c)bPsPi. He indicates that the first group prefers the air strike to an invasion or to a blockade, the invasion to the blockade and on down the line. From this information what is the collective decision of the committee?

The problem in this decision model quickly becomes evident. The preference orderings provide no clear guidance on what course of action the group supports the most. Bueno de Mesquita contends that a dominant decision-maker will attempt to impose or bargain his policy position to the top of the list. Using the preferences as defined above limits consideration to only two of the options at a time, for example: strike or invasion. In this instance the decision matrix indicates that a strike is more prudent. However, if the committee had first attempted to decide between an air strike and a blockade then the decision-matrix would have ended in the invasion being considered. Thus in such a group decision process the order in which the items for

⁵⁶ Bruce Bueno De Mesquita, *The war trap* (New Haven: Yale University Press, 1981), 14.

consideration are presented greatly influences the eventual outcome and that outcome is then conversely not dependent on the utility value associated with each option.

The impossibility theorem is a major blow to game theory literature in general and specifically aggregate decision-making. With multiple options in a group setting, a single rational outcome is unable to be achieved.

Bruce Bueno de Mesquita fleshes this aspect of the argument for a utility model of international conflict out in great detail. He highlights that most countries including the United States have provisions that lead to the executive being the final decision-maker in going to war or not.⁵⁷ This is important as moving forward in the development of a formal rational theory for the employment of a specific type of hostile action against opponent states, cyber. When discussing the development of rational decisions by states, theorists are implicitly assuming a single executive leader. This is not to insinuate that there are not other important actors in the decision-making process. Debates in legislatures, the general public, media, norm entrepreneurs, and other persons of influence all weigh heavily on a decision-making process leading to conflict. However, as Bueno de Mesquita argues all of these other actors influence the decision process, but the ultimate decision to engage in hostile activities typically is not made by group fiat. If all the actors of a state are warmongers and a single forceful executive finds the calculus of war too costly, it is often he alone who can make the decision to avoid war.

This decision is economic in nature and fits accordingly with Von Neumann and Morgenstern's utility models. A parallel economic example is that of an individual deciding between apples and oranges at the local grocery store. The apple and orange industries each attempt to influence the decision with advertising. Family members might express their preference for one type of fruit or another. Ultimately the decision between the apple and the

⁵⁷ Ibid., See Chapter 2

orange rests on an expected utility of pleasure or fulfillment derived from purchasing and eating the apple by the individual. This fulfillment is relative to the cost associated with each of the types of fruit. The consumer, as a rational actor, might have a strong preference for apples and only switch to oranges when the relative cost of apples exceeds the expected value of that apple relative to the cost of an orange.

The above example is painfully simple, yet it is meant to illustrate that the decision-process in many situations, though not all, boils down to an individual decision-maker. Further examples of an executive being the final say in the instigation of hostilities can be found easily within modern history. In 2011, President Barack Obama unilaterally without the consent of Congress instigated hostilities against Libya. During World War II elections were suspended, providing Winston Churchill with a well-defined executive power over the duration of the war. In dictatorships the relationship between the rational instigation of hostilities and the single decision-maker is less confusing. But, as President Truman said: "The buck stops here." Democracies typically shift away from consensus or majoritarian decision-making during hostilities.

A valid question is why does this really matter in the context of the three options listed above with regards to the broad classifications of international interaction being either bargaining, overt hostilities, or covert hostilities and action. If we are trying to understand the decision-making process of any of these aspects, we have to understand the relation between how we decide to use them and the utility that can be derived from such an application.

Decision-makers are essentially weighing the options of these three broad paths to influence the political environment. The ability to decide which path to take is based on a fully rational understanding of the value of each of the paths. Using each of these options contains risk

and uncertainty over whether they will achieve the desired change and create the political utility desired. It is by deconstructing this complex nested decision process that states are able to understand whether it is better to maintain normal international relations through diplomatic action, or engage in alternative means to shift the policy preferences of others. The emphasis in the following chapters will be on the two paths diverging from the diplomatic. These two paths are closely intertwined and often overlap either intentionally or accidentally. Specifically decision-makers are presented with a new set of tools, which can influence the decision to use one or both of these paths. These tools fall within the new and man-made cyber domain, but have very real and tangible aspects felt in the physical world.

Knowing a unitary decision-maker bases decisions on a utility calculus, and that this calculus is utility maximizing within rational choice, what necessitates a new study on decision-making within the cyber domain?

Bueno de Mesquita did a superb job of isolating the patterns how leaders decide if an overt war is rational or not, but his model is largely predicated on qualities not pertinent or applicable to cyber. His utility function is constructed on the overt nature of the international community with regards to declarations of war, peace, and understanding the interactions among states. His study reduces the error of predicting when a state will initiate a conflict and whether that state will win. His model is more successful than many of its pure power score counterparts and provides a logical chain of thought. This logical chain of thought is still applicable in the realm of conventional military action. Yet, this is only one part of the story of international politics.

Scholars have developed theories of diplomacy, and of conventional conflict initiation, but those are not the only ways to influence the policy positions of states. They have not been the

only ways to influence the policy positions of states dating back many millennia. As such the picture they provide us is one that is woefully inadequate. Scholarship currently stands like a deer caught in the headlights of major conflict and overt diplomacy all the while ignoring those hostilities that go unacknowledged, yet create a large amount of political utility.

This work particularly contends with the utility of one type of covert action computer network attacks (CNA). Beyond merely the consideration of the covert versus overt nature of options available to states, the cyber domain offers up a unique set of challenges to Bueno de Mesquita's model for the development of utility in a decision-making process. Conventional domains are currently classified under Bueno de Mesquita's rubric by using Composite Index of National Capability (CINC) scores affected by monotonic declines in power over distance. His rationale for this measure is logical and well reasoned from a traditional conflict decision-making perspective. A state that is better endowed with resources than its potential adversary has a higher probability of being successful in a conflict. The farther a state attempts to extend its power and resource capabilities out from its center of gravity, the more its relative power begins to decline.⁵⁸

For the cyber domain it is inappropriate to use CINC scores or monotonic declines in power over distance. In addition to these two inappropriate attributes cyber adds complexity of anonymity and attribution. These additional characteristics necessarily qualify CNA as a covert act to be examined in more detail in chapters 3 and 6. Why are CINC scores an inappropriate measure of cyber capabilities? Their inappropriateness is not hard to discern. CINC scores were first developed by David Singer in 1963, but have been used since as a measure of national

⁵⁸ Ibid.

power in the Correlates of War (COW) project.⁵⁹ When they were first developed and for first half of their history, the cyber domain was of little concern. More importantly for the types of conflict examined within COW they are applicable. As states become increasingly interdependent and their national securities are evermore tied to cyberspace, the power relationship within the conventional domains becomes increasingly limited in its explanatory power for this new form of conflict.

CINC scores incorporate measures of total population, urban population, iron and steel, primary energy, military expenditure, and military personnel. Each of these is an important consideration in conventional warfare and particularly in the decision to engage in conflict. Cyberspace, however, is virtual, meaning that total population, or urban populations, or any of the other constitutive parts of CINC scores do not adequately measure power in this domain. Cyber power, which is examined in chapter 4, is constructed by analyzing offensive and defensive technological strengths and weaknesses as well as dependencies leading to vulnerabilities. The power of these strengths and weaknesses do not monotonically decline over distance, as operations within cyberspace are almost instantaneous,⁶⁰ and there is little to no necessity in moving cyber units around the world. An operator can sit at CENTCOM and fly a drone over Afghanistan thousands of miles away with no loss of effectiveness.⁶¹

Beyond the inappropriateness of conventional measures of power is the way risk is formulated. Because the probability of success in a conventional conflict is relatively

⁵⁹ David J. Singer, "Reconstructing the Correlates of War Dataset on Material Capabilities of States, 1816-1985," *International Interactions* 14(1987).

⁶⁰ Richard Potter and Akihiro Nakao, "Mobitopolo: a portable infrastructure to facilitate flexible deployment and migration of distributed applications with virtual topologies," in *ACM SIGCOMM* (Barcelona: SIGCOMM, 2009). Potter and Nakao illustrate that the migration of virtual machines across networks can be routed in ways that are more efficient than current technological protocols. In so doing they illustrate that it is possible to map out more efficient routes on the internet. This indicates that all actions in cyberspace are not instantaneous and can be manipulated to speed or slow data flow.

⁶¹ C. Christine Fair, "Drone Wars," *Foreign Policy* 2010.

straightforward in pure military capability terms, it was adequate to use pure national military capability measures. But, cyber, as with many other forms of covert action, has added attributes influencing the probability of success for any type of attack. For simplification purposes this work combines the anonymity-attribution problem. In reality it should be parsed out based on intelligence as will be illustrated in chapter 7. In a conventional domain an attack is relatively unavoidable even if it is known beforehand. Iran cannot easily move its enriched uranium production facilities even if it knows Israel is about to attack. It can harden its facilities and attempt to weather an attack, but it cannot nullify an attack. With cyber attacks if it is known an attack is coming and where it is coming from, the defender can minimize or nullify its effect.

A server or computer with information on it and connected to the Internet is much like a ship in the ocean. The ship is fine so long as it knows the weather conditions in advance. The captain can steer the ship to safer waters or in the event of a hurricane can dry dock or harbor the ship. The same is essentially true of a country under imminent threat of a cyber attack from a known source. A network administrator can thwart an attacker in a number of ways if he knows whom that attacker is and when they are going to attack. In a worst-case scenario he can effectively dry dock the network by removing external connections or temporarily shutting systems down. There was even a bill proposed in the United States congress promoting the idea of an “Internet kill switch.”⁶² Because cyber is characteristically different from conventional forms of conflict, a decision-making model needed to assess the utility of an attack employing cyber tools as uniquely different from conventional military tools. The development of utility in a cyber decision-making model necessitates modified variable attributes and probability

⁶² S. 773: Cybersecurity Act of 2010 was last reported to committee on March 24,2010. No vote has currently taken place.

development. This modification in the development of probabilities greatly influences the subsequent development of political utility within Bueno de Mesquita's original theory.

Lastly, Bueno de Mesquita's model is largely based on state alliances. However, because cyber action occurs covertly, the consideration of alliances becomes largely irrelevant. This work therefore modifies the underlying probability functions associated with the utility theory developed by Bueno de Mesquita and remains firmly within his bi-lateral modeling of international conflict.

How this work is organized

The remainder of part one of this work focuses on the importance and attributes of the cyber domain in chapter 2 and the motivation for and utility of covert cyber action in chapter 3. Part II develops those attributes of the utility theory of international cyber conflict highlighted above and justifies the necessity of a revised model. Chapters 4 through six focus on the attributes of the probability for success in cyber action by defining cyber power, vulnerabilities, and attribution and anonymity. Chapter 7 then compares these attributes to their conventional counterparts. Part two closes with chapter 7, acknowledging the open source nature of this work by providing a logical platform for the inclusion of intelligence analysis to aid in developing this model to its fullest. Part three formally introduces the modified Bueno de Mesquita model by putting together the pieces of the probability components developed in part two. Part three is broken into three chapters. Chapter nine explains in detail the utility theory of international conflict and focuses on bi-lateral cyber conflict. Chapter ten combines the probability attributes from part two into the cyber model of bi-lateral conflict. Chapter eleven puts all the pieces together and illustrates how states formulate their utility for using cyber as an offensive tool providing evidence from collected data on significant cyber incidents. Part four concludes the

work with chapter twelve, a general overview and discussion of the theory of the decision to engage in cyber conflict.

CHAPTER 2

The Key Concepts of Cyber

There is a growing societal and military reliance on all things cyber. The previous chapter began by highlighting the evolution of a new domain of operation by comparing it to land, sea, air, and space. This chapter takes the next step and focuses on the first part of chapter one by answering two questions:

1. Why is cyber important to national security?
2. Why is cyber an inherently asymmetric domain?

These two questions build upon one another. The first question is answered identifying the four pillars of national security. Combined these pillars have been heavily influenced by cyber and have far reaching national security implications. The importance of these pillars also highlights how overarching network architectures have blurred the traditional conceptualizations of military versus civilian targets. Particularly important and adding to the theoretical development of the work is the concept of dependence on a man-made domain.

The second question on the asymmetric nature of cyber is brought in to illustrate that in most areas of national security, offense and defense, all players in the game are not equal. This asymmetry has specific qualities in the cyber domain, some of which are reminiscent of other domains of interaction, others, which are entirely unique. Asymmetry in any domain affects the decision-making process of leaders. Within the cyber domain it can have far reaching ramifications that can result in significant within domain blowback.

This chapter concludes by tying together the questions with their relationship to national security. The focus is on the dependency of the state on cyber, the interaction of cyber with a broad spectrum of modern military and intelligence affairs, and the inherent asymmetry present across nations within cyberspace. This chapter establishes the foundation on which many of the components of the new hybridized decision-making model will be based. Because this chapter covers such a broad area of focus it is not meant to provide a highly detailed analysis of any one particular aspect of cyber and instead serves to solidify the key concepts of cyber relevant to decision-making processes developed in parts two and three.

Why is cyber important to national security?

National security is the maintenance of the survival of the state. Cyber is important because it forms a modern infrastructure beneath the pillars supporting national security. Cyber infrastructure facilitates the connections of individuals, computers, systems, and at the most basic level, ideas, to one another. As a child grows from an infant, to toddler and into a young person their cerebral development facilitates the creation of new neural pathways. The progress is amazing to watch. An infant has jerky motor movements and is controlled by basic needs, a toddler begins putting together smoother movements, a child can put those movements into action, and an adult does not even notice the process. Cyber connects. With each new connection the development of the network increases in value and our relationship to the connections becomes second nature. Similarly these neural pathways allow us to control the environment around us. Not only do our connections facilitate our individual actions they become the framework for controlling production and economic processes. The connections and the control that follows become enablers. We become dependent upon these connections without even realizing our dependence.

Control goes beyond connection and facilitates action beyond the network itself. Cyber control allows robotics to construct products in factories, manage train and traffic systems, prevent airplanes from crashing into one another and much more. While, control is built on connections, the controlling aspects of cyber can take the connections and apply them. Whereas connections primarily facilitate information transference, the control aspects of cyber take the information and become managerial or productive. The most commonly referenced control mechanisms within cyber are supervisory control and data acquisition (SCADA) systems or programmable logic controllers (PLCs). These two devices take in information through connections and turn that information into processes. The increases in connections also increase our dependency upon those connections. The more our dependency increases the more vulnerable we become.

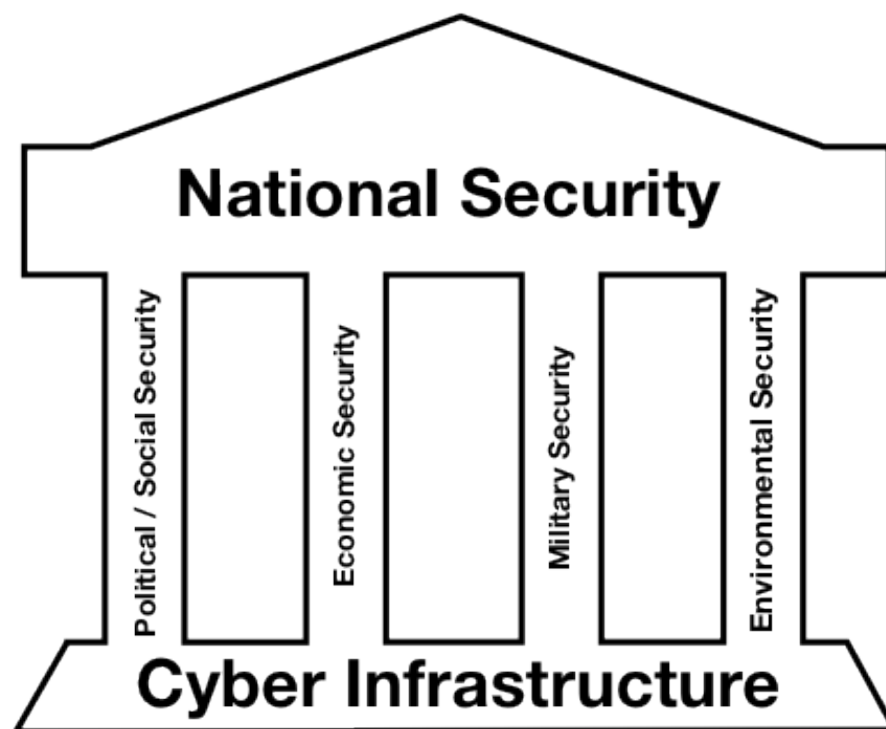


Figure 2.1 The modern structure of national security

Cyber has created four pillars of dependence. These pillars form a structure of dependence supporting national security. Figure 2.1 illustrates the structural dependence generated through the development of cyber. The connectivity and control of cyber has influenced political and societal, economic, military, and environmental security. Below the relationship of cyber within each of these categories to national security is examined in more detail.

The realpolitik of the new era is cyberpolitik, in which the actors are no longer just states, and raw power can be countered or fortified by information power. ~ David Rothkopf⁶³

⁶³ David J. Rothkopf, "Cyberpolitik: The changing nature of power in the information age," *Journal of International Affairs* 51, no. 2 (1998). p.326

Ideas are the lifeblood of politics and society. The control of ideas has for millennia been a strategic objective of rulers and later governments alike. The speed and quantity of ideas has significantly increased in the last 30 years. Information communications technologies have facilitated an information revolution that far exceeds the previous information revolutions of the written word, the printing press, the telegraph, the wireless, and television. While the inventions of ARPANET and later TCP/IP protocols were not necessarily intended to facilitate the transference of ideas, the connecting of computers has had enormous repercussions.

International Relations literature provides a basis for understanding the concept of information transference largely through neo-liberal institutionalism. Keohane and Nye in their seminal critique of realism identify complex interdependence as the driving force in international politics.⁶⁴ This interdependence is driven by an increase in the number of channels of communication between nations and within nations and the flattening of the hierarchy of political issues of importance. They indicate that the interconnections and the flattening of the hierarchy of issues reduce the need or the applicability of military force. Complex interdependence has been put on steroids in the cyber world with the near exponential increases in connections across societies. This complex interdependence has had a profound effect on more than just the transference of ideas; it has reshaped the forum in which those ideas are exchanged.

⁶⁴ Robert O. Keohane and Joseph S. Nye, *Power and interdependence : world politics in transition* (Boston: Little, Brown, 1977).

Fabien Miard brings the importance of Information Communications Technology (ICT)⁶⁷ for civil development more clearly to the forefront. He finds that mobile phones act as facilitators of mobilization and collective action for political purposes.⁶⁸ The facilitation of civil society strengthens national security; a theme reiterated by A. Lawrence Chickering.⁶⁹ The diffusion of information is simultaneously a strength and a weakness for the national security of some regime types as evidenced by recent revolutions across the Middle East and North Africa.

Deborah Wheeler indicates the evolution of the public forum and its subsequent impact on national security, while not directly caused by the creation of ICT technologies, can, given the right spark, facilitate revolutions.⁷⁰ This facilitation of political and societal revolutions by information technologies has increasingly become a tool of state power. This state power can be wielded by opposing states as tool of soft power. In 2009, Iranian activists organized and coordinated massive demonstrations across Tehran using the popular micro-blogging network Twitter. When Twitter planned to take its service off-line temporarily for a service update, the United States Secretary of State stepped in and asked them to delay the update until further notice.⁷¹

Information communications technology (ICT) has affected political and social movements through its communicative ability to expand the public forum. As the examples above indicate this can be a stabilizing and destabilizing factor. The communicative capacity of states themselves is also dramatically affected by the rise of ICT. Kristen Lord highlights the problems embedded in the rise of ICT's facilitation of transparency. She contends that despite

⁶⁷ Cyber and ICT can be used relatively interchangeably. Cyber is built on ICT.

⁶⁸ Costigan and Perry, *Cyberspaces and global affairs*. See Chapter 8: "Call for Power?"

⁶⁹ A. Lawrence Chickering, "Civil Society and Counterinsurgency," *Small Wars Journal*(2010).

⁷⁰ Costigan and Perry, *Cyberspaces and global affairs*. See Chapter 10: "Information (without) Revolution?"

⁷¹ Fleming, "U.S. State Department speaks to Twitter over Iran".

almost universal claims that transparency in government is a good thing, decentralizing control over information and empowering individuals and organizations, transparency can significantly hinder domestic and international political actions.⁷²

Of particular concern to Lord is the role transparency plays in diplomacy.⁷³ Transparency in diplomacy can have a constraining effect on governments, particularly democratic governments. Although constraints in many instances are of great value and can prevent leaders from making poor decisions not in the interest of the domestic public, often this transparency limits the ability of governments to build mutual trust. ICT has forced governments to become their own public affairs firms in a vain attempt to control their desired message. Often this message is subsumed in the mix of information, much of which may be inaccurate or biased. Examples such as the leaks by Bradley Manning to Wikileaks also indicate that sensitive communications between governmental departments might not stay secret and can affect a state's relationship with its peers.

ICT can in many instances enhance national security through increased democratic involvement, monitoring of leaders, and development of complex interdependencies; at the same time it poses many threats. The connections made within cyberspace are an evolving field of study in domestic politics and societal interaction. The ultimate outcome is still uncertain. What is certain is that the communicative capabilities developed in the last 30 years are affecting this pillar of national security. Because the cyber connections associated with the social and political pillar of national security is not entirely systemically necessary for the operation of social discourse and the dispersion of ideas it poses a lower level of threat to national security than the

⁷² Kristin M. Lord, *The perils and promise of global transparency : why the information revolution may not lead to security, democracy, or peace* (Albany: State University of New York Press, 2006).

⁷³ Ibid. See Pages 128-9

other pillars of dependence. However, as cyber becomes more and more ingrained in the development of social and political issues it will become increasingly important for national security.

“The healthy functioning of cyberspace is essential to our economy and our national security.”

~ George W. Bush⁷⁴

Cyber has come to undergird modern economics. Modern global economics according to Thomas Friedman has been flattened by cyber.⁷⁵ This flattening makes it possible for multinational corporations to expand their supply chains with electronic data interchanges (EDIs) around the world traversing physical borders using the relatively borderless expanse of cyberspace.⁷⁶ Multinational corporations are not the only beneficiaries of this digital revolution, small business and individuals are now able to connect and gain access to information and products from around the world.⁷⁷ More than facilitating the process of globalization the information communication technologies of cyber have become the backbone of everything from currency markets and stock exchanges, to production lines. It is now possible to order stock on the NASDAQ from Beijing with the click of a mouse.⁷⁸ Not only does this expand the possibility for global investment, it diversifies and spreads out the risk of investments. The functioning of modern finance and economics is wholly dependent on ICT. This dependence has had far

⁷⁴ *The national strategy to secure cyberspace.*

⁷⁵ Thomas L. Friedman, *The Lexus and the Olive Tree* (New York: Farrar, Straus, Giroux, 1999); Thomas L. Friedman, *The world is flat : a brief history of the twenty-first century* (New York: Farrar, Straus and Giroux, 2005).

⁷⁶ Erik Brynjolfsson and Brian Kahin, "Understanding the digital economy : data, tools, and research" (Cambridge, Mass., 2000).

⁷⁷ Ibid.

⁷⁸ Sabourin, Delphine and Thomas Serval, "Electronization of Nasdaq: will market makers survive?," in Eric Brousseau and Nicolas Curien, *Internet and digital economics : principles, methods and applications* (Cambridge: Cambridge University Press, 2006). 588-616.

reaching effects on both the management and the stability of economies, increasing transnational complex interdependencies.

The direct control over financial systems and markets combined with the rise in information technology has also affected regulatory and fiscal controls once previously the purview of national governments. Central banks are no longer fully able to control domestic markets. Part of this is clearly due to globalization, but globalization is largely due to information communications technology. The adage that if one economy catches a cold the world economy gets sick follows directly from the interconnection of global markets within cyber.⁷⁹ No longer are markets isolated from one another, they directly impact one another. The disruption of supply chains by natural disasters can cause ripple effects through entire industries.

While the risk on investments is diversified, the risk associated with the systems that facilitate those investments has grown. Bank accounts and transactions are digital data points stored in databases. John McCarthy et al. assert global finance and economics are based on the trust of domestic and international stakeholders.⁸⁰ This trust is predicated on the security of the information contained within the economic systems and financial networks. If this information were to be violated, modified, or destroyed the consequences would be enormous. Furthermore, because many of the corporate secrets of businesses are digitally stored or transit cyberspace in emails, they are increasingly susceptible to digital espionage. NSA insider Jack Brenner states

⁷⁹ Andy Jones, Gerald L. Kovacich, and Perry G. Luzwick, *Global information warfare : how businesses, governments, and others achieve objectives and attain competitive advantages* (Boca Raton, Fla.: Auerbach Publications, 2002). 87.

⁸⁰ McCarthy, John A., Chris Burrow, Maeve Dion, and Olivia Pacheco, "Cyberpower and critical infrastructure Protection: A Critical Assessment of Federal Efforts," in Kramer, Starr, and Wentz, *Cyberpower and National Security*. 550.

bluntly United States' economic, financial, and business infrastructure is one of the primary targets of economic espionage, further increasing the risk associated with the move to cyber.⁸¹

The vulnerabilities posed by the move of economic systems into the digital realm places the trust of domestic and international stakeholders at risk. This risk is justified on the basis of increase in economic efficiency and productivity. However, as was indicated in the introductory chapter if the electric grid goes down all normal economic transactions halt. This is not figment of the imagination. America's largest retailer, Wal-Mart, uses an inventory management system that tracks the sale of every single item on its shelves and when a store sells out of an item it automatically orders more.⁸² If these supply chain mechanisms fail, the inventory of major corporations can collapse.

The ties of the economy to cyberspace enable high degrees of efficiency so long as the systems function properly. If the systems fail, are hacked, data is manipulated, or stolen, the economic repercussions can dramatically affect stability and cause markets to crash. A modern market crash caused by a cyber attack would achieve the equivalent of a weapon of mass destruction, without destroying and physical property. Such an attack could cripple industrialized countries reliant on ICT.

The modern economy is also increasingly digitized through E-commerce. The Census Bureau, which tracks sales indicates that in 2009 E-commerce made up almost a whopping 20% of the wholesale merchant trade equating to more than \$700 billion.⁸³ Charts 2.1 and 2.2

⁸¹ Joel Brenner, *America the vulnerable : inside the new threat matrix of digital espionage, crime, and warfare* (New York: Penguin Press, 2011).

⁸² Charles Fishman, *The Wal-Mart effect : how the world's most powerful company really works-- and how it's transforming the American economy* (New York: Penguin Press, 2006).

⁸³ "E-Stats, 2009 E-commerce Multi-sector Report," (Washington, D.C.: U.S. Census Bureau, 2011).

illustrate the expansion of E-commerce in the U.S. economy. This expansion is only going to continue to grow as more and more services and businesses move online.

The advance of cyber in economics has profoundly affected the national security of states. It has brought states closer together and confirmed the complex interdependencies proposed by Keohane and Nye. But at the same time this interdependence relies on a man made system vulnerable to exploitation in many more ways than ever before. Advances in interdependence are not always symmetrical across nations as will be examined later in this chapter. Not all countries are as tied into the modern cyber structure for their economic well being. Those countries that are have an incentive to discourage any significant disruptions in the existing system. The economics pillar of national security rests on the assumption of stability. Any source of instability generates uncertainty and the digitization of economics clearly contains many potential vulnerabilities.

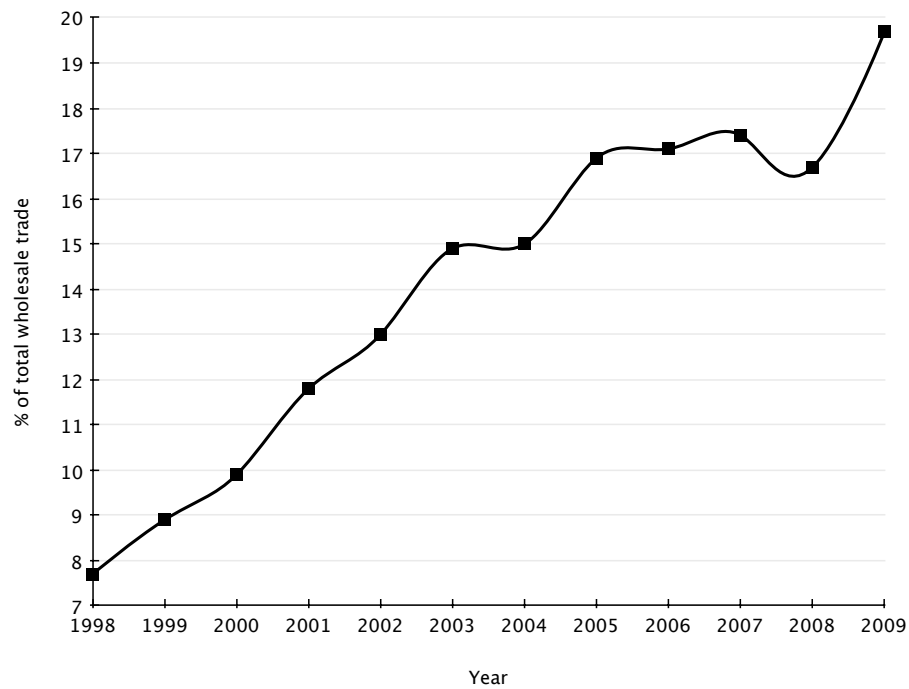


Chart 2.1 E-commerce as a % of total wholesale trade⁸⁴

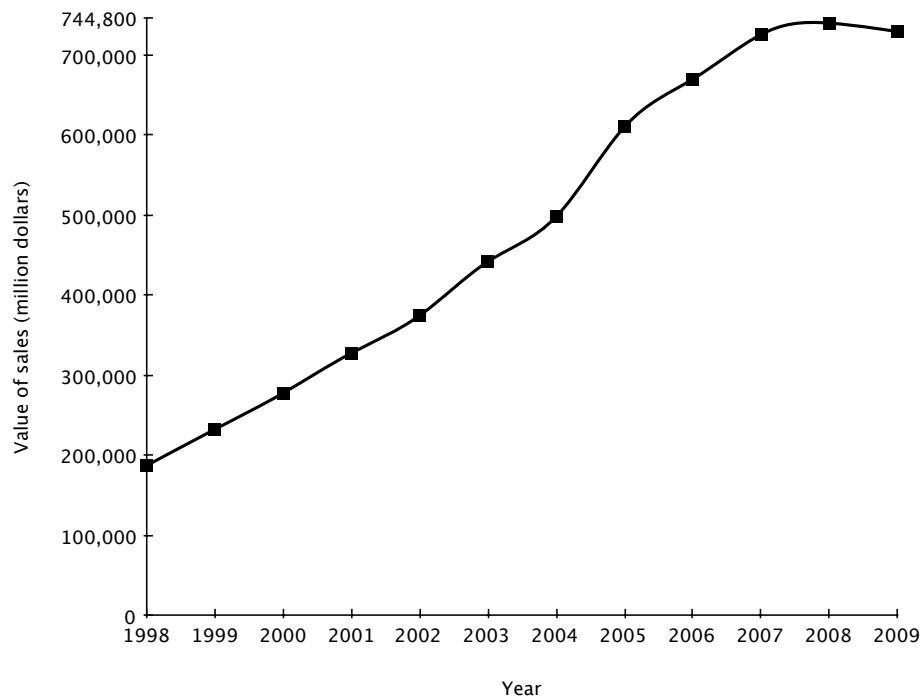


Chart 2.2 E-Commerce total value of sales (millions dollars)⁸⁵

⁸⁴ Ibid.

⁸⁵ Ibid.

Military security refers to the defense of the state against potential adversaries. Douglas Dearth writes “advanced militaries rely more than ever in modern times upon the civil national, and increasingly international transnational infrastructures.”⁸⁶ This reliance on infrastructures of both a civilian and military nature create vulnerabilities for the military security pillar. The vulnerabilities of this pillar are well known. What has given rise to the vulnerabilities are a combination of forces stemming from the increased communication and efficiency of the battlefield designed to reduce or eliminate what Clausewitz called the “fog of war.”⁸⁷

As was discussed in chapter 1 the increasing reliance of modern militaries upon information communications technologies has created the modern principle of Command and Control Warfare (C2W). The revolution is largely traced back to the use of C2W during the first Gulf War, often referred to as the first information war.⁸⁸ C2W is an important concept of war and it has affected the way in which wars are conducted. Yet, at a more fundamental level the evolution of military security has made it increasingly reliant on cyber infrastructure for every aspect of its operation. This trend is mirrored by the civilian world. The defense department’s Joint Vision 2020 outlines the movement towards a digitized military⁸⁹. The vision of a digitized battlefield is one that comprises dominant maneuver, precision engagement, focused logistics and full-dimensional protection.⁹⁰

⁸⁶ Douglas H. Dearth, "Operationalizing Information Operations: C2W...RIP" in Alan D. Campen and Douglas H. Dearth, *Cyberwar 3.0 : human factors in information operations and future conflict* (Fairfax, VA: AFCEA International Press, 2000). , 104.

⁸⁷ David S. Alberts, *Understanding information age warfare* (Washington, DC: CCRP Publication Series, 2001)., 36

⁸⁸ Campen, *The first information war : the story of communications, computers, and intelligence systems in the Persian Gulf War*.

⁸⁹ "Joint Vision 2020," (Washington, D.C.: US Government Printing Office, 2000).

⁹⁰ Ibid.

C2W is increasingly facilitated by the digitization of intelligence processes including the creation of INTELINK⁹¹, Intellipedia, and other intelligence dissemination tools providing real-time battlespace knowledge. Nick Cullather citing intelligence community agencies indicates that the future vision is to provide pilots in the air, and soldiers on the ground with integrated combat information.⁹² The military industrial complex has latched on to the idea of connectedness and begun working in earnest on projects attempting to further enhance the progression towards C2W across all operational domains.

The connectedness of modern militaries has been cited as a revolution in military affairs.⁹³ Beneath this connectedness is the cyber infrastructure itself. Military and civilian systems alike rely heavily on electricity. The modern electric grid according to a 2011 MIT study is best thought of as a system of systems increasingly vulnerable to attack.⁹⁴ The electric grid also powers, sewage and water treatment facilities, supports hospitals, provides electricity to air traffic controllers. More importantly each of the devices listed in the previous sentence are attached to SCADA systems and PLCs to manage their efficiency and to prevent accidents. Although many of these systems have redundancies they are of critical importance to the military and civilian communities and disruptions in these can significantly degrade or even possibly damage national security.

Beyond military reliance on services such as electricity, the military relies on cyber to conduct virtually all aspects of modern combat. As former Deputy Secretary of Defense William

⁹¹ Fredrick Thomas Martin, *Top secret intranet : how U.S. intelligence built Intelink--the world's largest, most secure network* (Upper Saddle River, N.J.: Prentice Hall PTR, 1999).

⁹² Nick Cullather, "Bombing at the Speed of Thought: Intelligence in the Coming Age of Cyberwar," *Intelligence and National Security* 18, no. 4 (2006).

⁹³ Jeffrey R. Cooper, "Another View of the Revolution in Military Affairs," in Arquilla and Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age*.

⁹⁴ Technology Massachusetts Institute of, "The future of the electric grid an interdisciplinary MIT study," Massachusetts Institute of Technology, http://web.mit.edu/mitei/research/studies/documents/electric-grid-2011/Electric_Grid_Full_Report.pdf.

Lynn wrote in *Foreign Affairs* “Information Technology enables almost everything the military does: logistical support and global command and control of forces, real-time provision of intelligence, and remote operations.”⁹⁵ The need for maintaining the critical infrastructures upon which military and civilian infrastructures depend is such a problem that the DoD established a new sub-unified command, United States Cyber Command (CYBERCOM) to manage the defense of networks. One of many aspects that General Keith Alexander cites as a reason for the establishment of this new command is the protection of the defense industrial base and the safeguarding of the technological tools that provide for national security.⁹⁶

Penetrations of defense networks hinder the overall operational of military security. Cyber incidents such as Titan rain, an attack, which focused on Defense Information Systems Agency, the Redstone Arsenal, the Army Space and Strategic Defense Command, and several computer systems critical to military logistics, have the potential to severely degrade the effectiveness of military security.⁹⁷ Military security has largely become a coordinated effort between foreign and domestic actions designed to provide for the physical defense of states. Cyber can enhance the military conduct of war, yet offers many challenges to military planners. The national security implications of the digitized military and the need for robust defenses both in conventional and cyber domains makes the military pillar of vital importance to national security.

The final pillar supporting national security in the evolving digitized world is environmental security. This is perhaps the most difficult of the pillars to directly conceptualize in relation to cyber and national security. While cyber cannot control the weather, it does control

⁹⁵ William J. Lynn, III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89(2010): , 98.

⁹⁶ Keith B. Alexander, "Building a New Command in Cyberspace," *Strategic Studies Quarterly* Summer(2011).

⁹⁷ Brenner, *America the vulnerable : inside the new threat matrix of digital espionage, crime, and warfare*.

many of the systems that manage chemicals, and products that if they were released would have far reaching environmental ramifications. But beyond the control of the systems that monitor wastewater, nuclear power plants, the navigation of oil tankers, cyber is also immensely dependent on environmental security in the form of fossil fuels, renewable energy, and more. Because cyber is a man-made domain it is heavily reliant on electricity for the connections and control mechanisms connected to it. Therefore environmental security is of critical importance not only for the maintenance of cyber infrastructure, but also upon cyber infrastructure to prevent man-made disasters from occurring.

Each of the pillars props up national security and supports the survival of the state. The dependence on cyber that each of these pillars has developed has largely become second nature. Like the development of neural pathways as a child ages national security has developed cyber connections that make it function. Damage, degradation, or disruption of any of these pathways also damages the national security of a state.

Why is cyber an inherently asymmetric domain?

The above discussion provided a rough explanation for how cyber has come to impact the pillars of national security. The discussion does however leave off one important concept that is necessary to consider in any discussion pertaining to the use cyber as an offensive mechanism. Conflict is rarely between equal parties. There have been few conflicts fought in which both sides matched man for man on each side of the battlefield. Conventional conflict contends with asymmetry in a straightforward mathematical function. The party with the better military capabilities has a higher probability of victory. Disadvantaged combatants are taught to exploit the weaknesses of their opponents on the field of battle. This difference often arose in technology and tactics. The asymmetries of tactics and technology gave the Roman legions an advantage for

hundreds of years. The Mongols were advantaged by their agile horsemanship and archery skills. Technology and tactics are tools of advantage. But within cyber the tool is both a strategic asset and vulnerability. This section argues cyber's contextual importance within national security is related to its complex relationship with the advantages and vulnerabilities it poses. This section focuses on why cyber is an inherently asymmetric domain of operation.

Asymmetry in cyberspace has risen to the level of national policy and was included in the 2009 National Infrastructure Protection Plan.⁹⁸ The Critical Information Infrastructure Protection Handbook also cites the United State's great fear of being caught off guard by asymmetric threats.⁹⁹ These and many other works portend a domain of conflict in which despite the best efforts of developed nations, these nations will forever be caught in a tangle of asymmetric threats. One problem is that it is difficult to pin down exactly what asymmetry is.

Steven Metz and Douglas Johnson define asymmetry as:

*"In the realm of military affairs and national security, asymmetry is acting, organizing, and thinking differently than opponents in order to maximize one's own advantages, exploit an opponent's weaknesses, attain the initiative, or gain a greater freedom of action. It can be political-strategic, military-strategic, operations, or a combination of these. It can entail different methods, technologies, values, organizations, time perspectives, or some combination of these. It can be short-term or long term. It can be deliberate or by default. It can be discrete or pursued in conjunction with symmetric approaches. It can have both psychological and physical dimensions."*¹⁰⁰

While the above definition is unnecessarily broad, Metz and Douglas and later Nir Ksetri go on to discuss positive and negative types of asymmetry. Positive asymmetries are those

⁹⁸ Security United States. Dept. of Homeland, *National infrastructure protection plan* ([Washington, D.C.]: U.S. Dept. of Homeland Security, 2006).

⁹⁹ *International CIIP Handbook 2008/2009: AN INVENTORY OF 25 NATIONAL AND 7 INTERNATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION POLICIES*, (Zurich: Center for Security Studies, 2008).

¹⁰⁰ Steven Metz, Douglas V. Johnson, and Institute Army War College . Strategic Studies, *Asymmetry and U.S. military strategy : definition, background, and strategic concepts* ([Carlisle Barracks, PA]: Strategic Studies Institute, U.S. Army War College, 2001).

strategic/tactical advantages one country has over another. Negative asymmetries are those, which a country's opponent has over it. Because asymmetry is such a frequently used word it is helpful to pare down the scope of its meaning in the context of cyber. Positive asymmetry in cyber refers to those technologies in cyber that provide an advantage over potential opponents; they refer more specifically to the potential vulnerabilities present with an opponent's systems. The zero-day exploits found on the PLCs that controlled the Iranian Uranium enrichment centrifuges would be consistent with an asymmetric exploit. Instead of hitting the centrifuges with a bomb they were hit with code at their weakest point. Negative asymmetry constitutes a weakness in systems that an opponent is likely to target. The Ghostnet exploitation of confidential information on U.S. defense networks would be consistent with this type of vulnerability.¹⁰¹ Essentially a positive asymmetry is an asymmetry viewed from the offensive perspective, whereas a negative asymmetry is viewed from the defensive perspective.

A November 2010 Chatham House report summarized the problem of asymmetry in cyber best by writing:

*“Cyber warfare could be the archetypal illustration of ‘asymmetric warfare’ - a struggle in which one opponent might be weak in conventional terms but is clever and agile, while the other is strong but complacent and inflexible.”*¹⁰²

The exploitation of asymmetry is frequent in modern conflict. But while it is not uncommon it is difficult to assess and adapt to. An example such as insurgents “blending in” to local populations to avoid detection is illustrative of asymmetric tactics.¹⁰³ The process of

¹⁰¹ "Tracking GhostNet: Investigating a Cyber Espionage Network," (Toronto: Munk Center for International Studies at the University of Toronto, 2009).

¹⁰² Paul Cornish et al., "On Cyber Warfare," (Chatham House, 2010).

¹⁰³ John Arquilla, *Insurgents, raiders, and bandits : how masters of irregular warfare have shaped our world* (Chicago; [Lanham, Md.]: Ivan R. Dee ; Distributed by National Book Network, 2011).

blending in allows them to work from inside out against the strategic weak point, the desire of most western militaries to avoid civilian casualties. The same occurs in cyber. Where a potential aggressor will pick on those areas of vulnerability.

What makes asymmetry such a pressing issue in cyber is what Ksetri refers to as his 7th proposition. He writes: “a higher degree of dependence on digital technologies increases a nations vulnerability to ICT related negative asymmetry.”¹⁰⁴ The previous section indicated that developed nations, the United States in particular, have increasingly focused on creating cyber capabilities across the entire spectrum of the pillars that support national security. This is directly in accordance with Ksetri’s prediction that a higher degree of dependence on digital technologies increases vulnerability. With everything from power stations, to command and control warfare centers linked via cyber means the dependence on digital technologies has moved closer and closer towards total saturation. Each new network and system within that network offers up more potential vulnerabilities.

Rod Thornton takes this a step further and writes that the increasing dependence on all things digital brings with it a concomitant of vulnerability.¹⁰⁵ Virtually all scholars agree that the new cyber domain is highly asymmetric. This asymmetry is problematic. Elihu Zimet and Charles Barry write: “cyberspace is a tool amenable to asymmetric warfare because it can be used anonymously...”¹⁰⁶ Jose Nazario also examines the nature of cyber hostilities writing that it

¹⁰⁴ Nir Kshetri, "Information and communications technologies, strategic asymmetry and national security," *Journal of Information Management* 11(2005)., 574

¹⁰⁵ Rod Thornton, *Asymmetric warfare : threat and response in the twenty-first century* (Cambridge; Malden, MA: Polity Press, 2007)., 55

¹⁰⁶ Elihu Zimet and Charles L. Barry, "Military Service Overview," in Kramer, Starr, and Wentz, *Cyberpower and National Security*., 285.

can be examined in the context of guerrilla and asymmetric theories used in conventional military conflict.¹⁰⁷

Where does the vulnerability from the digital world originate? The vulnerability largely originates out the sheer complexity of the systems upon which the national security infrastructure depends for its operation across all the pillars of national security. Even when a system is well tested an asymmetric challenges can arise in the most unexpected places, as was the case when a 75-year-old Georgian grandmother cut off the Internet to Armenia with a shovel.¹⁰⁸ At the time of the Internet outage, Georgia and Armenia blamed Russia, before the real culprit was identified.

There is no silver bullet vulnerability within the cyber infrastructure. Rather the vulnerabilities expose the dependent party to the potential for “a death by a thousand cuts.”¹⁰⁹ These cuts can range in size and scale and many if unchecked can fester and become lethal.

There are several basic causes of vulnerabilities. First, software often hides zero-day exploits, which are mistakes written into lines of code that are difficult to find. Most often these mistakes are unintentional, however, sometimes they are not. Software vendors try to rapidly patch these vulnerabilities as soon as they are discovered to minimize damage. Second, there are interactive vulnerabilities. Because networks combine multiple different systems they often interact in ways that could not have been predicted by the network designer. Third, there are resource vulnerabilities. As the number of systems expands the number of qualified security

¹⁰⁷ Jose Nazario, "Politically Motivated Denial of Service Attacks," in Christian Czosseck and Kenneth Geers, "The virtual battlefield perspectives on cyber warfare," Ios Press, <http://public.eblib.com/EBLPublic/PublicView.do?ptiID=501446>.

¹⁰⁸ Giorgi Lomsadz, "A Shovel Cuts Off Armenia's Internet," *The Wallstreet Journal*(2011).

¹⁰⁹ John Markoff, "Ideas & Trends: Blown to Bits; Cyberwarfare Breaks the Rules of Military " *New York Times*, Oct, 17 1999.

personnel to monitor them does not always keep pace. This is not an extensive list of the causes of vulnerabilities, rather a basic grouping of the more often discussed sources of vulnerability.

Each of these vulnerabilities can be minimized, and the goal of any systems administrator is to minimize threats system wide. However, as systems add on to systems the number of potential vulnerabilities increase. Therefore when considering asymmetry in cyber it is necessary to consider the importance of managing risk and the relationship that increasing digital dependence has on developed nations compared to potential less developed rivals.

Increasing imbalances in the dependence of actors within the cyber domain causes asymmetry. This increased dependence is a difficult measure because it spans so many systems within and between the pillars of national security. As will be examined in chapter 8 intelligence organizations can weigh in and provide insight into the areas where national dependence on cyber has generated the greatest vulnerabilities. Prior to intelligence assessments it is necessary to identify a broad outline of vulnerabilities. This identification process serves as a tool by which to identify the positive and negative asymmetries for both defensive and offensive decision-making. For general comprehension of the asymmetric nature of the domain it is possible to rely on a broad measure of digital dependence. Such a measure needs to be able to provide insight across all the pillars supporting national security.

A broad measure is necessary because asymmetry affects how decisions are made within the cyber domain. A decision-maker would have a hard time finding utility in attacking a country with few to no cyber assets via cyber means. The target's dependence on cyber is limited and the effect would be minimal therefore any resultant utility to be gained would also be minimal. Conversely it makes sense for a state with little to no cyber assets to engage in hostile cyber action against a highly cyber dependent state because it has little worry of in kind retaliation and

can have a much larger effect on the state with high cyber dependence. As Will Goodman writes: “at the very least, cyberspace asymmetry will cause defenders to think twice before responding asymmetrically or disproportionately...”¹¹⁰ This does not prevent states from developing the skills and technology necessary to engage in asymmetric conflict. On the contrary, China appears to be developing the cyber skills necessary to take advantage of American negative asymmetries according to James Lewis of the Center for Strategic and International Studies. Asymmetry poses problems for both the use and the defense of networks in conflict largely because of a poor formulation of what asymmetry is and how states should appropriately respond to asymmetric attacks within the cyber domain.

Because asymmetry is difficult to conceptualize on a broad scale decision-making basis it is necessary to create a generic measure that can cut across the pillars supporting national security. The best generic measure of dependence on ICT comes from the International Telecommunication Union’s (ITU) data on Internet penetration within countries. Figure 2.3 is a map representing the penetration rates of Internet use among individuals across countries. The map indicates a clear divide between the developed and developing world on Internet penetration rates.

¹¹⁰ Will Goodman, "Cyber Deterrence. Tougher in Theory than in Practice?," *Strategic Studies Quarterly* Fall(2010).

The percentage of individuals using the Internet is a good society-wide measure of digital

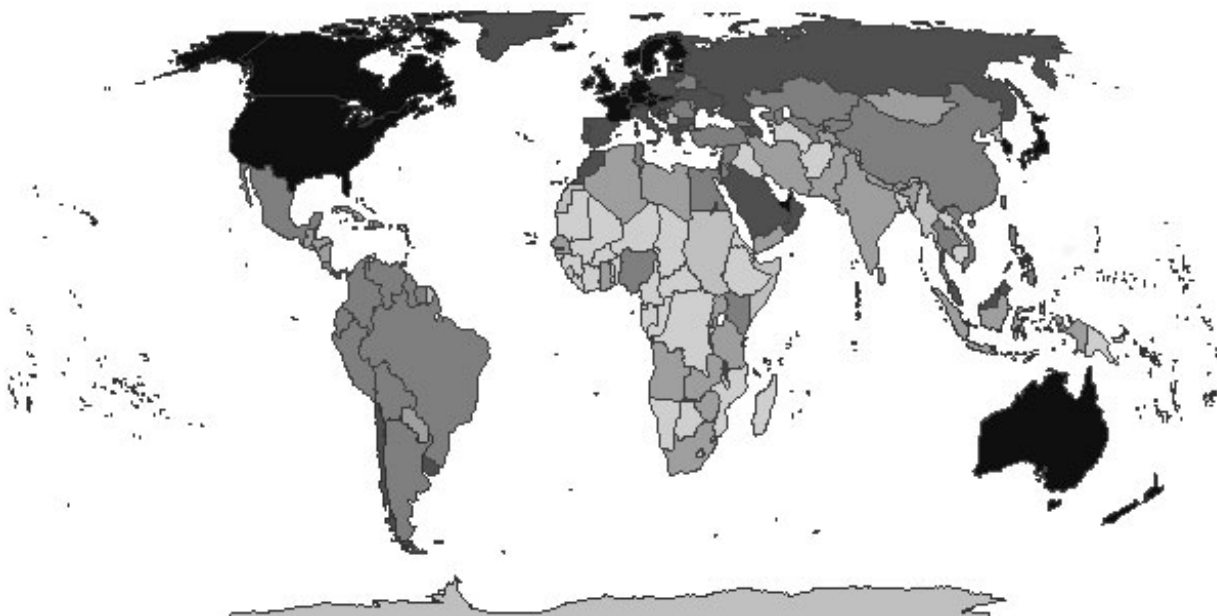


Figure 2.3 Percentage of individuals using the Internet

Darker colors represent higher Internet use. Data from "World Telecommunication/Ict Indicators Database Online." edited by International Telecommunications Union. Switzerland, 2011.

dependence because it captures the influence of ICT on the aggregate country basis. This ensures that the measure does not simply focus on military or civilian infrastructures, but rather an approximation of the dependence of national security as a whole. Because in cyber targets spread across military and civilian sectors it is inappropriate to separate them.

The ITU's data, as a broad aggregator of state cyber dependence, is informative in a general decision-making model. Without the applicable detailed intelligence it provides a means to scale power calculations in cyber to more accurately represent how the inherent asymmetry present within the domain can affect distributions of power. In this way the measure of ITU Internet penetration works similarly to Bueno de Mesquita's monotonic decline in power over distance. Where Bueno de Mesquita finds that power declines over distance in conventional conflict, the same is not true in cyber conflict as was discussed in chapter 1. However, power

does need to be scaled in accordance with its relative vulnerabilities. As the current chapter highlights cyber is immensely important to national security and as dependence on cyber increases so to do the number of vulnerabilities. In much the same way distance affects power in conventional conflict, increased digital dependence affects power in cyber conflict.

The measure of Internet penetration will be examined in more detail in chapter nine when the formal model is combined. What is important to take away from this chapter is that cyber extends across all the pillars of national security and therefore contains a novel set of problems not associated with conventional conflict. Furthermore, because distance in cyberspace is largely irrelevant, the decision to engage in hostilities must consider constraints pertinent to the cyber domain rather than attempt to fit conventional models into the cyber mold. Chapter 4 will focus more explicitly on how power in cyber is calculated. Moving forward with an understanding that cyber is vital to the maintenance of modern national security and that the importance of cyber is the result of increased dependence on the domain, a dependence that is not universal across all nations within the international system, this chapter serves as a foundation for understanding several key concepts relevant to cyber decision-making.

CHAPTER 3

The Motivation and Utility for Covert Action

“I know not with what weapons World War III will be fought, but World War IV will be fought with sticks and stones.” ~Albert Einstein¹¹¹

Covert actions are as old as political man. The subversive manipulation of others is nothing new. It has been written about since Sun Tzu and Kautilya. People and nations have always sought the use of shadowy means to influence situations and events. Covert action has even become a staple of the state system. A dark and nefarious tool often banished to philosophical and intellectual exile, covert action is in truth an oft-used method of achieving political utility overlooked by conventional academics. Modern scholars contend that for political utility to be achieved, activities such as war and diplomacy must be conducted transparently. This chapter illustrates the shortsighted naivety of the current conceptualization of political utility predicated largely on moral and ethical conceptualizations rather than the primacy of mathematics. Political utility is not the transparent achievement of political ends, instead it is best thought of in its original economic intent, a measure of satisfaction. Covert action is, and has always been, a tool aimed at achieving positive utility for political leaders. As with its overt counterparts it is not always successful, however, this lack of success does not diminish its ability in many circumstances to achieve political utility.

¹¹¹ Albert Einstein and Alice Calaprice, *The new quotable Einstein* (Princeton, N.J.: Princeton University Press, 2005), p173.

James Fearon states the central puzzle about wars is that they are costly, but still recur.¹¹² When creating a rational model for any form of conflict it is necessary to root that model in a motivation for conflict and furthermore, the result of any conflict must have a measureable utility. This chapter argues states employ covert action against adversaries to narrow the bargaining range on issues to prevent, preempt, or to minimize the extent of war. The motivation for using covert action is largely the same as that for all forms of conflict. The utility is defined in the ability to covertly alter an adversary's policy positions. Covert action, Track-II, or the silent option as it has often been known, allows for the bridging between the security dilemma of realism and the complex interdependencies of neo-liberalism.

This chapter proceeds in three sections. First, by building a rationalist argument predicated on James Fearon's "Rationalist Explanations for War."¹¹³ Second, by examining how political utility has been defined across the literature and matching these findings to covert action. Third, this chapter summarizes the motivation and utility for covert action and hones in on conventional and cyber covert action. Because expected utility theory is a constitutive part of rationality this chapter does not go into psychological-cognitive approaches to explain motivations for conflict.

Setting the basic assumptions

Before diving into the motivation and rationality for conflict, it is necessary to establish the basic assumptions contained within this chapter. First, rationality within this chapter is reflective of bounded rationality. Bounded rationality is used to more accurately reflect the conditions present within the international system, both within neo-realism and neo-liberalism.

¹¹² James D. Fearon, "Rationalist Explanations for War," *International Organization* 49, no. 3 (1995).

¹¹³ Ibid.

Herbert Simon serves as a guide in isolating what rationality means in this context when he wrote:

*“To deduce the procedurally or boundedly rational choice in a situation, we must know the choosing organism's goals, the information and conceptualization it has of the situation, and its abilities to draw inferences from the information it possesses. We need know nothing about the objective situation in which the organism finds itself, except insofar as that situation influences the subjective representation.”*¹¹⁴

Second, there are times when it is possible that a national leader might act out of self-interest rather than in the national interests. Covert action conducted by a state may have positive utility for an individual of a state and may at the same time be irrational because it has a negative utility for the state. Such an instance would indicate engaging in covert action would be irrational from a national security perspective. Leaders might act based on their individual rationality and still force their state to behave irrationally. Hitler would be a prime example of this. However, the argument of this chapter is that states act as unified rational actors in the national interest.

The motivation and rationality for conflict

Fearon cites three commonly held rationalist arguments for why states are willing to engage in conflict despite knowing they are forgoing the lesser ex-ante costs of bargaining in favor of higher ex-post costs associated with conflict. Anarchy, preventative war, and positive expected utility each have substantial literatures behind them.¹¹⁵ Each in some way develops a logic for *casus belli*. Waltz, Mearsheimer and other neorealists state that the security conundrum makes conflict inevitable because there is nothing within the international anarchic order that prevents states from engaging one another in hostilities. Fearon notes that while this is true, the

¹¹⁴ Herbert A. Simon, "Human Nature in Politics: The Dialogue of Psychology with Political Science," *The American Political Science Review* 79, no. 2 (1985), 294

¹¹⁵ See Waltz, *Theory of international politics*. for discussions on anarchy; See Michael W. Doyle and Stephen Macedo, *Striking first : preemption and prevention in international conflict* (Princeton, NJ: Princeton University Press, 2008). for why preemptive war is not a rational path for war instigation; See Bruce Bueno De Mesquita, "An Expected Utility Theory of International Conflict," *American Political Science Review* 74, no. 4 (1980). for a discussion on utility and conflict.

lack of constraints on war occurring and the fact that wars occur does not present sufficient grounds for rational conflict. He illustrates that despite a lack of constraints preventing war, the act of engaging in war is almost always ex-post inefficient and therefore irrational. Furthermore, he cites realist arguments that states engage in preventative wars as a rational act. Although realists argue it is rational to engage in a war in the present to minimize future costs, Fearon illustrates that this is a flawed logic. Ex-post inefficiencies are still present in both anarchic and preventative war, which according to Fearon makes them both irrational.

In this argument Fearon only briefly touches on what the real logic behind these causes of war indicate. They, in and of themselves, are not motivations or rational explanations for war, rather they are structural constraints that make war more likely. It is these structural constraints on the international system that facilitate those motivations forming the basis for the rational instigation of conflict.

Lastly, Fearon indicates basing conflict on a positive expected utility for conflict is also irrational.¹¹⁶ He largely bases this on a critique of Bruce Bueno de Mesquita's argument that states will not engage in conflict if they do not have a positive expected utility.¹¹⁷ However, Bueno de Mesquita is not arguing that states should go to war if they have positive expected utility, only that it is rational if they do decide to go to war.¹¹⁸ Nor does Bueno de Mesquita claim that both states need to have positive utility to engage in conflict, rather he finds that only the conflict initiator must have positive utility. He specifically does not indicate that both parties to a conflict need to find it rational, because this would be a violation of Arrow's impossibility

¹¹⁶ Fearon, "Rationalist Explanations for War.", 386.

¹¹⁷ Bueno De Mesquita, *The war trap*.

¹¹⁸ In the abstract Bueno de Mesquita states explicitly "An expected utility theory of necessary, but not sufficient, conditions for the initiation and escalation of serious international conflicts, including war, is proposed." in Bueno De Mesquita, "An Expected Utility Theory of International Conflict."

theorem.¹¹⁹ In theory it is possible for two states to both expect positive utility from conflict with one another, this would be a rational miscalculation of subjective probabilities.

Because the expected utility of international conflict is only one possible option in a range of policy options, its utility must be weighed against other options such as diplomacy. This creates an intrapersonal comparison of utilities, meaning that utilities are comparable across decisions within a single individual (state). This differs from assumed utility construction in which decisions are identical across individuals (states), or interpersonal utility construction. The subjective nature of utilities in a bounded sense of rationality makes interpersonal utility comparisons illogical.

Utilities help facilitate preference ordering through intrapersonal comparison of subjective utilities. This intrapersonal comparison indicates that if state A has a positive utility of .08 for conflict and a positive utility of .09 for covert action, covert action is likely to be ranked higher based on a cardinal preference ordering of utilities. The utilities are not intrapersonally independent. This is an important distinction that needs to be made in the rationalist explanations of war. While the first two explanations as posited by Fearon are clearly predicated on weak rational explanations (because they are not causal explanations but structural frameworks), the third is not and more accurately underpins all aspects of rationality as indicated by Simon.

¹¹⁹ Arrow, "A Difficulty in the Concept of Social Welfare."

Both Fearon and Bueno de Mesquita make the argument for the bounded rationality of actors. Within a bounded rationality model, the utility for conflict must be positive. Bueno de Mesquita does not explain why states go to war, only that the act of going to war with the conditions he presents is rational. The greater the utility, the more compelling the argument for conflict. He writes: "Being rational simply implies that the decision maker uses a maximizing strategy in calculating how best to achieve his goals"¹²⁰ This is a clear indication that rationality in Bueno de Mesquita's conceptualization is simply a way of ranking utilities to achieve the best result.

Claiming that rationality is predicated on a full understanding of the utility for conflict both ex-ante and ex-post, Fearon asserts that the motivation for conflict is largely based in three root causes. First, war can occur due to private information and incentives to misrepresent.¹²¹ Second, war can occur due to commitment problems between states.¹²² Third, War can occur due to issue indivisibilities.¹²³ These are three situations in which it is not possible to negotiate an ex-ante settlement to avoid hostilities within Fearon's bargaining range of possible ex-ante solutions.

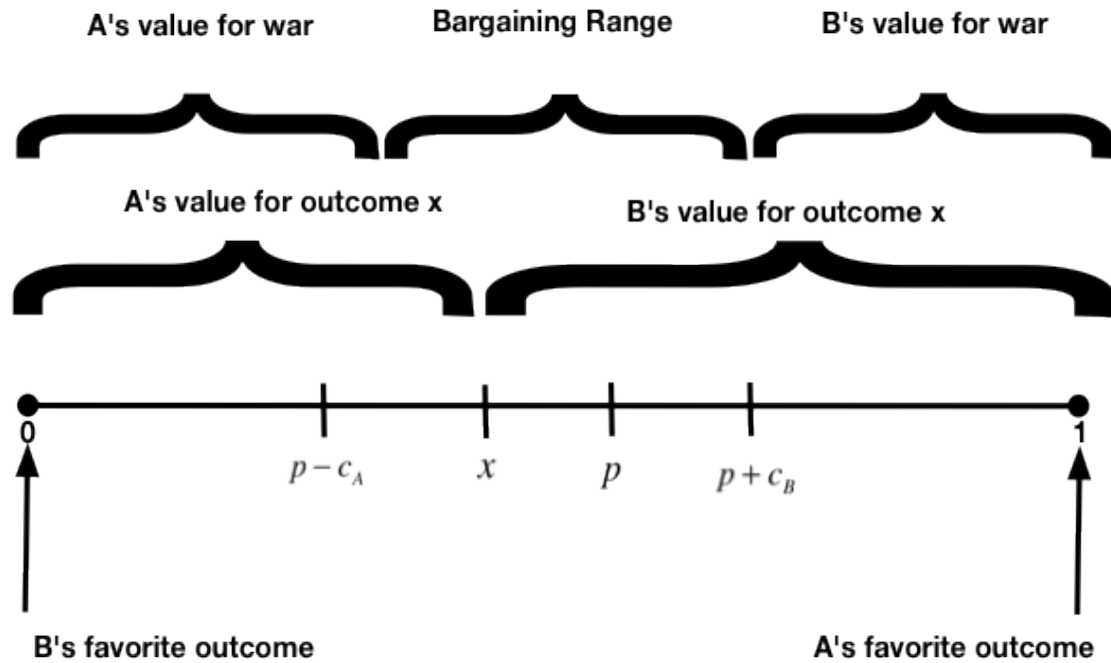
Figure 3.1 is Fearon's illustration of the bargaining range in which states are either unwilling or unable to maintain a commitment or attempt to conceal or misrepresent information. The bargaining range below is the space between $p - c_A$ and $p - c_B$. It is not in dispute that in many if not all instances there exists an ex-ante bargaining range. Nor is it believed that Bueno de Mesquita's expected utility theory of international conflict precludes such a bargaining range and provides a direct path to conflict.

¹²⁰ Bueno De Mesquita, *The war trap*, 31

¹²¹ Fearon, "Rationalist Explanations for War.", 390.

¹²² Ibid., 404.

¹²³ Ibid., 382.



From: Fearon, J. D. (1995). "Rationalist Explanations for War." *International Organization* 49(3): 379-414.

Figure 3.1: Fearon's bargaining range

If such a range were available it could possibly be subsumed within Bueno de Mesquita's model in the mathematical notation of changes in policy positions over time by $\Delta(U_{ii} - U_{ij})_{t0 \rightarrow t+n}$ for the conflict initiator and $\Delta(U_{ij} - U_{ii})_{t0 \rightarrow t+n}$ for the defensive party. The causes Fearon identifies as the locus for casus belli: indivisibilities, misrepresentation and miscalculation, and commitment problems are viable characteristics that can be incorporated into a construction of utility. Even if these are not adequately assumed into the mathematical notation it is logical to assume that each alternative option available to a policy maker also carries with it a unique expected utility function. These utilities are then intrapersonally comparable.

Based on Fearon's bargaining range there are three instances in which international conflict can be initiated rationally: (1) Rational miscalculation due to a lack of information or a disagreement about relative power due to information asymmetries, (2) issue indivisibilities, and (3) commitment problems. Each of these rationalist explanations for war is, however, predicated on the conflict initiator having a positive expected utility. Rarely if ever has there been a case in which two states have mutually declared to engage in hostilities at the same time against one another. Most if not all conflict has a conflict initiator. The definition of conflict initiator can at times be blurred, yet it has never been the case that two states mutually agreed to settle their differences by engaging in warfare without one having fired the first shot.

Motivation and utility should be rightly separated when discussing conflict. While in realism the world is black and white, us and them; the complex interdependencies of neo-liberalism offer hybrid model for conceptualizing how states interact. Although Fearon claims to be making an argument in support of realist rational explanations for war he is in fact making a neo-liberal argument. He is in essence claiming states are not defined purely by the one off zero-sum interactions, but rather are in truth defined by two competing measures of expected utility, the ex-ante and the ex-post. If anything the bargaining range represents what Arthur Stein refers to as coordination and collaboration.¹²⁴ Stein writes:

*"Regimes arise because actors forgo independent decision-making in order to deal with dilemmas of common interests and common aversions. They do so in their own self-interest, for in both cases, jointly accessible outcomes are preferable to those that are or might be reached independently."*¹²⁵

¹²⁴ See Arthur Stein "Coordination and Collaboration: Regimes in an Anarchic World" in David A. Baldwin, *Neorealism and neoliberalism : the contemporary debate* (New York: Columbia University Press, 1993). , 41.

¹²⁵ Ibid.

There is no mechanism within the neo-realist literature by which states can achieve a bargaining stance ex-ante. Instead the victor imposes his demands on the loser following the conclusion of hostilities, as a requirement for concluding hostilities, or as a requirement for avoiding hostilities. Both sides are caught in a prisoner's dilemma and are willing to defect, creating an irrational (inefficient) ex-post result. What Fearon is attempting to illustrate is a situation in which states can create a mutually established agreement, a regime that seeks efficiency. His argument is in line with Bueno de Mesquita's necessity for a positive expected utility. When an alternative policy option to conflict arises it is necessarily compared to Bueno de Mesquita's concept of expected utility for international conflict. If the alternative course of action offers a higher utility, that option would be the rational choice. If options with greater political utility exist, these options should alter the expected benefits to be gained by conflict and alter the utility of conflict, creating a diminishing utility for conflict over time.

If a state has a negative utility for conflict then, engaging in conflict would be irrational. Therefore it is possible to have multiple outcomes of the decision process. A state can find it rational to engage in conflict, yet have other preferences providing greater utility. Conflict could provide the greatest utility and therefore be chosen as the maximizing preference. Or, conflict could have a negative utility. In the final instance, choosing conflict would be irrational regardless of the structural constraints of the system. In such an instance it would be more logical for a state to seek out an alternative to conflict. Every option has a measure of utility to the decision-maker (the unitary actor). Having utility does not equate to choosing a preference unless that preference provides a utility maximization for the actor.

The above established that there are three instances in which conflict is rational and there is a mathematical means of assessing when it is rational to engage in conflict within these

instances (expected utility theory). The establishment of rationality behind conflict has thus far failed to sufficiently identify a motivation for conflict. Simply stating that there are issue indivisibilities is not a sufficient motivation for conflict; likewise information asymmetries and commitment problems also do not provide a motivation for conflict. They instead describe the characteristics in which conflict can occur.

A policy range in which states interact defines the bargaining range for states. Returning to the policy range illustrated in chapter 1, Figure 3.2 establishes the bi-lateral policy range between two states. Broadly stated international relations are the process by which states influence one another's policies. The bi-lateral policy range is a relationship of policies between two states. It is in this policy range that the rational explanations for conflict can occur. This paper specifically focuses on the bi-lateral policy range of states because covert action rarely occurs with multiple complicit national parties. The primary objective is covert and therefore is between two parties, the instigator and the target.

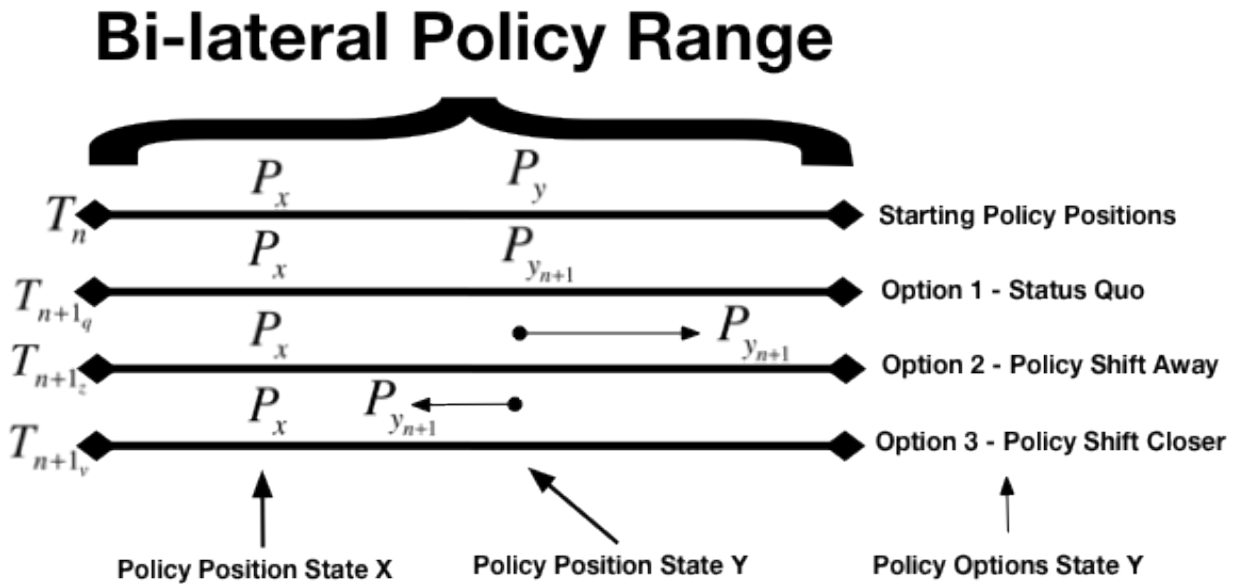


Figure 3.2 Bi-lateral state policy interaction possibilities.

At time T_n two states are aligned on a policy spectrum and the distance between them represents the difference between their respective policy positions. The more proximate the states are, the closer their policy positions. Likewise, the further they are apart, the more they diverge in their policy positions. Assuming state P_x is the potential conflict initiator it looks for movement in the policy position of state P_y . State P_y has three options, it can (1) maintain the status quo, (2) move its policy further away from P_x , or (3) move its policies more in line with P_x . In this situation state P_x will likely view a policy shift away from its position as an act of aggression, it might also view the maintenance of the status quo as an act of aggression. Lastly, it might view the policy shift of state P_y as occurring too slowly which could also be construed as a hostile action. In each of these instances there is a possibility for the potential conflict initiator to view the actions by its adversary as hostile. Option three is least likely to be viewed as hostile, while option two is most likely to be viewed as hostile, with option one somewhere in between.

The motivation for any conflict is rooted in the policy divergences between nations on issues. Neo-liberalism and Fearon's claims for rationality both indicate that in most instances there is a workable settlement, which can result in a more efficient outcome than conflict. Before resorting to an all out conflict and working within Fearon's identifiable areas preventing a ex-ante settlement are another set of options open to policy makers that have been used for millennia in an effort to mitigate the rationalist explanations for war and provide a mechanism for facilitating an ex-ante settlement.

Covert action steps into the breach short of overt armed conflict between two belligerents. Covert action can occur throughout the policy interactions of states. Covert action serves as a tool for the mitigation of information asymmetries, issue indivisibilities, and commitment problems. It can serve as a tool to improve the bargaining position of a state or to bring states back to the bargaining table.

The next section briefly examines what political utility is. This allows the discussion on the development of political utility for covert action to move forward directly from above discussion on the need for covert action. If covert action is truly a third option, then there is a need to express its utility in the context of the ex-ante and ex-post costs.

Political utility and the literature

Before engaging specifically the topic of "Political Utility" it is best to disaggregate the two terms. The first term "politics" is derived from the Greek term *politika* examined in detail by such philosophers as Aristotle and Sun Tzu, is of little help in understanding the term political utility. Politics simply refers to the "art or science of government."¹²⁶ "Utility," in contrast to politics, is a powerful economic concept developed in exhaustive detail and honed into its

¹²⁶Politics , in *Merriam Webster* (2012).

modern form by Jon Von Neumann and Oscar Morgenstern.¹²⁷ The economic concept of utility was first carried over to political science in the 1950's with the work of Anthony Downs.¹²⁸

Downs states that utility is simply a “measure of benefits.”¹²⁹ He follows directly in the footsteps of Von Neumann and Morgenstern and defines utility by stating that a rational individual, given a series of alternatives, will weigh the values of each and create a *complete* and *transitive* preference ordering. The individual will then choose the preference with the highest value. The economic terminology associated with utility is not related to both sides understanding the preference orderings of the other. Rather it is an individual decision-making process. Therefore, the utility of two individuals in the same situation can differ dramatically. This is essentially what Downs means when he writes that a voter will act towards “his own greatest benefit.”¹³⁰ If all voters had the same utility calculus, there would be little need for elections. To create political utility we aggregate the two terms: the art or science of government and the measure of benefits. Political utility is the measurement of the benefits to government in a unitary state centric system.

The concept of the benefits to government is not as straightforward as it might at first glance appear. In this instance it is assumed that the government is a representative of the collective will or interest of the people. This might not be true in non-representative systems, yet as individuals within these systems must respond to their government, it is possible by extension to assume a diffusion of collective benefit or cost associated with a government's actions. These benefits and costs are not always distributed equally among the citizens of a nation. However, often in such policy areas as national defense they are assumed to comprise common pool

¹²⁷ Von Neumann and Morgenstern, *Theory of games and economic behavior*.

¹²⁸ Anthony Downs, *An economic theory of democracy* (New York: Harper, 1957).

¹²⁹ Ibid., p36.

¹³⁰ Ibid.

resources. Whether the motivation for an action originates internally or externally the utility scores are calculated based on what can be gained or lost in relation to the opponent. National gain or loss differs significantly from what might be gained or lost politically within a nation. An argument predicated on domestic political utility development functions separately from the argument being posed in relation to state on state covert action in this present chapter.

Political utility is not perfect and contains many failings. Many of these failings are found in the inability to aggregate individual preference orderings, cognitive failings as examined by Amos Tversky and Daniel Kahneman, or even in group dynamics illustrated by Irving Janis.¹³¹ Despite its limitations, there is no piece of literature that finds rational choices must be conditional upon an opposing party's simultaneous choice. Robert Grafstein notes "Conditional expected utility maximizers are concerned with expected utility, whether or not they caused it."¹³² Rational decisions are reached independent of one another in most instances. Covert action has political utility because it seeks to maximize the benefits to a government and by extension its people in the same way as overt diplomatic bargaining and overt military conflict.

The use of covert action for political utility

The National Security Act defines covert action as "[a]n activity or activities of the United States Government to influence political, economic or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly."¹³³ Covert action goes by many names, often referred to as Track-II, the quiet option, or

¹³¹ Irving L. Janis and C. R. M. Productions, "Group dynamics groupthink," (New York: McGraw-Hill Films : Produced by CRM Educational Films, 1973); Daniel Kahneman and Amos Tversky, "Prospect Theory: An Analysis of Decision under Risk," *Econometrica* 47, no. 2 (1979).

¹³² Robert Grafstein, "Rationality as Conditional Expected Utility Maximization," *Political Psychology* 16, no. 1 (1995).

¹³³ "National Security Act of 1947," *National Security Act of 1947* (2009).

the third option.¹³⁴ In an international system where the formal declaration of war is becoming an increasing rarity, the gap between diplomatic and overt military dispute resolution has never been wider.

This work will now examine in detail the legal framework within which covert action applies within the American case, the focus lies in ascertaining those instances when covert operations were deemed necessary, what the motivation behind and the utility associated with those operations were. Furthermore, this is used as a bridge into isolating the constituent characteristics of covert action, types of covert action and where modern technologies have come to fit in this evolving domain of operations

First, covert action is not a rare occurrence. Gregory Treverton identifies more than 900 operations of various levels between 1951 and 1975 in which the “silent option” was used.¹³⁵ Loch Johnson indicates that covert action has been used very differently by each Presidential administration.¹³⁶ Not only do the aggregate number of covert actions vary from President to President, the intensity of those actions varies as well. More recently the administration of President Obama has sanctioned the use of at least 239 covert drone strikes in Pakistan.¹³⁷ The question still remains why do we use covert action?

Loch Johnson’s quote from Henry Kissinger provides a succinct logic for covert action. According to Kissinger: “We need an intelligence community that, in certain complicated situations, can defend the American national interest in the gray areas where military operations

¹³⁴ Mark M. Lowenthal, *Intelligence : from secrets to policy*, 5th ed. (Washington, DC: CQ Press, 2011); Loch K. Johnson, *America's secret power : the CIA in a democratic society* (New York: Oxford University Press, 1989).

¹³⁵ Gregory F. Treverton, *Covert action : the limits of intervention in the postwar world* (New York: Basic Books, 1987). 12.

¹³⁶ Johnson, *America's secret power : the CIA in a democratic society*: 103.

¹³⁷ David Rohde, "The Obama Doctrine: How the president's drone war is backfiring," *Foreign Policy*, no. March/April (2012).

are not suitable and diplomacy cannot operate.”¹³⁸ As was stated above in regards to Fearon’s bargaining range, there is quite frequently a middle area in which bargaining simply becomes too difficult. This is what Kissinger is referring to as the “grey area.” It is an important point to belabor because it provides nuance to the concept of covert action. By parsing out what covert action is, it is possible to contextualize modern covert acts. Below are a series of quotes from practitioners and scholars alike. Each helps to frame the rationale for covert action and to define its broader boundaries. The quotes often provide contradictory frameworks within which to understand covert action.

Practitioner Duane Clarridge writes in his memoir:

“Covert action entails special activities, such as political action and paramilitary operations, to advance U.S. foreign policy objectives by influencing events in foreign countries. I believe I concluded at this time that my purpose in life and the reason I was in the CIA was to advance the interests of the U.S. government and the American people abroad.”¹³⁹

Practitioner James M. Olson writes in his book on the morality of spying:

“Espionage is a crime in every country, and the United States practices it in almost every country. Covert action, defined as intervening secretly in the affairs of foreign countries, is a blatant violation of international law.”¹⁴⁰

Practitioner Theodore Shackley writes in his memoir:

¹³⁸ Johnson, *America's secret power : the CIA in a democratic society*: 17.

¹³⁹ Duane R. Clarridge and Digby Diehl, *A spy for all seasons : my life in the CIA* (New York, NY: Scribner, 1997). , 42.

¹⁴⁰ James M. Olson, *Fair play : the moral dilemmas of spying* (Washington, D.C.: Potomac Books, 2006). , digital location 791.

“Covert action operations can be as deceptively peaceful as a letter-writing campaign or as flagrantly violent as a guerrilla uprising. In every case, though, the instigating government must make at least a token effort to hide its hand.”¹⁴¹

Loch Johnson quotes Les Aspin as saying:

“...covert actions should be as consistent as possible with the moral character of the American public, so that if some action becomes public, it would not be terribly embarrassing to the government of the United States because it is not something most Americans would consider immoral.”¹⁴²

President Richard M. Nixon writes:

“Overt economic or military aid is sometimes enough to achieve our goals. Only a direct military intervention can do so in others. But between the two lies a vast area where the United States must be able to undertake covert actions. Without this capability, we will be unable to protect important U.S. interests.”¹⁴³

Each of the above quotes offers a perspective on the value of covert action ranging from the practical, moral, and legal. While each varies on the moral and legal ramifications of covert action, each to some extent acknowledges that covert action fills a necessary gap in foreign policy. Despite knowing there is a gray area of operations and knowing these operations occur at varying levels still leaves the gap of defining what constitutes covert action.

¹⁴¹ Theodore Shackley and Richard A. Finney, *Spymaster : my life in the CIA* (Dulles, Va.: Potomac Books, 2005). , digital location 658.

¹⁴² Loch K. Johnson, *The Threat on the Horizon: An Inside Account of America's Search for Security After the Cold War* (Oxford; New York: Oxford University Press, 2011). , digital location 10752.

¹⁴³ Quoted in William J. Daugherty, *Executive secrets : covert action and the presidency* (Lexington: University Press of Kentucky, 2004). , 9.

Defining covert action is less difficult than assigning its value. In defining what covert action is it is best to provide a rigorous framework within which to understand covert action. Here again it is beneficial to consider Loch Johnson who outlines four broad categories of covert action. Johnson identifies: Propaganda, Political Covert Action, Economic Covert Action, and Military Covert action. Each of the titles is somewhat self-evident. Johnson then takes it a step further and identifies a scale or ladder of covert action. Figure 3.3 is a modified version of Johnson's scale of covert action. The changes made to his original ladder include critical infrastructure destruction, pinpointed digital actions against combatants, critical infrastructure degradation/denial, and computer network exploitation. Each of these additions adds in a host of potential actions emanating from cyber domain and fall distinctly within the ladder at various locations.

Utility is not determined by the type of covert action, rather it is ascertained by the expected effect such a covert action might have on the intended target in relationship to the possible costs associated with failure. That being said, the further up the ladder of covert action a nation precedes, the greater the ramifications for failure and conversely the potential for great gain. A national leader with commitment problems is unlikely to be assuaged by covert actions on the lower thresholds. However, the consequences of an extreme covert action such as a failed state-sponsored coup d'état could lead to overt war and a great deal of negative utility. Covert actions must be tailored to meet the need and risks of a given situation. The most basic level - lower thresholds pose much less risk than higher thresholds of action. They also are likely to offer less reward. Yet because utility can be intrapersonally additive in many instances, a series of actions with little independent political utility might be more effective and result in a

combined utility greater than a single risky operation with a one-time possibility for a higher utility payoff.

Threshold Four: Extreme Options

- 34 Use of WMD
- 33 Major Secret Wars
- 32 Critical Infrastructure Destruction
- 31 Assassination
- 30 Small-scale coup d'état
- 29 Major economic dislocations; crop, livestock destruction
- 28 Environmental alternatives
- 27 Pinpointed covert retaliations against non-combatants
- 26 Torture to gain compliance for a political deal
- 25 Extraordinary rendition for bartering
- 24 Major hostage rescue attempts
- 23 Pinpointed digital actions against foreign combatants (non-civilians)
- 22 Sophisticated arm supplies

Threshold Three: High Risk Options

- 21 Massive increases of funding in democracies
- 20 Critical infrastructure degradation/denial
- 19 Small-scale hostage rescue attempt
- 18 Training of foreign military forces for war
- 17 Limited arms supplies for offensive purposes
- 16 Limited arms supplies for balancing purposes
- 15 Economic Disruption without loss of life
- 14 Information Communications Systems Disruption without loss of life
- 13 Modest funding in democracies
- 12 Massive increases of funding in autocracies
- 11 Large increases of funding in autocracies
- 10 Disinformation against democratic regimes
- 9 Disinformation against autocratic regimes
- 8 Truthful but contentious propaganda in democracies
- 7 Truthful but contentious propaganda in autocracies

Threshold Two: Modest Intrusions

- 6 Low-level funding of friendly groups
- 5 Computer Network Exploitation
- 4 Truthful, benign propaganda in democracies

Threshold One: Routine Operations

- 3 Truthful, benign propaganda in autocracies
- 2 Recruitment of covert action assets
- 1 Support for routine sharing of intelligence

Figure 3.3: Covert Action Ladder¹⁴⁴

¹⁴⁴ Loch K. Johnson, *Secret agencies: U.S. intelligence in a hostile world* (New Haven: Yale University Press, 1996). 62-3. See Also: Loch K. Johnson, "On Drawing a Bright Line for Covert Operations," *The American Journal of International Law* 86, no. 2 (1992).

The threshold of covert action(s), as in any diplomatic or military setting, must be targeted to achieve the greatest benefit with the lowest cost. Temporal problems aside, in attempting to bridge the gap there are many tools that can attempt to fill the bargaining range among which covert action is one typology. Overt forms of signaling including threats or the imposition of economic sanctions can be another.

The motivation and utility for conflict are those variable factors that lead states to engage in hostilities in the first place rather than negotiate. Although there are many theories analyzing the motivations for conflict ranging from misperceptions to outright irrationality, this work argues the reality behind the motivation for most major state on state wars and the utility assigned to those wars occurs because of an information gap between the potential belligerents. Furthermore, this information gap can be and has been altered by covert actions of states. Because covert action can fill the gap between war and diplomacy it can achieve political utility.

Positive utility through covert action occurs when narrowing the range of policy options minimizes issue indivisibilities, hidden information, or by changing the leadership of an opponent state. Below are several examples, examined in brief, of the use of covert action to achieve positive political utility in the gap between public diplomacy and outright war.

Afghanistan 1980s

Milt Bearden, the CIA Chief of Station in Islamabad during part of the 1980s worked extensively on providing weapons to indigenous fighters in Afghanistan.¹⁴⁵ The program popularized in such films as *Wilson's War* and others was a strategic opportunity to slip *between*

¹⁴⁵ The primary accounting for my mini-case comes from the Memoir of Milt Bearden - Milt Bearden and James Risen, *The Main Enemy: The Inside Story of the CIA's Final Showdown with the KGB* (New York: Random House, 2003); Daugherty, *Executive secrets : covert action and the presidency*.

the overt ends of the foreign policy spectrum. Afghanistan operations also received broad congressional support, a rarity in many covert actions.

By providing weapons indirectly to the Mujahedeen fighters the CIA was able to place pressure on the Soviet Military without having to commit any American boots on the ground and without having to make political concessions. While the origin of the weapons was less than secret, it was still covert and plausibly deniable. With the increasing power of the weapons, which eventually included Stinger anti-Aircraft missiles, the CIA gave the enemy of its enemy the tools to make life increasingly difficult. The Soviets lost thousands of soldiers and spent enormous sums of money, all of which helped to weaken their strategic position globally and reduce information asymmetries, and commitment problems as the regime began to crumble in the late 1980s.

The covert deployment of weapons provided political utility by increasing the pressure on an adversary and by forcing them to realize their geopolitical and strategic limitations. The ex-post costs of the weapons program was significantly less than the costs associated with an overt war and the results created benefits far greater and more efficiently than did the comparable diplomatic efforts. The morality of the endeavor has been questioned more than 20 years later when many of the same fighters to whom the CIA provided weapons are now directing their animosity against the United States, yet for a period of approximately 25 years the cost to benefit ratio provides an example of one of the best covert operations ever run.

Italy 1948

Following World War II and the rise of the Soviet Union, political concerns on the European continent were setting the stage for a hostile environment diametrically opposed to liberal Western Democracy. Before democracy could be removed and replaced with communism

in Italy, it had to overcome an electoral obstacle. This obstacle seemed to pose little hindrance to communism's progress. In this situation the political utility of outright diplomacy would have caused a series of problems. First, western democracies would be perceived as dictating the outcome of an election to the Italians. Such an action could have had large negative ramifications and created resentment among Italians. Second, meddling in the elections of another state is an overt hostile act and could be constitutive of an act of aggression. The CIA was directed to prevent a communist victory with plausible deniability for U.S. involvement. Again the foreign policy of the United States needed to act within the gap between outright military intervention in favor of liberal democracy and overt diplomatic efforts that could potentially harm regional relationships. Covert action was used to the benefit of American foreign policy objectives for the purpose of alleviating information problems in an environment where the overt representation of political positions could have resulted in negative consequences. The CIA, by covertly funding moderate western oriented parties, provided them with the resources to defeat a political adversary. The result was enough to keep Italy western focused throughout the cold war.

Estonia 2007

Shifting from traditional covert actions to cyber covert actions affects the construction of political utility. Cyber conflict complicates traditional notions of Covert Action. This increase difficulty of comprehension arose in the case of the 2007-cyber attacks against Estonia. In 2007 the Estonian government decided to remove a Russian war memorial from central Tallinn engendering a great deal of animosity among ethnic Russians as well as within the Russian Federation. In response large scale Distributed Denial of Service (DDoS) attacks were conducted against key governmental, financial, and press targets within the former Soviet republic.¹⁴⁶ The

¹⁴⁶ Kramer, Starr, and Wentz, *Cyberpower and National Security*: p177-8.

question is whether this type of bold and public attack against a country's cyber infrastructure is constitutive of a covert action. In this instance the answer is yes and no. All reports indicate that the attacks were sanctioned by the FSB, the modern version of the KGB.¹⁴⁷ The attacks, while not conducted by the Russian Federation, were likely condoned by or facilitated through official channels.¹⁴⁸

The overall consequence of the attacks against Estonia was severe in the short term, but mild over the long haul. This type of attack is classified on the ladder of covert action in the third threshold as a combination Economic Action without loss of life and Information Communications Systems Disruption without loss of life. The attack falls under these two categories within the third threshold because of the breadth of the attack spanning across both financial, media, and governmental organizations. If the attack had been solely directed at one type of institution it would have been more easily classifiable.

This type of action is covert because it achieves a political statement without directly implicating a national sponsor. In this instance the Russian Federation was able to achieve a significant political point without losing face through overt diplomacy. Thus, while the action was visible, the culprit(s) were not, making it covert. The political utility of the act lies in the ability to convey a significant foreign policy message without attribution from the sender. More simply, the result was a signal: "we can do significant damage to your information and economic infrastructure if you are disrespectful towards us." Such a signal increases political clout and can increase uncertainty of an opponent within the bargaining range of issues.

¹⁴⁷ Chris C. Demchak, *Wars of disruption and resilience : cybered conflict, power, and national security* (Athens: University of Georgia Press, 2011); Richard A. Clarke and Robert K. Knake, *Cyber war : the next threat to national security and what to do about it*, 1st ed. (New York: Ecco, 2010).

¹⁴⁸ "Cyberwar," *The Economist*, July 3 2010.

Syria 2007

A combined conventional-cyber covert action occurred in September 2007, when the Israelis invaded Syrian airspace undetected and bombed what the CIA later disclosed was a nuclear facility being developed jointly by the North Koreans and the Syrians.¹⁴⁹ This attack was a coordinated conventional military attack made possible by covert cyber actions. The Israelis, as Richard Clarke and others indicate, used cyber means to spoof the Syrian air defense mechanisms.¹⁵⁰ This type of attack is a dual covert, overt attack. Once the bombs were dropped the attribution and covert nature of the attack was eliminated. However, the ability to conduct the attack was predicated on the covert operation that shifted the tactical advantages wholly in favor of the Israelis.

Does this type of attack fit within the bargaining range above as defined by Fearon? Not quite, but the political utility associated with such a covert operation is plainly obvious. It is possible to claim that the combined attack eliminated an indivisible issue, the Syrian development of nuclear capabilities. Regardless of whether the attack falls within the bargaining range where covert action is most effective, it was both ex-ante and ex-post efficient from the Israeli perspective. They were able to eliminate a potential threat and neither side suffered casualties. By eliminating the nuclear facility, the Israelis forced Syria toward a more favorable policy position indicating a positive utility.

¹⁴⁹ Clarke and Knake, *Cyber war : the next threat to national security and what to do about it*: digital pages 12-26.

¹⁵⁰ Ibid.

Stuxnet 2009

This last mini-case involves a pure case of covert cyber action garnering political utility. In 2010 Iran admitted to experiencing problems with their nuclear enrichment facilities at Nantaz. The Wall Street Journal then reported that Iran was the victim of a highly sophisticated cyber attack.¹⁵¹ Other news organizations followed up with stories claiming that the malicious software specifically targeted Siemens systems in configurations typically used for centrifuges designed to enrich uranium. The result was a significant delay in the production capabilities of Highly Enriched Uranium (HEU).¹⁵² Software security agency Symantec followed up on the Stuxnet story by issuing a report detailing the malicious software.¹⁵³ Combined these news reports and corporate analyses of the software provide a unique picture of one of the first significant cyber covert actions.

While other chapters have detailed that the software was designed to be very specific in its attack protocol, of relevance to this chapter is the political utility of such an attack. To understand the political utility of the attack it is necessary to contextualize the situation. Iran had for years been vehemently denying it was working towards producing nuclear weapons capabilities. It had consistently claimed it was working on nuclear production solely for peaceful purposes. Because the Iranians would not allow inspectors from the IAEA into their facilities or there was no way to verify the veracity of their claims. This created a significant information asymmetry between Iran and its primary accusers, Israel and the United States. The situation increased in importance with heightened rhetoric by Iranian President Mahmoud Ahmadinejad.

¹⁵¹ Vanessa Fuhrmans, "Virus Attacks Siemens Plant-Control Systems," *Wall Street Journal - Eastern Edition* 256, no. 18 (2010).

¹⁵² William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times* 2011.

¹⁵³ Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier," (Symantec Security Response, 2011).

Ahmadinejad on numerous occasions called for the destruction of Israel. This led to worries that a potential nuclear weapon would be directed against Israel.

Diplomatic efforts were stalled and the predicament in Iraq with the long-term engagement in a counter-insurgency campaign made the possibility of an overt war against Iran highly unattractive. The objective became two-fold. First, reduce the information asymmetry of the situation by exposing an enrichment process that exceeded normal civilian use enrichment, and second, hinder the enrichment process to delay the eventual production of a nuclear weapon. The situation presented fell between both ends of the overt spectrum and provided a middle range within which to achieve two political objectives.

The Stuxnet worm was able to provide political utility by first illustrating that Iran was enriching Uranium beyond civilian use. This information transparency paved the way for enhanced sanctioning efforts on the international level and opened up new diplomatic alternatives. These diplomatic alternatives were only feasible because of the second aspect of Stuxnet, time. If the covert operation had only identified Iran's movement towards HEU, then it would have increased the need for overt armed conflict. However, because Stuxnet delayed the production of HEU, it provided time for overt diplomacy to have a chance at mitigating the need for conflict.

The operation was not perfect. Stuxnet did not have a self-delete function and was eventually released into the wild. Although it did not adversely affect other systems due to its programming structure, it would have been of greater benefit if the operation had remained completely secret.¹⁵⁴ At present it is uncertain what, if any, costs might be associated with a loss

¹⁵⁴ David E. Sanger, *Confront and conceal : Obama's secret wars and surprising use of American power* (New York: Crown Publishers, 2012).

of anonymity. As will be illustrated in subsequent chapters, this particular covert action was conducted by two nations with a significant power advantage over their adversary.

The Utility of Covert Action

Political utility and covert action are not mutually exclusive. Nor do both sides to a dispute need to be aware of the other's actions for one side to gain or lose in political utility. For too long scholars have focused on the overt world of political utility and ignored the bargaining range affected by actions in the shadows of international relations. This chapter sought to remedy this by citing a broad range of literature and by bringing in statements from scholars, politicians and practitioners alike. This chapter presented evidence that covert action can be examined using expected utility theory. Covert action is a tool of rational states. While leaders can abuse this tool, the argument set forth highlighted the mechanism by which states, acting as unitary actors, can determine the utility of covert actions whether they are conventional or cyber covert acts. Furthermore, this chapter illustrated that covert action works best in what James Fearon defined as the bargaining range between states.

Covert action so often falls to the sidelines of international relations because of its moral and ethical considerations. Additionally, the inability to gather current evidence on the state of covert action dissuades academics from engaging in a rigorous study of it and its implications. Although the gap between overt diplomacy and overt war can be large, to turn our eyes away from this bargaining range is to ignore the real world tools being used to affect it. Covert action can and does play a role in the space between diplomacy and war. The utility of covert action is derived from its ability to alter the policy relationships of states in international relations and achieve tangible benefits to a government.

Section II - The foundations of a rational decision

CHAPTER 4

Digital Power

“I hope our wisdom will grow with our power, and teach us that the less we use our power the greater it will be.” ~ Thomas Jefferson¹⁵⁵

This chapter explores traditional formulations of power at the national level and examines the failures of these traditional notions to incorporate the value of cyber. This chapter is largely a theoretical discussion debating the relevant literature and framing the debate for the concept of power in cyber. This chapter examines the material, political, economic, social, military, and intelligence qualities comprising national power and how each of these aspects of power is dependent on cyber. Building largely on previous works on power, the case is made for a dynamic and highly evolved understanding of national cyber power. Following the development of the logic of cyber power, the variable for cyber power is constructed. In defining national cyber power the chapter also brings to the forefront issues of asymmetry and the scalable nature of power in cyber.

Following the initial analysis of power the focus of the chapter turns intensely on developing the index variable components of cyber power. Broadly a theory of cyber power is comprised of three categories: theoretical capabilities, demonstrated capabilities, and national digital dependence. The aggregate measure of these categories provides a power score, which can be input into the utility theory of cyber conflict developed in the third section.

¹⁵⁵ Thomas Jefferson, *The Writings of Thomas Jefferson*, 20 vols., vol. 14 (1815). p308.

Power is an ambiguous concept. Power in the traditional sense is imagined as a brute force strength that overwhelms a potential adversary. Or as Jeffrey Hart explains, when looking at the definition of power there are common threads of “control, influence, and legal authority.”¹⁵⁶ In politics and international relations in particular there is one primary type of power, the ability to get one’s way. This can be linguistically construed as ability for a person to have influence. In this context, a weak person is forced, whereas a powerful person forces. Max Weber wrote of power that it is “the probability that an actor in a social relationship will be in a position to carry out his own will despite resistance, regardless of the basis on which this probability rests.”¹⁵⁷ The ability to carry out one’s own will can be derived from the psychological context, or it can be derived from physical brute force. Hence both psychologically and physically an atomic bomb is more “powerful” than a knife. This chapter examines the construction of a new form of power that straddles the psychological and brute force conceptualizations of power. Cyber power is a hybrid of psychological and physical concepts of power. Understanding what cyber power is provides insight into how states might decide to wield it.

Conventional studies on power within rational choice modeling of war have depended largely on physical brute force definitions of power. These brute force definitions include military and domestic production capabilities. The general assumption is Hobbesian in nature. A large brute army, with sufficient domestic capacity, can overwhelm a smaller one. As

¹⁵⁶ Jeffrey A. Hart, "Information and Communications Technologies and Power," in Costigan and Perry, *Cyberspaces and global affairs*: p204.

¹⁵⁷ Quoted from Steven Lukes (1986) in Jeffrey A. Hart, "Information and Communications Technologies and Power," in *ibid*.

Thucydides wrote in the Melian dialogues: “Right, as the world goes, is only in question between equals in power, while the strong do what they can and the weak suffer what they must.”¹⁵⁸

Concepts of power in international relations have evolved somewhat over the last 30 years led largely by Joseph Nye, who has made it his quest to define more accurately the concepts of power for the modern world. If the concepts of power as they have been traditionally used were wholly accurate in conceptualizing conflict, then organizational advances in military structure would not have greatly affected the battlefields of Europe during the Napoleonic era or during the two world wars.¹⁵⁹ However, as Nye notes the concept of power is highly complex and breaks down in to two broad classifications of soft and hard power.¹⁶⁰ Although the focus of this work is on hard power, or pushing an adversary to do as you wish, the concepts are deeply intertwined and in many cases indistinguishable.

This work is by no means the first to take up the definitional aspects of power in cyber and there is no need to redefine cyber power in a wholly novel way. As such this work leans heavily on the terminology developed by Franklin, Kramer and Wentz when they define cyber power as: “the ability to use cyberspace to strategic advantage to influence events in other operational environments and across the instruments of power.”¹⁶¹ What is however needed is a way to move this definition into an operationalizable measure that can be used in a rational choice model for the decision to use such power.

The problem that we run into is breadth of analysis. Because cyber power transcends many aspects of other domains measuring the cyber power of a state is difficult. The next two

¹⁵⁸ Thucydides, Rex Warner, and M. I. Finley, *History of the Peloponnesian War* (Harmondsworth, Eng.; Baltimore: Penguin Books, 1972). ch 5.89.1.

¹⁵⁹ Black, *War and the world : military power and the fate of continents, 1450-2000*.

¹⁶⁰ Nye, *The future of power*.

¹⁶¹ Kramer, Starr, and Wentz, *Cyberpower and National Security*: p38.

sections in this chapter attempt to parse out a workable definition for cyber power in the context of hard applications of power, or what Nye describes as “push” applications of power, rather than “pull.” First, what are the constitutive aspects of cyber power that can forcibly influence an opponent? This is comprised of several categories of variables: military units for cyber purposes, national ICT human and economic capabilities, legal and regulatory frameworks, technological infrastructure, industry application, and demonstrable threat spectrum capabilities. Second, what are the inherent vulnerabilities of cyber power? Lastly, how do these variables interact to create a measure of cyber power applicable to understanding decisions in international relations?

Defining the components of digital hard power

Joseph Nye writes: “Cyber power behavior rests upon a set of resources that relate to the creation, control, and communication of electronic and computer based information -- infrastructure, networks, software, human skills.”¹⁶² This indicates that cyber power, as an influencing force, is comprised of tangible components. As in conventional warfare there are physical attributes associated with the domain of conflict. Infrastructure, networks, and software, each represent the equivalent of modern combat systems, guns, and bombs. Likewise, as in conventional domains of conflict, human skills and the humans themselves are important attributes. A trained army is more effective than an untrained one.

The variables that comprise the indexed variable of power are largely derived from Charles Billo and Welton Chang’s study, “Cyber Warfare,” published by the Institute for Security Technology Studies at Dartmouth College and the Economist’s Intelligence Unit’s

¹⁶² Joseph S. Nye, "Cyber Power," (Cambridge, MA: Harvard Kennedy School of Government - Belfer Center for Science and International Affairs, 2010).

(EIU) “Cyber Power Index” developed with funding from Booz Allen Hamilton.¹⁶³ The Dartmouth study contains a highly detailed list of variables in its analysis of the motivation and capabilities of states to engage in cyber warfare. Many of the variables are aggregated in the present work. Specifically aggregated are those capability variables that measure similar attributes. In addition to the variables defined by the Dartmouth Study are those defined in the Economist Intelligence Unit’s dataset on cyber power. The Cyber Power index by the EIU includes four categories of variables each of which are included in the overall measure of cyber power. The measures used by the EIU are: legal and regulatory framework, economic and social context, technology infrastructure, and industry application.¹⁶⁴ The benefit of incorporating the EIU’s variables into the overall index of national power is an added dynamism to the theoretical conceptualization of cyber power.

The Cyber Power index by the EIU only included power scores on 19 different nations. This spatial limitation was corrected in two ways. First, data was collected on five additional countries including, Israel, Syria, Estonia, Georgia, and Iran. Data from these countries is from the most recent available year. Second, several of the subcategory variables included in the EIU’s data were unavailable for smaller countries. It was deemed these variables were of limited importance. To make up for their absence the weighting of the power scores was readjusted. All of the weights and the variables included as well as their sources are listed in the appendices.

¹⁶³ Charles Billo and Welton Chang, "Cyber Warfare: An Analysis of the Means and Motivations of Selected Nations," ed. Charles G. Billo (Institute for Security Technology Studies at Dartmouth College, 2004); James A. Lewis and Katrina Timlin, "Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization," (New York: Center for Strategic and International Studies United Nations Institute for Disarmament Research, 2011); "Cyber Power Index," ed. Economist Intelligence Unit (Booz Allen Hamilton, 2011).

¹⁶⁴ "Cyber Power Index."

Below each of the components of the theoretical conceptualization of cyber power are explained with their hypothesized effects on cyber power. However, before diving into each of the variables it is necessary to understand how they are combined to create a single measure of power to be used within a decision-making model of cyber.

To create a single robust measure of cyber power the next step in the process is this work develops an index variable of power. This index variable is similar to the Composite Index of National Capabilities (CINC) score. Singer et al., the creators of CINC scores, incorporate variables of conventional power ranging from population to military personnel, create an additive model and then divide the summation of the power scores by the number of variables.¹⁶⁵ Each of the variables included in their indexed variable is a country to world ratio. They use a country to world ratio to represent the finite number of resources presently available to engage in conflict. Equations 4.1 and 4.2 are a representation of their method of indexing to create CINC scores.

Indexing Equations for CINC Scores¹⁶⁶

$$4.1 \quad \text{Ratio of Variable } X_1 = \frac{\text{Country}}{\text{World}}$$

$$4.2 \quad \text{CINC Score} = \frac{X_1 + X_2 + X_3 + X_4 + X_5 + X_6}{6}$$

Although Singer et al. use a ratio of country to world to express a relationship of power within a finite resource system; this conceptualization is not applicable within the cyber domain. Because the resources and capabilities of the cyber domain expand and are not finite, even in a short temporal range, a ratio for the individual measures in the context of global capabilities in most instances would be meaningless. As such to create a meaningful measure for power each of

¹⁶⁵ David J. Singer, Stuart Bremer, and John Stuckey, "Capability Distribution, Uncertainty, and Major Power War, 1820-1965," in *Peace, War, and Numbers*, ed. Bruce Russett (Beverly Hills: Sage, 1972).

¹⁶⁶ Singer, "Reconstructing the Correlates of War Dataset on Material Capabilities of States, 1816-1985."

the variables is coded using available open source data and placed on a scale of 1 to 10. Variables adapted from the EIU are divided by 10 to give a number between 1 to 10. The variables are then measured relative to other countries to provide a rank ordering of nations in cyber space. The higher a score, the more capabilities a state has within that aspect of the indexed variable relative to other states.

The components of the indexed variable are as follows: approximate size of information (cyber) warfare units, legal and regulatory framework, economic and social context, technological infrastructure, industrial application, national military budget, and demonstrated cyber capabilities. Lastly these components are scaled against national digital vulnerability. Each of these variables in some way influences the cyber power of a state.

The first theoretical variable, information (cyber) warfare unit size, is a conventional measure of military strength within any domain. It is important to define the size of cyber units. In much the same way that conventional theorists define the size of standing armies as a measure of power, cyber warfare units represent the number of individuals a state can task on a particular problem.¹⁶⁷ This is important for both offensive and defensive operations. Larger units are capable of writing more code and monitoring more systems at the same time than smaller units. Despite the possibility of diminishing returns to scale, diminishing returns are system dependent and therefore not able to be adequately accounted for across nations, time, and space. It is therefore assumed that the more individuals a state places in its cyber units the more powerful it will be within the cyber domain. This variable is included because it is hypothesized, that cyber power is significantly influenced by cyber unit size. This data is obtained through open source

¹⁶⁷ See the inclusion of military personnel in Singer, Bremer, and Stuckey, "Capability Distribution, Uncertainty, and Major Power War, 1820-1965."; Singer, "Reconstructing the Correlates of War Dataset on Material Capabilities of States, 1816-1985."

reports and is not an exact measure of unit size rather an estimation of size relative to the state system. As such a 10 score for cyber unit size would indicate that a nation has very large dedicated cyber units, whereas a 1 would indicate very small and a 0 would indicate no cyber units.

Although it is possible to agree that similar to conventional warfare, in cyber it also matters how many “boots” are on the ground. Coding, like any great building project requires manpower. It is hypothesized that as manpower devoted to cyber units increases this increases the cyber power of a state. The manpower argument works up to the point of diminishing returns. Each type of project within the cyber domain has a different point of diminishing returns, so for simplification it is assumed at present an unlimited movement towards efficiency in much the same way conventional theorists assumed that large numbers would win the day on the traditional battlefield.

Boots in raw terms of cyber unit size is not sufficient to account for the quality of those boots. It is therefore necessary to divine a measure adequate to measure not only the military offensive and defensive unit size of states within the cyber domain, but to also determine what their possible quality is as well. To determine the quality of the potential cyber warfare units this work uses the indexed economic and social context variable developed by the EIU. This variable accounts for a range of qualities including educational levels, technical skills, trade, and innovation environment.¹⁶⁸ Higher scores in this variable would indicate a more powerful nation within the cyber domain.

¹⁶⁸ Lewis and Timlin, "Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization."

The increase in power is hypothesized as an effect of this variable because the more educated, the more technical and the more innovative individuals are within a state the more capable they are likely to be in writing code, developing new hardware and software platforms. Although holding a gun and pulling a trigger are skills that can be reasonably adapted to most soldiers, the writing of code, and the maintenance of information communications infrastructure require years of training. The power of a state and its ability to be successful are heavily dependent on a wide variety of characteristics within this economic and social context. These aspects of cyber power indexed into a single variable represent a human and market capital environment that facilitates offensive and defensive cyber action. A full breakdown of the components of the economic and social variable as well as all EIU variables can be found in Appendix B.¹⁶⁹

The economic and social context of cyber interacts with the next two variables, technological infrastructure and industrial application. The EIU indexes these two variables, each of which is comprised of multiple aspects.¹⁷⁰ Infrastructure and industrial application are expressions of the robustness of a country's cyber domain. Contained within this variable as defined by the EIU are measures of ICT networks, ICT access, ICT spending as a percentage of GDP, the use of smart grids, digital health, e-commerce, intelligent transportation, and e-government. These measures are reflections of what a nation is doing with the technology it has. Nations at the forefront of technology infrastructure are often less vulnerable to conventional exploits, they lead the world innovation and application of that innovation. It is hypothesized that as infrastructure increases in size and robustness it paradoxically becomes increasingly stable as

¹⁶⁹ "Cyber Power Index."

¹⁷⁰ See Appendix B

redundancies make up for potential weaknesses. More than simply increasing the capabilities of states, these measures pull in tangible qualities that affect the relative cyber power of states.

The technological infrastructure and industrial application ICT of a nation represent the hardcore present environment in which the economic and social context flourishes. The two feed off of one another and influence each other. As the economic and social context and the technological infrastructure of a state is developed so to are the industrial applications of these two variables. As infrastructure improves it becomes possible to conduct increasingly complicated industrial activities within the cyber domain. Although these three variables are measured independent of one another, each are input into the larger indexed variable for cyber power, because individually they represent important and unique attributes of state cyber power.

Military units, human resources in an economic and social context, the infrastructure and industrial application of ICT are only useful in the context of their legal and regulatory frameworks. As with conventional conflict, it is important to understand how both sides view potential actions and in what ways they will respond. Legal and regulatory frameworks, as defined by the Economist Intelligence Unit are composed of: government commitment to cyber development through a national cyber plan and public/private partnerships, a cyber protection policy composed of cyber enforcement authority, cyber security laws, cyber crime response, international cyber security commitments, and a cyber security plan, cyber censorship, political efficacy, and intellectual property protection.¹⁷¹ These legal and regulatory variables all combine to contextualize the organizational and operational aspects of a state's capability within a domain.

¹⁷¹ Lewis and Timlin, "Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization."; "Cyber Power Index." – See Appendix B for a more detailed explanation of this variable.

A state with a poor legal and regulatory framework in place as indicated by inadequate or poorly defined laws, policies, strategies, and plans will be at a disadvantage over more prepared rivals. Nowhere has this been illustrated better than during the working simulation conducted by the Bipartisan Policy Center's experimental war game, *Cyber ShockWave*, conducted in 2010.¹⁷² This exercise demonstrated the resultant chaos of a government with few legal and policy frameworks in place for responding to a large-scale attack against the homeland emanating from cyber. Of particular importance during this simulation was the amount of time spent attempting to determine who had the legal authority to respond, and what that legal authority constituted. It is therefore hypothesized that as the legal and regulatory frameworks of a state increase this has a positive significant affect on a state's cyber power.

This variable is an index variable of legal and regulatory frameworks within nations and is derived from the EIU dataset.¹⁷³ The more detailed a framework, the more likely it is a state will not experience the same problems experienced during the *Cyber ShockWave* war game. States with more highly defined legal and regulatory structures are better able to assign responsibility to various government and private sector actors to facilitate offensive and defensive actions within cyber. Included within this variable are public private partnerships. States with low levels of industry, and or academic collaborations are less likely to have robust dynamic defensive and offensive capacity. The Dartmouth report on cyber capabilities of states explicitly that collaborations of states with academic and private entities as an important aspect of cyber power.¹⁷⁴ Understanding who is responsible for what in the cyber domain, and defining what constitutes attacks, or hostile actions is vital to establishing power within the domain.

¹⁷² "Cyber ShockWave - Simulation Report and Findings," (Washington, D.C.: Bipartisan Policy Center, 2010).

¹⁷³ "Cyber Power Index."

¹⁷⁴ Billo and Chang, "Cyber Warfare: An Analysis of the Means and Motivations of Selected Nations."

Lastly, an overall measure of relative potential military capability is included. This measure is included here as the relative country-to-world military budget. This inclusion is hypothesized to increase the power of a state within the cyber domain as it does in conventional forms of conflict. The larger a state's relative military budget, the more funds it is able to allocate to offensive and defensive cyber operations relative to potential opponents. In many ways this variable distorts overall power score of states. However, because a state has a larger military budget it can conceivably allocate these financial resources towards cyber related endeavors. Although the relationship between the aggregate military budget of a state and its allocation of funds towards cyber is not direct, the case could be made that the ability to redistribute funds, should the need arise, exists within the military apparatus.

The above measures are each rooted in tangible numbers, yet their effect on the ability of a state to influence or impose its will on other states is less certain. Years of evidence and a host of academic studies indicate a significant correlation between material capabilities available for a conventional war and the increased the power of a state, but the same is not necessarily true in the cyber context. Therefore these human, material, legal, economic, infrastructure, industrial, and budgetary variables are best regarded as theoretical aspects of cyber power. Based on theory each of these variables proportionately affects the resultant theoretical scope of power of states in a different way. Based on previous studies and on available data this work assumes the variables each affect the resultant power of a state differently. The proportion of their affect is represented in table

Each of the above variables combines to form the theoretical aspects of cyber power of a state. In much the same way it is possible to look at the statistics of baseball players and determine what the ideal team would be based on a collection of numbers and information. The

variables in the above sections all combine to create the theoretical quality of a nation state within the cyber domain. This is not sufficient for adequately defining power relationships. Two additional features must be added that extend the construction of power beyond a purely theoretical conceptualization. These variables are demonstrated capabilities and national digital vulnerabilities.

The historical context of cyber within a state adds to the construction of an accurate power score by illustrating what a state is actually capable of. Although a state might have large budgets, training programs, collaborations with universities and industries, each of these attributes of the indexed variable remains largely theoretical until that state demonstrates a threshold level of capabilities in the real world. Just because a student buys, and reads books on medicine does not make him a medical doctor. To become a doctor a student must train with patients and demonstrate his abilities. In this context it is important to understand whether a state has conducted or defended against a cyber attack, and what the scale and complexity of the attack was.

This type of historical variable is imperfect, but it provides a comparative way of understanding a state's demonstrated cyber capabilities. By adding in actual demonstrated capabilities of states the indexed variable adds in actual technical capabilities rather than assumed. For example, the Russian Federation's cyber attacks against Georgia in 2008 would be illustrative of an operational and organizational complexity unique in many respects in the cyber domain. Likewise the Israeli cyber attacks against Syrian air defense systems also illustrate a level of capabilities that differentiates it from other state actors. In this instance it is possible to use history of actual capabilities to inform a model largely predicated on theoretical capabilities. This variable is separated from the others and constitutes its own multiplicative aspect of the

indexed variable. Fortunately there are no states that haven't, to some extent, been tested in the cyber domain. A historical realistic perspective of cyber capabilities is referred to here as demonstrated threat spectrum capabilities. It is separate from the other variables specifically because it is not theoretical in nature. The historical or demonstrated capabilities measure is derived from contextual analysis of cases written up by the United Nations Institute for Disarmament Research, Security and Defense Agenda report on cyber security, the Center for Strategic and International Studies and the Dartmouth Report on Cyber Warfare, and Robert Carr's book on cyber warfare.¹⁷⁵

The data was coded on a scale of capability and complexity ranging from 1 to 8. The scale ranges from cyber propaganda to compromising of hardware systems. The scores were then standardized against one another to fall on a scale of 1 to 10, where 10 represents extensive threat spectrum capabilities and 1 represents minimal capabilities. This score then interacts with the theoretical dimensions of power to provide a numerator of cyber power without taking into consideration national digital vulnerabilities.

The above variables form the top portion of the equation in the indexed variable illustrated in equation 4.3. Each represents a fundamental aspect of cyber power without specifically focusing on what types of systems and computers a particular country uses in its networks and infrastructure. To delve down into infrastructure composition would be extremely difficult and illustrate only moments in time rather than examining the true power of a state within the domain. Although each of these variables creates a model similar to the one illustrated

¹⁷⁵ Lewis and Timlin, "Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization."; Brigid Grauman, "Cyber-security: The vexed question of global rules," (Security and Defense Agenda, 2012); James Andrew Lewis, "Significant Cyber Incidents Since 2006," (Washington: Center for Strategic and International Studies, 2011); Billo and Chang, "Cyber Warfare: An Analysis of the Means and Motivations of Selected Nations."; Jeffrey Carr, *Cyber Warfare* (Sebastopol: O'Reilly Media, Inc., 2010).

in 4.2 it is impossible to conceptualize the cyber domain without adding one more unique attribute that scales power to accurately reflect the real world. Equation 4.3 is a representation for how the indexed variable and its components should be conceptualized within the cyber domain.

Below in table 4.1 are the variable names with their corresponding variable codes. The first six variables all proportionately influence cyber power differently. For instance, although it is important to have military units assigned to conduct cyber operations, those units are ineffective without the legal and regulatory framework to organize and control them, and the economic and social context providing trained personnel. The theoretical aspects of cyber power are combined to result in a meaningful measure of theoretical cyber power. This measure is then multiplied by the demonstrated capabilities of a state within cyber offense or defense. In this way, we are able to gain a holistic picture of what constitutes cyber power. A complete break down of the proportional values for each of the variables is included in Appendices A through C.

Table 4.1 Components of Power

Variable Name	Proportional Influence	Variable Code
Military Unit Designation	15%	MUD
Legal and Regulatory Frameworks	25%	LRF
Economic and Social Context	25%	ESC
Technological Infrastructure	15%	TI
Industrial Application	10%	IA
Military Budget Allocation	10%	MBA
Threat Spectrum Capabilities		TSC
National Digital Vulnerability		NDV

Indexing Equation for Cyber Power

$$4.3 \quad \text{Cyber Power} = \frac{(MUD + LRF + ESC + TI + IA + MBA) \times TSC}{NDV}$$

Equation 4.3 represents the construction of cyber power. The present section focused solely on developing the top portion of the equation. The next section will focus solely on the concept of national digital vulnerabilities as a way to realistically scale power to reflect the actual operating environment.

Cyber and its vulnerabilities

Cyberspace is a porous domain. Whereas in land warfare it is theoretically possible to lay out a line of tanks to form an impenetrable wall, in cyberspace, even the strongest firewall has weaknesses. Cyberspace is dominated by billions of systems, millions of security devices and petaflops of data. Although certain countries are likely to have specific vulnerabilities within their cyber infrastructures, no two countries are likely to be the same. Such a situation would lead to a multitude of models all with different measures for vulnerabilities. Chapter 7 illustrates that it is possible when focusing on a single target to use intelligence to more accurately hone the vulnerability measure. However, when creating a model attempting to explain cyber power across all actors it is not possible to delve down into the details.

Cyber vulnerabilities can range from poorly configured systems, old software and hardware, bugs, open ports, and many more, to insider threats posed by employees. The variations in vulnerabilities are as numerous as the number of systems. A case from 2000 illustrates the seriousness of even low-level vulnerabilities.

Vitek Boden worked for Hunter Watertech, an Australian firm responsible for installing the control systems for a county sewage facility in Australia. Upon completion of the contract

Boden applied to work for the same county. When his application for employment was denied he decided to take revenge by driving around to all the various control mechanisms he had helped to install and via radio link he caused them to release raw sewage into public parks and waterways. The result was an environmental disaster.¹⁷⁶ The case illustrates that vulnerabilities can arise just about anywhere. There was no system in place to protect against a disgruntled former employee and the result was a cyber attack.

Cases such as Vitek Boden's in Australia are not unique and occur on a regular basis according to the Secret Service.¹⁷⁷ But this is only one category of vulnerability. Most scholars agree vulnerabilities to the cyber environment are present in almost unlimited forms. One report that highlights the problem is a Government Accounting office report from 2008 specifically focused on vulnerabilities present within the national critical infrastructure.¹⁷⁸

With a near infinite variation in the number of vulnerabilities how can we operationalize the concept of vulnerability into a measure applicable for conditioning cyber power and why is this necessary? Vulnerability is vital to understanding power. In 1990 Saddam Hussein had an enormous military with nearly half a million active duty military personnel. If we rely on numbers alone the first Gulf war should not have been a won as quickly as it was. The relative power based on aggregate numbers was not such that it should have facilitated a speedy American victory. However, the Iraqi military had strategic vulnerabilities and command and control vulnerabilities that when exploited, made it difficult for Iraqi commanders to

¹⁷⁶ Marshall Abrams and Joe Weiss, "Malicious Control System Cyber Security Attack Case Study—Maroochy Water Services, Australia," (2008).

¹⁷⁷ Michelle Keeney et al., "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors," (Washington, D.C.: United States Secret Service and Carnegie Mellon Software Engineering Institute, 2005).

¹⁷⁸ "Defense Critical Infrastructure: GAO-08-373R," *GAO Reports* (2008).

communicate with deployed divisions. This indicates that power is not a pure numbers game even in conventional conflict. In the cyber world it is even less so.

A nation such as North Korea can develop an offensive cyber unit and ignore the need for a defensive cyber unit because it has almost no reliance on cyber technologies in its homeland. Its economy is not cyber dependent, and its electric grids are not connected to smart grids. The exploitation of North Korean cyber vulnerabilities would have little to no effect. The same was not true of the attacks against Estonia in 2007. The nation of Estonia, sometimes referred to as “E-Stonia,” was highly digitally connected. When Russian activists used DDOS attacks to assault its media, banks, and government systems connected to cyber it brought the country to a temporary standstill.¹⁷⁹

What these two examples illustrate is that while a state might have a large cyber offensive capability, it might have no defensive needs at all. And while a state might have little to no offensive capabilities, it might have a great defensive need. This poses the question of how

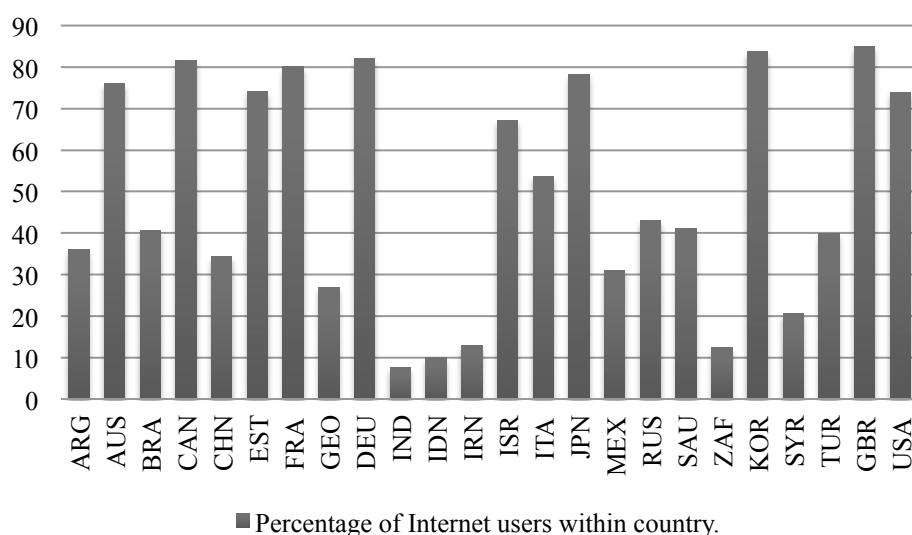


Figure 4.1: Percentage of individuals using the Internet within countries in the sample

¹⁷⁹ M. Landler and J. Markoff, "Digital Fears Emerge After Data Seige in Estonia," *New York Times* 2007.

to measure this complex relationship between those aspects, which enhance the power of a state in the cyber domain and those, which increase its vulnerability?

Because it is difficult to isolate specific vulnerabilities of a state and because national security within cyber blurs the civilian/military boundary this model incorporates an aggregate measure of national digital dependence. The logic behind this measure is simple. The more digitally dependent a society is, the more vulnerabilities it is likely to have. To measure national digital dependence this work uses the International Telecom Union's (ITU) data on percentage of individuals within a country using the Internet. Figure 4.1 is a graphical representation of the ITU data.¹⁸⁰ The darker the country, the higher the percentage of Internet use and therefore the greater the systemic vulnerability of the nation to threats emanating from cyberspace.

This data are collected by the ITU from national statistical offices and combines to provide the best overall collection of meaningful information on potential cyber vulnerabilities. This variable is measured in the same way as the other variables on scale of 1 to 10 according to percentage of individuals within a country using the Internet. This variable is best thought of as expressing the higher likelihood of vulnerabilities within a nation. It is an imperfect variable as it is unable to account for problems associated with the speed of connection or the frequency of use. It also fails to account for system construction and age or vulnerability of systems. Despite these failings, this is at present the most robust variable on the aggregate vulnerability of a nation within cyberspace.

¹⁸⁰ "World Telecommunication/ICT Indicators Database Online," ed. International Telecommunications Union (Switzerland 2011).

Conceptualizing cyber power

The present chapter examined the concept of power and built an argument for a measure of power unique to the cyber domain. This measure incorporates theoretical and actual aspects of capability and capacity. It then takes a step further and indicates that power in the cyber domain is heavily conditioned on the vulnerabilities of a state. Whereas in conventional conflict vulnerabilities are primarily measured in the capability and capacity of a state to wage war, in cyber if a state has few vulnerabilities it also has few targets an adversary can attack or retaliate against.

Equation 4.4 is a representation of cyber power in the simplest possible terms and can be expressed in words with aggregated variables as the theoretical cyber force (F) by its demonstrated threat spectrum capabilities (T) over its national digital dependence vulnerabilities (D) represents the absolute power of any one state within the cyber domain. Such a measure can be developed in excruciating detail through the use of intelligence as will be examined in chapter 7, or it can be examined through more broad brush strokes as done here.

Equation for Cyber Power

$$4.4 \qquad \qquad \qquad \text{Cyber Power} = \frac{F \times T}{D}$$

What is important to take away from this chapter is that cyber power can be operationalized in such a way to convey meaning within the cyber domain. This operationalized measure than can be used in facilitating a decision-making model for action within the cyber domain. As should be apparent, the domain is unique from conventional domains and must take into consideration those attributes that best account for a new and evolving form of power.

Based on the variables and their relationships to one another, table 4.2 provides a ranking of the cyber power of each of the states within this work. The table includes two power scores for each country; however, they are ranked based on the weighted model. The unweighted power score assumes an equal weight of all variables and is considered to be of lower accuracy. While the resultant rank order of the weighted power score seems to counter the notion the of the United States being the most powerful nation in terms of cyber power it is important to remember that power score is only one aspect of the probability for success. The next chapter will add to the concept of the probability of success in the cyber domain and examine anonymity's influence on cyber decision-making. Unlike in conventional conflict a raw estimation of power is only one part of the whole decision to engage in cyber conflict.

Table 4.2 Power Scores by Country

	Country	Power Score	Weighted Power Score
1	Germany	3.17	9.41
2	Japan	2.03	9.36
3	UK	3.81	9.35
4	South Korea	3.01	9.17
5	Canada	3.24	9.02
6	France	3.20	8.89
7	Australia	3.79	8.36
8	Estonia	2.27	8.27
9	USA	10.86	7.44
10	Israel	9.02	7.27
11	Italy	2.80	5.72
12	Turkey	2.13	4.82
13	Brazil	2.93	4.58
14	Russia	5.56	4.57
15	Saudi Arabia	1.72	4.49
16	Argentina	1.33	4.29
17	Mexico	3.41	3.63
18	China	6.47	3.58
19	Georgia	3.20	3.03
20	Syria	0.98	2.39
21	South Africa	6.12	1.57
22	Iran	7.38	1.33

23	Indonesia	4.87	1.33
24	India	23.24	0.81

This chapter has looked beyond the broad definition of cyber power provided by Kramer, Starr, and Wentz and focuses on the push aspects of cyber in the same way Bruce Bueno de Mesquita incorporated CINC scores into his concept of power in his expected utility theory of international conflict.¹⁸¹ Cyber power is the ability of a state to create, manipulate, modify, degrade, or deny the use of information communication technologies to a target(s), while simultaneously minimizing any and all potential threats against itself. Creating, manipulating, modifying, degrading, or denying the use of ICT allows a state to impose its will on another. A state with high offensive capabilities and low defensive vulnerabilities within the cyber domain will be considered powerful. Power in this context indicates a powerful state will have an increased ability to exert its will within the domain. A state with greater cyber power will have a relative advantage within the cyber domain over states with lower levels of cyber power. This will be an increasingly important concept as we move forward in developing a rational model for how a state decides when to attack within the cyber domain.

¹⁸¹ Bueno De Mesquita, *The war trap*.

CHAPTER 5

Anonymity and Attribution in Cyberspace

“There is a powerful tension in our relationship to technology. We are excited by egalitarianism and anonymity, but we constantly fight for our identity.” ~ David Owens¹⁸²

“We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us.” ~ Anonymous¹⁸³

Anonymity and by extension attribution are two fundamental aspects of the cyber domain. When a state decides to attack another state it is not only concerned solely with its relative power to its adversary. Instead a state is concerned with the power of its adversary and its ability to conduct an attack against an adversary while maintaining anonymity. Webster’s defines anonymity as:

- 1: of unknown authorship or origin
- 2: not named or identified
- 3: lacking individuality, distinction, or recognizability¹⁸⁴

This chapter focuses on the origin or instigating actor, the target that is not identified, and the recognition that an attack is occurring. Specifically the concept of anonymity is approached from the offensive perspective of a state considering instigating a cyber attack against a potential opponent.

To understand anonymity it is necessary to ask basic questions of international politics. First, why is anonymity important to a cyber attacker? Second, is it possible to conduct a

¹⁸² "Anonymous 'takes down' CIA website," *Aljazeera*(2012).

¹⁸³ We Are Anonymous, We Are Legion to, 2009, <http://www.yalelawtech.org/anonymity-online-identity/we-are-anonymous-we-are-legion/>.

¹⁸⁴ "Anonymous," in *Merriam-Webster* (2012)., <http://www.merriam-webster.com/dictionary/anonymous>

political act and remain anonymous? Third, why is attribution important to a cyber defender? This chapter answers these three questions in order and closes with a summary of the importance of understanding anonymity and attribution in cyber decision-making.

The importance of anonymity

Most of the literature on cyber attacks makes clear that one of the most valuable aspects of the cyber domain is anonymity. Anonymity is a distinctive asset in covert operations, providing political plausible deniability while allowing for the attainment of a strategic or tactical objective. It is difficult to assess the true value of anonymity in cyber. From an offensive perspective the objective is to remain anonymous as long as possible while still achieving an objective. This is likely to lead an attacker to obfuscate their operation. As was described in earlier chapters if a target of a potential attack emanating from cyberspace knows where an attack will occur, or who will perpetrate an attack, it is much more likely to be able to defend against that attack.

Anonymity in cyber is multifaceted. The layers of anonymity are constructed by the following characteristics: inability to identify a perpetrator (state instigator) of an attack, the inability to recognize an attack is occurring, and the inability to isolate the target or objective of an attack. These characteristics build upon the two characteristics of attribution within Susan Brenner's legal framework for understanding cyber attacks.¹⁸⁵ These three characteristics are important for both legal and practical reasons. As National Strategy to Secure Cyberspace accurately notes: "The speed and anonymity of cyber attacks makes distinguishing among the actions of terrorists, criminals, and nation states difficult..."¹⁸⁶ Beyond simply being unable to

¹⁸⁵ Susan W. Brenner, "'At Light Speed': Attribution and Response to Cybercrime/Terrorism/Warfare," *The Journal of Criminal Law and Criminology* 97, no. 2 (2007).

¹⁸⁶ *The national strategy to secure cyberspace*.

identify the perpetrator, as is often the case in cyber attacks, it is difficult to recognize when a cyber attack is even occurring.

Titan Rain, a cyber espionage operation targeting various defense systems, including U.S. logistics, is an example of a cyber attack that stayed beneath the radar.¹⁸⁷ A defender that does not know an attack is occurring is even less likely to know what the target of that attack is. Several of the more severe attacks against U.S. interests even when discovered have provided little to know information on what the target of the attack was. This is because the data that was stolen was encrypted on the way out, making it virtually impossible to know what the purpose of the attack was. The only way to judge the significance of the attack was the measure the volume of the data taken in terabytes.

Anonymity within cyberspace is a valuable tool to both the perpetrators of attacks and the average user alike. Over the last several years I have worked with democracy NGOs around the Middle East and other regions building training platforms for democracy activists. These websites are designed to offer potential democracy activists the maximum amount of anonymity to protect them against government persecution. In this instance anonymity is a tool that safeguards liberties. This same ability to remain anonymous facilitates nefarious groups and nation states that wish to do harm.

Although this work is primarily concerned with the decision-making processes of state actors, the quote at the beginning of this chapter by the group “Anonymous” is illustrative of the power a disparate group of non-state actors can have in cyberspace. If states are unable to prevent ad-hoc organizations such as Anonymous from taking down the websites of major

¹⁸⁷ Brenner, *America the vulnerable : inside the new threat matrix of digital espionage, crime, and warfare*: , kindle digital location 1227.

governmental agencies such as the FBI or CIA, then how is it possible to defend against state actors with infinitely more resources?¹⁸⁸

Numerous scholars have indicated that one of the fundamental problems associated with the structure of the Internet is that it was never designed to provide tracking and referencing of users.¹⁸⁹ It is prudent to remember that the Internet as we know it was started as a private collaboration tool between universities and U.S. laboratories. In fact, at its beginning commerce was prohibited on the Internet. As the value and the volume of connections has increased the value of anonymity has been both a blessing and a curse. For a state deciding whether to use cyber as a means of attack against another state, one of its primary considerations should and does often rightly center on anonymity.

The value of anonymity is supported by both anecdotal evidence as well as sound political logic. In every major case of state on state hostile cyber interaction, ranging from Computer Network Exploitation (CNE) to Computer Network Attack (CNA) anonymity has been a central feature. The answer as to why anonymity is a central feature of hostile state interactions within cyber has been discussed in previous chapters, but it does not hurt to reiterate its central premise and applicability to the decision to instigate hostile actions within cyber.

A bullet or bomb launched from a gun or plane has a defined trajectory. It is possible to harden a target against them with either a bulletproof vest, or a bunker. But once that trajectory has been established the target is virtually assured of impact. In much the same way it is possible to harden cyber assets against cyber weapons. Network administrators can build firewalls or air

¹⁸⁸ "Anonymous 'takes down' CIA website".

¹⁸⁹ David A. Wheeler and Gregory N. Larsen, "Techniques for Cyber Attack Attribution," (Institute for Defense Analyses, 2003); Jeffrey Hunker, Bob Hutchinson, and Jonathan Margulies, "Role and Challenges for Sufficient Cyber-Attack Attribution," (Dartmouth College: Institute for Information Infrastructure Protection, 2008).

gap networks to protect them against incoming bits and bytes. But unlike the bulletproof vest that works against any bullet regardless of type, up to a certain caliber, a firewall only protects against identified threats. Furthermore, just as a bulletproof vest offers little protection against a howitzer round, a firewall can be overcome by larger inflows of bits and bytes (a DOS attack). If a larger round is coming towards an individual will attempt to fortify himself in a bunker and survive. The same is true of a cyber attack. If it is known that a large-scale attack is being implemented, network administrators will expand the fortifications and weather the attack. If the network administrators do not know an attack is coming then they are likely to be a casualty. In cyber if it is known an attack is being conducted, a network administrator can also take systems off-line and remove targets all together, making an attack ineffective for want of a target.

If the objective of an attack is to make small changes in the defenses of another state's systems then the goal is to hide those changes for as long as possible. Not only is it prudent to hide the attacker's identity, it is prudent to hide the knowledge of the attack as well. Once an opponent knows it is being attacked its security personnel begin implementing defensive measures as a response. Defenders can increase the robustness of their firewall(s), increase their network capacity, or in worst-case scenarios, remove the systems all together. The same is not true of conventional attacks. Once an attack is ongoing it typically must be weathered, and or responded to.

Any probability for success in cyber is dependent largely on a relationship between the objective of an attack and the ability to remain anonymous to the point at which that objective is completed. Furthermore, even if the anonymity of the attack is lost it can still preserve the anonymity of the attacker. This makes it difficult, if not impossible, for the victim to retaliate

with any meaningful accuracy. The combination of the three characteristics of anonymity combine to significantly condition the decision-making process of actors in cyber.

Many scholars note anonymity is such a strong characteristic of the cyber domain that it makes it possible for certain actors to achieve disproportionate amounts of political utility from acts conducted in cyberspace.¹⁹⁰ The disproportionate amount of power achieved in the cyber domain is actually a misnomer in relative terms. A small state wielding cyber weapons does not have more power than a large state. As was examined in the previous chapter, power in cyber is a relationship between cyber force, threat spectrum capabilities, and national digital dependence. If being small doesn't actually affect the power of the state, yet still affects the utility of the state, what is occurring?

The answer lies in the range of all possible actors. Chapter 7 provides a graphical representation of the scale and complexity of attacks in relation to the feasibility. The relationship of complexity and scale with feasibility indicates an inverse relationship. The more difficult an attack, the more likely it is to be significant in either size, complexity, or both. There are only a few select countries with the technical capabilities to conduct a highly complex attack such as Stuxnet, or the attack on Syrian air defense systems. There are nearly 100 countries and large numbers of sub-state actors capable of conducting the type of attacks used against Estonia in 2007. The disproportionate relationship between the size of a state and anonymity is directly related to the number of potential actors and the ability to remain anonymous. Although the Stuxnet attack has not been claimed officially, the range of possible actors based on factors such as complexity and scale of attack alone is quite small. If the attack is contextualized in foreign policy and international relations, the range narrows to possibly three and more likely two actors.

¹⁹⁰ Cornish et al., "On Cyber Warfare," p8.

Anonymity is a complex measure. The three characteristics of anonymity are extremely difficult to maintain indefinitely. The key is to prolong a combination of the characteristics long enough to achieve an objective in cyber. Furthermore, if the identity of the attacker remains anonymous, it denies the legal justification for retaliation by the targeted state as well as denying the identification of a proper institutional format for recourse.¹⁹¹

Political action and anonymity

Is it possible to conduct a political act and remain anonymous? If we follow the logic of Thomas Rid that “history does not know acts of war without eventual attribution,” then do cyber attacks constitute political acts?¹⁹² With anonymity being a central feature that influences the success of cyber attacks, does anonymity remove the political aspect of attacks? Rid goes on to say: “...aggressors engaging in subversion, espionage or sabotage do act politically; but in sharp contrast to warfare, they are likely to have a permanent or at least temporary interest in avoiding attribution. This is one of the main reasons why political crime, more than acts of war, has thrived in the cyber domain, where non-attribution may be easier to achieve than waterproof attribution.”¹⁹³

This work largely steps over the linguistic gap between what constitutes an act of war and what constitutes a crime or other form of action. For the purposes of understanding anonymity the definition is largely based on the perception of the aggrieved party. However, Rid does make it clear, through his linguistic maneuvering, that certain acts within cyber can contain political utility. Virtually all other scholars agree on this point.¹⁹⁴ While the linguistic distinction between

¹⁹¹ Brenner, ““At Light Speed”: Attribution and Response to Cybercrime/Terrorism/Warfare,” p381.

¹⁹² Thomas Rid, “Cyber War Will Not Take Place,” *Journal of Strategic Studies* (2011): , p5.

¹⁹³ Ibid., , p11-12.

¹⁹⁴ Kramer, Starr, and Wentz, *Cyberpower and National Security*; Demchak, *Wars of disruption and resilience : cybered conflict, power, and national security*.

war and political crime has caused a degree of animosity within the subfield, this animosity is likely misplaced, and represents different linguistic traditions and conceptualizations of the state of modern conflict in regards to historical frameworks.¹⁹⁵

The focus on the debate over whether anonymous acts that take place constitute different types of conflict is dependent on the framework of definitions a scholar uses. What is evident is that regardless of how cyber attacks are referred to in the conventional typology, they are capable of generating utility as was demonstrated in chapter three.

The value of anonymity

Acts that occur in cyberspace are not necessarily anonymous, yet anonymity is a desired characteristic for the conduct of offensive cyber actions. How then can we operationalize the concept of anonymity within a rational choice decision-making model so it is logical to the decision maker?

Bueno de Mesquita's utility theory simply compares the power scores of different states. By using this capability (power) relationship between states he is able to determine the probability of success for the instigator of a potential conflict. It is this probability of success that greatly affects the decision to engage in an act. In theory it would be possible to use Bueno de Mesquita's model to explain any type of decision to engage in interstate interactions ranging from diplomacy to war. It would be possible to rearrange the probability function of the model to incorporate those characteristics that influence successful diplomatic interactions to derive a model for bargaining. However, Bueno de Mesquita's model is focused on overt conflict. He uses power to assess the probability of success. Yet because he works in a domain of interaction

¹⁹⁵ See debate in John Arquilla, "Cyberwar Is Already Upon Us," *Foreign Policy*, no. March/April (2012). and Thomas Rid, "Think Again: Cyberwar," *Foreign Policy*, no. March/April (2012).

where distance has an effect, his power relationship is scaled by distance.¹⁹⁶ Distance as was examined in previous chapters does not matter in cyber as attacks can occur with no diminishing capability due to distance. A virus code in China does not need to be resupplied by a virus code in the United States. What does affect the probability of success is time. However, the probability of success affected by time does not interact with the power of a state, as is often the case in conventional conflict. Instead it influences the overall probability of success.

There are several ways to represent the relationship to time in mathematical models and probability. One of the more standard statistical methods available to test time to an event is by using a hazard or survivability model. This model is not testing the changes in the power relationship over time, rather it is examining the probability any given type of attack can remain anonymous within the three above combined characteristics long enough to achieve the objective of the attack. More simply how long until the target knows it is being attacked, knows the target of the attack, and knows who is doing the attacking.

This is important to the development of a decision-making model for the instigation of cyber attacks as has been mentioned several times. Once a victim recognizes an attack it can begin taking defensive measures to protect itself. Once it knows the target of the attack it can harden that target. Once it knows the perpetrator of the attack it can begin retaliation. The question the decision maker then asks is what is the probability at a point in from time t to time t_c or from instigation to completion of the attack that the instigator is able to maintain anonymity. This probability changes over time. At time t , the initiation of the attack, the likelihood that anonymity is lost is relatively low. The longer the attack takes to complete the more likely the attacker is to lose anonymity. This then becomes a fluid measure expressed in

¹⁹⁶ Bueno De Mesquita, *The war trap*.

moments in time that can be graphed. Because each type of attack is unique, no two hazard models are the same.

The hazard model is composed of those factors essential to maintaining anonymity discussed above in this chapter. It is important to know the scale (S) of an attack. The larger the attack, the more difficult it is to accomplish. Next it is important to understand the complexity (C) of the attack. The more complex an attack, the more difficult it is to accomplish. These two variables interact as well. A large and complex attack is more difficult than a small complex attack or a large simple one. Next, as was mentioned above, it is important to contextualize the attack by determining the level of hostility (H) between nations. If State X has only two primary adversaries, it can quickly isolate the instigator of an attack against its interests. By understanding the level of hostility, it is possible to begin narrowing the number of countries in the system. The more potential actors (Q) within a grouping the more likely a perpetrator is to remain anonymous. The expression of the hazard function is listed below in equation 5.1.

Hazard Function for Anonymity

$$5.1 \quad A = \log h_1(t) = \alpha + C_i\beta + S_i\beta + (C_iS_i)\beta + H_i\beta + Q_i\beta + e$$

Using this function with complete data it is possible to isolate at any given point in time from the initiation of an attack to the completion of an attack the probability of maintaining anonymity across the three characteristics of anonymity. As will be examined in chapter 7, this model can be greatly influenced by the collection of intelligence. Such intelligence would influence all variables within the above hazard function.

Because there is an assumption of anonymity necessary to instigate any attack due to the characteristics of cyber attacks as defined above, the model is not filled in in this work by data. Instead the probability of maintaining anonymity at the point of initial decision to instigate an

attack will be kept constant at 1. The probability of maintaining anonymity changes over time. Therefore anonymity at time t_0 is always kept at 1. The probability of anonymity at $t_{0 \rightarrow n}$ is here defined on the type of attack, rather than using the hazard function for which data is not available. Attacks are broken into eight categories each with a probability of maintaining anonymity over time. The categories and their corresponding probabilities are listed below in table 5.1. These probabilities are anecdotal and assumed. Actual probabilities for each attack would depend on the intricacies of the attack, the hostility between nations and all of the other features included in the hazard function for anonymity.

Table 5.1 Probability of Maintaining Anonymity by Attack

Propaganda	99%
Web-Vandalism	95%
Denial of Service	90%
Distributed Denial of Service	85%
Computer Network Exploitation	80%
Equipment Disruption	70%
Critical Infrastructure	60%
Compromised Hardware Systems	50%

The above indicates that the more complicated the attack the more difficult it is to maintain anonymity. Although the numbers are rough, they are meant to illustrate the intersection of all three categories of anonymity. Many groups and organizations can participate in web propaganda and it is therefore a low level and common form of attack. Only a few states are currently capable of fully compromising hardware systems it is therefore more difficult to maintain anonymity during such an attack.

Anonymity, attribution, and decisions

Although many works focus on the term attribution, here the focus is on anonymity. This has been done this for several reasons. First, an anonymous actor is one who avoids attribution. Many legal scholars, including Susan Brenner, tend to focus only on the attribution aspect of cyber. They do this primarily because they are concerned with the defensive capabilities of states. The ability for states to respond to cyber attacks and their perpetrators is an important aspect of cyber defense. But when we consider the offensive strategy of a state the concern is a combination of achieving the objective and avoiding attribution. For an attack to gain political utility a state must achieve its stated objective. If a state cannot achieve even the minimum threshold of its objective, and attack remains unattributed it did not gain any political utility. Anonymity is a fundamental aspect of cyber offense. Attribution is a fundamental aspect of cyber defense. As this work is focused on developing a model that examines how states decide to attack, here attribution is largely ignored from a defensive orientation except where it affects the probability of success.

Wheeler and Larson define attribution as: “determining the identity or location of an attacker or an attacker’s intermediary.”¹⁹⁷ Once a targeted country begins the attribution process it is often after an attack has been completed. It is doubtful that the Israelis cared that the Syrian’s knew they invaded their airspace to bomb the nuclear facilities. They had already gained the benefit they sought. The Syrians did not respond militarily, because they had already lost that which they sought to protect. In cyber it is more important to identify that an attack is occurring, what the target of that attack is, and how to prevent the achievement of an attacker’s goal, than to in the moment identify who is actually conducting the attack.

¹⁹⁷ Wheeler and Larsen, "Techniques for Cyber Attack Attribution."

Deterrence does not work the same in cyber as in conventional conflict. Simply identifying the attacker and threatening response is typically not possible. And even when it is possible it is only feasible with a cross-domain response. Such a response would likely escalate a conflict significantly with unforeseen consequences.

The response mechanism to a cyber attack is theoretically confined in the short term to cross-domain actions due to an inability to quickly and efficiently plan meaningful on the fly attacks against an adversary. Cyber attacks are tailored to specific systems and require extensive planning and development to be successful. Unless the groundwork was laid out in advance, making it possible to conduct retaliatory in-domain attacks a state's primary function is to remove the first two characteristics of anonymity by determining that an attack is occurring, and second, what the target of that attack is.

Joel Brenner created a hypothetical scenario in which attribution is attained, but matters far less than the recognition that an attack was occurring and a comprehension of the target of that attack.¹⁹⁸ The scenario is one in which a previously laid groundwork for a coordinated attack against U.S. critical infrastructure begins to take down vital U.S. systems coinciding with a foreign policy flap occurring with China. The decision makers are paralyzed because at first it is not known whether the critical infrastructure malfunctions are due to an attack or normal error. As the malfunctions continue to occur it becomes apparent the malfunctions are due to an attack and not an error. Although the likely attributable source is China, that is of little importance. The anonymity of the attack and the targets of the attack are more important than pointing fingers. The ability to hide an attack and the target of an attack facilitates it. In Brenner's case by the time it was recognized as an attack it was too late to do anything let alone isolate future targets, and

¹⁹⁸ Brenner, *America the vulnerable : inside the new threat matrix of digital espionage, crime, and warfare* : , Kindle digital location 2186.

the U.S. didn't have assets in place to retaliate in kind. Brenner notes that a cross-domain response would have been a prelude to all out war with unforeseen consequences between two nuclear-armed states. The systems affected were such that even the kill switch mechanism once proposed in Congress would not have been of much use.¹⁹⁹

Moreover to publicly attribute the system failures within the United States critical infrastructure without having a means to stop them also has many negative side effects. Such an attack could compel the defensive party to work in tandem with the attack initiator to maintain their anonymity. Should information on an attack become known, it could severely degrade public confidence in critical infrastructure and cause widespread panic. Furthermore without being able to identify the various targets of the attack the defender risks inciting even more damage against its systems. In this particular case Brenner indicates that the Chinese were using a cyber attack to prevent an armed military response while they asserted control over vast swathes of sea. In this instance it is equally important to know that an attack is occurring, and what the targets of that attack are, as it is to attribute the attack to a particular actor. But because the systems of systems we depend on every day for every aspect national security and stability are subject to their own problems it can be difficult to identify when hostile activity is occurring.

Summarizing the debate

Kenneth Geers accurately sums up the need for attribution when he writes: "The challenge of cyber attack attribution means that decision-makers will likely not have enough information on an adversary's cyber capabilities, intentions, and operations to respond in a timely fashion."²⁰⁰ Attribution is a defensive necessity. Anonymity is an offensive necessity.

¹⁹⁹ See proposed bill by Joseph Lieberman, "S. 3480 (111th): Protecting Cyberspace as a National Asset Act of 2010," ed. United States Senate (Washington, D.C.2010). - Killed in committee

²⁰⁰ Kenneth Geers, "The challenge of cyber attack deterrence," *Computer Law & Security Review* 26, no. 3 (2010).

The probability of maintaining the anonymity of an attack and a target is equally important to maintaining the anonymity of the actor involved. This chapter has attempted to focus on the offensive dynamic of the anonymity-attribution debate and outline a methodological solution for assessing the probability for maintaining anonymity at specific points in time during an attack. The probability for maintaining anonymity influences the probability of success in a cyber attack as much as the relative cyber power of the state engaging in the cyber attack. Adding a measure of anonymity into the decision-making model adds to the robustness of its findings and facilitates a more accurate understanding of when a state will decide to engage in offensive cyber actions.

CHAPTER 6

Cyber and Conventional: The Dynamics of Conflict

The decision to engage in conventional conflict has for centuries remained largely unchanged. For millennia there have been no alternatives to conventional kinetic action. The creation of a virtual domain of interaction has offered an alternative threat spectrum with real world applicability both within the virtual domain and beyond it. This chapter examines the decision to engage in cyber attacks as either standalone attacks or in combination with conventional attacks. It does so by examining cyber in the context of the strengths and weaknesses highlighted in previous chapters. To achieve utility, a cyber attack can be a standalone event or can occur in conjunction with conventional military attacks and act as a force multiplier. Cyber, similar to Duhet's proposed uses for air power during World War I illustrates that new technologies can offer new vectors of attack, but do not necessarily achieve, by their ends alone, the objectives of those attacks sufficient to generate political utility.

This chapter is broken into several sections. The first section examines what is meant by conflict and why when examining decisions it is important to accurately frame the context of the decision on a scale of conflict. The second section focuses on the combination of cyber and conventional tactics. The second section hones in on how a decision-making model can be constructed across two different types of capabilities measures both influencing one another. The third section returns to stand alone cyber attacks and examines their place within the scale of conflict and highlights the necessity of specified objectives. The chapter concludes with a summary of the main points.

The language of conflict

Previous chapters have avoided the linguistic debate pertaining to conflict this chapter by necessity directly confronts. Although linguistics has been danced around in the opening chapters it is important to differentiate the levels of conflict themselves and the relationship of utility to conflict. Whereas in overt diplomatic bargaining it is possible to achieve political gains and losses, these gains and losses are easily understood along a scale of gain and loss. There is no realistic expectation of complete subservience of one party to another. Or as Fearon illustrates there is a bargaining range in which both sides attempt to negotiate for the best possible deal. The same is not true in war.

In war the traditionally conceptualized objective has been total victory or the forced submission of an enemy to one's will. Clausewitz writes: "If we wish to gain total victory, then the destruction of his armed forces is the most appropriate action and the occupation of his territory only a consequence."²⁰¹ War in the Clausewitzian sense is an all or none endeavor, victory in its totality is the objective. Wars are waged to provide unambiguous victory for a policy position. They are not waged for strategic ambiguity. It is therefore easy to define war as a concept that is far in excess of mere diplomacy. The bargaining range of war is designed to force an absolute position on another country. This conceptualization of war was largely adequate when wars were waged as pitched battles between armies staring each other down on the battlefield. War is imagined as two or more armies each banging into one another until one side

²⁰¹ Clausewitz, Howard, and Paret, *On war*: , p92.

acquiesces. This concept of war is largely a pre-20th Century conceptualization. War is according to Clausewitz:

*“As a total phenomenon its dominant tendencies always make war a paradoxical trinity—composed of primordial violence, hatred, and enmity, which are to be regarded as a blind natural force; of the play of chance and probability within which the creative spirit is free to roam; and of its element of subordination, as an instrument of policy, which makes it subject to reason alone.”*²⁰²

Clausewitz’s definition of victory and war is wholly adequate and in the traditional sense, but as Jan Angstrom and Isabelle Duyvesteyn indicate in their edited volume, war has largely changed.²⁰³ The bargaining range rarely if ever is simply defined. Victories have largely become ambiguous and limited. The involvement of populations into war has not had the same effect as Clausewitz once imagined. And in truth declarations of war themselves have largely fallen by the wayside in favor of more ambiguous terms such as operation and action. As Zelizer notes in the context of American movements towards conflict, there has been a significant shift away from formal declarations of war as the concentration of power has focused on the office of the executive.²⁰⁴ War has become a term unused in explaining most forms of modern conflict between states except in the popular vernacular for conflict. Therefore it is necessary to establish the idea of interstate conflict independent of war and within the constraints of defined objectives.

Conflict can be placed along a scale with war defined in the Clausewitzian sense at its ultimate point. Such a conflict would be unambiguous in its eventual outcome. However, as

²⁰² Ibid., p88.

²⁰³ Jan Angstrom and Isabelle Duyvesteyn, "Understanding victory and defeat in contemporary war," Routledge, <http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=178957>.

²⁰⁴ Julian E. Zelizer, *Arsenal of democracy : the politics of national security-- from World War II to the War on Terrorism* (New York, N.Y.: Basic Books, 2010).

modern history illustrates, most conflicts are highly ambiguous and often have no ultimate objective, but rather a series of objectives that shift over time. This scale can be seen in most modern forms of conflict. The goal of one state is not to permanently dominate another state, but rather to establish an allied state capable of falling in line with its stated policy objectives. The objective of conflict is no longer merely to eliminate the enemy it is rather to coerce them. The Department of Justice notes prior to 2001 at least 125 instances of undeclared conflict by the Office of the President.²⁰⁵ The large number of conflicts that have gone undeclared far exceeds the five formal declarations of war and the thirteen authorizations for military engagements. The sheer volume of conflict indicates a utility involved on some level otherwise such conflicts would be irrational and would not have been repeated with such frequency. If conflict can occur without war, and both the formal declaration of war or engagement in military activities is not necessary for conflict to occur then how is it feasible to reconcile conflict within and across different domains. How can we examine when it is rational and when it is not to engage in conflict?

Bueno de Mesquita and numerous other scholars define war in terms of casualties. The Correlates of War (COW) project fails to define war according to its outcome and rather defines it by its costs.²⁰⁶ Cow largely avoids the term War in its internal definitions and instead ambiguously uses the term "Militarized Interstate Disputes."²⁰⁷ War has become a term determined by break points assigned by scholars in datasets with different datasets defining war at different levels of casualties. This mathematical definition does not equate to the philosophical definitions from Clausewitz or vice versa. Although Erik Gartzke wrote that mathematically war

²⁰⁵ "THE PRESIDENT'S CONSTITUTIONAL AUTHORITY TO CONDUCT MILITARY OPERATIONS AGAINST TERRORISTS AND NATIONS SUPPORTING THEM," ed. Department of Justice, (2001), <http://www.justice.gov/olc/warpowers925.htm>.

²⁰⁶ Singer, "Reconstructing the Correlates of War Dataset on Material Capabilities of States, 1816-1985."

²⁰⁷ Ibid.

represents the “Error Term,” it is perhaps more accurate to say war is measured by the terms of loss.²⁰⁸ But decision makers don’t think of war in terms of loss of soldiers, land, they think of war in terms of gain and loss ambiguously. If a president sending soldiers off to battle were to dwell on each and every soldier he would lose or have injured he would have surely not made the decision to engage in the battle. Conflict should in all its forms is largely disembodied and examined in terms of utility. Conflict at the highest decision-making level is economic. Because there are divergent terms defining, both war and what constitutes a victory in war, a utility calculus assists in looking purely at what each side hopes to gain by instigating a conflict and helps us to understand what tools they need to use to accomplish their objectives.

To understand the dynamics of conflict and the relationship of cyber attacks in the broader field of conflict studies it is helpful to take a step back and examine other forms of attacks in the context of a scale of conflict. This work is different from Bueno de Mesquita’s work in that it does not subsume all conflict into the same generalized rubric defined generally as war. Instead this work focuses on the decision to engage in cyber conflict. Cyber is a domain of war and it is a cross-domain tool of war. To understand what it means to engage in a cyber attack means placing it within the context of conflict and war in general. To do this it is necessary to follow in the footsteps of other technologies and domains preceding it.

World War I saw the rise of airplanes as a strategic tool of the battlefield. Giulio Douhet an Italian air power theorist believed that air power could quickly and effectively end wars through strategic bombing. He was followed by the likes of Billy Mitchell and others continuing to the present who believe air power is a tool sufficiently capable of winning wars. Robert Pape notes that in World War II only about 18 percent of American bombs fell within 1,000 feet of

²⁰⁸ Erik Gartzke, “War Is in the Error Term,” *International Organization* 53, no. 3 (1999).

their intended targets.²⁰⁹ He further finds that these numbers improved to 70 to 80 percent of munitions falling within 10 meters of their intended target by the Persian Gulf War.²¹⁰ However in no instance was airpower capable of unilaterally winning a war in the context of the objectives stated by the decision maker. In World War II, it was believed that strategic bombing would cut off the German war machine and demoralize the civilian population. Although it had a significant effect on the former it did little to the latter. Furthermore the bombing alone was incapable of halting the German army.

Michael Horowitz and Dan Reiter examine the ability of states to use air power to coerce an opponent in conflict and largely support Pape in his assessments.²¹¹ They find the ability to coerce an opponent is also due to the availability of targets to put at risk through strategic air campaigns. However, all authors indicate that airpower alone is unable to win a war in the Clausewitzian sense. Although it is conceivably possible to use a nuclear bombing campaign to completely obliterate an opponent nation, the result would likely end in a negative utility as either the land would be uninhabitable at best and at worst the attacker could expect a similar retaliation in response resulting in a net loss.

Deciding to engage in any type of conflict requires an examination the scale and objectives of the conflict. Total domination of a state generating absolute victory is often not possible or desired. An accurate understanding of what the goals are can facilitate an accurate assessment of what tools are needed to accomplish an objective. Whereas World War II required total societal mobilization for victory, rarely has this type of effort been undertaken. The next

²⁰⁹ Robert A. Pape, "The True Worth of Airpower," (2004).

²¹⁰ Ibid.

²¹¹ Michael Horowitz and Dan Reiter, "When Does Aerial Bombing Work?: Quantitative Empirical Tests, 1917-1999," *Journal of Conflict Resolution* 45, no. 2 (2001).

section focuses on the use of a combination of tools to achieve defined objectives less than the all out conduct of total war.

Combinatory attacks

In many types of conflict it is necessary to combine tools across domains of interaction to achieve a desired objective. This is referred to as a combinatory attack. As was examined in the previous section it is necessary to establish the objective of an attack to determine what types of tools are necessary. While it is illogical to use certain tools out of context, in other applications the combination of tools can serve to enhance functional capabilities of one or both tools.

Returning to the air power examples from the previous section, Daryl Press indicates that air power used in the Gulf war limited the ability of the enemy to successfully reinforce its lines and created gaps in which ground units were able to exploit weaknesses.²¹² Press finds that the use of air power facilitates a coordinated strike in war and increases the likelihood of a Clausewitzian type victory, but is unable to produce one independent of other tools. The combinatory approach examined by Press was however facilitated by the Command and Control Warfare mechanisms as examined in detail in Alan Campen's edited volume on the first Gulf War.²¹³ Campen and others note that the first Gulf War was facilitated by multiple tools all working in coordination with one another. Cyber alone would not have been able to achieve the objective of removing Iraqi forces from Kuwait nor would a strategic bombing campaign. The result was a coordinated effort of cyber, ground, and air units. This led to what press and others note as the use of C2W generating a functional application of tools resulting in the increased efficiency of the conduct of conflict.

²¹² Daryl Press, "The Myth of Airpower: the Persian Gulf War and the Future of Airpower," (2001).

²¹³ Campen, *The first information war : the story of communications, computers, and intelligence systems in the Persian Gulf War*.

Within the cyber and conventional debate there has been an ongoing feud over the capabilities of cyber to accomplish military objectives. When Thomas Rid writes that cyber war does not and will not exist, he is correct in the Clausewitzian sense. Cyber just as air power is incapable of winning an absolute victory over an opposing force. Therefore cyber war, just as air war, is more a popular term than functional descriptor of reality. Cyber conflict does exist and does in fact work to achieve objectives both in conjunction with conventional military technologies and independent of them. Just as air power can greatly enhance the effectiveness of a ground army and enhance the projection of force against an enemy, cyber weapons offer similar capabilities.

Richard Clarke, a former National Coordinator for Security, Infrastructure Protection, and Counter-terrorism, was one of the first to write about the combinatory strategy of the Israelis in their operation to bomb the Syrian nuclear facilities.²¹⁴ Whereas the United States has been known to use stealth aircraft to infiltrate and bomb targets in foreign airspace, few other nations possess this technology. Typically in an air attack a state will use radar-jamming devices to prevent surface to air missiles (SAMs) from shooting down their planes. This tactic has some obvious drawbacks. Instead of entering into another country's airspace undetected this method alerts everyone to his or her presence and essentially works by preventing SAMs from being effective. The Israeli attack on Syria's nuclear facility was unique in that it neither utilized stealth technology nor employed radar jammers. Instead the Israelis first conducted a cyber attack against the Syrian air defense system. This attack allowed the Israeli planes to enter Syrian airspace undetected without stealth capabilities to bomb their targets and exit the airspace without their planes even showing up on Syrian radar. This is a clear combinatory attack

²¹⁴ Clarke and Knake, *Cyber war : the next threat to national security and what to do about it*.

facilitating a conventional tool, air power, with a cyber tool, to achieve a limited objective to gain utility.

The Syrian example is not the only example of this type of tactic. In 2008 prior to the instigation of hostilities between Russian and Georgia, Russian hackers began to systematically target Georgian governmental and media outlets. While the attack was not nearly as complicated as the Israeli attack, the effect was to slow or minimize the communication capabilities of the Georgian government with its own people and the rest of the world. This isolationist tactic likely increased the ability of the Russian invasion force to conduct its operations. Conventional tactics along the same lines have included the bombing of communications facilities and power stations to eliminate the enemy's ability to effectively employ C2W over its defense forces. The Russian case is one of the first instances in which the physical structures were left largely undamaged while the still achieving largely the same effect.

Chris Bronk, a former State Department official and cyber researcher at the Baker Institute at Rice University provides a scary foreshadowing for potential combinatory attacks in an article titled "Blown to Bits."²¹⁵ Bronk paints a story in which China uses a new type of computer virus to effectively hinder the operation U.S. command and control capabilities. In his story he hits on a large number of areas in which a combined cyber and conventional strategy can assist in the conduct of conflict. The creation of confusion within an enemy's leadership limits an effective response. Similar to a Pearl Harbor strategy like the one the Japanese hoped would effectively cripple the U.S. response to their aggression in in the Pacific with a massive strike against the U.S. Pacific fleet in 1941, the attack by the Chinese in Bronk's story cripples the ability of U.S. forces to mount an effective response actions against Taiwan.

²¹⁵ Christopher Bronk, "Blown to Bits: China's War in Cyberspace, August–September 2020," *Strategic Studies Quarterly* 5, no. 1 (2011).

In each of the three above examples cyber is employed in a capacity referred to as a “force multiplier.” A 2005 Pentagon report to Congress states: “China’s latest Defense White Paper deployed authoritatively a new doctrinal term to describe future wars the PLA must be prepared to fight: “local wars under conditions of informationalization.”” This term acknowledges the PLA’s emphasis on information technology as a force multiplier and reflects the PLA’s understanding of the implications of the revolution in military affairs on the modern battlefield.”²¹⁶ This assessment is confirmed by further testimony in 2011 stating: “these capabilities are being developed as weapons which themselves produce strategic effects as well as serving as key force multipliers for conventional “kinetic” warfare operations.”²¹⁷ Other reports indicate that China is not alone in their assessment that cyber is a force multiplier. They are joined by nation states such as the United States and Russia, as well as sub-state actors including various terrorist organizations.²¹⁸

Cyber can be used to enhance various aspects of conflict across domains of operation. It can be used for information sharing purposes, it can be used to hinder information sharing, it can be used in psychological operations against foreign armies, it can immobilize targets with digital components, and cyber can be used as an enhanced recruitment and training tool for warriors around the world. The term force multiplier can mean many things however in the military context it refers to attributes, which make a given type of military force more effective than if such a multiplier were absent.

²¹⁶ "The Military Power of the People’s Republic of China," (Washington, D.C.: Department of Defense, 2005).

²¹⁷ Oversight and Investigations Subcommittee of the Foreign Affairs Committee of the United States House of Representatives, for its Hearing On: “Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology”, *Cyber Warfare Challenges and the Increasing Use of American and European Dual-Use Technology for Military Purposes by the People’s Republic of China (PRC)*, 15 April 2011.

²¹⁸ Timothy L. Thomas, "Cyber Mobilization: A Growing Counterinsurgency Campaign," (Fort Leavenworth, KS: Department of Defense, 2006).

Although the term multiplier would indicate a straightforward mathematical relationship between the conventional force and its multiplier, the relationship is not straightforward. It is not possible to combine the probabilities of the success of a cyber action and the success of a conventional action in order to gain a complete understanding of the probability for success in any type of conflict in all situations. The Russia - Georgia War example highlights a simple example of why such a probability function would be inappropriate. Although Russian forces used the degradation in information communications capabilities of their Georgian counterparts to their advantage, their overwhelming force and military capabilities effectively assured a conventional military victory. This is not to indicate that if this cyber multiplier had not been present that the utility would have been the same. However, the relationship is not direct in this instance.

The Israeli case nuances the multiplier debate. If the cyber attack had been unable to hide the Israeli actions the attack would have had a significantly lower probability of success. This indicates a direct relationship in the force multiplier of cyber.

Force multiplier is a weak generalized term, as not all conventional attacks require a force multiplier to succeed. Yet often this force multiplier can condition the overall utility calculation. It is important when constructing a combinatory model that involves cyber and conventional tactics in which cyber acts as a force multiplier to take into consideration the effect cyber has on the overall probability of success. Not all types of conflict carry with them the same relationship. Just as in regression modeling it is often necessary to interact variables in different ways, the relationship between a conventional attack and a force multiplier such as cyber need to be interacted in different ways. Once this relationship is understood in the context of the particular military action a dynamic decision-making model can be developed.

Stand-alone conflict

Cyber can be used as an independent tool for accomplishing military and strategic objectives. The standalone of cyber is predicated on attacking those targets specifically attached to or impacted by cyber. Whereas air power is typically limited to the destruction of targets or the maintenance of zones of denial, cyber extends across multiple facets of national security as was illustrated in chapter 2. Using cyber as a standalone tool in conflict requires an accurate understanding of its capabilities as will be further examined in chapter 7. This section however contends that with specified and realistic objectives cyber can independently accomplish these objectives without assistance from other conventional tools.

Amit Sharma indicates cyber can be used as a strategy of warfare independent of other tools by harnessing its ability to affect what he refers to as the trinity of national security.²¹⁹ Sharma defines the components of the trinity of national security as “government, military, people (economic).”²²⁰ A cyber attack, he argues can overwhelm simultaneously different aspects of the trinity and provide what amounts to a Clausewitzian victory. Although he attempts to make a valid point and follows a logical train of thought throughout his argument, his thesis suffers dramatically in its ability to provide any meaningful examples of such an event occurring. This is not to say that it is not possible, but rather that it is unlikely given the current state of technology.

More reasonable estimations of conflict are found in practical applications of current technologies to actionable strategic and tactical objectives. The best example of a standalone cyber attack to achieve an actionable objective was Stuxnet. Stuxnet specifically targeted a

²¹⁹ Amit Sharma, "Cyber Wars: A Paradigm Shift from Means to Ends," *Strategic Analysis* 34, no. 1 (2010).

²²⁰ Ibid.

system of an opponent state and damaged its functional capability. This damage slowed the acquisition of a capability deemed to be politically unacceptable by the attacking nations. Stuxnet is a clean example of a cyber tool achieving an objective in cyberspace. Its effect was direct and was not dependent on what is best referred to as potential positive intended externalities.

One of the problems associated with standalone attacks dependent on positive intended externalities is that they often make assumptions about the results of an attack not supported by the direct action effect of the attack. As Horowitz and Reiter note air power is often assumed to be a coercive instrument of military force, yet the coercive nature of the tool is not related directly to its effect.²²¹ Instead it is an indirect result. Likewise had the intended objective of the Stuxnet attacks been to cause Iran to give up its nuclear program, Stuxnet would have been largely ineffective.

As Joel Brenner notes in telling about a set of coding instructions embedded in pipeline management software stolen by the Soviet Union in the 1980s, the indirect goal was to disrupt Soviet Oil production capabilities, whereas the direct effect was to damage a single pipeline.²²² In this instance the direct goal of creating an explosion facilitated an indirect goal that followed logically from the direct goal. However, much like lining up dominoes it is important to understand the how one domino falling at point A can eventually effect a different domino's collapse at point F. This indicates one of the fundamental flaws in Sharma's argument that cyber can be used as a tool to wage and win a Clausewitzian type of conflict. The more moving parts are added to a particular chain the more difficult it becomes to ensure that all the dominoes fall.

²²¹ Horowitz and Reiter, "When Does Aerial Bombing Work?: Quantitative Empirical Tests, 1917-1999."

²²² Brenner, *America the vulnerable : inside the new threat matrix of digital espionage, crime, and warfare*.

Cyber is a very powerful tool that crosses over multiple domains, but it is very difficult to plot the indirect consequences of cyber attacks beyond their initial objective. As the blitz on London demonstrated during World War II, while the bombing inspired fear, it also hardened resolve, having the exact opposite effect of the intended indirect externality.

Cyber and conventional tools a tale of objectives

Understanding the decision to attack first requires understanding the objectives of a potential attack. Conflict is a tale of objectives. The larger and more complex an objective the more tools are required to achieve it. War in the Clausewitzian sense historically requires all available tools. As societies become more and more connected through cyberspace the need for using cyber tools in conflict increases. However, as the Department of Justice numbers indicate, Clausewitzian wars occur few and far between. What we are left with is a range of military encounters with an even more diverse set of objectives associated with each encounter. Because no two encounters are identical it is useful to have a robust tool bag of weapons. Frequently weapons will be used in conjunction with one another. However, often they will be used independent of one another. It is the objective that dictates the weapons not the weapons that dictate the objective. Understanding the objective of a type of attack defines how the utility calculation should be formulated.

Figure 6.1 illustrates the relationship of conflict, tools, and objectives. Although the figure only gives the roughest of outlines for conceptualizing conflict, it does provide a concise visual overview.

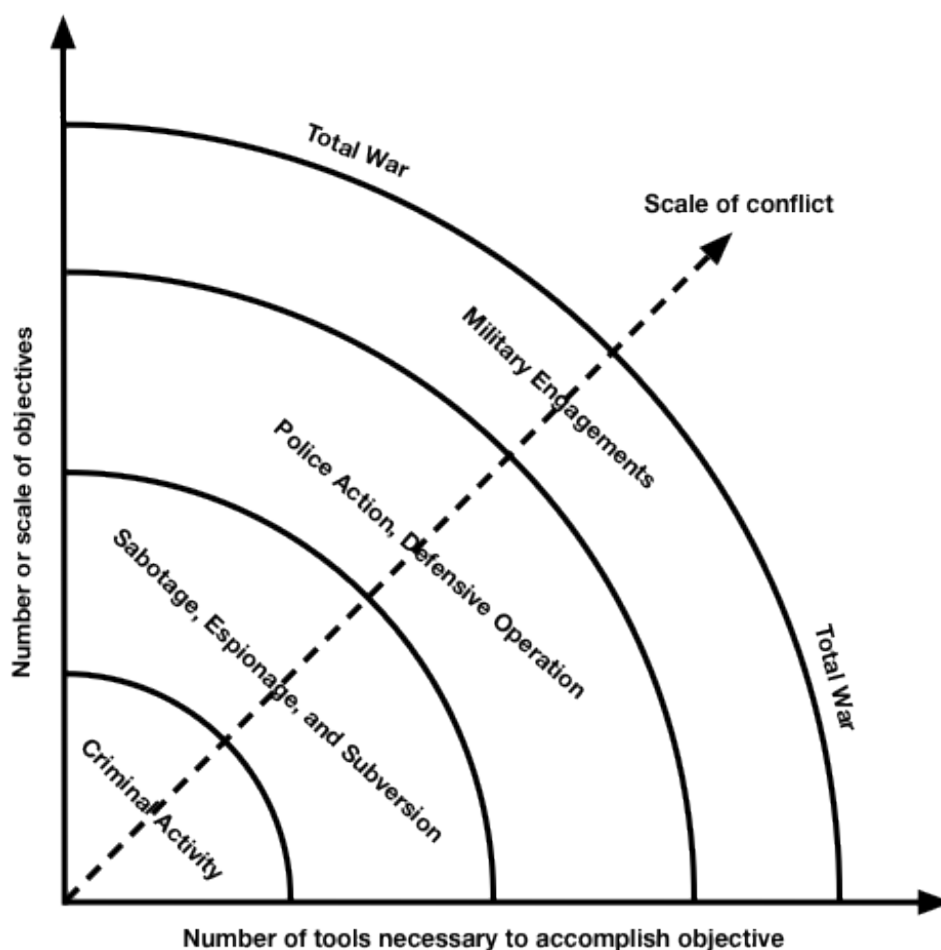


Figure 6.1: Objective, Scale and Tools of Conflict

As figure 6.1 illustrates there is a relationship between the number or scale of objectives of an attack and the number of tools needed. Similarly overall scale of conflict increases in size in comparison to the number and scale of objectives and the number of tools employed in a conflict. Although the relationship is not as direct as this figure would indicate there is general a relationship between what is being requested and the eventual size of a conflict. With this figure in mind it is evident that a tool such as cyber is unlikely to be the sole tool engaged in a large-scale conflict with a large number of objectives. Despite the way in which cyber crosses domains it is unlikely to be able to take the place of an occupying army or a bomb dropped from a plane.

Although this chapter focuses on the relationship between standalone and combinatory types of attacks, this work primarily focuses on demonstrating how standalone attacks can be examined as generating utility. This is a necessary step, with an eventual goal being a thorough understanding of the utility of any type of attack, combinatory or stand-alone can be calculated. Bueno de Mesquita sufficiently explains how utility can be examined in the context of conventional conflicts, but when these types of conflicts do not occur and are instead replaced by cyber conflicts his model is inadequate.

What should be taken away from this chapter is that cyber is a tool capable of working with other tools used in conflict, as well as independent of them. Terms such as ground war, air war, cyber war, space war, are vernacular terms denoting the domain of operations for a particular type of conflict, they do not denote the conflict itself. It is far more accurate to conceptualize these aspects as cyber battle, ground battle, and air battle. Although Bueno de Mesquita and others refer to the utility of war they are subsuming an enormous number of variables into a single mathematical variable. In this work war is less important a term than the objective (goal) of instigating a type of conflict through a cyber attack. Once the objective has been decided upon a decision maker can then begin to determine what tools are necessary to achieve that objective. If an objective is sufficiently limited it can be accomplished with a single tool. It is the achievement of that objective that generates utility.

CHAPTER 7

Defining the Role of Intelligence in Cyber

"If ignorant both of your enemy and yourself, you are certain to be in peril."

~Sun Tzu

Information is the lifeblood of modern states. Intelligence is increasingly facilitating information superiority through an understanding of the cyber domain. The Department of Defense Joint Vision 2020 establishes the goal of information superiority on the battlefield.²²³ This information superiority enables decision superiority and favorably tilts the strategic and tactical balance.²²⁴ Information superiority is built on cyber power, scale and complexity of attacks, robustness of defense, policy positions, systemic vulnerabilities and dependencies, and actor anonymity and attribution issues. Intelligence plays a mission critical role in assessing these characteristics. This paper examines the role of intelligence in identifying these characteristics within the cyber domain and examines how it influences the decision-making process of leaders. Specifically, intelligence increases the effectiveness of identifying potential attackers within the cyber domain and informs the decision-making logic of the state when engaging in covert cyber action directed against a potential adversary.

Cyberspace is not tangible in the same way as more conventional domains and therefore necessitates a new form of dynamic intelligence evolving from all-source collection of conventional and novel intelligence sources. A recent National Research Council report states

²²³ "Joint Vision 2020."

²²⁴ Ibid.

that intelligence in the cyber domain is useful for both strategic and tactical purposes.²²⁵ The strategic and tactical importance of intelligence for influencing decision-making within the cyber domain falls within the concept of all-source intelligence. Loch Johnson defines all-source intelligence as one of the fundamental propositions of a theory of strategic intelligence.²²⁶ More importantly, for the purposes of understanding the operational and political environments within which offensive and defensive actions in cyberspace can occur, it is necessary to understand, what intelligence is within, and how intelligence influences, decisions regarding the cyber domain.

This work particularly examines how intelligence influences the utility calculus of computer network operations (CNO). The cyber domain offers up a unique set of challenges to Bueno de Mesquita's model for the development of utility in a decision-making process. Conventional domains are currently classified under Bueno de Mesquita's rubric by using Composite Index of National Capability (CINC) scores affected by monotonic declines in power over distance. His rationale for this measure is logical and well reasoned from a traditional conflict decision-making perspective. A state that is better endowed with resources than its potential adversary has a higher probability of being successful in a conflict. The farther a state attempts to extend its power and resource capabilities out from its center of gravity, the more its relative power begins to decline.²²⁷ Equations 1-3 are Bruce Bueno de Mesquita's probability functions from his utility theory of international conflict model.²²⁸ Where P_i is the probability of success for the initiator and $1 - P_i$ is the probability of failure. Bueno de Mesquita uses

²²⁵ Owens et al., *Technology, policy, law, and ethics regarding U.S. acquisition and use of cyberattack capabilities*.

²²⁶ See chapter 3, Proposition 14 in Peter Gill, Stephen Marrin, and Mark Phythian, *Intelligence theory : key questions and debates* (London; New York: Routledge, 2009).

²²⁷ Bueno De Mesquita, *The war trap*.

²²⁸ Bueno De Mesquita, "An Expected Utility Theory of International Conflict."

cap_{ij} represents the capabilities of a conflict initiator at the defender's territory and cap_{jj} represents the capabilities of the defender.

Equations 1-3²²⁹

$$\text{Capabilities} \quad \text{adjusted capabilities} = \text{composite capabilities}^{\log[(\text{miles/miles per day})+(10-e)]} \quad (1)$$

$$\begin{array}{l} \text{Probability of} \\ \text{Success} \end{array} \quad P_i = \frac{cap_{ij}}{cap_{ij} + cap_{jj}} \quad (2)$$

$$\begin{array}{l} \text{Probability of} \\ \text{Failure} \end{array} \quad 1 - P_i = 1 - \left[\frac{cap_{ij}}{cap_{ij} + cap_{jj}} \right] \quad (3)$$

For the cyber domain it is inappropriate to use CINC scores or monotonic declines in power over distance. In addition to these two inappropriate attributes, cyber adds complexity of anonymity and attribution. Moreover additional characteristics necessarily qualify computer network attacks (CNA) as covert acts. Conventional intelligence can inform the utility model by providing detailed analysis on measures such as CINC scores. But CINC scores are an inappropriate measure of cyber capabilities. Their inappropriateness is not hard to discern. CINC scores were first developed by David Singer in 1963 but have been used since as a measure of national power in the Correlates of War (COW) project.²³⁰ When they were first developed and for the first half of their history, the cyber domain was of little concern. More importantly, for the types of conflict examined within COW they are applicable. As states become increasingly interdependent and their national securities are evermore tied to cyberspace, the power relationship within the conventional domains becomes increasingly limited in its explanatory power for this new form of conflict.

²²⁹ Ibid.

²³⁰ Singer, "Reconstructing the Correlates of War Dataset on Material Capabilities of States, 1816-1985."

CINC scores incorporate measures of total population, urban population, iron and steel, primary energy, military expenditure, and military personnel. Each of these is an important consideration in conventional warfare and particularly in the decision to engage in conflict. Cyberspace, however, is virtual, meaning that total population, or urban populations, or any of the other constitutive parts of CINC scores do not adequately measure power in this domain. Cyber power is constructed by analyzing offensive and defensive technological strengths and weaknesses as well as dependencies leading to vulnerabilities. The power of these strengths and weaknesses does not monotonically decline over distance, as operations within cyberspace are almost instantaneous,²³¹ and there is little to no necessity in moving cyber units around the world. An operator can sit at Central Command (CENTCOM) and fly a drone over Afghanistan thousands of miles away with no loss of effectiveness.²³²

Beyond the inappropriateness of conventional measures of power is the way risk is formulated. Because the probability of success in a conventional conflict is relatively straightforward in military capability terms, it was adequate to use pure national military capability measures enhanced by conventional intelligence collection. But, cyber, as with many other forms of covert action, has added attributes influencing the probability of success for any type of attack. In a conventional domain an attack is relatively unavoidable even if it is known beforehand. Iran cannot easily move its enriched uranium production facilities even if it knows Israel is about to attack. It can harden its facilities and attempt to weather an attack, but it cannot

²³¹ Potter and Nakao, "Mobitopolo: a portable infrastructure to facilitate flexible deployment and migration of distributed applications with virtual topologies." Potter and Nakao illustrate that the migration of virtual machines across networks can be routed in ways that are more efficient than current technological protocols. In so doing they illustrate that it is possible to map out more efficient routes on the internet. This indicates that all actions in cyberspace are not instantaneous and can be manipulated to speed or slow data flow.

²³² Fair, "Drone Wars."

mitigate an attack. On the contrary with cyber attacks, if it is known an attack is coming and where it is coming from, the defender can minimize or nullify its effect.

A server or computer with information on it and connected to the Internet is much like a ship in the ocean. The ship is fine so long as its captain knows the weather conditions in advance. The captain can steer the ship to safer waters or in the event of a hurricane can dry dock or harbor the ship. The same is essentially true of a country under imminent threat of a cyber attack from a known source. A network administrator can thwart an attacker in a number of ways if he knows whom the attacker is and when they are going to attack. In a worst-case scenario he can effectively dry dock the network by removing external connections or temporarily shutting systems down. There was even a bill proposed in the United States Congress promoting the idea of an "Internet kill switch."²³³ Because cyber is characteristically different from conventional forms of conflict, a decision-making model is needed to assess the utility of an attack employing cyber tools uniquely different from conventional military tools. The development of utility in a cyber decision-making model necessitates modified variable attributes and probability development. This modification in the development of probabilities greatly influences the subsequent development of political utility within Bueno de Mesquita's original utility theory of international conflict.²³⁴

Equations 4-7 represent a revised probability function that can be heavily influenced by more accurately defining the role of intelligence in cyber. In the below equations F represents cyber force, a measure that includes policy considerations, training, organizational structures and many other attributes to be examined in more detail in subsequent sections. T represents the threat spectrum capabilities of a country within the cyber domain. The threat spectrum is based

²³³ S. 773: Cybersecurity Act of 2010 was last reported to committee on March 24, 2010. No vote has currently taken place.

²³⁴ Bueno De Mesquita, "An Expected Utility Theory of International Conflict."

on demonstrated threat capabilities on both levels of complexity and size of potential attacks. D represents the number of digital vulnerabilities possessed by a country. It can be broadly measured using Internet penetration or, as argued in this paper, it can be examined with excruciating detail using intelligence. The hazard model is designed to provide a mathematical means, using intelligence to determine the probability of maintaining anonymity at a point in time. This is useful in determining whether a particular type of attack has enough time to be completed before its effectiveness begins to be challenged. This model is composed of C the complexity of the attack, S the size of the attack, H the level of hostility between nations, and Q the number of countries in a given system. Q is particularly important because not all countries have equivalent cyber capabilities and in truth many have none at all, limiting the overall size of the system increases the chances of attribution. Intelligence's major role is to more accurately define each of the constituent parts of the probability function. These equations fill in the probability for success in assigning utility to a decision and are uniquely constructed to be applicable to cyber.

Equations 4-7 Modified Cyber Probability function

Cyber Force by
Threat Spectrum
Capabilities over a
measure of digital
dependence.

$$\frac{(F \times T)}{D} = \text{Capabilities} \quad (4)$$

This is the hazard
function for the
probability of
maintaining
anonymity at
time(t)

$$A(t) = \pi(T > 1) \quad (5)$$

$$A = \log h_1(t) = C_i\beta + S_i\beta + (S_iC_i)\beta + H\beta + Q\beta + e \quad (6)$$

The full probability
function for cyber.

$$P_{ic} = A \left[\frac{F_i \times T_i}{D_i} / \left(\frac{F_i \times T_i}{D_i} + \frac{F_j \times T_j}{D_j} \right) \right] \quad (7)$$

One additional change to the overall calculation of utility predicated on the reality that most cyber actions are covert in nature; Bueno de Mesquita's consideration of alliances becomes largely irrelevant. Time constraints within the domain also limit the importance of alliances.

Cyber, much like conventional domains, is predicated on power and vulnerabilities. Any decision to use cyber or to defend against it is defined in the context of a probability for success or failure. Intelligence helps decision makers accurately define the power versus vulnerabilities calculus of conflict seen in the equations above. By defining the role of intelligence in cyber, I am focusing on how intelligence influences how decision makers calculate utility within the domain. Intelligence estimates on the power and vulnerabilities of states as well as attribution and anonymity of particular types of attacks can greatly affect how states interact in this ever-evolving domain. Much progress has been made but there has been insufficient focus on what role intelligence can play in influencing decisions within this domain. Before diving into analyzing the role intelligence can play within the cyber domain it is necessary to start with a parsimonious definition of intelligence.

Defining Intelligence

There are dozens of different definitions of intelligence each of which is in some way applicable to understanding cyber action. One of the more succinct and conceptually ordered comes from Michael Warner. Warner defines intelligence as a "secret, state activity to understand or influence foreign entities."²³⁵ His definition establishes the fundamental premises of both collection and analysis while not leaving off actions designed to influence. Intelligence is

²³⁵ Michael Warner, "Wanted: A Definition of 'Intelligence'," *Studies in Intelligence* 46, no. 3 (2002).

vital to the cyber domain because foreign entities are increasingly storing, managing, and directing their governmental, public, private, and military functions in a digitized world.

The traditional intelligence collection types (INTs) are still of immense value, yet they must be combined with aspects of the digitized target spectrum to provide a holistic view of both threats, and opportunities. At present the majority of studies in the public domain have focused on defense.²³⁶ This defensive posture is made clear by General Keith Alexander, the Director of the National Security Agency and Commander of United States Cyber Command when he writes:

*“US Cyber Command’s efforts and planning aim to ensure that the DoD has done all it can to defend and deter determined adversaries, mitigate, dangerous threats, and address nagging vulnerabilities, so that even our most capable opponents will know that interfering with our nation’s equities in cyberspace is a losing proposition.”*²³⁷

This defensive and deterrent reliant posture is limiting and prone to inadequacies. Echoing Machiavelli and to some extent Sun Tzu, the adage “the best defense is a good offense,” offers a novel way of considering action and intelligence within cyber. More accurately, it allows for a systematic approach to both national cyber defensive and offensive resource allocations. Beyond the efficiency argument for shifting the focus from solely defense to a balance between defense and offense, intelligence collection can help to inform offensive strategies and the decision to use cyber as a weapon. The role of intelligence within cyber becomes increasingly

²³⁶ Alexander, "Building a New Command in Cyberspace."; Dzheng, "Securing Cyberspace for the 44th Presidency," (2009); Wesley K. Clark and Peter L. Levin, "Securing the Information Highway," *Foreign Affairs* 88, no. 6 (2009); Jr. Daniel E. Geer, "Cybersecurity and National Policy," *Harvard National Security Journal* 1(2010).

²³⁷ Alexander, "Building a New Command in Cyberspace."

important when considering the difficulty of achieving any significant measure of deterrence within the cyber domain.²³⁸

The defensive orientation of the majority of cyber literature has a constraining effect on decision-making processes for the use of offensive cyber weapons. This defensive focus is largely due to both the alarmist calls of some scholars and policymakers and an information communications technologies (ICT) industry orientation offering many more strategies for defense than for offense. While not disputing the need for defense, this defensive focus leads the national security establishment down a path of attempting to create an impenetrable system. If there is one thing that is abundantly clear in the cyber domain it is that the only impenetrable system is the one that has not been made. Cyber is based on physics and algorithms. The mathematics and science behind security measures can be immensely complex and take massive computing power to penetrate, but that does not make them impenetrable.

Instead of focusing on a solely *carte blanche* defensive posture towards cyber security, intelligence can provide both an offensive and defensive picture more effective at safeguarding national security. This paper takes a step back from the conventional cyber security literature and examines how intelligence can direct cyber security efforts to not merely safeguard national security, but also provide an offensive tool for use against other states. The vast literature on intelligence, ranging from the way intelligence influences the policy-making process, to how it helps to understand aspects of the development of utility for actions, serves as a guide in defining the role of intelligence within the cyber domain.

Reflecting on Warner's definition of intelligence, the spectrum of intelligence collection methods from Human Intelligence (HUMINT) to the more technical collection methods of

²³⁸ Martin C. Libicki and Project Air Force (U.S.), *Cyberdeterrence and cyberwar* (Santa Monica, CA: RAND, 2009).

Signals (SIGINT), Measurement and Signatures (MASINT), Geospatial (GEOINT), and Open Source (OSINT), all work together in an all-source environment to provide an accurate understanding of foreign entities. (Table 7.1 provides a quick definitional reference for the various intelligence collection types.) The understanding provided by intelligence has largely been focused in the conventional domains and in political decision-making. However, as decisions in conventional domains increasingly migrate towards cyberspace, and the systems controlling the tools used in these domains increasingly become digitally connected, the importance of understanding the technical schematics and decision processes becomes vital to national security.

Table 7.1: Intelligence collection methods²³⁹

Intelligence Source Type	Definition
Open Source (OSINT)	Overtly available information found, selected, and acquired from publicly available source.
Measurement and Signatures (MASINT)	Intelligence detected and classified from targets, that identifies or describes signatures (distinctive characteristics) of fixed or dynamic target sources
Human (HUMINT)	Intelligence collected through interpersonal contact via human collection officers
Geospatial (GEOINT) ²⁴⁰	The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information
Signals (SIGINT)	Intelligence-collection by interception of signals through various communications technologies.
Cyber (CYBERINT) ²⁴¹	Obtaining prior knowledge of threats and vulnerabilities to information communications systems through a variety of technical means. Also referred to as Computer Network Exploitation (CNE)

²³⁹ Definitions are largely adapted from: Mark M. Lowenthal, *Intelligence : from secrets to policy*, 4th ed. (Washington, D.C.: CQ Press, 2009).

²⁴⁰ U.S. Code Title 10, §467

²⁴¹ Based on: Phil Williams, Timothy Shimeal, and Casey Dunlevy, "Intelligence Analysis for Internet Security," *Contemporary Security Policy* 23, no. 2 (2010). CYBERINT is considered independent of traditional SIGINT. However, as in many of the other types of intelligence collection techniques and agencies often overlap.

Nick Cullather in his article on the digital connections on the battlefield indicates significant advances in the development of network centric warfare. He notes that the rise of this revolution in military affairs has largely not been matched by the intelligence community's ability to keep up.²⁴² This is of particular importance as we look beyond the network centric battlefield of conventional weapons to the new zone of confrontation within cyberspace itself. Similarly, Michael Herman finds that counter-terrorism intelligence analysis requires a broad spectrum of information sources brought together.²⁴³ ICT facilitates the mitigation of "stovepipes" and increases the efficiency in information transference.²⁴⁴ Information transference has also been facilitated following the Intelligence Reform and Terrorism Prevention Act of 2004 by the creation of "fusion" centers.²⁴⁵ ICT has a role to play not only in the conduct of war on the battlefield but also in the management of a conventional traditional threat spectrum within the fusion centers and beyond in the wider intelligence community.

Terrorism is not commonly regarded as part of the conventional threat-spectrum, but in reality most terrorist acts take place in the physical world and require bombs and explosives. But the information transference necessary to organize, plan, and conduct warfare, terrorist acts, and plan political strategies has largely shifted to cyberspace. Unfortunately, with available open source information there appears to be only a limited focus on the ability to realistically size up threats and targets within cyberspace itself. Furthermore, Joel Brenner a former Inspector General of the National Security Agency and head of U.S. counterintelligence indicates there is

²⁴² Cullather, "Bombing at the Speed of Thought: Intelligence in the Coming Age of Cyberwar."

²⁴³ Michael Herman, "Counter-Terrorism, Information Technology and Intelligence Change," *Intelligence and National Security* 18, no. 4 (2003).

²⁴⁴ Ibid.

²⁴⁵ Edward G. Amoroso, *Cyber attacks : protecting national infrastructure* (Oxford: Butterworth-Heinemann, 2010).

already an enormous threat emanating from within cyberspace that is not being adequately addressed.²⁴⁶

Modern warfare, command and control warfare (C2W), is network based. Operators at CENTCOM control modern weapons systems such as drones flying over remote battlefields²⁴⁷ and much of the national critical infrastructures in states that pose a conventional security and economic threat to the United States are controlled by digital systems. The literature is less focused on the need for understanding these vulnerabilities than it is on safeguarding them. This, in essence, places the importance of defensive above offensive capabilities.

One work that makes the case for the defensive necessity of intelligence to inform national cyber security is that of Phil Williams et al. Williams and his colleagues make a well-reasoned case arguing for focused intelligence efforts on identifying those threats to national cyber security²⁴⁸. Williams, et al. make a valid point that needs to be and is being addressed by several national strategy documents on the topic including the *National Strategy to Secure Cyberspace*,²⁴⁹ and the *International Strategy for Cyberspace*.²⁵⁰ One report of particular importance, addressing many of the issues brought up by Williams, et al., is the October 2011 report by the Office of the National Counterintelligence Executive on cyber espionage.²⁵¹ Each of these strategies and reports, including many others across the U.S. Federal government, has made identification and protection against vulnerabilities a top priority.

²⁴⁶ Brenner, *America the vulnerable : inside the new threat matrix of digital espionage, crime, and warfare*.

²⁴⁷ Fair, "Drone Wars."

²⁴⁸ Williams, Shimeal, and Dunlevy, "Intelligence Analysis for Internet Security."

²⁴⁹ "The national strategy to secure cyberspace," (Washington, D.C.: United States Department of Homeland Security, 2003).

²⁵⁰ "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," ed. The President of The United States (Washington, D.C.2011).

²⁵¹ "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace," (Washington, D.C.: Office of the Director of National Intelligence, 2011).

Currently cyber security is based on attacks in progress or attacks that have already occurred. It is difficult if not impossible to defend against an unknown attack. Therefore much of the effort in the United States cyber community now seems to be the equivalent of saying, "Let's plug the holes in the dyke after it floods." Most types of cyber attacks are repeat attacks and originate at the lower end of the threat spectrum. The strategy to begin filling in holes makes sense from the perspective of attempting to prevent further intrusions of the same types of attacks, but largely fails to address the more serious problem of accurately anticipating what the next type of attack is going to be. Cyber planners are similar to the French prior to World War II. They learned from the prior war and built the Maginot line, but damn if those Germans didn't just go around it. The real challenge is how to develop an intelligence strategy that prevents future attacks before they happen.

In a world of known unknowns and unknown unknowns to paraphrase Secretary Rumsfeld,²⁵² cyber security is likely the former rather than the latter. How can intelligence be used to better the cyber security situation to not only protect the national infrastructure in a more systematic and logical manner, but also to use this information to inform the decision-making processes of leaders?

One problem with the U.S. cyber community is proximity. Because the community develops, tests, and employs its own tools, it is unable to take into account methods of testing that have not yet threatened systems in the past. This is what is best referred to as an in the box, out of the box problem. The designers of systems, software, and networks are incredibly talented and smart individuals, they lead the world in technical innovation, but because they are inside their own systems it makes it intrinsically difficult to isolate unforeseen problems.

²⁵² Secretary of Defense Donald H. Rumsfeld, "DoD News Briefing - Secretary Rumsfeld and Gen. Myers," (2002), <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=2636>.

Solutions are best achieved by dividing the resources of the intelligence and technical community in several ways. First, the current orientation towards plugging the holes must continue. While this post-hoc process is frustrating it prevents or at least slows further intrusions. The mentality of these individuals is one of defense. The objective is to secure and defend systems against all possible or known types of attacks. The most realistic approach is to defend against known types of attacks. The systems therefore become fortified against repeat incidents or at least can minimize their severity.

To safeguard systems defenders must step outside of their box and see the proverbial box from the outside. Intelligence organizations must use all-source methods to collect as much intelligence on potential opponents as possible. This means profiling every aspect of other nations' cyber offensive and defensive capabilities. This requires a robust all-source collection methodology. Signals intelligence must look for transmissions and communications as well as spikes in Internet traffic and geo-locate them using IP addresses. These geo-located IP-addresses need to be analyzed using satellites and drones to provide accurate geospatial information on the areas in question. Open Source intelligence collection should attempt to gain as much publically available information on areas of interest as possible through legal means. Once all of this information has been compiled and assessed, targeted HUMINT operations should begin working on developing assets within these areas or with connections to these areas. These agents should be recruited for multiple purposes. First, they should be used to secure intelligence on the capabilities of potential adversaries. These capabilities will be defined in more detail below. Second, agents should also be recruited to become potential insider threats, a tool of particular importance on those systems, which are air-gapped.²⁵³ Lastly, intelligence agencies should also

²⁵³ An air gap is a security measure often taken for computers and computer networks that must be extraordinarily secure ensuring that a network is physically, electrically, and electromagnetically isolated from insecure networks,

place an emphasis on Computer Network Exploitation and attempt to probe and map out network infrastructure, vulnerabilities, and strengths of adversaries. The last point is of importance both from an offensive and defensive strategic orientation.

Another of the major problems with the cyber domain arises out of its systemic complexity. As Williams et al. accurately note, cyber defenders often do not have a realistic or accurate picture of their own systems let alone the systems of those who are attacking them.²⁵⁴ Following their recommendations it is prudent for the national security community to make use of the principle of knowing yourself. This requires a consistent focus on domestic systems. However, only focusing on domestic systems leads to the Maginot line tendency in which it is assumed networks are created to be impenetrable.

Intelligence and the cyber battlespace

The cyber domain is a modern battlespace and necessitates a holistic understanding. When defending against or engaging in hostile actions it is necessary to have an accurate understanding of the operational environment. Any battlespace whether offensive or defensive according to Edward Waltz requires a combination of dominant battlespace awareness (DBA) and dominant battlespace knowledge (DBK).²⁵⁵ The process of identifying what is and is not important to understanding a particular battlespace largely falls to the discretion of policy makers within the intelligence cycle. (See Figure 7.1).

Stephen Marrin writes about intelligence and decision-making that:

“the intelligence cycle starts with decision-maker information requirements levied on intelligence collection capabilities, the processing of collected raw intelligence and transmission

such as the public Internet or an insecure local area network. This often includes creating a network with independent electric supplies from public utilities.

²⁵⁴ Williams, Shimeal, and Dunlevy, "Intelligence Analysis for Internet Security."

²⁵⁵ Waltz, *Information warfare : principles and operations*.

*of this processed material to analysts who decipher its meaning, and relay that understanding back to the decision-makers...*²⁵⁶

The decision-maker engages in tasking through a number of different “pull” mechanisms including governmental reports, hearings before Congress, Presidential directives, and executive orders. These tasking methods and others all combine to facilitate within the intelligence community an accurate understanding of what constitutes the battlespace in the eyes of the policy-maker. Often the planning and direction can be informal requests from the executive or from congress and at other times it can be official strategy documents. Prior to 9/11 terrorism was a priority, but the planning and direction of resources had not yet reached a critical mass sufficient to prevent the terrible attacks on the World Trade Center and the Pentagon. Marrin and others find the intelligence process frequently fails to adequately define what constitutes a tasking priority for the intelligence community, necessitating a “push” from within the community outward. There are many instances in which policy-makers ignore, misinterpret, or misuse intelligence despite adequate tasking and intelligence production and dissemination²⁵⁷.

The push mechanism of the intelligence community can happen in several ways. Often it can follow what constructivists call “norm entrepreneurs.” Entrepreneurs in the cyber domain include Richard Clarke,²⁵⁸ or John Arquilla and David Ronfeldt²⁵⁹ among others. These individuals bring to national policy-makers’ attention issues of importance and help direct the intelligence community’s efforts. If, however, they make outlandish claims and statements, their push for new norms can have a backlash and inspire counter entrepreneurs such as Thomas Rid

²⁵⁶ See chapter 8 in Gill, Marrin, and Phythian, *Intelligence theory : key questions and debates*.

²⁵⁷ Paul R. Pillar, *Intelligence and U.S. foreign policy : Iraq, 9/11, and misguided reform* (New York: Columbia University Press, 2011).

²⁵⁸ Clarke and Knake, *Cyber war : the next threat to national security and what to do about it*.

²⁵⁹ See chapter 2: “Cyberwar is coming” in Arquilla and Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age*.

who writes that cyber war does not and will not occur.²⁶⁰ Most traditional intelligence push comes from within the Intelligence Community itself.²⁶¹ Because the intelligence community is pushing intelligence not requested by the decision-makers the concept of the intelligence cycle can, as Marrin notes, become linear.²⁶² The reality is likely to be a combination of the two and the eventual decision-making process on what to do based on available intelligence is legally within the hands of the decision-maker.

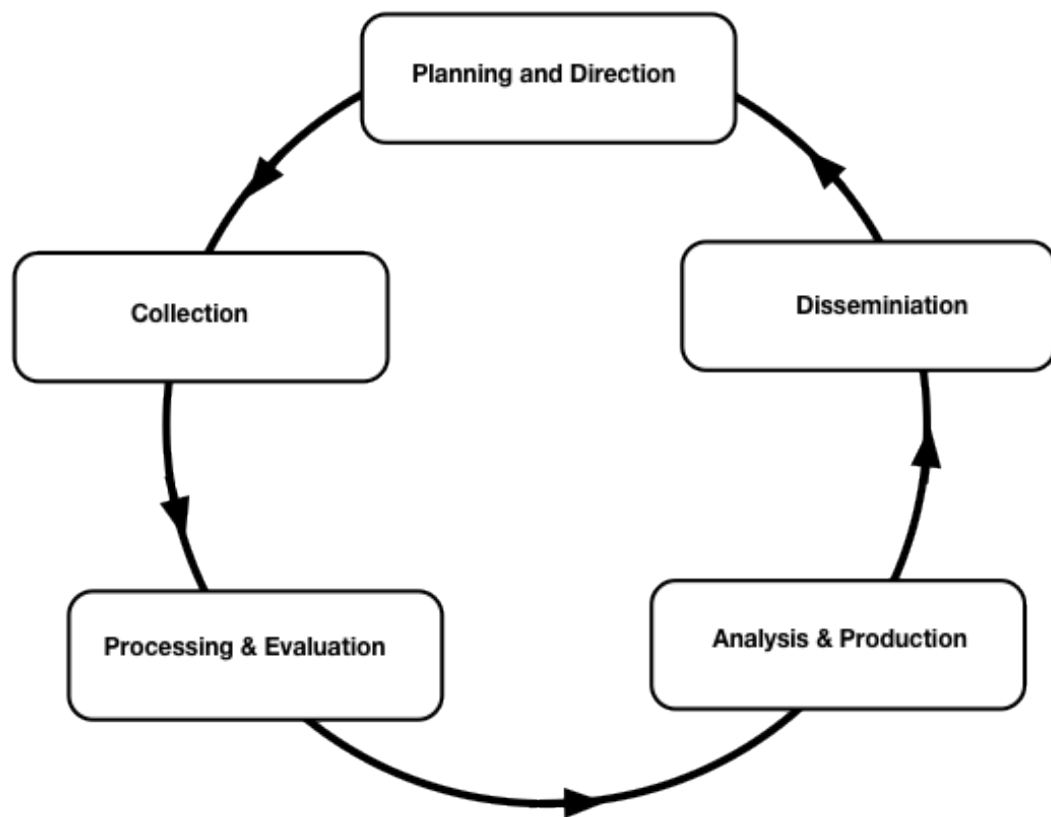


Figure 7.1 The Intelligence Cycle²⁶³

²⁶⁰ Rid, "Cyber War Will Not Take Place."

²⁶¹ See Chapter 8 in Gill, Marrin, and Phythian, *Intelligence theory : key questions and debates*.

²⁶² Ibid.

²⁶³ Adapted from Lowenthal, *Intelligence : from secrets to policy*. See also: Loch K. Johnson, *National security intelligence* (Cambridge: Polity, 2012).

For intelligence to adequately focus its sights on any battlespace, planning and direction from policy-makers must occur. Once policymakers have established the importance of a battlespace the intelligence community must find ways to deliver accurate and reliable intelligence. The objective of intelligence collection is not solely to provide real-time information on the battlespace, rather it is best thought of as battlespace preparation or what Waltz refers to as “intelligence preparation of the battlespace” (IPB).²⁶⁴ Although Waltz specifically refers to IPB in the context of coordinated conventional warfare and the use of information operations in network-centric warfare, the theoretical principles apply across all domains. IPB according to Waltz includes providing an understanding of the “physical, political, electronic, cyber, and other dimensions of the battlespace.”²⁶⁵ Alan Campen reiterates the concept of IPB in *Cyberwar 3.0*.²⁶⁶ Campen states that information warfare requires an accurate knowledge of the battlespace as well as real-time awareness of situations within the battlespace as they arise.

Before moving directly into how each collection type can add to a holistic picture of the battlespace, it is necessary to define what constitutes the battlespace in the cyber domain. The battlespace according to Waltz constitutes “all decision-relevant elements within a defined battlespace, and the ability to predict with very high confidence near-term enemy actions and outcomes.”²⁶⁷ More specifically this requires an understanding of capabilities in the form of human, material, technical and the relationship of these capabilities within themselves and to other aspects of the operational environment. It is also important to understand the political

²⁶⁴ Waltz, *Information warfare : principles and operations*.

²⁶⁵ Ibid.

²⁶⁶ Campen and Dearth, *Cyberwar 3.0 : human factors in information operations and future conflict*.

²⁶⁷ Waltz, *Information warfare : principles and operations*.

implications of alterations in capabilities and the environment over time. A battlespace for cyber can be domestic or foreign. Intelligence must inform policy-makers on both.

Capabilities can be broadly defined as including mechanisms of offensive and defensive military strength such as size and number of offensive cyber units, it can include doctrinal measures or indicators such as official cyber security and warfare doctrines. The capabilities can include the size and complexity of systems and their connections to other systems of importance. And it can include technical capabilities such as programming skill within the environment.

The capabilities matrix included below is overly simplified, yet it indicates a host of areas where the intelligence community can provide significant assistance to decision-makers. What is important to consider is that these capabilities are not limited to the United States or its allies. Capabilities need to be assessed on a nation-by-nation basis and likely on a sub-state basis as well. Together these and many other unmentioned cyber capabilities combine to provide an accurate picture of the battlespace.

Identifying the capabilities and political situation of a new battlespace is difficult under the best of circumstances. Cyber is immensely complicated and therefore necessitates a logical template within which to examine capabilities. There is a need for a differentiation between the domestic (defensive) and the foreign (offensive) battlespace. This distinction is important both for tasking and decision-making. By logically separating the two battlespaces they are able to inform one another. Table 7.2 highlights many of the primary areas for consideration within the two battlespaces necessary for DBA and DBK.²⁶⁸

²⁶⁸ Dominant Battlespace Awareness (DBA) and Dominant Battlespace Knowledge (DBK) see page p152.

Table 7.2 Components of cyber DBA & DBK

Domestic (Defense Oriented)	Foreign (Offense Oriented)
Policy Considerations (Offensive & Defensive)	Policy Considerations (Offensive & Defensive)
Domestic Network Mapping	Foreign Network Mapping
Budget Allocations	Budget Allocations
ICT Collaboration (Alliances, Partnerships)	Offensive Unit Size & Training
Defensive Unit Size & Training	Defensive Unit Size & Training
Critical Infrastructure	Critical Infrastructure
Insider Threats for Defensive Purposes	Insider Threats for Offensive Purposes
Threat Spectrum Capabilities	Historical Record of Attack and Defense
Known Vulnerabilities	Threat Spectrum Capabilities
Time to Attack Recognition	Known Vulnerabilities
Time to Attack Attribution	ICT Collaborations (Alliances, Partnerships)
Systemic Dependencies	Time to Attack Recognition
Monitoring	Time to Attack Attribution
	Systemic Dependencies
	Surveillance
	Reconnaissance

The INTs from the previous section of this paper can and should be focused on these and related areas within the cyber domain. A holistic picture of the above components of the domain will provide decision-makers with a clear visualization of the battlespace. Again following Waltz,²⁶⁹ a visualization of any battlespace includes:

1. Developing a clear understanding of the state with relation to the enemy and environment
2. Envisioning a desired goal or objective representing the successful completion of the mission.
3. Visualization of the sequence of activities that move the current state to the desired state.

Edward Amoroso argues the intelligence community should focus on creating an addition to the conventional intelligence briefs that consists solely of information pertaining to cyber.²⁷⁰

Amoroso indicates such a report should focus on: *current security posture, top and new security*

²⁶⁹ Waltz, *Information warfare : principles and operations*.

²⁷⁰ Amoroso, *Cyber attacks : protecting national infrastructure*.

risks, automated metrics, human interpretation (emphasis in original).²⁷¹ Amoroso's case for the creation of a cyber specific intelligence is sound and works towards promoting an accurate and realistic understanding of the threats, and opportunities within this new and evolving domain relevant to national security.

Policy considerations

The Joint Chief's of Staff have placed an increasing emphasis on the cyber domain within various joint doctrine publications. These joint doctrines provide insight into both the needs of the services and policy-makers in the employment of, and defense against cyber attacks. These documents also include many of the ways cyber has come to rely heavily on intelligence assets. Information dominance has become a mission critical aspect of defending national security. The Joint Doctrine for Command and Control Warfare dating back to 1996 highlights the importance of intelligence products in support of C2W. The document indicates that the use of intelligence assists in the conceptualization of all aspects of a battlespace.²⁷²

Comprehension of any battlespace, including the cyber domain, requires understanding the policy environment in which an action takes place. Is there a national cyber defense strategy within the targeted country? How have they publicly or privately declared they would respond to hostile actions within the cyber domain? An example of the policy environment can be found in the Department of Defense Strategy for Operating in Cyberspace. The strategy outlines five strategic initiatives in its declassified report.²⁷³

²⁷¹ Ibid.

²⁷² "Joint Doctrine for Command and Control Warfare (C2W)," ed. Joint Chiefs of Staff (Washington, D.C.: Department of Defense, 1996).

²⁷³ "Department of Defense Strategy for Operating in Cyberspace."

Strategic Initiative 1: Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential

Strategic Initiative 2: Employ new defense operating concepts to protect DoD networks and systems

Strategic Initiative 3: Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy

Strategic Initiative 4: Build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity

Strategic Initiative 5: Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation

The classified sections of the report cited in the media indicate a doctrinal shift in the way the DoD approaches the cyber domain. These journalistic accounts write the DoD finds that some instances of cyber attacks can constitute an act of war.²⁷⁴ The understanding of the policy positions within the domestic battlespace and in the foreign battlespace will help to alleviate information asymmetries and establish clearly identifiable patterns for response. Whether it is the knowledge that Germany and Holland both have official cybersecurity doctrines or that China has begun implementing a policy of making offensive cyber capabilities a strategic priority, the overt and covert collection of policy positions provides decision-makers a foundation on which to understand intelligence related to cyber.

Policy platforms also help to codify international law, to create zones of norms or an identifiable policy framework in which states will interact or respond within to incidents emanating from cyberspace.²⁷⁵ While both the United States and Russia have made known a cyber attack could constitute an act of war, there has been little elaboration on specific characteristics of such an attack. Often states will intentionally leave room for policy ambiguity

²⁷⁴ Siobhan Gorman and Julian E. Barnes, "Cyber Combat: Act of War," *Wall Street Journal*(2011), <http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html>.

²⁷⁵ Brenner, "'At Light Speed': Attribution and Response to Cybercrime/Terrorism/Warfare."

as a mechanism of deterrence.²⁷⁶ Understanding ambiguity, information gaps, and information asymmetry is crucial particularly in comprehending how leaders arrive at decisions. As such, just as in conventional warfare, in cyber conflict the minimization of, or the knowledge about what a potential adversary will do in a given situation provides a strategic edge.

CNE - Network Mapping, Systemic Dependencies, and Historical Records

Understanding the policy environment both domestically and among foreign adversaries is only part of the larger intelligence process. Computer network exploitation (CNE) constitutes a series of technological and analytical approaches to cyber specific espionage. CNE for the purposes of conventional intelligence collection can include the penetration of foreign networks to secure information on weapons systems, policy positions, and much more. CNE is invasive, but does not disrupt, deny, or destroy data, it collects. When CNE operations focus intelligence on the cyber domain for offensive and defensive purposes the objective is to understand the systems themselves. The goal becomes identifying the strengths and weaknesses of systems, the connectivity of systems to points of interests, and the interaction of those systems with strategic and tactical objectives.

There are numerous methods of CNE; for the purposes of simplicity only a few will be examined. Network mapping is a form of CNE that studies the physical connectivity of networks or the availability of insecure ports. This type of mapping provides information on what types of systems and servers operate on different networks and identifies the characteristics of the various component parts these systems constitute. Network mapping can drill down to very low levels of on particular networks and provide significant information. This information can then be used to isolate portions of networks to pick at vulnerabilities.

²⁷⁶ Brian M Mazanec, "The Art of (Cyber) War," *The Journal of International Security Affairs* 16, no. Spring (2009).

Network mapping is also useful for illustrating the potential for any particular targeted attack to extend beyond its directed target and result in collateral damage or blowback. Conceptually network mapping is not dissimilar from attempting to map radar or surface to air missile locations prior to a bombing campaign. The intent of network mapping to gain an operational knowledge of an adversary's systems prior to engaging in hostilities. Figure 7.2 illustrates a comprehensive network map with a focused section pulled out. The numbers in the pulled out section are IP addresses of devices connected within the focused network. Such a tool is critical to understanding how potential cyber weapons will function within a networked environment.

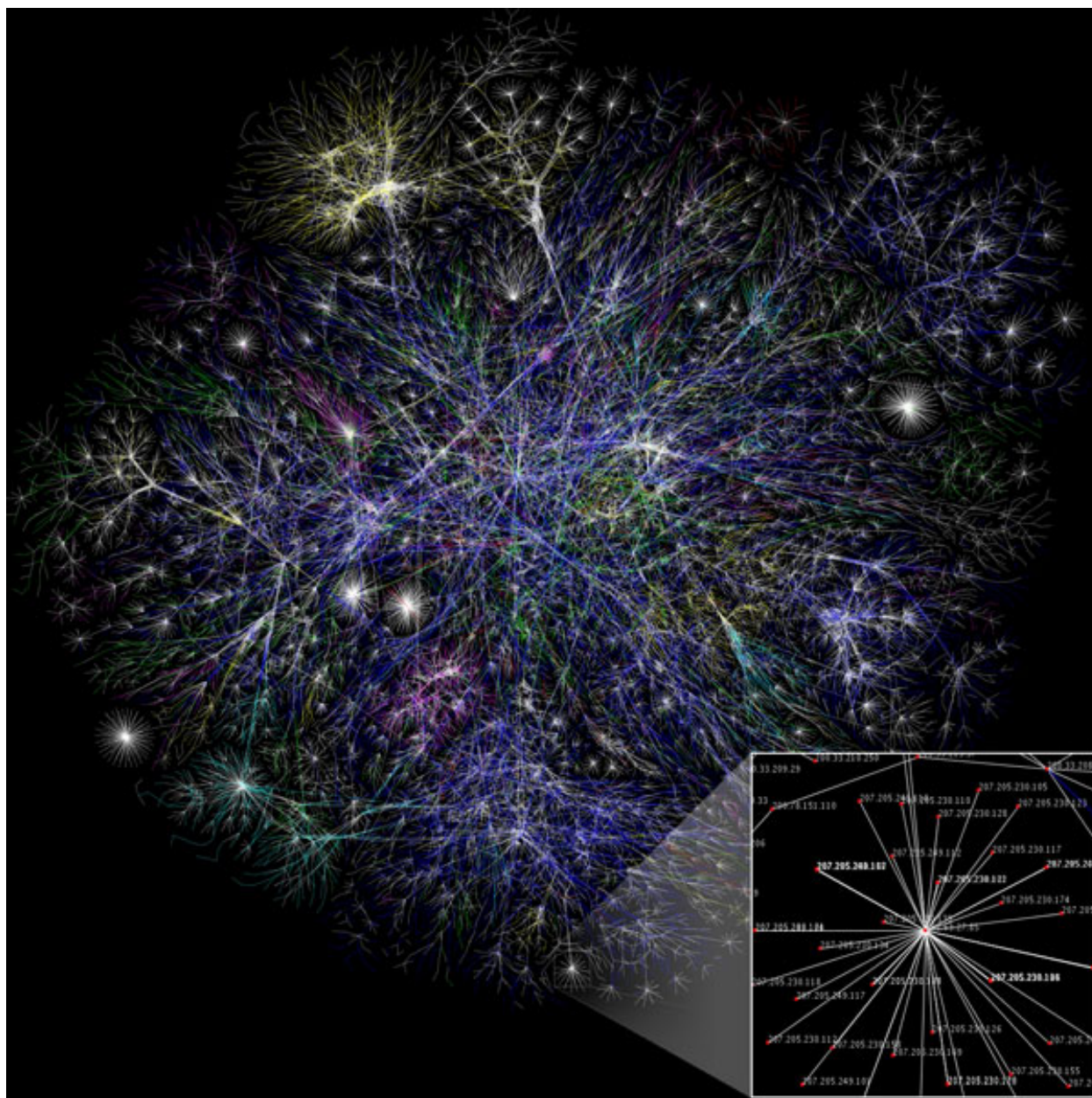


Figure 7.2 Detailed Network Map²⁷⁷

The forensic analysis of the Stuxnet worm found that the worm partially made use of network mapping to target its attacks and focused on isolated networks using memory sticks as the initial method of transmission.²⁷⁸ Once in, Stuxnet focused its attack on networks with

²⁷⁷ The Opte Project, "Internet Map," in *Graphviz* (<http://www.opte.org/maps/>: The Opte Project, 2005).

²⁷⁸ Falliere, Murchu, and Chien, "W32.Stuxnet Dossier."

Programmable Logic Controllers (PLCs) of a specific type²⁷⁹ and caused uranium enrichment centrifuges to malfunction.²⁸⁰ The level of sophistication required to drill down to get to this level of detail to plan an attack is remarkable particularly when one considers the complexity and number of overall systems and that the Iranian systems appear to have been air-gapped.

Network mapping is both an offensive and defensive intelligence endeavor. To adequately prepare both the defensive and offensive battlespaces, an accurate picture of systems is needed. Arguably the dual domestic-foreign pictures are complimentary and help to avoid violating part 2.13 of Executive Order 12333, which prevents any covert action from influencing U.S. political processes, public opinion, policies, or media.²⁸¹

Network mapping and monitoring is a double-edged sword. Legally network mapping can be considered CNE and therefore domestic network mapping by U.S. intelligence agencies without a warrant would be prohibited. However, network mapping is of critical importance to the maintenance of national security infrastructures. Thus far the Intelligence community does not have a formal commitment from the White House or the Justice Department to engage in any domestic CNE operations.²⁸² Currently in the United States there is an uneasy public-private commitment to providing information on network security across critical infrastructure. A thorough understanding of domestic and foreign networks assists in visualization for both offensive and defensive purposes and efforts to push reasoned analysis of threats has begun to make its way into Congress.²⁸³

²⁷⁹ The PLCs affected were Siemens S7-315 and S7-417

²⁸⁰ Paulo Shakarian, "Stuxnet: Cyberwar Revolution in Military Affairs," *Small wars Journal*(2011).

²⁸¹ Ronald Reagan, "Executive Order 12333-United States intelligence activities," ed. Office of the President (Washington: US Federal Register, 1981).

²⁸² Ellen Nakashima, "White House, NSA weigh cybersecurity, personal privacy," *Washington Post*, Feb 27, 2012.

²⁸³ Ibid.

In addition to network mapping CNE operations explore systemic vulnerabilities. Mapping the network provides information on the various component parts of a network and their availability. Once the components are known it becomes necessary to explore areas of vulnerability within these systems. Often these types of vulnerabilities are referred to as Zero-day vulnerabilities. Zero-day vulnerabilities are vulnerabilities in computer applications that even the system administrators are unaware of. The Stuxnet attack exposed a Zero-day vulnerability in the software of the PLCs causing the centrifuges to spin outside of their safe operational standards.



Systemic vulnerabilities necessitate a thorough understanding of the historical record of different types of attacks and exploits. The identification of Zero-day vulnerabilities should lead network administrators to immediately patch these gaps. Intelligence plays a role in identifying what types of attacks have been used in the past and what vulnerabilities these attacks attempted to exploit. This historical accounting is important for both offensive and defensive preparation of the battlespace. For obvious reasons it is important to prevent repeat attacks on domestic systems, at the same time it is important not to engage in repeat attack methods once a vulnerability on an opposing system has been fixed. Such an attack would likely be ineffective and lead to anonymity-attribution problems.

The historical accounting of attack types by countries and sub-state actors also alerts operators within the intelligence community to the threat spectrum capabilities of a particular cyber adversary. Understanding the threat spectrum capabilities of states facilitates and accurate conceptualization of their power to operate within the domain. Table 7.3 is a representation of known threat spectrum capabilities. The historical record of these capabilities indicates the

effectiveness of cyber unit training and the motivations of a state. The further a state progresses along the spectrum the more dangerous it becomes in the cyber domain.

The above areas of consideration within CNE are only a small sampling of the overall tasking priorities for intelligence using CNE methods. They hint at a broad applicability for CYBERINT methods in the preparation of the battlespace. The information provided by a systematic study and analysis of intelligence from the cyber domain facilitates a more accurate and reasoned understanding of defensive and offensive actions.

Table 7.3 Cyber threat spectrum

Levels (Types) of Attack	Description	Feasibility High	Complexity Low
Propaganda	The propagation of information via the internet to affect public, private or governmental opinion. This can be combined with web vandalism		
Web Vandalism	The defacement of websites either official or private for non-political or political purposes		
Denial of Service Attack (DOS)	The denial of service to a user or users of a computer, server, website, network or system		
Distributed Denial of Service Attack (DDOS)	The denial of service to a user or users of a computer, server, website, network or system – this type of attack is similar to a DOS attack but is distributed across a botnet or other computer systems remotely activated		
Computer Network Exploitation	The secret collection and reproduction of digital data from computers or networks		
Equipment Disruption	The disruption or interception of communications or information flow from systems		
Critical Infrastructure	The targeted disruption of systems designed to provide for or maintain critical infrastructures of vital importance – systems include power, water, fuel, communications, commercial and transportation		
Compromised Hardware Systems	The implantation of malware designed to affect systems in the production phase of a product		
This is not an all inclusive threat spectrum.		Low	High

Conventional Intelligence

Intelligence collected on budgetary allocations, offensive and defensive cyber unit sizes and training methodologies provides the clearest parallel to conventional intelligence. As in conventional intelligence, most countries are frequently unwilling to release their absolute military expenditures or the sizes of their individual force structures within their military. Military capabilities are a closely guarded secret in many, but not all countries. These capabilities are particularly secretive in the cyber domain for the reason that if capabilities are exposed they are no longer capabilities. Once the initial wave of Stuxnet attacks occurred, defensive measures were taken to “plug” the holes the Stuxnet attack employed. This dramatically reduces the effect a repeat Stuxnet attack would have on any other nation. Whereas a missile can continuously be launched with repeated success because the ability to defend against a moving projectile is difficult, a similar cyber weapon is more easily defended against once it has been identified. Anti-virus software can be reprogrammed to identify and isolate repeat threats.

One of the best reports on cyber capabilities of a foreign state available in the public domain comes from Stokes et al.²⁸⁴ Stokes et al. go into explicit detail on the construction, location, leadership, and mission of many aspects of the Chinese People’s Liberation Army information warfare programs. Their report is an example of high value detailed analysis that could be supplemented by conventional intelligence to enhance policy-maker and combatant commander comprehension of the battlespace.

The implications for conventional intelligence collection methods indicate that intelligence on cyber does not necessarily need to remain cyber bound or exclusively within the

²⁸⁴ Mark A. Stokes, Jenny Lin, and L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," (Arlington, VA: Project 2049 Institute, 2011).

realm of CNE. Some of the same metrics, such as force size matter in the cyber can be examined to create a better assessment of potential adversaries. Cyber force size is particularly important from a malware development perspective. Complex coding scripts typically take large numbers of programmers to develop and test. The ability for an individual to pull off highly complex attacks is possible but less likely than a large cyber warfare unit all working with the same objective. Likewise knowing where a unit is located or how they were trained can help planners determine the best response to a particular attack, or how best to manipulate their organizational structure. This is what Derek Clark and Kai Konrad refer to as identifying the weakest link.²⁸⁵ The identification of the weakest link is particularly important in cyber defense and offense. There are multiple fronts (systems) needing defense. All it takes is one “best shot” to achieve significant damage. While this weakest link can be identified through CNE operations identified in the previous section, it can also be identified within the training, command, and organizational structure of units charged with conducting or protecting against cyber attacks.

Closely related to the conventional military metrics above, but likely unique to the cyber domain are public-private ICT collaborations. Although most countries have programs for military public and private collaborations with universities and businesses for research and development, within the cyber domain the importance of this relationship is magnified for multiple reasons. First, much of the training and education necessary to conduct offensive or defensive CNO within cyberspace is, or can be learned at public institutions or can be crafted for private sector use. This extends far beyond the development of technology to the actual training of the warfighter, the development of the platforms upon which the domain rests, and more. Second, these collaborations spread out, but do not diffuse potential vulnerabilities. It is unlikely

²⁸⁵ Derek J. Clark and Kai A. Konrad, "Asymmetric Conflict: Weakest Link against Best Shot," *The Journal of Conflict Resolution* 51, no. 3 (2007).

that any modern army will turn to a university or corporation to teach their soldiers how to fire a gun. The same is not true for a warrior training to defend or attack within the cyber domain.²⁸⁶

Because collaborations can form the foundational aspects of not only the cyber warriors within offensive and defensive units, they can train and equip and prepare national security in ways far different from conventional military means. Most countries have a balance between civilian and military protection of their national cyber infrastructures based largely on the development of Computer Emergency Response Teams (CERTs). An intelligence assessment of the strength and quality of ICT collaborations is of critical importance in understanding the cyber battlespace.

ICT collaborations are not necessarily official and do not need to be highly structured and regimented. Alexander Klimburg provides evidence that Russia and China are in the process of generating cyber power by creating plausibly deniable cyber attackers.²⁸⁷ Creating an accurate open source measure of unofficial collaborations is difficult at best and down right impossible in most situations. An intelligence focus on unofficial collaborations with entities can contextualize cyber incidents such as the 2007 cyber attacks against Estonia.²⁸⁸ The 2007 attacks were directed at Estonian governmental, bank, and communications websites.²⁸⁹ The attacks were instigated by a decision to move a Russian war memorial from central Tallinn. While initial reports indicated Russia was the culprit, Russia denied any participation in the cyber attacks.²⁹⁰ The reality is

²⁸⁶ There are training programs sponsored by the Department of Defense at Dartmouth, Carnegie Mellon, and at the various national laboratories to name just a few of the many programs available.

²⁸⁷ Alexander Klimburg, "Mobilising Cyber Power," *Survival* 53, no. 1 (2011).

²⁸⁸ Landler and Markoff, "Digital Fears Emerge After Data Seige in Estonia."

²⁸⁹ "Europe: A Cyber-Riot; Estonia and Russia," *The Economist*, May 12 2007.

²⁹⁰ Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia," *The Guardian*(2007), <http://www.guardian.co.uk/world/2007/may/17/topstories3.russia>.

somewhat murkier and more akin to an unofficial sanction or condoning of cyber attacks by the Russian government.²⁹¹

The collection and production of intelligence on these above more conventional attributes of pertinence to the cyber domain are a role the intelligence community is likely already engaged in. Occasionally reports on issues relating to this category of intelligence are published for public consumption. A recent report of this type was produced for the U.S.-China Economic and Security Review Commission to examine China's capability to conduct cyber warfare and computer network exploitation.²⁹² Knowledge of capabilities is still applicable to the cyber domain and is greatly influenced through intelligence collection using conventional intelligence collection methods and subsequent analysis, which contextualizes the meaning the raw intelligence.

HUMINT and Cyber

Human intelligence (HUMINT) stands out in cyber for two particular reasons. First, HUMINT agents can provide accurate internal information on systems and access to those systems unavailable through CNE and other intelligence collection methods. Second, human assets can serve as a bridge between the external world and air-gapped or other forms of secure networks. As was indicated above, it is likely that the Stuxnet virus was distributed using a thumb drive which needed to be inserted into a machine within an air-gapped network. HUMINT agents can serve as a vulnerability most network administrators will be unable to provide significant protection against.

The role of a HUMINT asset with access to information on networks can be extremely damaging. Even if the agent is on a lightly classified network, the repercussions of his or her

²⁹¹ Klimburg, "Mobilising Cyber Power."

²⁹² Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," (McLean, VA: Northrop Grumman Cooperation 2009).

actions can be enormous. The Wikileaks scandal caused by Bradley Manning leaking more than 260,000 diplomatic cables is illustrative of the problem posed by internal threats.²⁹³ These threats need to be developed and enhanced for offensive intelligence and protected against for domestic national security counterintelligence. Gaining access to the technical schematics, documents, information, login procedures, or any of a multitude of other targets of intelligence, a HUMINT asset could provide are critical aspects added directly by intelligence to the understanding of the cyber domain.

Beyond the collection of intelligence from HUMINT sources, these insiders can assist in the implementation of cyber actions. Information within a 2005 report by the United States Secret Service in cooperation with Carnegie Mellon indicated that up to 29% of all attacks against a surveyed group of critical infrastructure stakeholders were initiated by insiders.²⁹⁴ The majority of motivations behind these attacks were not intelligence or covert action related. This, however, does not preclude the possibility of using insiders to affect or gain information-access on adversary systems. The recruitment and maintenance of insider threats by the intelligence community should likely be a top priority. These agents can offer a mission critical component often during times when more lengthy intelligence collection processes are constrained by events.

Time to Attack Recognition, Completion, and Attribution

As has been discussed, attack recognition and attribution are critical for both a defensive and offensive battlespace planning. All of the intelligence collection methods and the focus of the Intel process of trying to understand the cyber domain culminates in understanding, from a mission critical orientation, the progression of cyber attacks. Figure 7.3 is a simplified model for

²⁹³ Brenner, *America the vulnerable : inside the new threat matrix of digital espionage, crime, and warfare*.

²⁹⁴ Keeney et al., "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors."

understanding attack planning and progression within a battlespace modeled loosely on the JP 3-51 electronic warfare-planning model.²⁹⁵ This model is informed by intelligence collection. Line one of the figure indicates a policy-maker's perspective on the process of engaging in conflict. A conflict initiation is (0) planned, (1) implemented, and (2) completed. Policy-makers want to know what resources any given action will take and how long it will take to complete it. In cyber a more accurate timeline for action in cyberspace requires (0) intelligence collection, (1) operational planning of the attack with an informed knowledge of the battlespace, (2) understanding of the time it takes for the attack to be completed, (3) how long until the attack is recognized as an attack by the adversary, (4) how long until that adversary can do something about the attack, (5) how long until the adversary assigns attribution for the attack. The ordering of the items listed above greatly affects the ability for an attack to be conducted successfully.

Intelligence informs the policy-maker and the combatant commander as to the feasibility of a particular type of attack and the probability of success. If recognition of an attack occurs early in the timeline of events the probability of success is diminished.

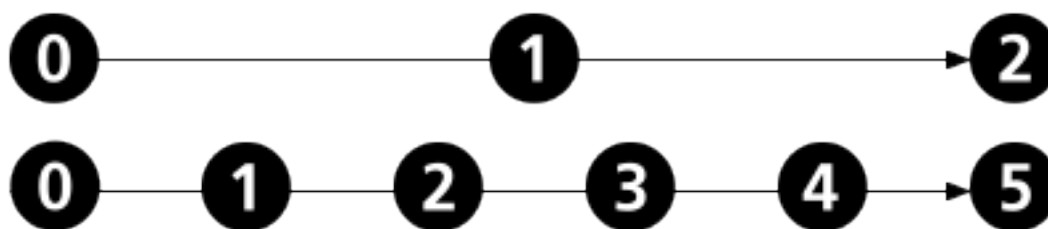


Figure 7.3 Timeline for attack implementation

The timeline can be tested in much the same way conventional weapons are tested. It would be absurd to send a bomber over a potential target with a completely untested bomb, or to send a soldier into battle with an untested model of rifle. Just as weapons are tested in the

²⁹⁵ "Joint Doctrine for Electronic Warfare Joint Publication 3-51," ed. Department of Defense (Washington, D.C. 2000).

physical world they need to be tested in the cyber as well. This testing provides added information to both the policy-maker and the combatant commander as to the effectiveness of the weapon and the timeline of events above. If a cyber weapon is slow and easily detectable its probability for success is diminished. This lowered probability for success does not nullify its use but it does condition it.

One aspect of this phase of IPB is that it is extremely beneficial to both the offensive and defensive strategic and tactical operations. By planning and testing potential attacks against theoretical adversarial systems, the intelligence community provides the much needed out of the box perspective necessary to prevent similar attacks against domestic targets. This logic would indicate that an attempt to use a worm like Stuxnet against the U.S. infrastructure would run into greater problems than if the weapon had been developed first elsewhere.

IPB and its impact on cyber

The role of intelligence in cyber is not dissimilar from its role in the conventional domains. There are new areas in which collection and analysis need to occur but its overall objective remains the same. Returning to Waltz's concept of information preparation of the battlefield, Figure 7.4 illustrates the influence accurate intelligence can have on operations originating within the cyber domain. The role of intelligence in cyber is to accurately facilitate understanding of and the possible tools by which to influence those entities. The cyber domain is surrounded with hype and hysteria. Many of the claims are accurately based in reality. But the known unknowns are still enormous within this evolving domain and it is incumbent on intelligence to provide an accurate assessment of the current state of affairs.

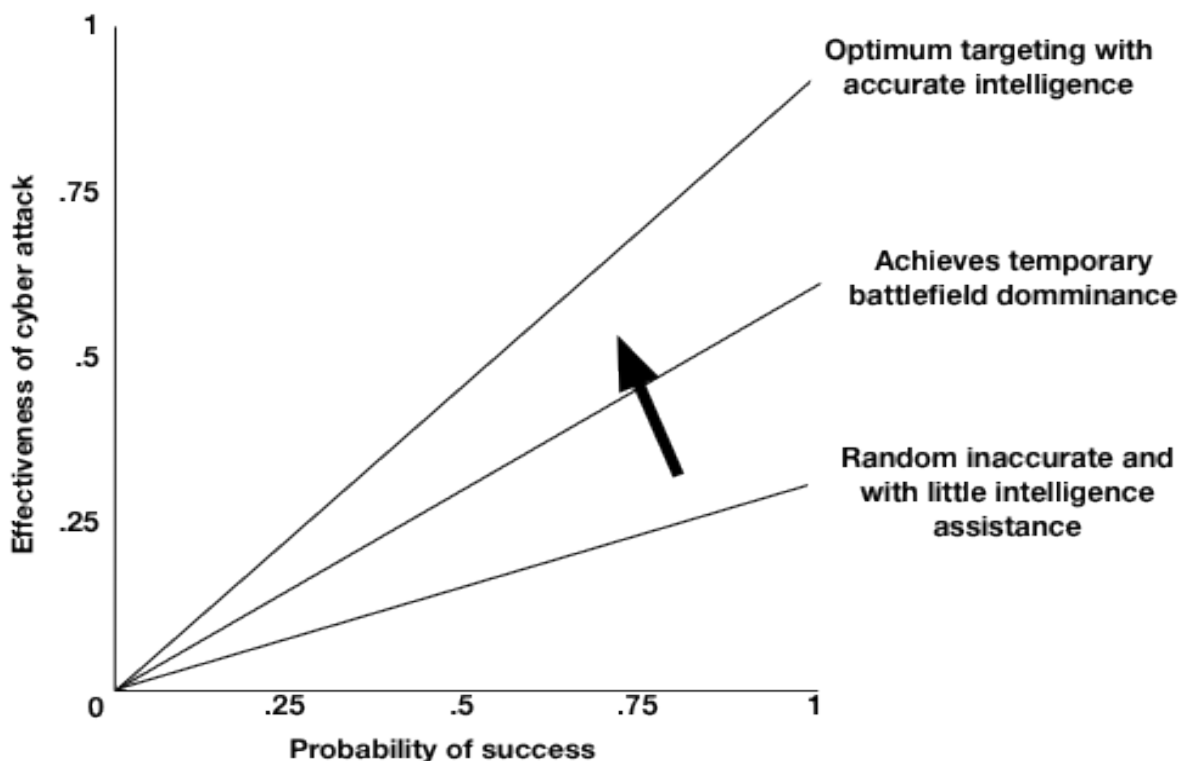


Figure 7.4: The influence of intelligence on cyber operations.²⁹⁶

All source intelligence for cyber requires the intelligence community to think beyond domestic system defense. The focus should be balanced between the foreign and domestic intelligence because they mutually inform one another and create a better systemic defense for national assets as well as provide decision-makers with a more accurate picture of how a potential cyber attack might succeed or fail.

Cyber as Covert Action

To further define the role of intelligence in cyber, it is necessary to look more deeply into the laws codifying the conduct of the intelligence community. All of the above sections provide a framework for defining the role of intelligence with regards to IPB. But, cyber conflict is by its

²⁹⁶Modified from Waltz, *Information warfare : principles and operations*.

very nature covert. Even if the attack is discovered most often attribution is unavailable. More often than not attacks are designed to go unnoticed and affect changes to systems and their components for days, weeks, or months without detection. Even in the instances where groups such as Anonymous publically take credit for their attacks, they typically only do so after the fact. Virtually all examples of state-on-state cyber attacks have been covert. If a potential victim knows an attack is imminent, protection is more likely.

The covert nature of cyber brings us full circle to Warner's definition of intelligence as attempting to influence. Covert action is a secret operation to influence a foreign entity. At least in theory, most, if not all, cyber attacks begin covertly. Under section 1.7(a)(4) of Executive Order 12333 regarding the Intelligence community elements concerning covert action and states:

*"Conduct covert action activities approved by the President. No agency except the Central Intelligence Agency (or the Armed Forces of the United States in time of war declared by the Congress or during any period covered by a report from the President to the Congress consistent with the War Powers Resolution, Public Law 93-148) may conduct any covert action activity unless the President determines that another agency is more likely to achieve a particular objective;"*²⁹⁷

Already evident in the structuring of the governmental response to cyber covert action, the Department of Defense has taken the lead with General Keith Alexander as the head of both NSA and Cyber Command. This indicates the President has established an agency other than the Central Intelligence Agency as the primary covert operator within this domain. While the logic behind having military intelligence organization commander and an organizational structure that falls under STRATCOM runs counter to EO 12333, the institutional capacity of the DoD in the

²⁹⁷ Sec 1.7(a)(4), in Reagan, "Executive Order 12333-United States intelligence activities."

technical domain and the scale of the problem being faced within this new domain make the assignment appropriate.

Utility and Cyber Intelligence

Just as intelligence influences the construction of probabilities for success in conventional conflict it can also inform decision makers for cyber conflict. Because the construction of the domain is significantly different from conventional domains of land, sea, air, and space, it necessitates the addition of the above characteristics. When Bruce Bueno De Mesquita outlined the construction of probabilities in his original utility theory of international conflict he defined the probability of success in conflict based on identifiable attributes commonly examined in conventional intelligence collection and analysis.²⁹⁸ Within the cyber domain conventional capabilities do not compute the same way with regards to cyber conflict. For cyber conflict it is necessary to consider the role of attribution and anonymity and how they affect the probability of success, furthermore cyber imposes time constraints.

Intelligence can affect the development of power scores and examine the levels and types of vulnerabilities used to assess the probability of success in any type of conflict. In cyber conflict the power score that influences probability of success is influenced by the all-source collection of intelligence scaled against the vulnerabilities of the state and is conditioned on the estimated probability of remaining both anonymous and unattributed. This is why the foreign and domestic aspects of the cyber domain influence one another. The greater the number of vulnerabilities present on the domestic side of the equation the lower the probability of success in a cyber conflict will be against an equally paired adversary.

Beyond the way in which intelligence influences the development of the relationship between the offensive and defensive capabilities and their ability to predict the probability of

²⁹⁸ Bueno De Mesquita, *The war trap*.

success in the way conceptualized by Bueno De Mesquita, they must also be scaled against the anonymity attribution issues listed above. Because virtually all cyber action is covert its probability for success is dependent on how long it can stay covert in order to accomplish its stated objective. Furthermore, because an action that begins covertly is best-kept covert or at least plausibly deniable intelligence and assist in assessing the time frame in which an attack will also remain unattributed. Intelligence through all source analysis influences all aspects of this utility construction process. First, it assists in defining capabilities and vulnerabilities for both offense and defense. Second, it assists in doing the same for potential adversaries.

Summarizing the role of intelligence within the cyber domain

In defining the role of intelligence within the cyber domain it is necessary to take a holistic approach. From a collection perspective, the intelligence community should and has been working in coordination with a hybrid push and pull intelligence cycle to both elevate the importance of this domain and to facilitate collection within it. The emphasis has been heavily defensive up to this point and largely focused on countering threats rather than anticipating them. This needs to change. The only way this can change is if the intelligence community begins to actively turn its sights on adversaries and develop more rigorous all-source intelligence combining novel CYBERINT technologies to augment reporting on this domain. Parroting Amoroso's assertion, cyber should be included on the daily intelligence briefs of policy-makers. The inclusion would likely start the process of demystification of this immensely complicated domain.

Cyber is a domain that can be used to fulfill all aspects of Warner's definition of intelligence to some degree. It is a domain in which we can gain understanding about other states beyond and within the domain itself, but it is also a domain that can serve to influence other

states' policy decisions as well as perceptions. In particular, accurate intelligence on both sides of the domestic-foreign divide can mutually inform decision makers about vulnerabilities and the eventual decision to use cyber as an offensive weapon or how best to defend against attacks. Furthermore, intelligence can reign in the debate on cyber to a more realistic area of operations predicated on sound estimates rather than on grandiose speculation.

The intelligence community itself is and rightly should be the point of origin for hostile actions emanating from the domain and will likely serve as a force multiplier in instances where a combined conventional cyber attack is necessary. To engage in cyber conflict, just as in conventional conflict, intelligence is needed to prepare the battlespace and facilitate an accurate assessment of the probability for success and utility for any type of operation. This preparation hones the weapons, decisions, and effect of a potential attack. More importantly for national security, a thorough and accurate preparation of both the foreign and domestic battlespaces will serve to inform one another and enhance cyber security.

Part III

A formal decision-making model for actions within the cyber domain

CHAPTER 8

How actors decide to use cyber - a rational choice approach

“Man is a rational animal-so at least I have been told. Throughout a long life I have looked diligently for evidence in favor of this statement but so far I have not had the good fortune to come across it.”

~ Bertrand Russell²⁹⁹

Rationality is predicated on assumptions. These assumptions when applied beyond the domain of pure economic theory pose philosophical problems. To apply rationality it is necessary assume the world is simpler than it actually is. This simplification or theoretical conceptualization of the world is helpful and dangerous. Virtually all social science to some extent makes an effort to simplify the world through the construction of theories. When attempting to understand decisions in any context it is important to focus on casual factors.

The causal variables within economic theory directly influence the value assigned to different options. In social science the values assigned are not easily quantifiable. Whereas in economics the value of a product can be determined by inputs, supply and demand, and expectant value all measured by tangible monetary amounts, in political science the inputs and outputs are often more ambiguous in nature. Some studies attempt to rigorously quantify the inputs by looking at aggregate numbers of materials and derive from these raw numbers assumed capabilities; others take a more nuanced approach and focus on the component aspects of the raw materials and attempt to assess capabilities on how the parts combine to make the whole. This chapter examines the development of a rational choice approach to decisions within the cyber

²⁹⁹ Bertrand Russell, *An outline of intellectual rubbish ; a hilarious catalogue of organized and individual stupidity* (Girard, Kan.: Haldeman-Julius publications, 1943).

domain by focusing on how a combination of raw numbers can lead to a rational choice. A decision maker can create, with these numbers, inputs into a mathematical model resulting in a degree of objectivity, making it possible for a rational choice between alternative options.

Part II focused on the constituent aspects for determining probability of success within the utility model for state actors within cyber. Previous chapters have examined such concepts as power, vulnerability, anonymity, and intelligence as variables influencing the probability for success. Each of these factors is an integral part of the larger utility calculation for interaction within the cyber domain. Although previous chapters all focused on developing a thorough understanding of the cyber domain and what it entails, it is now necessary to hone in on the decision process, to examine cases, and develop the rational model for cyber decision-making.

Focusing now on the cyber decision-making model this chapter moves forward in four steps. First, what is rationality? Second, how do risk and uncertainty play a role in decisions? Third, what is the model for bilateral expected utility of cyber conflict? Lastly, this chapter concludes by explaining how this utility formula is applied moving forward. In part this chapter reiterates and reinforces some concepts from previous chapters, it is, however, intended to re-orient the reader specifically on the mathematical construction of a decision in a social science context.

Rationality

Rationality is a common concept in both economics and international relations and it is not necessary to reinvent the wheel. This work uses John Von Neumann and Oscar Morgenstern's fundamental characteristics of rationality defined as:³⁰⁰

1. *Completeness* - for any two simple lotteries A and B , a choice must be either $A \geq B$ or $A \leq B$ (or both).
2. *Transitivity* - for any three lotteries A, B, C , if $A \geq B$ and $B \geq C$, then $A \geq C$.

³⁰⁰ Von Neumann and Morgenstern, *Theory of games and economic behavior*.

Although there are other more detailed aspects that can be added to the above definition of rationality those are the two central assumptions. The two central assumptions of rationality above constitute the foundation of utility theory as explained by Bruce Bueno de Mesquita. Bueno de Mesquita states utility theory essentially constitutes the following aspects: ³⁰¹

1. *Individual decision-makers order alternatives in terms of their preferences;*
2. *The order of preferences is transitive so that if A is preferred to B and B p C (where p is to be read as "is preferred to") then A p C;*
3. *Individuals know the intensity of their preferences, with that intensity of preference being known as utility;*
4. *Individuals consider alternative means of achieving desirable ends in terms of the product of the probability of achieving alternative outcomes and the utility associated with those outcomes; and*
5. *Decision-makers, being rational, always select the strategy that yields the highest expected utility.*³⁰²

Rationality is essentially consistent across decision-making models. There are forms of bounded or conditional rationality, which limit the information available to actors, however, within these models the basic tenets expressed above are consistent. Whether a rational choice is being made in conventional warfare, diplomatic negotiations, or in cyber conflict, the core assumptions of rationality remain the same.

With the basic tenets of rationality above in mind it is important to provide several additional clarifications relating to the model developed within this work. (1) Decision makers are regarded as a unitary single actor. This principle was illustrated in the first chapter and in several subsequent chapters. This is necessary to avoid Arrow's impossibility theory stating: when three

³⁰¹ Bruce Bueno de Mesquita, "The Contribution of Expected Utility Theory to the Study of International Conflict," *The Journal of Interdisciplinary History* 18, no. 4 (1988).

³⁰² As is noted by Bueno de Mesquita and others there are cognitive dimensions of choice that can influence this aspect of rationality as demonstrated in: Kahneman and Tversky, "Prospect Theory: An Analysis of Decision under Risk."

or more distinct options are available, no community-wide system can convert the ranked preferences of individuals (multiple) into an aggregate - complete and transitive - rank order.³⁰³

Because of a focus on a unitary actor decision maker this model is confined to those entities, which employ a single unitary decision maker on matters relating to the instigation of cyber attacks. This eliminates groups such as Anonymous, which function as collective decision-making entities and do not fulfill the requirements of rationality. Groups that do not function with a unitary decision maker likely cannot be examined as rational actors and therefore the utility construction of these actors would serve little ultimate purpose.

(2) Preference orderings are able to incorporate aspects relevant to the cyber domain. Just as conventional conflict can incorporate variable factors defining the value of options for a given choice, cyber variable can also influence the value of potential options within a given decision.

(3) A common misperception is that value for preferences of an actor instigating conflict must be related to the values assigned by the target of a conflict initiation. Such an understanding would indicate two states engaging in a conflict both have an identical understanding of the ex-ante choice. As this would violate Arrow's theorem it is important to recognize that a decision whether overt or covert is predicated on the preferences of the individual actor, not on the dyad. This means it is not necessary for both actors to consider conflict initiation rational for conflict to occur. This is particularly important in cyber as it is a covert act.

These three additional considerations are not unique to the cyber domain, yet are highlighted here to prevent any misunderstandings about what the decision-making model is illustrating. The rational choice for an actor is predicated on the utility of the options available to it. The actor then creates a rank order model based on the value of each option. This choice functions independent of the utility construction of options for a potential opponent. A divergence in the

³⁰³ Arrow, "A Difficulty in the Concept of Social Welfare."

utility calculations between to potential parties to a conflict is best referred to as an information asymmetry and is one of Fearon's rationalist explanations for war. Even as the discussion turns from the basic tenets of rationality it is important to consider that most if not all rational choices occur under conditions of risk and uncertainty. The next section focuses on how this work conceptualizes these two terms and how they are applicable to decisions related to cyber.

Uncertainty & Risk

Uncertainty and risk both play a role in the ability of a decision maker to arrive at an ultimate decision as to whether or not to engage in conflict. Although Bueno de Mesquita uses a measure of coalition cohesiveness within a nation's geopolitical region, such a tool is not applicable within the cyber framework for several reasons. Bueno de Mesquita establishes that what states are uncertain about is the likely response of other nations to the instigation of conflict.³⁰⁴ First, as has been discussed, alliances and coalitions are not of clear importance to decisions made regarding the instigation of conflict within cyber. Second, a constraint to a geopolitical region would also be inappropriate as the regional delineations of the cyber domain make geopolitical delineations unreasonable. What is left is a consideration of uncertainty that is difficult to comprehend within the cyber domain.

Uncertainty occurs when a decision must be made in the absence of objective or subjective probability values attached to alternative outcomes. Because this is an emerging field of study and there is no immediately logical measure of uncertainty within the cyber domain, it is necessary to assume states making decisions within cyber are doing so based on objective epistemological foundations. Unlike in conventional conflict where epistemological limits are best isolated in the complexities of alliances, within the cyber domain the limits of knowledge are a function of anonymity. Being discovered in the act of a cyber attack critically influences

³⁰⁴ Bueno De Mesquita, *The war trap*: p118.

the certainty or uncertainty of a probability of success within cyber. Anonymity is examined in two unique contexts both of which influence the risk behavior of a state. This is a major departure from Bueno de Mesquita's conceptualization of uncertainty.

First, anonymity affects the probability of success and is included in the measure of the probabilities explained in the next section. Second, anonymity influences the expectation of the changes demanded should a state lose a bilateral conflict. As will be examined in more detail below. A state with greater certainty of its anonymity fears losing less and is therefore increasingly risk-acceptant. For the purposes of the bilateral model for decision-making within the cyber domain it is assumed that as the probability of maintaining anonymity decreases and the effect of anonymity on the perception of what might be lost. Because uncertainty is embedded directly into the utility calculation in the form of a measure and effect of anonymity here risk and uncertainty are combined into a single measure. Here uncertainty represents the ability to maintain the effect of anonymity on the perception of what might be lost. A state that is risk averse is less willing to take a risk on any form of loss. As the potential for loss increases a risk averse state becomes less willing to instigate conflict. A state with a high degree of anonymity has a low degree of uncertainty and vice-versa. This uncertainty is measured at two points in time, both at time t_0 and $t_0 \rightarrow t + n$. Time $t_0 \rightarrow t + n$ is indicative of the time at which an attack is completed. Because anonymity is measured using a hazard function model it is possible to derive two different probabilities at two different points in time. Because anonymity changes over time the certainty of its effect changes as well.

At the outset of attacks most actors should find their level of certainty of maintaining anonymity quite high. Anonymity should be high at the point of conflict initiation because anonymity interacts with the probability of success. This certainty diminishes as the attack

progresses. This is akin to estimating that alliances at the beginning of a conflict are likely to alter as a conflict proceeds. Whereas Bueno de Mesquita's model relies on a single point estimate of certainty based on cohesiveness of the alliance ex-ante, this measure is more accurate as it evolves and can be defined at both the point of conflict initiation and the point of time estimate necessary for the successful completion of an attack. In conventional conflict it would be reflected as alliances shifting over the duration of a conflict. In cyber, because alliances don't have the same importance, it indicates a change in the certainty of states expectations of loss in a conflict as a given attack proceeds towards completion.

Risk-acceptant actors are more likely to decide to attack even in an increasingly uncertain environment than are risk-averse actors. Risk-averse actors are less likely to decide to attack as uncertainty increases. Both of these influence the ultimate decision to attack. However, unlike in Bueno de Mesquita's model, uncertainty has a direct effect on the overall utility function of states deciding to attack within cyber.

Utility Theory of (Cyber) Conflict

The construction of utility theory for cyber conflict is at its aggregated level no different than the construction of utility for any type of decision. In truth Bueno de Mesquita's development of an expected utility theory for international conflict is immensely robust and can be applied with specific modifications to virtually any political decision. Below the entirety of his expected utility theory is laid out. It is important to remember the constraints of the cyber domain likely mitigate the extension of the theory beyond bilateral conflict.

Just as Bueno de Mesquita states in his work, the same holds true here. Utility can be estimated to be a "random walk" between +1 and -1 or a difference between perfect agreement in

policy positions ranging to a complete divergence in policy positions.³⁰⁵ This represents, as noted by Bueno de Mesquita, a bounded range for utility. The boundedness of utility in economics is a reflection of diminishing marginal utility reaching a point at which value ceases to increase.

The theory of boundedness has been examined in detail by Bernoulli, Von Neumann and Morgenstern, Fishburn, and others. Although it is possible to have an unbounded utility function, in the political context or what Quiggin refers to as a Rank Dependent Expected Utility (RDEU) model, the issue of diminishing marginal utility of value is revealed.³⁰⁶ Contextually it is reasonable to assume that once two states perfectly align in policy positions (+1) there is nothing to be gained indicating actions to achieve additional utility from such a situation would be inefficient. Similarly once two states are at their maximum divergence in policy positions (-1) there is nothing more that can be lost. Note that loss and gain in this context do not indicate the possibility to shift an opposing state's policy position, but rather indicate the distances on the policy spectrum between the two states.

Policy positions within this model are measured by using Strezhnev and Voeten's data derived from the United Nations General Assembly.³⁰⁷ They create a measure of affinity based on what percentage of votes each country agreed on. Within their coding abstention represents a half-agreement. This gives a score between 1 and 0. This work assumes that .5 represents a midpoint in policy affinity between two states and sets .5 at 0. The resultant number is then multiplied by 2 to give a proportional distance to 1. Because this proportional distance is inverted, the proportional distance is multiplied by -1. This provides a standardized score of vote difference within the United Nations General Assembly during a given year ranging from 1 to –

³⁰⁵ Bueno De Mesquita, "An Expected Utility Theory of International Conflict," p922.

³⁰⁶ John Quiggin, *Generalized expected utility theory : the rank-dependent model* (Boston: Kluwer Academic Publishers, 1993). p57.

³⁰⁷ Anton Strezhnev and Erik Voeten, "United Nations General Assembly Voting Data," (2012).

1, with 0 as the midpoint. This measure is used to estimate the potential utility to be gained from engaging in hostile actions with another state at its maximum, ignoring anonymity and probability for success.

The conventional expected utility model for international conflict identifies 7 types of nations each having an effect on the calculations about the instigation of international conflict. These nation types are:³⁰⁸

Included in the cyber decision-making model:

1. The potential initiator (hereafter called *i*);
2. The potential defender (hereafter called *j*);

Not included in the cyber decision-making model:

3. Those nations with policies viewed by *i* as friendly toward *i*, but not toward *j* (hereafter called *k*₁);
4. Those nations with policies viewed by *i* as friendly toward *j*, but not toward *i* (hereafter called *k*₂);
5. Those nations with policies viewed by *i* as friendly toward both *i* and *j* (hereafter called *k*₃);
6. Those nations whose policies are viewed by *i* as neither friendly toward *i* nor toward *j*, but as friendly toward other third parties (hereafter called *k*₄);
7. Nonaligned nations with policies viewed by *i*, as neither friendly toward *i*, nor toward *j*, nor toward other states (hereafter called *k*₅).

Bueno De Mesquita asserts that when a leader contemplates the expected utility of the initiation of conflict, the following variables are significant:³⁰⁹

1. The relative strength of *i* and *j*;
2. The value *i* places on changing *j*'s policies to be more in line with its own preferences, relative to the possible changes in policy *i* might be forced to accept if it loses to *j*; and
3. The relative strength and perceived policy interests of all *k*₁, *k*₂, *k*₃, *k*₄, and *k*₅ (as seen through the eyes of *i*) that might intervene in the ensuing conflict.

Bueno De Mesquita defines the component aspects of the utility for the instigation of bilateral conflict as:³¹⁰

³⁰⁸ Bueno De Mesquita, "An Expected Utility Theory of International Conflict," p919.

³⁰⁹ Ibid.

³¹⁰ Ibid., p920.

$E(U_i)_b = i's$ expected utility for the instigation of bilateral hostilities

$U_{ii} = i's$ utility for $i's$ own policies is by definition $U_{ii} = 1$.

$U_{ij} = i's$ utility for $j's$ policies. This can vary between +1 and -1.

$(U_{ii} - U_{ij})_{t0} = i's$ perception of what might be gained by succeeding in a bilateral conflict with j in which i can then impose new policies on j

$(U_{ij} - U_{ii})_{t0} = i's$ perception of what might be lost by failing in a bilateral contest with j in which j can then impose new policies on i .

$P_i = i's$ current perception of its probability of succeeding against j in bilateral conflict.

$1 - P_i = i's$ current perception of its probability of losing against j in bilateral conflict.

$\Delta(U_{ii} - U_{ij})_{t0 \rightarrow t+n} = i's$ perception of anticipated change in the difference between $i's$ policies and $j's$ policies over the period $t0$ (the present) to some future time $(t + n)$.

$\Delta(U_{ij} - U_{ii})_{t0 \rightarrow t+n} = i's$ perception of anticipated change in how much j would want to alter $i's$ policies in the future compared to $j's$ current perceived policy differences with i .

Based on the above components Bueno de Mesquita indicates, and this holds true for cyber and any other political decision, that i believes j is moving closer in regards to policy positions, therefore indicating an improvement in relations between the two nations if:³¹¹

$$\Delta(U_{ii} - U_{ij})_{t0 \rightarrow t+n} < 0$$

Such a change as in conventional conflict might alleviate or minimize the potential need to engage in any form of hostile action. However, this also indicates the reverse is true: ³¹²

$$\Delta(U_{ii} - U_{ij})_{t0 \rightarrow t+n} > 0$$

When i believes j is moving further away in relative policy position as indicated above, this indicates deterioration in relations and will likely increase the probability of conflict. The improvement or deterioration in relative policy positions over time can either enhance or mitigate the drive to conflict. This principle illustrated by Bueno de Mesquita is not unique to conventional conflict. An appropriate example would be the 2007 cyber attacks against Estonia. It is conceivable that if the policy position of the Estonian government had been one of shifting towards closer relations with the Russian Federation the likelihood of attacks would have been

³¹¹ Bueno De Mesquita, *The war trap*: p47.

³¹² Ibid.

diminished. The reality was that the change in policy positions was increasingly divergent, the attacks served as a reminder of the country's vulnerability.

Just as relative policy position over time is important in influencing the utility of any potential conflict, the probability of success in conflict is also important to influencing the utility of engaging in conflict. The probability of success in conflict is largely determined by a measure such as power (capabilities) to achieve one's stated goals as was examined in chapter 4. This power score can be ascertained as a function of material capabilities or other determinants. Bueno De Mesquita represents the probability function for conventional conflict as:³¹³

$$P_i = \frac{cap_{ij}}{cap_{ij} + cap_{jj}} \quad 8.1$$

Where *cap* (Capabilities) for Bueno de Mesquita represents:³¹⁴

$$\text{Adjusted Capabilites} = \text{composite capabilities}^{\log[(\frac{\text{miles}}{\text{miles per day}})+10-e]} \quad 8.2$$

Capabilities are constructed using CINC scores from Singer and Small 1977 and a representation of the debilitating effect distance has on conventional capabilities.³¹⁵

Because actions occurring within cyber are unique in composition and application from conventional methods of conflict as examined by Bueno de Mesquita, they must contain constraining assumptions different from those of conventional conflict. Although Bueno de Mesquita identifies three combinations of potential combatants, at present in cyber, it is only reasonable to consider one.

³¹³ Bueno De Mesquita, "An Expected Utility Theory of International Conflict," p925.

³¹⁴ Ibid.

³¹⁵ Singer, Bremer, and Stuckey, "Capability Distribution, Uncertainty, and Major Power War, 1820-1965."

Bueno de Mesquita's combatant combinations.³¹⁶

- a. conflicts between nonaligned states;
- b. conflicts between aligned states; and
- c. conflicts between nonaligned and aligned states;

As has been discussed in previous chapters because cyber attacks require anonymity to be successful. In a situation of anonymity it is not logical to assess the alignment of states, as such an alignment would likely only come to full fruition for the benefit of either party after the success or failure of a potential attack. Therefore, a cyber attack on a state that is aligned is unlikely to be different than an attack on a state that is unaligned. If there is any doubt on this issue historical precedence should suffice to explain.

In 2007 the cyber attacks conducted against Estonia, an aligned nation within NATO should have indicated a combined strength of alliances sufficient to thwart the decision process of any potential attack initiator. The combined power scores of the alliance are substantial. Yet not only did the alliance fail to recognize the attack as an act constituting an alliance response its entire response was muted.

The same can be seen in the instances of other attacks ranging from the Israeli attack on Syrian nuclear facilities, to the attacks of Stuxnet. Although the later was likely created through national collaboration, the measure of alliances associated with each country likely had little to no effect on the outcome of the attack. It is therefore unreasonable to consider any form of alliance in the present modeling of decisions within cyber as having any significant influence. This therefore leads us to assumption one.

Assumption 1: In cyber conflict alliances are of little or no importance, as they fail to affect either the conduct or the success of a potential attack within the cyber domain.

³¹⁶ Bueno De Mesquita, "An Expected Utility Theory of International Conflict," p922.

This assumption is consistent with the reality of the cyber domain and attacks occurring within it. If however, cyber attacks are used as force multipliers it is best to combine their utility function with the conventional utility formulas including alliances as indicated by Bueno de Mesquita.

While the utility formula for bilateral conflict can function adequately for virtually any decision process in international relations, the probability for success must be contextually tailored. Although it could be tailored to account for diplomatic negotiations as well as conventional military operations, this work, as was developed in chapters 4 and 5, illustrated a way in which it can be adapted to the cyber domain. This adaptation leads to a set of cyber specific assumptions on capabilities:

Assumption 2: Capabilities in the cyber domain are not the equivalent of capabilities in other more conventional domains of interaction. Cyber capabilities are constructed by a measure of theoretical capabilities interacting with demonstrated capabilities, scaled by a measure of national digital dependence. These capabilities are not dependent on distance as interactions within the cyber domain are almost instantaneous and suffer no loss of effectiveness as their distance from origin increases.

Assumption 2 is predicated on virtually all works on cyber security and development ranging from Kramer, Starr, and Wentz, to Nye, Betz and Stevens, and others.³¹⁷ Cyber does not have the same capability characteristics as conventional conflict. Cyber requires a unique set of variables to explain capabilities within this domain and a unique comprehension of these capabilities independent of conventional forms of conflict.

³¹⁷ Kramer, Starr, and Wentz, *Cyberpower and National Security*; Nye, "Cyber Power."; David Betz, Tim Stevens, and Studies International Institute for Strategic, *Cyberspace and the state : toward a strategy for cyber-power* (Abingdon; New York: Routledge, for the International Institute for Strategic Studies, 2011).

Below are the variables developed in previous chapters:

Variable Name	Variable Code
Military United Designation*	MUD
Legal and Regulatory Frameworks*	LRF
Economic and Social Context*	ESC
Technological Infrastructure*	TI
Industrial Application*	IA
Military Budget Allocation*	MBA
Threat Spectrum Capabilities	TSC
National Digital Vulnerability	NDV

*indicates weighted variables

These variables combine to create the cyber capability model below in equation 8.3.

$$Cyber\ Power = \frac{(MUD + LRF + ESC + TI + IA + MBA) \times TSC}{NDV} \quad 8.3$$

This is simplified to where F represents theoretical cyber force capabilities, T represents demonstrated threat spectrum capabilities, and D represents national digital dependence.

$$Cyber\ Power(capabilities) = \frac{F \times T}{D} \quad 8.4$$

Despite a reconceptualization of capabilities in cyber terms the probability for success or P_i , success in cyber is not solely dependent on cyber capabilities as conventional conflict is on conventional capabilities. As was illustrated in chapter 5, anonymity plays a vital role in determining the success of any potential attack within the cyber domain. This leads to assumption three:

Assumption 3: *Capabilities within the cyber domain must be interacted with a measure of anonymity. Because the cyber domain is a virtual domain controlled by human agents it has the ability to be turned off and on, and managed in ways unique to its virtual qualities. Therefore it is necessary to include in the probability of success not only a measure of capabilities between potential adversaries unique to cyber, but also a measure for anonymity.*

As the ability to maintain anonymity decreases, its effect forces the probability of success towards zero. Anonymity also functions in another way that doesn't merely influence the probability of success in conflict; it influences the perception of the potential loss a state might face. Anonymity is a powerful feature of cyber and heavily influences the decision-making model. Notation for Anonymity within the cyber model is represented as:

A_i = i 's perception of its probability for maintaining anonymity.
 $1 - A_{i_{t_0}}$ = the effect of i 's perception of its probability for maintaining anonymity.
 $1 - A_{i_{t_0 \rightarrow t+n}}$ = the effect of i 's perception of its probability for maintaining anonymity at the time of the completion of attack.

As the ability to maintain anonymity increases its effect approaches zero. This relationship is inverse in nature. When this number reaches zero its effect increases. This effect interacts with the perception of what might be lost by failing in a bilateral contest. The best way to conceptualize this term is to think like a criminal. If there was no chance of being caught for a crime, *ceteris paribus*, it is more likely an individual would attempt such a crime regardless of its overall probability of success.

The above two assumptions also lead to the following measure of P_i (i 's current perception of its probability for success), where F represents theoretical force capabilities interacted with T, demonstrated threat spectrum capabilities, scaled against D, a measure of national digital dependence. P_i for cyber actors is represented in equation 8.5 as:

$$P_i = (A_i) \left(\frac{\frac{F_{ij} \times T_{ij}}{D_{ij}}}{\frac{F_{ij} \times T_{ij}}{D_{ij}} + \frac{F_{jj} \times T_{jj}}{D_{jj}}} \right) \quad 8.5$$

This can be simplified to Bueno de Mesquita's notation as:

$$P_i = (A_i) \left(\frac{cap_{ij}}{cap_{ij} + cap_{jj}} \right) \quad 8.6$$

Combined these three assumptions fundamentally change the way in which utility is assessed for cyber within the expected utility theory of international conflict. Recognizing that the probability function of the utility for international conflict is different than the one conceived of by Bueno de Mesquita it is possible to restate the utility function for bilateral cyber conflict initiation from equation 8.7 to reflect both the incorporation of the construction of P_i and the influence of anonymity on a perception of potential loss in equation 8.8.

$$E(U_i)_b = (P_i (U_{ii} - U_{ij}) + (1 - P_i)(U_{ij} - U_{ii}))_{t_0} \quad 8.7^{318}$$

$$+ P_{i_{t_0}} (\Delta(U_{ii} - U_{ij}))_{t_0 \rightarrow t_n} + (1 - P_i)_{t_0} [(\Delta(U_{ij} - U_{ii}))_{t_0 \rightarrow t_n}]$$

For this work Bueno de Mesquita's utility for the initiation of bilateral conflict is modified to include the effect of anonymity on the perception of loss in the present and at a future point in time. This is reflected in the equation 8.8 below:

$$E(U_i)_b = (P_i (U_{ii} - U_{ij}) + (1 - P_i)[(U_{ij} - U_{ii})(1 - A)])_{t_0} \quad 8.8$$

$$+ P_{i_{t_0}} (\Delta(U_{ii} - U_{ij}))_{t_0 \rightarrow t_n}$$

$$+ (1 - P_i)_{t_0} [(\Delta[(U_{ij} - U_{ii})(1 - A_{i_{t_0 \rightarrow t+n}})])_{t_0 \rightarrow t_n}]$$

³¹⁸ Bueno De Mesquita, "An Expected Utility Theory of International Conflict," p919., note that there is no inclusion in this work of his other models illustrating the inclusion of the other 5 national types. Because cyber is largely a bilateral venture this work focuses on bilateral conflict initiation and utility.

The general utility function for bilateral conflict as defined by Bueno de Mesquita above in equation 8.7 functions the same way for cyber conflict with only minor modifications seen in equation 8.8. These modifications take into account the influence of anonymity as explained above. Again, it is important to remind the reader that in addition to the visible changes in the structure of the utility formula accounting for the effect of anonymity, the composition of the probability function P_i has been modified to incorporate cyber specific variables. Although the calculation is fundamentally different, the general utility function is only slightly altered. This change still allows many of Bueno de Mesquita's original propositions to be adapted into a decision-making model for cyber with only modest alterations. What follows are Bueno de Mesquita's propositions modified with language conducive to and incorporating the assumptions of the cyber domain.³¹⁹

PROPOSITION 1: States involved in a purely bilateral conflict cannot rationally attack a more powerful state within the cyber domain, regardless of whether their choice occurs under risk or uncertainty, and regardless of their risk propensity unless they are assured positive utility predicated on anonymity across all three characteristics of anonymity.

Proposition one is consistent with most concepts of rational conflict initiation up to the point where anonymity begins to play an important role. Bueno de Mesquita notes that this proposition is inline with Organski and Kugler and others.³²⁰ Although it is consistent with much of the conventional literature on the rational instigation of conflict it seems to fly in the face of much of the cyber literature on asymmetry. While asymmetry is important, it is important to contend that the power score in cyber is scaled by national digital dependence. If anonymity

³¹⁹ Ibid.

³²⁰ Ibid.; A. F. K. Organski and Jacek Kugler, *The war ledger* (Chicago: University of Chicago Press, 1980).

cannot be maintained indefinitely, ultimate probability of success decreases to zero. This indicates that while the domain is asymmetric attacks are only rational if (A) there is a preponderance of power, or (B) a state can assure its anonymity so as to prevent retaliatory action.

Just as Bueno de Mesquita notes, this proposition does not preclude the possibility of a state engaging in hostile actions against a more powerful state, even if it can't maintain its anonymity, only that such an act is irrational. Under this proposition it is not possible to include the revealed policy preferences among other states (indicated by Bueno de Mesquita) as those policy preferences are largely irrelevant in coming to the aid in either the instigation of or defense against conflict.

PROPOSITION 2: A risk-acceptant leader calculating expected utility under risk could initiate a cyber conflict against a stronger ally if it is assured a high probability for indefinite anonymity.

This proposition largely flies in the face of conventional wisdom. It is assumed $(U_{ij} - U_{ii})_{t0} = i's$ perception of what might be lost by failing in a bilateral contest with j in which j can then impose new policies on i . However, as was examined above anonymity can virtually prevent the imposition of $j's$ policies on i if anonymity can be maintained over time. If an attacker never expects to be discovered, even if the attack fails to accomplish its stated goals, such an attack might be conducted with a low utility gains because the consequences of failure are virtually non-existent.

If such attacks are compared to peer-to-peer sharing of movies, music, and other forms of media it is evident that out of the millions of users only a small number are ever prosecuted for theft of intellectual property. The number is so small as a percentage of the overall number of

individuals engaging in theft that it becomes statistically insignificant. Statistical insignificance eliminates meaningful deterrents that prevent individuals from engaging in illegal behavior.

PROPOSITION 3:³²¹ *When $U_{ii} - U_{ij}$ reaches its maximum value (i.e., when $U_{ij} \rightarrow -1$), the probability, given the random walk principle or boundedness, i anticipates that $\Delta(U_{ii} - U_{ij})_{t0 \rightarrow t+n}$ is negative increases, as does the likelihood that i anticipates that $\Delta(U_{ij} - U_{ii})_{t0 \rightarrow t+n}$ is positive. Under these circumstances, Bueno de Mesquita indicates i is likely to anticipate an improvement in future relations with j . This proposition holds true within the cyber context and can indicate a situation in which even if $E(U_i)_b \geq 0$ as indicated by current values (at t_0) can be altered to reflect $E(U_i)_b \leq 0$. This alteration is predicated on future expectations and can prevent conflict between two parties.*

Cyber conflict decision-making just as conventional conflict decision-making is based on present and future changes in positions. Although this particular proposition is difficult if not impossible to illustrate using case examples, its proof of concept is logical. It is possible to assume two nations, both hostile to one another, avoiding conflict based on anticipated changes at a future point in time.

PROPOSITION 4:³²² *Let $U_{ii} = U_{ij} = 1$, so that $U_{ii} - U_{ij} = 0$. If $U_{ij} = U_{ii}$, then the policies of i and j are, by definition, indistinguishable. Consequently, regardless of whether i is risk-acceptant or risk-averse, and regardless of whether a decision is being made under risk or uncertainty, in this circumstance, it is always true that $E(U_i) = E(U_i)_b$. Now, by the random walk assumption (discussed above), if $U_{ii} - U_{ij} \rightarrow 0$, it is likely that $\Delta(U_{ii} - U_{ij})_{t0 \rightarrow t+n} \geq 0$ and $\Delta(U_{ij} - U_{ii})_{t0 \rightarrow t+n} < 0$. Since the sign of $E(U_i)_b$ is determined by the magnitude of P_i relative*

³²¹ Bueno De Mesquita, "An Expected Utility Theory of International Conflict," p924. - Note that this is Bueno de Mesquita's 4th proposition, not his third. Proposition 3 does not apply in the context of cyber as it deals with alliances.

³²² Ibid., p924.

to $1 - P_i$, it follows that, among closest allies, if i is stronger than j , $E(U_i)$ cannot be less than zero, and if i anticipates a deterioration in relations in the future, $E(U_i)$ must be greater than zero. Then, as noted by Bueno de Mesquita, there is a paradox. Under these circumstances in any form of conflict, cyber included, when anticipated future changes indicate a decline in relations between two close allies, conflict initiation by the stronger nation should be expected.

The logic of the above proposition is counterintuitive as is noted by Bueno de Mesquita.³²³ Similar behavior arising between allies in the cyber domain has not been documented, however it stands to hold that in this regard cyber conflict is no different from conventional conflict. The effectiveness of using cyber conflict in this regard independent of other tools of force is likely of limited value.

The above propositions indicate, based on the expected utility theory developed when it is and is not rational to instigate conflict within the cyber domain. The propositions should indicate the differences between conflict initiators and their targets, the likely victor of any given attack, when conflicts are irrational and therefore not necessary, and when the use of cyber is rational. The next section explains how these propositions will be tested in the next chapter.

Next Steps

The expected utility theory for international cyber conflict constructed above by modifying the expected utility theory for international conflict works in many of the same ways as its archetype. The construction of the new utility formula is still based on the assumptions of rationality. By testing the revised theory for how states make decisions within the cyber domain it is possible to ascertain the validity of the propositions. The purpose of the next chapter is to test the expected utility theory developed above on actual open source data derived from various

³²³ Ibid., p924.

cyber attacks of significance. A complete reference of all data used is listed by country in the appendices.

The analysis in the next chapter inputs the values of probability and anonymity into the utility formula as developed above. The higher the utility stronger the choice for the use of cyber becomes. It is important to note the utility for bilateral cyber conflict is not directly comparable to multilateral conventional conflict as the later contains summations of the alliance capabilities. Therefore it is only possible to intradependently examine utilities derived from bilateral conflict at present.

The primary goal of the next chapter is to identify whether or not states that have engaged in cyber attacks have done so with a positive expected utility as defined above in a statistically significant portion of the cases. If it is confirmed that states in a statistically significant number of instances instigated attacks with positive utility the validity of the above expected utility theory of international cyber conflict would be maintained. Should the majority of cases not hold up and prove statistically significant then the theory as established will be invalidated. The central theory proposed suggests states are rational actors and will only instigate a cyber attack with a positive expected utility.

CHAPTER 9

Applying the Expected Utility Theory of International Cyber Conflict

It is extremely difficult to test a field where secrecy and ambiguity dominate. This chapter attempts to use the methodologies established in the previous chapters to identify when states are more likely to decide to engage in hostile activities in the cyber domain and when they are not. Each of the cases has been tested in four separate ways in an attempt to put all the cards on the table. The types of testing include: (1) Static changes in policy over time with the inclusion of a measure of anonymity, (2) dynamic changes in policy over time with the inclusion of a measure of anonymity, (3) static changes in policy over time excluding a measure of anonymity, (4) dynamic changes in policy over time excluding a measure of anonymity. These four measures are meant to illustrate when it is and is not rational to instigate a cyber attack based on different assumptions.

This chapter focuses on testing the propositions presented in chapter 8 and on examining the broader logic of rationality in international cyber conflict. However, before moving directly into the statistical tests it is helpful to examine the power relationships of states as a rank ordering and to provide a small discussion. Figure 9.1 is a rank ordering of the states measured for this work and includes their cyber power score. Note that the power score is separate from anonymity associated with the type of attack employed. The figure clearly illustrates India was an outlier in the unbiased measure of cyber power.

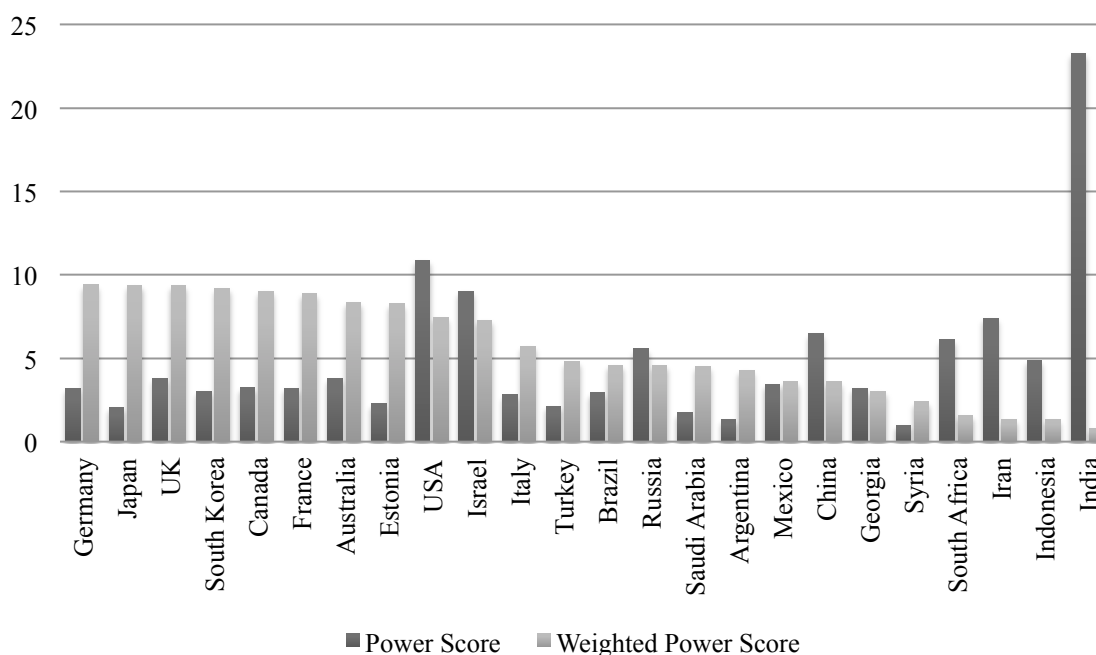


Figure 9.1: State Cyber Power Scores

Figure 9.1 includes two power scores. The first is a raw power score based on an equal weighting of all aspects of a state's cyber power. Using this rubric India would be the most powerful state followed at a distance by the United States. The question is why would India, a state with a small percentage of its population using the Internet and only moderate scores in all categories rank so highly in terms of power score?

The basic definition of power score indicates that a state's power is scaled by its vulnerabilities, and this is where India thrives. Because only a small percentage of India's population uses the Internet its national digital vulnerability is proportionately very low. This measure is deceiving. To correct the measure over the influence of vulnerability, cyber power scores were weighed according to their components. Just as all weapon systems are equal in

conventional conflict, not all aspects of cyber power are equal. The actual weighting of power scores can be found in the appendices. The weights of the components of cyber power are predicated on a modification Economist Intelligence Unit's report on cyber power.³²⁴ The result is that India, goes from being one of the most powerful nations because of its low penetration rates of information communications technology to one of the least powerful states overall.

The power scores indicate Germany is the most powerful country overall within cyber space and that the United States comes in a mediocre 9th place. This is not to say that the United States has ineffective military cyber units. If military units were all that mattered the United States would be at the top of the cyber power rankings with its enormous defense budget. Unlike in conventional conflict where it is possible to protect a nation with sheer offensive power, the cyber domain extends across the military and civilian divide, making it necessary for a powerful state in cyber space to excel in all areas of cyber power. Currently the United States does not excel in all areas and is therefore not as powerful as other nations. Cyber power requires a combined national effort and a failing in one area of cyber power can diminish a nation's overall cyber potential.

Just because the United States isn't as powerful as other nations, does not mean it doesn't have a sufficient number of potential targets. The next section outlines how states working under the assumption of anonymity can generate positive utility even against a much more powerful ally. The next section looks at the data and attempts to draw preliminary conclusions. These preliminary conclusions are based on the evidence presented and not on statistical tests. This is done because often a study will jump right into the statistics without examining the results in the

³²⁴ "Cyber Power Index."

broader context of the individual cases involved. Because this study only has 25 cases it is possible to provide a more in depth look at the processes occurring.

The expected utility of states across incidents

This section outlines the utility calculations of 25 cases (23 unique) in which two countries were identified as likely participants to a cyber action. These cases are from the Center for Strategic and International Studies (CSIS) report on significant cyber incidents dating back 6 years.³²⁵ Significance is largely a subjective measure. The CSIS defines significant for its cases as “successful attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars.”³²⁶ For the purposes of this study significance was parsed out to an even more rigorous degree. This analysis includes only successful attacks by governments on other governments and their national security assets. Within this condensed listing, targets must be government agencies or related national critical infrastructure targets. These critical infrastructure targets include, targets within the defense industrial base, electric, financial or radar systems. Disruption of these systems or severe damage and/or theft occurring to these systems must past the test of posing a reasonable clear and present national security threat.

Policy affinity was measured in the year prior to an attack for the static models, and measured as the change policy affinity in the 2 years prior for the dynamic tests. Prior years are used rather than the current year because vote counts are completed on a yearly basis. Although this work uses prefabricated anonymity data predicated on anecdotal data, a decision-maker using the hazard model and the relevant data from chapter 5 would arrive at similar results. The purpose of this chapter is to illustrate when decision makers decide to attack they are acting

³²⁵ Lewis, "Significant Cyber Incidents Since 2006."

³²⁶ Ibid.

rationally based on a positive utility score predicated on realistic assumptions. The assumptions for construction of power and the influence of anonymity are unique to the cyber domain and are necessarily included.

Of the twenty-five incidents documented in which two states are identified, the attacking party had a positive utility in every case when anonymity is included in the model. If Anonymity is removed from the model there are only nine instances in which it would have been rational to engage in hostile activities within the cyber domain. Right off the top these results provide a cursory story that states appear to be behaving rationally within the assumptions established in previous chapters. Table 9.1 lists the resultant expected utility across the four categories for all incidents. The table also identifies the type of attack and whether there is a certain attribution or an uncertain attribution associated with the attack.

Table 9.1 Expected Utilities Across Incidents

Year	Type	Attribution	Static Policy Change	Static Change Ignoring Anonymity	Dynamic Policy Change	Dynamic Ignoring Anonymity
2006	CNE	Undefined	0.87	-1.18	0.87	-1.19
2006	ED	Undefined	0.28	-0.74	0.28	-0.73
2007	DDOS	Undefined	0.28	-0.26	0.29	-0.27
2007	CNE	Undefined	0.33	-0.72	0.32	-0.69
2007	CNE	Undefined	0.32	-0.64	0.32	-0.63
2007	CNE	Undefined	0.24	-0.53	0.24	-0.53
2007	CID	Defined	2.48	2.10	2.41	2.04
2007	CNE	Undefined	0.32	-0.64	0.32	-0.63
2007	CNE	Undefined	0.38	-0.51	0.39	-0.54
2008	CNE	Undefined	0.21	-0.45	0.21	-0.45
2008	CNE	Undefined	0.29	0.23	0.30	0.24
2008	DDOS	Defined	0.55	0.19	0.56	0.20
2009	CNE	Undefined	0.37	-0.75	0.37	-0.76
2009	CNE	Undefined	0.21	-0.45	0.22	-0.46
2010	CNE	Undefined	0.38	0.30	0.34	0.27
2010	WD	Undefined	0.05	-0.09	0.04	-0.08
2010	CNE	Undefined	0.40	-0.70	0.40	-0.71
2010	CNE	Undefined	0.38	0.30	0.34	0.27
2010	CH	Defined	2.77	2.38	2.72	2.33
2010	CH	Defined	2.27	1.95	2.41	2.07
2011	CNE	Undefined	0.43	-0.86	0.42	-0.84
2011	CNE	Undefined	0.25	-0.53	0.25	-0.51
2011	CNE	Undefined	0.24	-0.52	0.23	-0.50
2011	CNE	Defined	2.64	2.20	2.67	2.22
2011	CNE	Defined	2.75	2.30	2.68	2.24

CNE-Computer Network Exploitation, ED-Equipment Disruption, DDOS-Distributed Denial of Service, WD-Website Defacement, CH-Compromised Hardware, CID-Critical Infrastructure Disruption

The data in table 9.1 illustrates within the confines of the anonymity assumption that states are rational to engage in hostile actions emanating from cyber. It is reasonable to assume based on the discussions in previous chapters that the assumption of anonymity is necessary to some degree for any type of cyber attack. If the assumption of anonymity is removed only nine cases indicate a positive utility for attack. This would indicate that 61% of attacks initiated

without the assumption anonymity were irrational. A high percentage of irrational actors in interstate conflict do not conform to Bueno de Mesquita results on the expected utility of international conflict.³²⁷ This can lead to several potential conclusions. First, the number of cases is too small to accurately define whether states act rationally or not within the cyber domain. Second, there is something about the cyber domain that makes states act irrationally. Third, states are acting rationally because they assume a degree of anonymity.

Although there are a limited a limited number of cases, the number of cases closely represents the publicly known actual population, indicating that the results accurately reflect the population. If states were acting irrationally they would have likely suffered the consequences of their losses and been dissuaded from engaging in such actions. What is observed, however, is that certain states engage in repeat behavior against multiple targets. This documented state behavior indicates either a cognitive psychological issue or that the states are acting on a rational belief of gain. This work has made the case for the later. Lastly, the decision to engage in attacks is rational if the actors make even modest assumptions of anonymity prior to engaging in their attacks. When those assumptions are not present or weak the only time a state engages in hostile actions against another state is when it has an overwhelming cyber power advantage.

The nine cases in which anonymity does not matter have several common characteristics. Including a small number of potential hostile actors, and a power advantage by the attack initiator.

The Stuxnet and Flame incidents, broken into four separate incidents represented as the utility of the United States versus Iran, and Israel versus Iran, are unique in many ways. The attacking party in both of these incidents had an extreme negative policy affinity with the target

³²⁷ Bueno De Mesquita, *The war trap*.

and an enormous cyber power advantage. In both these instances the scale, complexity, and target of the attack immediately began to degrade the probability of maintaining anonymity. Likewise the Israel - Syria attack of 2007 and the Russian - Georgia Attack of 2008 were combined kinetic - cyber attacks diminishing the need for long-term anonymity. This indicates that in six of the nine instances where anonymity was not important over time, the attacker had both a significant power advantage and had little to no need for maintaining indefinite anonymity.

The remaining three incidents in which anonymity was of little importance were all China - India attacks. In each of these cases the policy goal was limited and the attacker always had a positive utility. Although they are close in policy affinity scores, they do not fall neatly in line with proposition 4 because in two out of the three instances the affinity scores seemed to be growing closer together, while diverging in the third. A source of potential measurement problems is located in the inability of power scores to reflect any shift in relative power over such a short time frame. However, in all of these instances the attack was limited to computer network exploitation.

Because the two countries are neighbors it is possible China feared an increase in relative power, however such an increase is unlikely. What is clear is that China acted not only with anonymity in its favor, but also with a clear cyber power advantage. The incidents all occurred within a span of four years.

Out of the 25 incidents recorded here only six have a defined attribution. Of those six, all had positive utility across the four types of measurement regardless of anonymity and regardless of changes in policy affinity. Two of the attacks are easily attributable after the fact because they were combined with kinetic operations following the success of the cyber operations. The other

four incidents are Flame and Stuxnet, revealed to be a mix of operations between the United States and Israel, were disclosed through intelligence leaks.³²⁸

The remaining incidents in which the attacking party remained undefined were identified as probable attacker with no definitive attribution, indicating that at least part of the triad anonymity had been maintained. By maintaining anonymity states such as China are able to engage in offensive cyber actions against other states with limited fear of retribution. This limited fear of retribution as influenced by anonymity allows them to attack more powerful states. Often the attacks are limited in scale and size, however, the possibility for gain makes such attacks worthwhile.

The next section of this chapter examines how the results hold up against the propositions presented in the previous chapter. Each proposition is examined in detail using the available data.

Examining the propositions

Proposition 1 indicates that states will not engage in cyber conflict if they are at a power disadvantage unless they are assured a moderate to high degree of anonymity across all three dimensions of anonymity. This is illustrated using the data by running t-tests at $\alpha = .05$. The results indicate that when accounting for anonymity in either a dynamic or static policy environment it is rational to engage in hostile actions against opponents. However, when anonymity is excluded there is no statistical significance associated with the instigation of hostilities. Figure 9.2 illustrates the box plots of the distribution of the utilities for each case within the sample. Table 9.1 includes the hypothesis tests across all four categories of tests.

³²⁸ Sanger, *Confront and conceal : Obama's secret wars and surprising use of American power*.

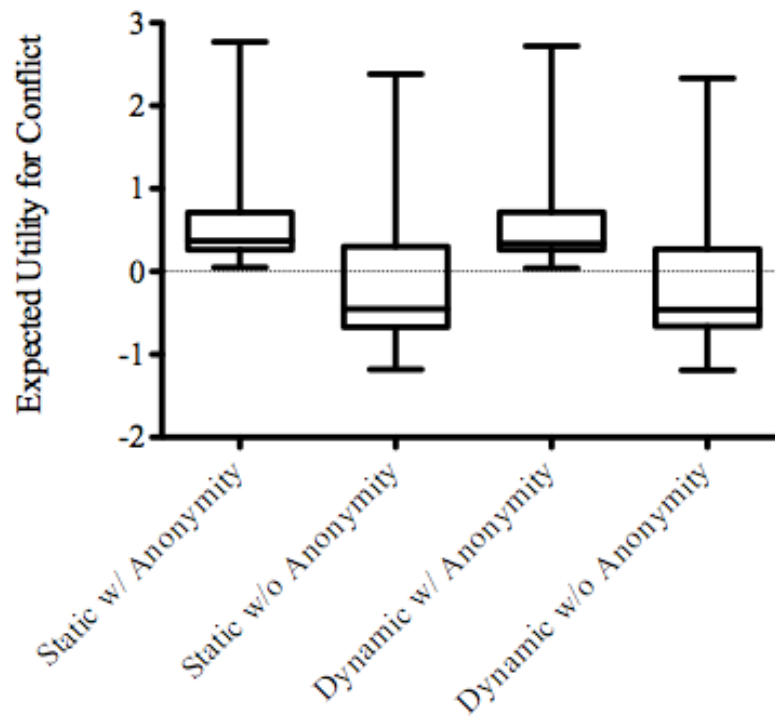


Figure 9.2: Expected Utilities Boxplot

The results indicate a relationship between positive utility and an assumption of anonymity in the decision to attack. If *Proposition 1* is to hold it would be unlikely that a state with low anonymity and a relative power disadvantage would engage in hostile activities against another state. There are no data on cases in which a state with little to no anonymity and a power deficit are available. This proposition is currently supported by the robustness of the evidence suggesting a relationship between positive utility and anonymity. The lack of cases in which an instigator was at an overall utility disadvantage makes it impossible to make definitive claims on proposition 1. If the assumption that states are rational actors holds across models, then the below data would indicate that in most instance states would not have engaged in hostile actions in the absence of anonymity.

To further drive home the point about anonymity, there is no evidence of any retaliatory actions by victimized states towards their likely aggressors. This lack of response indicates that most, if not all attacks resulted in a degree of victory for the attack instigator.

Table 9.2: Results of t-Tests of utilities

	Static w/ Anonymity	Static w/o Anonymity	Dynamic w/ Anonymity	Dynamic w/o Anonymity
Number of values	25	25	25	25
Minimum	0.05	-1.18	0.04	-1.19
Mean	0.7876	0.0952	0.784	0.0944
Std. Deviation	0.9309	1.131	0.929	1.126
Std. Error	0.1862	0.2262	0.1858	0.2252
One sample t test				
Theoretical mean	0	0	0	0
Actual mean	0.7876	0.0952	0.784	0.0944
Discrepancy	-0.7876	-0.0952	-0.784	-0.0944
95% CI of discrepancy	0.4033 to 1.172	-0.3716 to 0.5620	0.4005 to 1.167	-0.3704 to 0.5592
t, df	t=4.230 df=24	t=0.4209 df=24	t=4.220 df=24	t=0.4192 df=24
P value (two tailed)	0.0003	0.6776	0.0003	0.6788
Significant (alpha=0.05)?	Yes	No	Yes	No

Proposition 2 builds on *proposition 1* and indicates that even if a state is at a power disadvantage, it might, given conditions of anonymity, engage in hostile actions against a more powerful state. Although there are no instances in which a state with no assumption of anonymity attacked from a position of relative weakness, the data from table 9.3 seems to support this proposition. If the assumption of anonymity is correct then it goes a long way towards supporting China's risk acceptant behavior in attacking through the cyber domain, states with a relative power advantage. However, since there is no way to test this assumption, the anecdotal evidence from the data must suffice at present.

Propositions 3 and 4 are interesting because they both propose conditions under which states would be more or less likely to engage in hostilities. To test these propositions it was necessary to examine changes in policy affinity over a defined period of time to see if states were more or less likely to engage in or abstain from hostilities depending on changes in policy preferences. Table 9.3 shows the results of a simple t-Test on whether changes in policy affinity are statistically significant. The results indicate changes in policy affinity have no bearing on whether a state is more or less likely to engage in hostilities. Although the results provide some anecdotal evidence that states are more likely to engage in cyber hostilities when there is a decrease in policy affinity, the relationship is not significant. Figure 9.3 illustrates the distribution of changes in affinity over time and provides a good visualization for where states fall with regards to when they decide to attack in relation to their policy affinities. Of note is that the mean of changes affinities for states engaging in hostile actions within the cyber domain is negative. However, as mentioned above no statistical inference can be derived.

Table 9.3: t-Tests of affinity of state likelihood of conflict

Number of values	25
Mean	-0.0072
Std. Deviation	0.05997
Std. Error	0.01199
Lower 95% CI of mean	-0.03195
Upper 95% CI of mean	0.01755
One sample t test	
Theoretical mean	0
Actual mean	-0.0072
Discrepancy	0.0072
95% CI of discrepancy	-0.03195 to 0.01755
t, df	t=0.6003 df=24
P value (two tailed)	0.5539
Significant (alpha=0.05)?	No

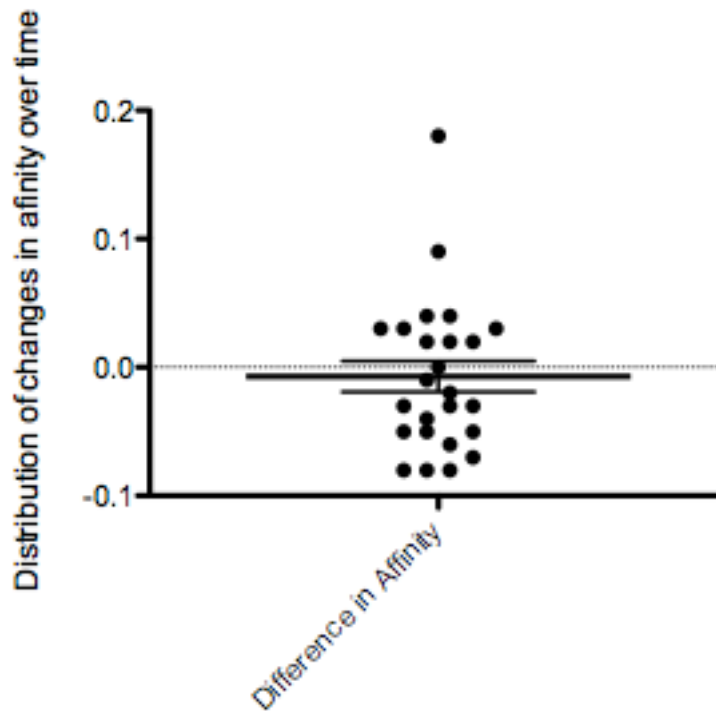


Figure 9.3: Distribution of changes in affinity over time

One other aspect arising out of *Propositions 3* and *4* is the question of whether states are more likely to attack when they have close policy positions or more divergent policy positions. *Proposition 4* indicates that conflict is more likely when states have close affinity because they are concerned more about negative shifts in policy than states that are extremely divergent in policies. This is contrasted with *Proposition 3* indicating that states are less likely to engage in conflict with states that are at the polar opposite end of the policy affinity spectrum because there is only truly room for improvement. Table 9.4 indicates the affinity scores of states in the year prior to attack. This is a static number. The question is whether conflict is more likely between states with close affinity scores, or more divergent affinity scores? In other words, are states with very similar policies more likely to attack one another through the cyber domain than states with

dramatically divergent policies? Figure 9.4 illustrates the distribution of the affinity scores around the mean.

Table 9.4: t-Test of state affinity in year prior to conflict

Number of values	25
Mean	0.1804
Std. Deviation	0.5016
Std. Error	0.1003
Lower 95% CI of mean	-0.02664
Upper 95% CI of mean	0.3874
One sample t test	
Theoretical mean	0
Actual mean	0.1804
Discrepancy	-0.1804
95% CI of discrepancy	-0.02665 to 0.3875
t, df	t=1.798 df=24
P value (two tailed)	0.0847
Significant (alpha=0.05)?	No

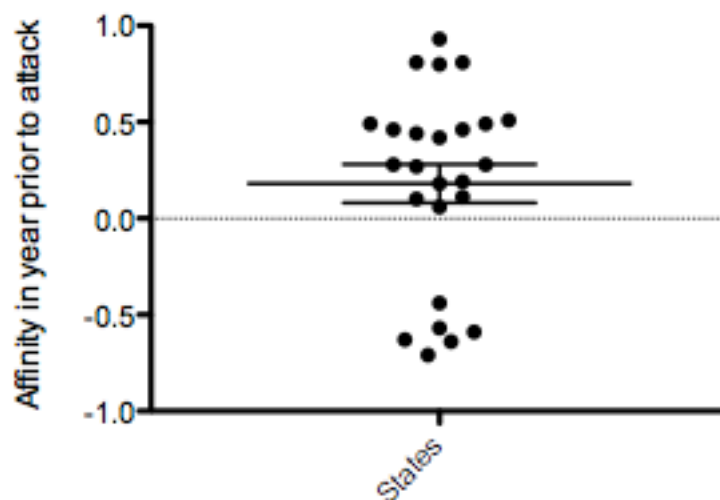


Figure 9.4: Distribution of state affinities in year prior to hostilities

The data in table 9.4 does not indicate significance at an $\alpha = .05$. The data does indicate significance at an $\alpha = .1$. Because this is not the pre-established threshold and because there are a limited number of cases it is impossible to draw statistical significance from these results. If, however, the results are examined using the $\alpha = .1$ threshold, it is possible to indicate that cyber attacks are more likely between states with positive affinity scores than between states with negative affinity scores. Anecdotally it is possible based on the data to infer that states with close policy affinity scores are more likely to engage in cyber hostilities against one another than states with negative affinity scores.

Taking a step back and looking at the six of 25 cases with negative affinity scores several striking characteristics stand out. First, all of the cases in which there was a negative affinity score included either the United States or Israel. Second in 5 of the six instances with a negative affinity score the attacking party(s) had a significant power advantage. Only one instance, a CNE attack by China against the United States stands out.

These results indicate that at an $\alpha = .1$ there is a statistically significant relationship between positive state affinity likelihood of conflict. Although Bueno de Mesquita indicates that this relationship is likely due to anticipated changes at a future time, the results are inconclusive and do not support such a conclusion with the limited data available.³²⁹

The tests of *Propositions 3* and *4* are broken into two separate tests because the propositions intrinsically encompass two different hypotheses. The first hypothesis is that states are more likely to attack states when the expectation is that there is deterioration in the relationship over time. The second, hypothesis is that states are more likely to attack when states

³²⁹ Bueno De Mesquita, "An Expected Utility Theory of International Conflict."

are more closely aligned along the policy spectrum. Neither of these hypotheses is proved significant at the $\alpha = .05$ threshold.

The next, and final section of this chapter examines the implications of the results and what they mean in the context of the expected utility theory of international cyber conflict.

Data in context

The data presented in this chapter spans 23 unique incidents with 25 cases. What is evident from the data is theoretical connection between anonymity for instigators of cyber incidents and rational behavior. If anonymity is removed from the decisions making process then attacks within the cyber domain are irrational. In the present context and based on everything known about interaction within the cyber domain, anonymity is a defining concept of cyber conflict. Beyond the necessary inclusion of anonymity for decisions to be rational, the data indicate a propensity – although not statistically significant - for conflict between states with positive policy affinity scores and indicate no definable relationship in changes in policies over the established one-year time frame to the instigation of conflict.

It is not unsurprising that the majority of incidents occur between states with relatively positive affinity scores. To be worthy of an attack a target must possess a level of development that exceeds a minimum threshold in most instances. This is particularly true when considering the impact or the potential take from mid-range attacks. Because most of the targets exist at the higher end of the developmental spectrum of states, it is intuitive to assume that is where the attacks go. When the attacks extend beyond simple attacks into more complex attacks such as Stuxnet, they are focused not on a broad take of information or a systemic damage; rather the focus becomes a single system of value. It doesn't do much good for a developed country to attempt cyber attacks against an undeveloped one unless that country has definable targets.

However, because developed countries share many of the same interests, it is not unreasonable to assume that targets within these countries hold special value to their developed nation counterparts. This indicates that as states diverge on policy issues, even if they are still positive in policy affinity, it makes sense to seek out why the divergence is occurring or attempt to shift this divergence in another direction. This then leads to cyber attacks. To more closely examine this aspect of cyber conflict far more data is necessary that is currently available.

Availability of data is one of several major areas of room for improvement within this work. This work contains several areas in need of improvement. These areas are less methodological in nature than they are data driven. First, this work does not include an exact measure of anonymity. The measure of anonymity at present is a rough estimation predicated on type of attack. As was indicated in chapter 5 it would be best to use a statistical function such as a hazard function filled in with intelligence collected as was indicated from chapter 7. Such a measure of anonymity would dramatically increase the accuracy of the results.

Second, There are a limited number of cases include within this study. To fully parse out each of the propositions would require more cases. Many of these cases are available, but are currently classified or kept confidential and are therefore unavailable for public scholarly research.

Third, the power score in this model is kept artificially static over time. The static nature of the power score is due to insufficient data availability across time even within the limited sample of nations present within this study. Any study attempting to expand the data outward either longitudinally or latitudinally will quickly run into data collection problems on even the most basic indicators of digital power. This data issue is rapidly improving as organizations such as the International Telecom Union continue to compile robust data. Fourth, it is possible that the

use of United Nations voting affinity scores artificially places nations in closer policy proximity than other measures of state policies within the international context.

Lastly, because there are no evident cases in which a state initiated conflict with a negative political utility, and because there is no accurate measure of the success of different types of attacks in the form of peace treaties or other documents delineating the victor to a particular conflict, data analysis is limited to disaggregated hypothesis testing. This is a departure from Bueno de Mesquita's use of Yule's Q tests as a means of identifying a proportional reduction in error. The study of conflict within the cyber domain is a new and evolving field of research. While there are millennia of data on conventional conflict, cyber conflict has only been around 30 years in its present form. Over time, as the number of cases increases, the ability to employ more robust statistical methods will only enhance the ability to study this new domain.

Part IV

Conclusion

CHAPTER 10

Finding meaning in the expected utility of international cyber conflict

Cry "Havoc!" and let slip the dogs of war, that this foul deed shall smell above the earth, with carrion men, groaning for burial. ~ Mark Antony in Julius Caesar³³⁰

The cyber domain is, as the previous chapters have demonstrated, a unique and important domain affecting various aspects of national security. The importance of cyber to modern society is undeniable. This work has attempted to provide insight into the decision-making process associated with use of this new domain to achieve utility for states. By focusing on a rational choice approach to the decision-making process and honing the decision process using expected utility this work illustrates a novel approach to understanding how states interact within cyber. This final chapter examines the implications of the expected utility theory of international cyber conflict and examines how these implications influence a wide spectrum of issues related to international relations.

This chapter proceeds in three sections. First, it examines the most important take away lessons within this work. Second, it examines, in brief, the failings of this work and proposes a path for rigorous future study. Lastly, it summarizes the importance of this line of research in the context of international relations.

Take away lessons

There are several take away lessons contained within this work. Paramount among these lessons is a conceptualization of decision-making that includes novel characteristics such as anonymity. Second, this work has made the case that the concept of political utility itself has

³³⁰ William Shakespeare and Alvin B. Kernan, *The tragedy of Julius Caesar*, Rev. ed., The Yale Shakespeare (New Haven, Yale University Press, 1959).

been narrowly conceptualized and needs readjustment to more accurately reflect real world condition. The third lesson to take away from this work is that, the data and concepts are still evolving and will continue to evolve. This evolution can be greatly aided through multiple vectors, including, but not limited to the intelligence community.

The most important lesson drawn from this work comes from the assumption of anonymity. If, as it is assumed, states are rational actors, then the decision to engage in hostile activities within the cyber domain must include a measure of anonymity. Without such a measure the results from part III indicate a majority of the incidents of state on state cyber action would have been irrational. With the inclusion of modest measures of anonymity it is possible to conclude that states are engaging in rational behavior.

The condition of anonymity opens Pandora's box for cyber conflict on the state level. Anonymity makes it possible for states at a traditional power disadvantage to engage in hostile actions against more powerful states. This leads directly to the quote at the beginning of this chapter from Shakespeare's Tragedy of Julius Caesar.³³¹ Because anonymity reduces the ability to deter by means of power or skill in most instances, the proverbial dogs of war are unleashed.

Cyber conflict on a midrange scale, where anonymity is strongest, is likely to continue to grow until states are able place constraints on actions. Because the probability of maintaining anonymity decreases with the complexity and size of attacks, the likelihood of major state on state cyber conflict at present seems unlikely. However, as was noted earlier in chapter 2, midrange cyber conflict results in a death by a thousand cuts. Because much of the technology, and many of the strategic plans associated with national security are stored at these lower levels, this death by a thousand cuts decreases the relative conventional power of states.

³³¹ Ibid.

The data illustrate that although China is at a relative power disadvantage and would likely not engage at present in conventional attacks against many states in the international system, it is willing to engage in cyber attacks because it can do so with impunity, while at the same time increasing its conventional power, relative to its potential adversaries within the international system. Although there is insufficient evidence to make broad generalizations, the trend established by the Chinese is likely not isolated. Anonymity favors the attacker in virtually all situations within the cyber domain. Because anonymity favors the instigator of a conflict, it is likely that cyberspace will become an increasingly hostile domain until such time as there is a reasonable method for reducing the probability for maintaining anonymity.

Next, cyber power is important to take into consideration. A state's development affects its relative power to other states within the international system far more acutely within the cyber domain than in conventional domains. Because cyber power is fundamentally different than conventional power it is not sufficient to simply build cyber weapons, it is necessary to educate engineers, to build stable infrastructure, and to establish laws and regulations that can adapt to a rapidly changing environment. The power scores indicate that it requires a balance between multiple aspects of a nation's development to achieve cyber power. As a state becomes increasingly dependent on the cyber domain the importance of improving the various qualities associated with cyber power increases. Although cyber power does not mitigate the effects of anonymity it helps to influence the decisions of states. A state with a higher power score is more likely to undertake more complex actions even if it is unable to maintain indefinite anonymity. Combined power and anonymity are important within the decision-making process of state actions within the cyber domain. These two concepts interact with each other to create a dynamic decision process suited to the domain.

The decision to engage in actions in the cyber domain is, however, not predicated on anonymity and power. The motivation for engaging in hostilities within the cyber domain necessitated a reconsideration of the concept of political utility. This concept was developed in detail in chapter 3. It was argued that covert actions of any type should be considered as instruments of state designed to achieve political utility. The case that political utility can be achieved through covert acts facilitates an understanding of not only why states engage in actions considered to be traditional covert action, but also why they engage in actions within the cyber domain as well. If as it was argued, covert acts work within the bargaining range between overt conflict and overt diplomacy, this middle and underexplored territory broadens the understanding of conflict processes.

The motivation for achieving this political utility is connected not to the realist notions of relative gains preventing iterative processes, but rather to a neo-liberal notion of complex interdependence in which large-scale conflicts produce aggregate loss and bargaining does not always work. Utility, or more simply political gain is the ability to shift an opponent's policies to a more favorable position or to prevent them from moving even further away. To this end, the motivation for covert actions is a tangible realization of political benefit. If this realization of political benefit occurs through anonymous actions in cyber or through loud overt bombs, the objective is still the same.

The study of utility derived through covert means and the motivation behind those means lags behind other areas of international relations largely because data is not readily available. This lack of data leaves the study of covert action understudied and ignored or misunderstood. Although this work primarily examined covert cyber acts, the data on broader covert acts is difficult at best to come by. This work attempted to use cases all from the same field to provide a rigorous study into the potential for political gain through acts conducted anonymously. The data

are limited and although there are aspects that are statistically significant, it will be necessary to expand this work as data becomes available to more accurately study the motivation and decision processes associated with not only cyber conflict but more broadly, covert action in general.

After having examined several of the take away important take away lessons from this work it is necessary to consider some of the failings present. The next section focuses on the failings or areas, which might be improved in future analyses.

Failings and areas for improvement

Like any new vein of research there are likely to be areas that could use improvement. This work in particular could improve in three primary categories. These categories are data, methodology, and theory. The categories are presented in this order because the failings are dependent upon one another in this order. This section explains how these failings can be improved upon, and why they weren't within the present work.

Data is a social scientist's best friend. Unfortunately, it is also a social scientist's worst enemy. When studying any form of covert action, cyber included, data on a large scale is often missing. If states acknowledge a role in either the defense or instigation of a cyber attack they release information about their capabilities and defeat much of the advantage associated with covert actions. Therefore within the study of cyber, the first major obstacle is data on attacks themselves. Often this lack of data is due to an unwillingness of a state to admit it has fallen victim to an attack, however, it is equally as likely they are aware they have fallen victim to an attack or are unaware of the source of the attack.

Data problems do not end with the inability to accurately identify attacks and participants within the cyber domain. To fully develop utility it is necessary to construct an accurate measure of cyber power. Chapter 4 developed this measure in detail. Data availability on this measure span legal and regulatory, economic and social, infrastructure, industrial, military, and

demonstrated capability measures. Longitudinal availability of data across these measures is severely limited. The limited availability of this data is due in many respects to the newness of the field. Collection on even the most basic indicators related to the cyber domain is new and primarily limited to developed countries. This makes a thorough analysis over time at present impossible.

Data limitations create methodological problems preventing more robust statistical analyses. Although this work employed t-tests to test the various propositions it is possible that with more data across a larger sample would result in more robust results. Likewise because data on the probability of maintaining anonymity were assumed based on the classification of attack rather than on more specific information analyzed in a hazard model it is possible the results are skewed to favor anonymity in incidents where anonymity is less important. Continued collection of data will only increase the accuracy of the results. It would also be useful to examine the results using alternative statistical methodologies such as Bayesian methods. These alternative methods are reserved for future examinations.

Beyond the methodological and data issues present within this new line of research are some fundamental theoretical questions that need to be briefly addressed. Any study on decision-making should consider the theoretical foundations of a decision. In this work rational choice was used as that theoretical foundation. It is important to concede that there are numerous cognitive studies indicating human beings are in fact not rational arbiters, the most famous of which is Kahneman and Tversky's study on prospect theory.³³² Does a real world lack of rationality diminish the results of this analysis? Based on the assumptions presented and the results of this analysis there is a mathematical logic behind state instigation of cyber conflict.

³³² Kahneman and Tversky, "Prospect Theory: An Analysis of Decision under Risk."

Although the theoretical foundation of this logic is based on rational choice and rational choice has been shown to have inconsistencies the results indicate a significant relationship between positive utility and instigation of conflict. Within the Center for Strategic and International Studies report on significant cyber incidents in which two states were listed as party to a cyber conflict in either a defined or undefined fashion there was no incident in which a state instigated a hostile cyber act with a negative utility when taking into consideration the assumption of anonymity.

The results indicate that even though there are failings to rational choice theory itself from a theoretical standpoint, the theory accurately predicts state interaction. Echoing Milton Friedman's thoughts, an economic theory should be judged not by its realism, but rather by its ability to predict phenomena.³³³ Although in many instances it is likely that cognitive approaches to decision-making might be more accurate, the simplicity offered by a rational choice - expected utility approach to decisions within the cyber domain offers a parsimonious conceptualization of the world.

Despite a dependence on rational choice, it would be useful for future analyses to examine the effect of cognitive behaviors such as prospect theory. These other veins of research will become increasingly helpful in understanding the decision-making processes involved in conflict within the cyber domain as data availability increases. Until data availability improves, studying these cognitive theories in the cyber domain is likely going to be difficult if not impossible.

In closing, the final section specifically addresses the research question proposed in the introductory chapter and what it means to have a more thorough understanding of the decision-

³³³ Milton Friedman, "The Methodology of Positive Economics," in *The Methodology of Positive Economics: Reflections on the Milton Friedman Legacy*, ed. Uskali Maki (Cambridge and New York: Cambridge University Press, 2009; reprint, [1984]).

making process associated with hostile actions on the state level within the cyber domain. This final section builds on all of the lessons learned and the problems encountered, and discusses the importance of this research in the broader context of international relations scholarship.

The implications of the expected utility theory of international cyber conflict

Returning full circle to the research question, this work focused on investigating how unitary state actors rationally decide to employ cyber in military and intelligence operations against other states. This work contextualized broader cyber decision-making processes into a systematic expected utility - rational choice approach to provide a mathematical understanding behind the use of cyber weapons at the state level. Understanding the rational choice decision-making process states employ in deciding to use cyber tactics formed a contextual foundation upon which to build rational offensive and defensive strategies for cyberspace. This dissertation provided the evidence and theoretical foundation for an expected utility - rational-choice decision-making model for the instigation of cyber attacks. To investigate this it was necessary to construct a new decision-making model with its foundations rooted in Bueno de Mesquita's expected utility theory of international conflict.³³⁴

First, as the major lessons learned section earlier in this chapter suggests there are three concepts that have been developed with regards to the cyber domain, that are either unique to the domain, or necessary for actions to take place within it. The concepts of power, anonymity, and political utility for covert acts are pivotal to understanding state on state interactions within this new domain. Just as there are indicators of international political economy, conventional conflict, and every other subject area within the subfield of international relations, there are qualities within the cyber domain that must be included for a study of decisions within cyber to be successful. The lessons open up a realm of discussion not only on topics pertaining to the

³³⁴ Bueno De Mesquita, *The war trap*; Bueno De Mesquita, "An Expected Utility Theory of International Conflict."

cyber domain, but also other types of covert action more broadly. The subfield of international relations has long ignored covert action by theoretically and methodologically pushing it aside. This study attempts to bring back into the fold this often-overlooked area of action.

The data on utility when taking into consideration anonymity are clear and unambiguous. It is possible to generate political utility within the cyber domain through hostile acts. This work illustrates features such as asymmetry between states matters in the context of anonymity. It shows that brute power can still overwhelm, but that attacks can originate from anywhere if the conditions are favorable. Much of the previous literature on cyber has made claims that states act asymmetrically within the cyber domain, but there have been few studies employing rigorous methods testing these claims. This work tests this claim and finds that in many cases a less powerful state can and does initiate hostile acts against a more powerful opponent.

When anonymity was excluded the conventional thought process on power prevailing still holds in all instances with regards to utility. The evidences suggests the largest and most complex types of attacks are still relatively limited to large powerful states, and that those attacks offering higher probabilities of anonymity are still viable to middle range actors.

The power scores indicate a complex understanding of state power within the domain. This understanding of power might surprise many defense theorists who assume that military budgets alone make the biggest difference in all around national security. Instead, what the power scores indicate, in both their theoretical development and their combination into an overall measure of state power, is a complex relationship of a domain that relies on a broad and concerted effort across government and civil society. As a country becomes more dependent on the domain, the more it becomes necessary to ensure the security of that domain through the education of engineers, and the writing of logical rules and regulations.

More than simply generating a better power score the construction of the expected utility of international cyber conflict makes clear the need for an accurate understanding of both one's own and one's adversaries capabilities. More specifically the anonymity function developed indicates a defined niche best filled by the intelligence community. This niche requires an accurate understanding of many aspects of the targets and the tools used to attack those targets. Because anonymity is so important, the role filled by accurate and timely intelligence can make the difference between a decision to engage in conflict and a decision to abstain.

Although the construction of this model and the power variable in particular were done with a focus on hard power, it is not a far stretch to apply many of the same characteristics to the creation of soft power within the domain. Many of the same concepts used to develop a measure of state cyber power can also be used to develop a measure of the capability to employ soft cyber power.

Data constraints at present are the most significant roadblock to creating more robust and meaningful models over time and space. These constraints are falling away quickly and it is likely scholars attempting to make use new data to examine state on state cyber interactions will provide new studies that will build upon the work presented here. It is important that the field not be consumed by studies only constructed with anecdotal evidence. To truly make this area of study applicable to modern international relations it is vital that the anecdotal evidence be supported by rigorous theoretical testing conducted with actual data.

With a small sample of 25 incidents (23 unique) the evidence thus far falls squarely in favor of this model for the expected utility of international cyber conflict. The body of evidence presented here although limited in many ways, does offer a glimpse into how states decide to employ cyber in military and intelligence operations. This work has made a strong case for the rational use of cyber to gain political utility. It has predicated this rational use of the domain on

hard evidence and anecdotal evidence derived from case studies of the various types of attack. It is possible to walk away from this first preliminary attempt at understanding decision-making within this domain with an accurate notion that the cyber domain is not some wild west frontier existing outside the bounds of rationality, but rather it is an environment in which actors continue to act rationally within a new set of constraints.

APPENDIX A: POWER SCORE COMPONENTS & SCORE³³⁵

COUNTRY	MUD	LRF	ESC	TI	IA	MBA	TSC	NDV	Power Score	Weighted Power Score
Argentina	4	5.45	3.71	2.55	1.50	0.05	1.67	3.60	1.33	4.29
Australia	6	8.73	5.95	7.59	6.00	0.33	5	7.60	3.79	8.36
Brazil	6	6.05	3.73	2.23	3.00	0.49	3.33	4.07	2.93	4.58
Canada	6	8.13	5.76	5.76	5.75	0.33	5	8.16	3.24	9.02
China	10	3.25	5.46	3.21	3.00	1.73	5	3.43	6.47	3.58
Estonia	6	9.40	4.29	5.10	5.50	0.00	3.33	7.41	2.27	8.27
France	6	9.25	4.82	4.10	5.75	0.84	5	8.01	3.20	8.89
Georgia	4	3.33	3.00	4.17	1.00	0.00	3.33	2.69	3.20	3.03
Germany	6	10.00	5.06	5.70	3.75	0.64	5	8.20	3.17	9.41
India	8	5.30	2.36	2.10	2.50	0.66	5	0.75	23.24	0.81
Indonesia	0	3.45	3.32	1.36	0.50	0.06	3.33	0.99	4.87	1.33
Iran	4	2.85	2.63	3.96	3.75	0.10	5	1.30	7.38	1.33
Israel	10	9.25	4.75	6.43	5.75	0.20	10	6.72	9.02	7.27
Italy	4	7.73	3.60	4.03	7.25	0.50	3.33	5.37	2.80	5.72
Japan	6	9.08	6.62	3.94	2.25	0.78	3.33	7.82	2.03	9.36
Mexico	4	5.60	4.43	2.01	3.00	0.07	3.33	3.11	3.41	3.63
Russia	8	4.15	3.49	2.26	2.75	0.84	6.67	4.30	2.77	4.57
Saudi Arabia	2	3.18	2.39	2.21	2.25	0.64	3.33	4.10	1.72	4.49
South Africa	2	5.93	3.03	1.80	0.75	0.06	3.33	1.23	6.12	1.57
ROK	6	6.65	5.62	7.03	4.50	0.39	5	8.37	3.01	9.17
Syria	0	1.38	2.46	1.91	1.50	0.03	1.67	2.07	0.98	2.39
Turkey	4	5.45	2.98	1.83	0.75	0.25	3.33	3.98	2.13	4.82
UK	8	10.00	6.35	7.66	6.00	0.83	5	8.50	3.81	9.35
USA	10	10.00	6.40	6.09	5.75	10.00	10	7.40	10.86	7.44

³³⁵ Variables LRF, ESC, TI, and IA are from "Cyber Power Index." In. 2011. ed. Economist Intelligence Unit: Booz Allen Hamilton. NDV is derived from "World Telecommunication/ICT Indicators Database Online." In. 2011. ed. International Telecommunications Union. Switzerland. MUD and TSC are from the case studies of national cyber capabilities presented in Billo, Charles, and Welton Chang. 2004. *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nations*. Institute for Security Technology Studies at Dartmouth College and Lewis, James A., and Katrina Timlin. 2011. *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization*. New York: Center for Strategic and International Studies United Nations Institute for Disarmament Research and Carr, Jeffrey. 2010. *Cyber Warfare*. Sebastopol: O'Reilly Media, Inc. MBA information from "SIPRI Military Expenditure Database." In. 2012. ed. Stockholm International Peace Research Institute (SIPRI). Stockholm.

APPENDIX B: MODIFIED ECONOMIST INTELLIGENCE UNIT COMPONENT VALUES³³⁶

			Argentina	Australia	Brazil	
Legal and Regulatory Framework			Total	54.5	87.25	60.5
Commitment to cyber development*			30.00%	15	26.25	22.5
National cyber plan	Rating 0-4 (4=best)	50.00%	50	100	75	
Public-private partnerships	Rating 0-4 (4=best)	50.00%	50	75	75	
Cyber protection policy*			30.00%	12	21	10.5
Cyber enforcement authority	Rating 0-4 (4=best)	20.00%	50	100	50	
Cyber security laws	Rating 0-4 (4=best)	20.00%	50	100	50	
Cyber crime response	Rating 0-4 (4=best)	20.00%	75	100	50	
International cyber security commitments	Rating 0-4 (4=best)	20.00%	25	25	0	
Cyber security plan	Rating 0-4 (4=best)	20.00%	0	25	25	
Cyber censorship*	Rating 0-2 (2=Best)	15%	15	15	15	
Cyber censorship	Rating 0-2 (2=Best)	15.00%	100	100	100	
Intellectual property protection*	Rating 0-4 (0=Best)	25%	12.5	25	12.5	
Intellectual property protection	Rating 0-4 (0=Best)	25.00%	50	100	50	
Economic and Social Context			Total	37.05	59.47	37.34
Educational levels*			25.20%	18.72	17.8	13.96
Tertiary student enrollment	% of gross enrollment	50.00%	92.35	41.25	73.28	
Expected years of education	primary to tertiary, in years	50.00%	56.25	100	37.5	
Technical skills*		27.40%	10.11	16.76	7.46	
Labour productivity growth	% change between 2009-2010	25.00%	76.72	15.52	56.9	
Researchers in R&D	per million population	25.00%	20.87	90.57	14.75	
S&E degrees	% of total degrees	25.00%	0	38.6	12.28	

³³⁶ Data for all countries except Georgia, Iran, Israel, Syria, and Estonia are from "Cyber Power Index." In. 2011. ed. Economist Intelligence Unit: Booz Allen Hamilton. The 5 additional countries added include data from the same sources as the EIU data including: Economist Intelligence Unit, Billo, Charles, and Welton Chang. 2004. *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nations*. Institute for Security Technology Studies at Dartmouth College; Lewis, James A., and Katrina Timlin. 2011. *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization*. New York: Center for Strategic and International Studies United Nations Institute for Disarmament Research; Carr, Jeffrey. 2010. *Cyber Warfare*. Sebastopol: O'Reilly Media, Inc; Kelly, Sanja, and Sarah Cook. 2011. "Freedom on the Net 2011: A Global Assessment of Internet and Digital Media." In, ed. Freedom House. Washington, D.C.; . 2012. ed. Scientific and Cultural Organization (UNESCO) Institute for Statistics United Nations Educational. New York; "United Nations Commodity Trade Statistics Database." In. 2012. ed. United Nations. New York: United Nations; World, Bank, Group World Bank. International Economics Dept. Development Data, and Group World Bank. Development Data. 2012. World development indicators. World development indicators; "2012 Global E-Government Survey." In. 2012. ed. United Nations Public Administration Network. New York: United Nations. Several of the variables included in the Cyber Power Index were omitted due to data limitations across nations. All data from the newly added countries was included from the most recent year to date with available data from the same sources as used by the Economist Intelligence Unit to maintain consistency. Where variables were dropped the weighting percentages were proportionally distributed.

		Argentina	Australia	Brazil	
English literacy	Rating 0-4 (4=Best)	25.00%	50	100	25
Trade*		17.30%	6.22	7.62	6.54
ICT exports	% of total exports	33.33%	1.36	4.75	6.1
ICT imports	% of total imports	33.33%	46.67	47.5	47.5
Openness to trade	Rating 1-5 (5=Best)	33.33%	60	80	60
Innovation environment*		30.10%	1.99	17.29	9.38
R&D investment	% of GDP	33.33%	10.64	44.68	23.4
Domestic patent filings	filings per million population	33.33%	8.69	82.83	7.42
Private equity investment	% of GDP	33.33%	0	40	60
Technology Infrastructure		Total	25.46	75.91	22.25
ICT access*		22.00%	10.52	16.31	7.37
Internet penetration	internet users per 100 people	50.00%	29.7	83.08	25.44
Mobile cellular penetration	mobile cellular subscriptions per 100 people	50.00%	65.98	65.15	41.56
ICT quality*		23.00%	3.56	9.27	2.57
Fixed broadband subscribers	% of all internet subscribers	50.00%	25.21	67.05	17.19
International internet bandwidth	bits/second/person	50.00%	5.72	13.57	5.19
Telecom Investment as % of GDP*	% of GDP	20.00%	6.17	15.37	8.31
Telecom Investment as % of GDP	% of GDP	20.00%	30.85	76.84	41.54
ICT affordability*		10.00%	4.75	3.49	3.29
Mobile phone tariffs	PPP \$	50.00%	68.92	82.91	19.67
Broadband internet tariffs	PPP \$	50.00%	26.1	-13.21	46.12
Secure servers*	secure servers per million	25.80%	0.45	31.48	0.71
Secure servers	secure servers per million	25.80%	1.75	122.03	2.77
Industry Application		Total	15	60	30
Smart grids	Rating 0-4 (4=best)	60%	0	50	25
E-Health	Rating 0-4 (4=best)	20%	50	75	50
E-Government	Rating 0-1 (1=best)	20%	25	75	25

			Canada	China	France
Legal and Regulatory Framework					
	Total		81.25	32.5	92.5
Commitment to cyber development*	30.00%		26.25	11.25	30
National cyber plan	Rating 0-4 (4=best)	50.00%	75	50	100
Public-private partnerships	Rating 0-4 (4=best)	50.00%	100	25	100
Cyber protection policy*		30.00%	15	15	30
Cyber enforcement authority	Rating 0-4 (4=best)	20.00%	50	75	100
Cyber security laws	Rating 0-4 (4=best)	20.00%	75	50	100
Cyber crime response	Rating 0-4 (4=best)	20.00%	50	50	100
International cyber security commitments	Rating 0-4 (4=best)	20.00%	50	50	100
Cyber security plan	Rating 0-4 (4=best)	20.00%	25	25	100
Cyber censorship*	Rating 0-2 (2=Best)	15%	15	0	7.5
Cyber censorship	Rating 0-2 (2=Best)	15.00%	100	0	50
Intellectual property protection*	Rating 0-4 (0=Best)	25%	25	6.25	25
Intellectual property protection	Rating 0-4 (0=Best)	25.00%	100	25	100
Economic and Social Context					
	Total		57.56	54.6	48.2
Educational levels*	25.20%		10.41	9.55	14.25
Tertiary student enrollment	% of gross enrollment	50.00%	24.25	63.29	53.7
Expected years of education	primary to tertiary, in years	50.00%	58.33	12.5	59.38
Technical skills*		27.40%	18.3	16.86	14.03
Labour productivity growth	% change between 2009-2010	25.00%	30.17	98.28	25.86
Researchers in R&D	per million population	25.00%	91.35	22.84	74.93
S&E degrees	% of total degrees awarded	25.00%	45.61	100	54.09
English literacy	Rating 0-4 (4=Best)	25.00%	100	25	50
Trade*		17.30%	8.92	17.28	7.57
ICT exports	% of total exports	33.33%	14.92	100	18.98
ICT imports	% of total imports	33.33%	40	100	32.5
Openness to trade	Rating 1-5 (5=Best)	33.33%	100	100	80
Innovation environment*		30.10%	19.93	10.91	12.34
R&D investment	% of GDP	33.33%	38.3	29.79	42.55
Domestic patent filings	filings per million population	33.33%	74.78	15.86	17.01
Private equity investment	% of GDP	33.33%	80	60	60
Technology Infrastructure					
	Total		57.63	32.11	40.97
ICT access*		22.00%	13.12	4.67	14.39
Internet penetration	internet users per 100 people	50.00%	90.85	23.56	79.45
Mobile cellular penetration	mobile cellular subscriptions per 100 people	50.00%	28.39	18.87	51.32

			Canada	China	France
ICT quality*		23.00%	14.21	3.01	19.38
Fixed broadband subscribers	% of all internet subscribers	50.00%	83.09	24.64	95.13
International internet bandwidth	bits/second/person	50.00%	40.43	1.55	73.37
Telecom Investment as % of GDP*	% of GDP	20.00%	2.78	16.47	0.55
Telecom Investment as % of GDP	% of GDP	20.00%	13.92	82.34	2.77
ICT affordability*		10.00%	5.41	7.94	1.38
Mobile phone tariffs	PPP \$	50.00%	58.46	92.52	7.64
Broadband internet tariffs	PPP \$	50.00%	49.74	66.24	19.94
Secure servers*	secure servers per million	25.80%	22.11	0.02	5.28
Secure servers	secure servers per million	25.80%	85.69	0.08	20.46
Industry Application		Total	57.5	30	57.5
Smart grids	Rating 0-4 (4=best)	60%	50	25	50
E-Health	Rating 0-4 (4=best)	20%	50	50	75
E-Government	Rating 0-1 (1=best)	20%	87.5	25	62.5

			Germany	India	Indonesia
Legal and Regulatory Framework					
	Total		100	53	34.5
Commitment to cyber development*	30.00%		30	15	15
National cyber plan	Rating 0-4 (4=best)	50.00%	100	50	50
Public-private partnerships	Rating 0-4 (4=best)	50.00%	100	50	50
Cyber protection policy*		30.00%	30	10.5	12
Cyber enforcement authority	Rating 0-4 (4=best)	20.00%	100	50	75
Cyber security laws	Rating 0-4 (4=best)	20.00%	100	50	50
Cyber crime response	Rating 0-4 (4=best)	20.00%	100	50	75
International cyber security commitments	Rating 0-4 (4=best)	20.00%	100	0	0
Cyber security plan	Rating 0-4 (4=best)	20.00%	100	25	0
Cyber censorship*	Rating 0-2 (2=Best)	15%	15	15	7.5
Cyber censorship	Rating 0-2 (2=Best)	15.00%	100	100	50
Intellectual property protection*	Rating 0-4 (0=Best)	25%	25	12.5	0
Intellectual property protection	Rating 0-4 (0=Best)	25.00%	100	50	0
Economic and Social Context					
	Total		50.59	23.62	33.19
Educational levels*		25.20%	8.61	2.89	13.71
Tertiary student enrollment	% of gross enrollment	50.00%	9.99	22.96	79.64
Expected years of education	primary to tertiary, in years	50.00%	58.33	0	29.17
Technical skills*		27.40%	18	10.18	6.05
Labour productivity growth	% change between 2009-2010	25.00%	41.38	28.45	39.66
Researchers in R&D	per million population	25.00%	75.7	2.78	4.24
S&E degrees	% of total degrees awarded	25.00%	70.76	92.4	44.44
English literacy	Rating 0-4 (4=Best)	25.00%	75	25	0
Trade*		17.30%	9.32	8.62	9.2
ICT exports	% of total exports	33.33%	23.05	12.88	19.32
ICT imports	% of total imports	33.33%	38.75	36.67	40.42
Openness to trade	Rating 1-5 (5=Best)	33.33%	100	100	100
Innovation environment*		30.10%	14.66	1.94	4.22
R&D investment	% of GDP	33.33%	53.19	17.02	0
Domestic patent filings	filings per million population	33.33%	48.82	1.72	0.9
Private equity investment	% of GDP	33.33%	40	0	40
Technology Infrastructure					
	Total		56.97	21.02	13.57
ICT access*		22.00%	19.06	6.92	2.86
Internet penetration	internet users per 100 people	50.00%	89.1	1.52	3.88
Mobile cellular penetration	mobile cellular subscriptions per 100 people	50.00%	84.19	61.42	22.1

			Germany	India	Indonesia
ICT quality*		23.00%	17.55	0.03	0.02
Fixed broadband subscribers	% of all internet subscribers	50.00%	88.54	0.29	0
International internet bandwidth	bits/second/person	50.00%	64.11	0	0.2
Telecom Investment as % of GDP*	% of GDP	20.00%	0.05	4.04	2.65
Telecom Investment as % of GDP	% of GDP	20.00%	0.23	20.21	13.25
ICT affordability*		10.00%	4.75	10	8.02
Mobile phone tariffs	PPP \$	50.00%	94.07	100	98.76
Broadband internet tariffs	PPP \$	50.00%	0.85	99.99	61.66
Secure servers*	secure servers per million	25.80%	15.57	0.02	0.02
Secure servers	secure servers per million	25.80%	60.33	0.1	0.09
Industry Application		Total	37.5	25	5
Smart grids	Rating 0-4 (4=best)	60%	25	25	0
E-Health	Rating 0-4 (4=best)	20%	75	25	25
E-Government	Rating 0-1 (1=best)	20%	37.5	25	0

			Italy	Japan	Mexico
Legal and Regulatory Framework					
	Total		77.25	90.75	56
Commitment to cyber development*	30.00%		22.5	30	15
National cyber plan	Rating 0-4 (4=best)	50.00%	75	100	50
Public-private partnerships	Rating 0-4 (4=best)	50.00%	75	100	50
Cyber protection policy*		30.00%	21	27	13.5
Cyber enforcement authority	Rating 0-4 (4=best)	20.00%	50	100	75
Cyber security laws	Rating 0-4 (4=best)	20.00%	75	100	50
Cyber crime response	Rating 0-4 (4=best)	20.00%	75	100	50
International cyber security commitments	Rating 0-4 (4=best)	20.00%	100	50	25
Cyber security plan	Rating 0-4 (4=best)	20.00%	50	100	25
Cyber censorship*	Rating 0-2 (2=Best)	15.00%	15	15	15
Cyber censorship	Rating 0-2 (2=Best)	15.00%	100	100	100
Intellectual property protection*	Rating 0-4 (0=Best)	25%	18.75	18.75	12.5
Intellectual property protection	Rating 0-4 (0=Best)	25.00%	75	75	50
Economic and Social Context					
	Total		35.95	66.23	44.34
Educational levels*		25.20%	12.34	9.67	16.26
Tertiary student enrollment	% of gross enrollment	50.00%	67.7	27.76	92.61
Expected years of education	primary to tertiary, in years	50.00%	30.21	48.96	36.46
Technical skills*		27.40%	8.96	18.72	10.88
Labour productivity growth	% change between 2009-2010	25.00%	24.14	53.45	49.14
Researchers in R&D	per million population	25.00%	34.54	119.54	7.41
S&E degrees	% of total degrees awarded	25.00%	47.08	50.29	52.34
English literacy	Rating 0-4 (4=Best)	25.00%	25	50	50
Trade*		17.30%	6.8	9.21	15.25
ICT exports	% of total exports	33.33%	10.17	49.83	77.63
ICT imports	% of total imports	33.33%	27.92	50	87.08
Openness to trade	Rating 1-5 (5=Best)	33.33%	80	60	100
Innovation environment*		30.10%	7.85	28.64	1.95
R&D investment	% of GDP	33.33%	25.53	72.34	10.64
Domestic patent filings	filings per million population	33.33%	10.52	185.07	8.24
Private equity investment	% of GDP	33.33%	40	20	0
Technology Infrastructure					
	Total		40.27	39.38	20.11
ICT access*		22.00%	16.6	14.92	6.08
Internet penetration	internet users per 100 people	50.00%	50.13	88.85	23.56
Mobile cellular penetration	mobile cellular subscriptions per 100 people	50.00%	100.75	46.77	31.71

			Italy	Japan	Mexico
ICT quality*		23.00%	10.68	10.25	3.11
Fixed broadband subscribers	% of all internet subscribers	50.00%	60.46	74.79	26.36
International internet bandwidth	bits/second/person	50.00%	32.42	14.36	0.7
Telecom Investment as % of GDP*	% of GDP	20.00%	4.72	1.82	2.52
Telecom Investment as % of GDP	% of GDP	20.00%	23.62	9.09	12.62
ICT affordability*		10.00%	5.52	0.79	8.04
Mobile phone tariffs	PPP \$	50.00%	71.6	-0.09	90.52
Broadband internet tariffs	PPP \$	50.00%	38.83	15.92	70.35
Secure servers*	secure servers per million	25.80%	2.75	11.6	0.35
Secure servers	secure servers per million	25.80%	10.64	44.95	1.38
Industry Application		Total	72.5	22.5	30
Smart grids	Rating 0-4 (4=best)	60%	100	0	25
E-Health	Rating 0-4 (4=best)	20%	50	50	50
E-Government	Rating 0-1 (1=best)	20%	12.5	62.5	25

			Russia	Saudi Arabia	South Africa
Legal and Regulatory Framework					
		Total	41.5	31.75	59.25
Commitment to cyber development*		30.00%	18.75	15	15
National cyber plan	Rating 0-4 (4=best)	50.00%	75	50	75
Public-private partnerships	Rating 0-4 (4=best)	50.00%	50	50	25
Cyber protection policy*		30.00%	9	10.5	10.5
Cyber enforcement authority	Rating 0-4 (4=best)	20.00%	75	75	0
Cyber security laws	Rating 0-4 (4=best)	20.00%	25	50	50
Cyber crime response	Rating 0-4 (4=best)	20.00%	50	50	50
International cyber security commitments	Rating 0-4 (4=best)	20.00%	0	0	50
Cyber security plan	Rating 0-4 (4=best)	20.00%	0	0	25
Cyber censorship*	Rating 0-2 (2=Best)	15%	7.5	0	15
Cyber censorship	Rating 0-2 (2=Best)	15.00%	50	0	100
Intellectual property protection*	Rating 0-4 (0=Best)	25%	6.25	6.25	18.75
Intellectual property protection	Rating 0-4 (0=Best)	25.00%	25	25	75
Economic and Social Context					
		Total	34.86	23.89	30.34
Educational levels*		25.20%	9.27	4.33	7.38
Tertiary student enrollment	% of gross enrollment	50.00%	35.02	0	31.52
Expected years of education	primary to tertiary, in years	50.00%	38.54	34.38	27.08
Technical skills*		27.40%	12.73	10.4	12.22
Labour productivity growth	% change between 2009-2010	25.00%	44.83	33.62	55.17
Researchers in R&D	per million population	25.00%	68.38	3.39	8.27
S&E degrees	% of total degrees awarded	25.00%	47.66	89.77	64.91
English literacy	Rating 0-4 (4=Best)	25.00%	25	25	50
Trade*		17.30%	6.74	6.92	7.35
ICT exports	% of total exports	33.33%	2.03	1.02	6.78
ICT imports	% of total imports	33.33%	35	19.17	40.83
Openness to trade	Rating 1-5 (5=Best)	33.33%	80	100	80
Innovation environment*		30.10%	6.11	2.24	3.39
R&D investment	% of GDP	33.33%	21.28	0	19.15
Domestic patent filings	filings per million population	33.33%	17.94	1.66	13.68
Private equity investment	% of GDP	33.33%	20	20	0
Technology Infrastructure					
		Total	22.61	22.09	17.99
ICT access*		22.00%	12.39	12.19	7.11
Internet penetration	internet users per 100 people	50.00%	27.94	39.1	5.14
Mobile cellular penetration	mobile cellular subscriptions per 100 people	50.00%	84.69	71.69	59.52

			Russia	Saudi Arabia	South Africa
ICT quality*		23.00%	3.52	2.04	0.24
Fixed broadband subscribers	% of all internet subscribers	50.00%	29.23	13.47	2.01
International internet bandwidth	bits/second/person	50.00%	1.35	4.25	0.1
Telecom Investment as % of GDP*	% of GDP	20.00%	-2.06	1.38	3.68
Telecom Investment as % of GDP	% of GDP	20.00%	-10.29	6.9	18.39
ICT affordability*		10.00%	8.41	6.19	5.86
Mobile phone tariffs	PPP \$	50.00%	88.46	82.25	66.99
Broadband internet tariffs	PPP \$	50.00%	79.83	41.48	50.14
Secure servers*	secure servers per million	25.80%	0.35	0.3	1.1
Secure servers	secure servers per million	25.80%	1.36	1.16	4.28
Industry Application		Total	27.5	22.5	7.5
Smart grids	Rating 0-4 (4=best)	60%	25	25	0
E-Health	Rating 0-4 (4=best)	20%	50	25	25
E-Government	Rating 0-1 (1=best)	20%	12.5	12.5	12.5

			South Korea	Turkey	United Kingdom
Legal and Regulatory Framework					
	Total		66.5	54.5	100
Commitment to cyber development*	30.00%		30	15	30
National cyber plan	Rating 0-4 (4=best)	50.00%	100	75	100
Public-private partnerships	Rating 0-4 (4=best)	50.00%	100	25	100
Cyber protection policy*		30.00%	16.5	19.5	30
Cyber enforcement authority	Rating 0-4 (4=best)	20.00%	100	75	100
Cyber security laws	Rating 0-4 (4=best)	20.00%	75	75	100
Cyber crime response	Rating 0-4 (4=best)	20.00%	75	75	100
International cyber security commitments	Rating 0-4 (4=best)	20.00%	0	50	100
Cyber security plan	Rating 0-4 (4=best)	20.00%	25	50	100
Cyber censorship*	Rating 0-2 (2=Best)	15%	7.5	7.5	15
Cyber censorship	Rating 0-2 (2=Best)	15.00%	50	50	100
Intellectual property protection*	Rating 0-4 (0=Best)	25%	12.5	12.5	25
Intellectual property protection	Rating 0-4 (0=Best)	25.00%	50	50	100
Economic and Social Context					
	Total		56.23	29.8	63.52
Educational levels*	25.20%		13.86	10.27	20.08
Tertiary student enrollment	% of gross enrollment	50.00%	42.28	66.93	100
Expected years of education	primary to tertiary, in years	50.00%	67.71	14.58	59.38
Technical skills*		27.40%	19.31	9.24	17.64
Labour productivity growth	% change between 2009-2010	25.00%	56.03	37.93	24.14
Researchers in R&D	per million population	25.00%	99.22	14.45	91.53
S&E degrees	% of total degrees awarded	25.00%	76.61	82.46	41.81
English literacy	Rating 0-4 (4=Best)	25.00%	50	0	100
Trade*		17.30%	12.88	6.47	8.81
ICT exports	% of total exports	33.33%	49.49	7.8	29.15
ICT imports	% of total imports	33.33%	94.17	24.58	43.75
Openness to trade	Rating 1-5 (5=Best)	33.33%	80	80	80
Innovation environment*		30.10%	10.18	3.82	16.99
R&D investment	% of GDP	33.33%	68.09	14.89	40.43
Domestic patent filings	filings per million population	33.33%	10.52	2.1	24.14
Private equity investment	% of GDP	33.33%	20	20	100
Technology Infrastructure					
	Total		70.32	18.27	76.56
ICT access*		22.00%	16.05	9.84	18.63
Internet penetration	internet users per 100 people	50.00%	93.73	38.6	89.6
Mobile cellular penetration	mobile cellular subscriptions per 100 people	50.00%	52.15	50.83	79.8

			South Korea	Turkey	United Kingdom
ICT quality*		23.00%	13.24	4.17	21.55
Fixed broadband subscribers	% of all internet subscribers	50.00%	100	25.5	88.25
International internet bandwidth	bits/second/person	50.00%	15.09	10.74	99.16
Telecom Investment as % of GDP*	% of GDP	20.00%	15.04	-2.89	5.95
Telecom Investment as % of GDP	% of GDP	20.00%	75.2	-14.47	29.77
ICT affordability*		10.00%	5.86	5.4	5.49
Mobile phone tariffs	PPP \$	50.00%	62.86	41.05	59.31
Broadband internet tariffs	PPP \$	50.00%	54.27	66.97	50.46
Secure servers*	secure servers per million	25.80%	20.14	1.76	24.93
Secure servers	secure servers per million	25.80%	78.06	6.8	96.61
Industry Application		Total	45	7.5	60
Smart grids	Rating 0-4 (4=best)	60%	25	0	50
E-Health	Rating 0-4 (4=best)	20%	50	25	75
E-Government	Rating 0-1 (1=best)	20%	100	12.5	75

			United States	Israel	Syria
Legal and Regulatory Framework					
	Total		100	92.5	13.75
Commitment to cyber development*	30.00%		30	30	0
National cyber plan	Rating 0-4 (4=best)	50.00%	100	100	0
Public-private partnerships	Rating 0-4 (4=best)	50.00%	100	100	0
Cyber protection policy*		30.00%	30	22.5	7.5
Cyber enforcement authority	Rating 0-4 (4=best)	20.00%	100	100	75
Cyber security laws	Rating 0-4 (4=best)	20.00%	100	75	25
Cyber crime response	Rating 0-4 (4=best)	20.00%	100	100	25
International cyber security commitments	Rating 0-4 (4=best)	20.00%	100	0	0
Cyber security plan	Rating 0-4 (4=best)	20.00%	100	100	0
Cyber censorship*	Rating 0-2 (2=Best)	15%	15	15	0
Cyber censorship	Rating 0-2 (2=Best)	15.00%	100	100	0
Intellectual property protection*	Rating 0-4 (0=Best)	25%	25	25	6.25
Intellectual property protection	Rating 0-4 (0=Best)	25.00%	100	100	25
Economic and Social Context					
	Total		63.95	47.54	24.58
Educational levels*	25.20%		15.01	6.74	9.63
Tertiary student enrollment	% of gross enrollment	50.00%	60.83	0.389	67.06
Expected years of education	primary to tertiary, in years	50.00%	58.33	53.13	9.38
Technical skills*		27.40%	18.47	15.87	9.65
Labour productivity growth	% change between 2009-2010	25.00%	45.69	31.9	91.38
Researchers in R&D	per million population	25.00%	100	33.56	0.46
S&E degrees	% of total degrees awarded	25.00%	23.98	91.23	23.98
English literacy	Rating 0-4 (4=Best)	25.00%	100	75	25
Trade*		17.30%	11.92	9.2	5.09
ICT exports	% of total exports	33.33%	44.07	41.69	0
ICT imports	% of total imports	33.33%	62.92	37.92	8.33
Openness to trade	Rating 1-5 (5=Best)	33.33%	100	80	80
Innovation environment*		30.10%	18.54	15.73	0.22
R&D investment	% of GDP	33.33%	59.57	100	2.13
Domestic patent filings	filings per million population	33.33%	100.05	12.42	0
Private equity investment	% of GDP	33.33%	20	40	0
Technology Infrastructure					
	Total		60.87	64.26	19.1
ICT access*		22.00%	16.36	18.01	4.75
Internet penetration	internet users per 100 people	50.00%	101.25	78.57	20.3
Mobile cellular penetration	mobile cellular subscriptions per 100 people	50.00%	47.52	85.18	22.85

			United States	Israel	Syria
ICT quality*		23.00%	12.07	19.51	4.42
Fixed broadband subscribers	% of all internet subscribers	50.00%	76.79	69.63	24.16
International internet bandwidth	bits/second/person	50.00%	28.14	100	14.27
Telecom Investment as % of GDP*	% of GDP	20.00%	-0.01	11.18	4.13
Telecom Investment as % of GDP	% of GDP	20.00%	-0.07	55.92	20.65
ICT affordability*		10.00%	6.65	8.49	5.8
Mobile phone tariffs	PPP \$	50.00%	73.2	72.99	26.99
Broadband internet tariffs	PPP \$	50.00%	59.76	96.74	89.09
Secure servers*	secure servers per million	25.80%	25.8	7.07	0
Secure servers	secure servers per million	25.80%	100	27.41	0
Industry Application		Total	57.5	57.5	15
Smart grids	Rating 0-4 (4=best)	60%	50	50	0
E-Health	Rating 0-4 (4=best)	20%	50	50	0
E-Government	Rating 0-1 (1=best)	20%	87.5	87.5	75

			Estonia	Iran	Georgia
Legal and Regulatory Framework					
	Total		94	28.5	33.25
Commitment to cyber development*	30.00%		30	15	7.5
National cyber plan	Rating 0-4 (4=best)	50.00%	100	25	25
Public-private partnerships	Rating 0-4 (4=best)	50.00%	100	75	25
Cyber protection policy*		30.00%	24	13.5	12
Cyber enforcement authority	Rating 0-4 (4=best)	20.00%	75	75	0
Cyber security laws	Rating 0-4 (4=best)	20.00%	75	75	25
Cyber crime response	Rating 0-4 (4=best)	20.00%	50	50	50
International cyber security commitments	Rating 0-4 (4=best)	20.00%	100	0	100
Cyber security plan	Rating 0-4 (4=best)	20.00%	100	25	25
Cyber censorship*	Rating 0-2 (2=Best)	15%	15	0	7.5
Cyber censorship	Rating 0-2 (2=Best)	15.00%	100	0	50
Intellectual property protection*	Rating 0-4 (0=Best)	25%	25	0	6.25
Intellectual property protection	Rating 0-4 (0=Best)	25.00%	100	0	25
Economic and Social Context					
	Total		42.88	26.34	29.96
Educational levels*	25.20%		13.04	7.71	15.18
Tertiary student enrollment	% of gross enrollment	50.00%	48.25	37.22	92.35
Expected years of education	primary to tertiary, in years	50.00%	55.21	23.96	28.13
Technical skills*		27.40%	17.11	11.94	7.58
Labour productivity growth	% change between 2009-2010	25.00%	55.17	0	52.59
Researchers in R&D	per million population	25.00%	53.45	15.97	0
S&E degrees	% of total degrees awarded	25.00%	91.23	133.33	33.1
English literacy	Rating 0-4 (4=Best)	25.00%	50	25	25
Trade*		17.30%	7.86	4.61	6.52
ICT exports	% of total exports	33.33%	26.44	0	0.68
ICT imports	% of total imports	33.33%	30	0	32.5
Openness to trade	Rating 1-5 (5=Best)	33.33%	80	80	80
Innovation environment*		30.10%	4.87	2.08	0.67
R&D investment	% of GDP	33.33%	23.4	14.89	4.26
Domestic patent filings	filings per million population	33.33%	3.79	5.28	2.27
Private equity investment	% of GDP	33.33%	20	0	0
Technology Infrastructure					
	Total		51.02	39.61	41.69
ICT access*	22.00%		18.05	6.73	8.67
Internet penetration	internet users per 100 people	50.00%	87.09	10.65	28.07
Mobile cellular penetration	mobile cellular subscriptions per 100 people	50.00%	76.99	50.5	50.75

			Estonia	Iran	Georgia
ICT quality*		23.00%	14.62	11.92	8.83
Fixed broadband subscribers	% of all internet subscribers	50.00%	69.63	28.65	14.33
International internet bandwidth	bits/second/person	50.00%	57.47	74.98	62.47
Telecom Investment as % of GDP*	% of GDP	20.00%	4.99	14.64	20
Telecom Investment as % of GDP	% of GDP	20.00%	24.95	73.19	100
ICT affordability*		10.00%	5.62	6.33	3.99
Mobile phone tariffs	PPP \$	50.00%	70.7	94.95	79.75
Broadband internet tariffs	PPP \$	50.00%	41.77	31.56	-0.02
Secure servers*	secure servers per million	25.80%	7.74	0	0.2
Secure servers	secure servers per million	25.80%	30.02	0	0.77
Industry Application		Total	55	37.5	10
Smart grids	Rating 0-4 (4=best)	60%	50	50	0
E-Health	Rating 0-4 (4=best)	20%	50	0	0
E-Government	Rating 0-1 (1=best)	20%	75	37.5	50

Of note within the above appendix, duplications appear. These are not duplications of numbers and are instead weighting of values within various categories. For instance, within the subcategory of ICT affordability are mobile phone tariffs and broadband tariffs. These two combine to make up the sub category ICT affordability. Because secure servers is independent its weighted value is placed above it with the * symbol to indicate the within variable weighted value per country. * denotes the weighted sub categories that make up the variable. These sub categories can contain other variables within them. Bold represents the variables used within the model.

APPENDIX C: AFFINITY SCORES³³⁷

Instigator	Target	Year	Type	t-2	t-1	Difference in Affinity
China	USA	2006	CNE	-0.69	-0.71	0.02
China	UK	2006	Equipment Disruption	0.17	0.19	-0.02
Russia	Estonia	2007	DDOS	0.55	0.51	0.04
China	UK	2007	CNE	0.19	0.27	-0.08
China	France	2007	CNE	0.25	0.28	-0.03
China	Germany	2007	CNE	0.41	0.42	-0.01
Israel	Syria	2007	Critical Infrastructure Disruption	-0.52	-0.44	-0.08
China	France	2007	CNE	0.25	0.28	-0.03
China	UK	2007	CNE	0.27	0.18	0.09
China	ROK	2008	CNE	0.49	0.49	0
China	India	2008	CNE	0.82	0.8	0.02
Russia	Georgia	2008	DDOS	0.52	0.49	0.03
China	Canada	2009	CNE	0.13	0.11	0.02
China	ROK	2009	CNE	0.49	0.46	0.03
China	India	2010	CNE	0.76	0.81	-0.05
Iran	China	2010	Website Defacement	0.9	0.93	-0.03
China	Australia	2010	CNE	0.13	0.1	0.03
China	India	2010	CNE	0.76	0.81	-0.05
U.S.	Iran	2010	Compromised Hardware Systems	-0.71	-0.64	-0.07
Israel	Iran	2010	Compromised Hardware Systems	-0.41	-0.59	0.18
China	Canada	2011	CNE	0	0.06	-0.06
China	ROK	2011	CNE	0.39	0.44	-0.05
China	Japan	2011	CNE	0.42	0.46	-0.04
Israel	Iran	2011	CNE	-0.59	-0.63	0.04
U.S. or Israel	Iran	2011	CNE	-0.65	-0.57	-0.08

³³⁷ Strezhnev and Voeten, "United Nations General Assembly Voting Data."

WORKS CITED

"Joint Doctrine for Command and Control Warfare (C2W)." edited by Joint Chiefs of Staff. Washington, D.C.: Department of Defense, 1996.

"Joint Vision 2020." Washington, D.C.: US Government Printing Office, 2000.

"Joint Doctrine for Electronic Warfare Joint Publication 3-51." edited by Department of Defense. Washington, D.C. , 2000.

"The President's Constitutional Authority to Conduct Military Operations against Terrorists and Nations Supporting Them." In ed. Department of Justice, (2001). <http://www.justice.gov/olc/warpowers925.htm>.

The National Strategy to Secure Cyberspace. [Washington, D.C.]: President's Critical Infrastructure Protection Board, 2003.

"The National Strategy to Secure Cyberspace." Washington, D.C.: United States Department of Homeland Security, 2003.

"The Military Power of the People's Republic of China." Washington, D.C.: Department of Defense, 2005.

"Europe: A Cyber-Riot; Estonia and Russia." *The Economist*, May 12 2007.

"Defense Critical Infrastructure: Gao-08-373r." *GAO Reports* (2008): 1.

International CIIP Handbook 2008/2009: An Inventory of 25 National and 7

International

Critical Information Infrastructure Protection Policies. Edited by Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty Zurich: Center for Security Studies, 2008.

"Tracking Ghostnet: Investigating a Cyber Espionage Network." Toronto: Munk Center for International Studies at the University of Toronto, 2009.

"National Security Act of 1947." *National Security Act of 1947* (2009): 1.

"We Are Anonymous, We Are Legion." In *Yale Law & Technology*. Yale Law Tech, 2009.

"Cyber Shockwave - Simulation Report and Findings." Washington, D.C.: Bipartisan Policy Center, 2010.

"What Are Information Operations." Cyberspace and information operations study center, <http://www.au.af.mil/info-ops/what.htm>.

"Cyberwar." *The Economist*, July 3 2010.

"E-Stats, 2009 E-Commerce Multi-Sector Report." Washington, D.C.: U.S. Census Bureau, 2011.

"Department of Defense Strategy for Operating in Cyberspace." edited by Department of Defense. Washington, D.C.: Department of Defense, 2011.

"Cyber Power Index." edited by Economist Intelligence Unit: Booz Allen Hamilton, 2011.

"World Telecommunication/Ict Indicators Database Online." edited by International Telecommunications Union. Switzerland, 2011.

Oversight and Investigations Subcommittee of the Foreign Affairs Committee of the United States House of Representatives, for its Hearing On: "Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology". *Cyber Warfare Challenges and the Increasing Use of American and European Dual-Use Technology for Military Purposes by the People's Republic of China (PRC)*, 15

April 2011.

"International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World." edited by The President of The United States. Washington, D.C., 2011.

"Internet Map." In *Graphviz*. <http://www.opte.org/maps/>: The Opte Project, 2005.

"Foreign Spies Stealing U.S. Economic Secrets in Cyberspace." Washington, D.C.: Office of the Director of National Intelligence, 2011.

"Presidential Directives and Executive Orders." Federation of American Scientists, <http://www.fas.org/irp/offdocs/direct.htm>.

Merriam Webster. 2012.

"Anonymous 'Takes Down' CIA Website." In, *Aljazeera* (2012).

Abrams, Marshall, and Joe Weiss. "Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia." 2008.

Alberts, David S. *Understanding Information Age Warfare*. Washington, DC: CCRP Publication Series, 2001.

Alexander, Keith B. "Building a New Command in Cyberspace." *Strategic Studies Quarterly* Summer (2011): 3-12.

Amoroso, Edward G. *Cyber Attacks: Protecting National Infrastructure*. Oxford: Butterworth-Heinemann, 2010.

Angstrom, Jan, and Isabelle Duyvesteyn. "Understanding Victory and Defeat in Contemporary War." Routledge, <http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=178957>.

- Arquilla, John. *Insurgents, Raiders, and Bandits: How Masters of Irregular Warfare Have Shaped Our World*. Chicago; [Lanham, Md.]: Ivan R. Dee ; Distributed by National Book Network, 2011.
- . "Cyberwar Is Already Upon Us." *Foreign Policy*, no. March/April (2012): 84-86.
- Arquilla, John, and David Ronfeldt. *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica, CA: Rand Coporation, 1997.
- Arrow, Kenneth. "A Difficulty in the Concept of Social Welfare." *The Journal of Political Economy* 58, no. 4 (Aug. 1950): 328-46.
- Baldwin, David A. *Neorealism and Neoliberalism: The Contemporary Debate*. New York: Columbia University Press, 1993.
- Bearden, Milt, and James Risen. *The Main Enemy: The Inside Story of the CIA's Final Showdown with the KGB*. New York: Random House, 2003.
- Benkler, Yochai. *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven [Conn.]: Yale University Press, 2006.
- Betz, David, Tim Stevens, and Studies International Institute for Strategic. *Cyberspace and the State: Toward a Strategy for Cyber-Power*. Abingdon; New York: Routledge, for the International Institute for Strategic Studies, 2011.
- Billo, Charles, and Welton Chang. "Cyber Warfare: An Analysis of the Means and Motivations of Selected Nations." edited by Charles G. Billo: Institute for Security Technology Studies at Dartmouth College, 2004.
- Black, Jeremy. *War and the World: Military Power and the Fate of Continents, 1450-2000*. New Haven, Conn.: Yale University Press, 1998.

- Blainey, Geoffrey. *The Causes of War*. 3rd ed. New York: Free Press, 1988.
- Brenner, Joel. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: Penguin Press, 2011.
- Brenner, Susan W. "'At Light Speed': Attribution and Response to Cybercrime/Terrorism/Warfare." *The Journal of Criminal Law and Criminology* 97, no. 2 (2007): 379-475.
- Broad, William J., John Markoff, and David E. Sanger. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay." *New York Times*, 2011, A1.
- Bronk, Christopher. "Blown to Bits: China's War in Cyberspace, August–September 2020." *Strategic Studies Quarterly* 5, no. 1 (2011).
- Brousseau, Eric, and Nicolas Curien. *Internet and Digital Economics: Principles, Methods and Applications*. Cambridge: Cambridge University Press, 2006.
- Brynjolfsson, Erik, and Brian Kahin. "Understanding the Digital Economy: Data, Tools, and Research." Cambridge, Mass., 2000.
- Bueno De Mesquita, Bruce "An Expected Utility Theory of International Conflict." *American Political Science Review* 74, no. 4 (1980): 917-31.
- . *The War Trap*. New Haven: Yale University Press, 1981.
- . "The Contribution of Expected Utility Theory to the Study of International Conflict." *The Journal of Interdisciplinary History* 18, no. 4 (1988): 629-52.
- Campan, Alan D. *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War*. Fairfax, Va.: AFCEA International Press, 1992.
- Campan, Alan D., and Douglas H. Dearth. *Cyberwar 3.0: Human Factors in Information*

- Operations and Future Conflict*. Fairfax, VA: AFCEA International Press, 2000.
- Carr, Jeffrey. *Cyber Warfare*. Sebastopol: O'Reilly Media, Inc., 2010.
- Cerf, Vinton G. "The Day the Internet Age Began." *Nature* 461, no. 7268 (2009): 1202-03.
- Chickering, A. Lawrence. "Civil Society and Counterinsurgency." In, *Small Wars Journal* (2010). Published electronically Nov 3, 2010.
- Clark, Derek J., and Kai A. Konrad. "Asymmetric Conflict: Weakest Link against Best Shot." *The Journal of Conflict Resolution* 51, no. 3 (2007): 457-69.
- Clark, Wesley K., and Peter L. Levin. "Securing the Information Highway." *Foreign Affairs* 88, no. 6 (Nov/Dec 2009): 2-10.
- Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. 1st ed. New York: Ecco, 2010.
- Clarridge, Duane R., and Digby Diehl. *A Spy for All Seasons: My Life in the CIA*. New York, NY: Scribner, 1997.
- Clausewitz, Carl von, Michael Howard, and Peter Paret. *On War*. Princeton, N.J.: Princeton University Press, 1976.
- Clinton, Hillary Rodham. "Conference on Internet Freedom." Paper presented at the Conference on Internet Freedom, The Hague, Netherlands, 2011.
- Conkey, Christopher, Elizabeth Williamson, and Cam Simpson. "Washington Metro Delayed Upgrades." *The Wall Street Journal*, 24 June 2009.
- Cornish, Paul, David Livingstone, Dave Clemente, and Claire Yorke. "On Cyber Warfare." Chatham House, 2010.
- Costigan, Sean S., and Jake Perry. *Cyberspaces and Global Affairs*. Farnham, Surrey;

Burlington, VT: Ashgate, 2012.

Cullather, Nick. "Bombing at the Speed of Thought: Intelligence in the Coming Age of Cyberwar." *Intelligence and National Security* 18, no. 4 (2006): 141-54.

Czosseck, Christian, and Kenneth Geers. "The Virtual Battlefield Perspectives on Cyber Warfare." Ios Press,
<http://public.eblib.com/EBLPublic/PublicView.do?ptiID=501446>.

Daugherty, William J. *Executive Secrets: Covert Action and the Presidency*. Lexington: University Press of Kentucky, 2004.

Demchak, Chris C. *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*. Athens: University of Georgia Press, 2011.

Dockrill, M. L., and David French. *Strategy and Intelligence: British Policy During the First World War*. London; Rio Grande, Ohio: Hambledon Press, 1996.

Downs, Anthony. *An Economic Theory of Democracy*. New York: Harper, 1957.

Doyle, Michael W., and Stephen Macedo. *Striking First: Preemption and Prevention in International Conflict*. Princeton, NJ: Princeton University Press, 2008.

Drezner, Daniel W., and Henry Farrell. "Web of Influence." *Foreign Policy*, no. 145 (2004): 32-41.

Dzheng. "Securing Cyberspace for the 44th Presidency." (Apr 12 2009): 1-96.

Einstein, Albert, and Alice Calaprice. *The New Quotable Einstein*. Princeton, N.J.: Princeton University Press, 2005.

Eriksson, Johnan, and Giampiero Giacomello. "The Information Revolution, Security, and International Relations: (Ir) Relevant Theory?". *International Political Science Review* 27, no. 3 (2006): 221-44.

- Fair, Christine C. "Drone Wars." *Foreign Policy*, 2010.
- Falliere, Nicolas, Liam O Murchu, and Eric Chien. "W32.Stuxnet Dossier." Symantec Security Response, 2011.
- Faucon, Benoit. "New Sanctions Target Iran Oil Sales." *Wall Street Journal*, 2012.
- Fearon, James D. "Rationalist Explanations for War." *International Organization* 49, no. 3 (1995): 379-414.
- Fishman, Charles. *The Wal-Mart Effect: How the World's Most Powerful Company Really Works-- and How It's Transforming the American Economy*. New York: Penguin Press, 2006.
- Friedman, Milton. "The Methodology of Positive Economics." In *The Methodology of Positive Economics: Reflections on the Milton Friedman Legacy*, edited by Uskali Maki. 3-43: Cambridge and New York: Cambridge University Press, 2009. Reprint, [1984].
- Friedman, Thomas L. *The Lexus and the Olive Tree*. New York: Farrar, Straus, Giroux, 1999.
- . *The World Is Flat: A Brief History of the Twenty-First Century*. New York: Farrar, Straus and Giroux, 2005.
- Fuhrmans, Vanessa. "Virus Attacks Siemens Plant-Control Systems." *Wall Street Journal - Eastern Edition* 256, no. 18 (2010): B5.
- Gartzke, Erik. "War Is in the Error Term." *International Organization* 53, no. 3 (Jul 01 1999): 567-87.
- Geer, Daniel E. "Cybersecurity and National Policy." *Harvard National Security Journal* 1 (April 2010): 204-15.

Geers, Kenneth. "The Challenge of Cyber Attack Deterrence." *Computer Law & Security Review* 26, no. 3 (2010): 298-303.

Gill, Peter, Stephen Marrin, and Mark Phythian. *Intelligence Theory: Key Questions and Debates*. London; New York: Routledge, 2009.

Goodman, Will. "Cyber Deterrence. Tougher in Theory Than in Practice?". *Strategic Studies Quarterly* Fall (2010): 102-35.

Gorman, Siobhan, and Julian E. Barnes. "Cyber Combat: Act of War." In, *Wall Street Journal* (2011). Published electronically May 11.
<http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html>.

Grafstein, Robert. "Rationality as Conditional Expected Utility Maximization." *Political Psychology* 16, no. 1 (1995): 63-80.

Grauman, Brigid. "Cyber-Security: The Vexed Question of Global Rules." *Security and Defense Agenda*, 2012.

Hafner, Katie. "Laurels for Giving the Internet Its Language." *New York Times*, 2005.

Halpin, Edward F. *Cyberwar, Netwar and the Revolution in Military Affairs*. Basingstoke England ; New York: Palgrave Macmillan, 2006.

Herman, Michael. "Counter-Terrorism, Information Technology and Intelligence Change." *Intelligence and National Security* 18, no. 4 (2003): 40-58.

Horowitz, Michael, and Dan Reiter. "When Does Aerial Bombing Work?: Quantitative Empirical Tests, 1917-1999." *Journal of Conflict Resolution* 45, no. 2 (2001): 147-73.

Hunker, Jeffrey, Bob Hutchinson, and Jonathan Margulies. "Role and Challenges for

- Sufficient Cyber-Attack Attribution." Dartmouth College: Institute for Information Infrastructure Protection, 2008.
- Jackson, Joab. "Google: 129 Million Different Books Have Been Published." In, *PCWorld* (2010). Published electronically 6 August.
http://www.pcworld.com/article/202803/google_129_million_different_books_have_been_published.html.
- Janis, Irving L., and C. R. M. Productions. "Group Dynamics Groupthink." New York: McGraw-Hill Films: Produced by CRM Educational Films, 1973.
- Jefferson, Thomas. *The Writings of Thomas Jefferson*. 20 vols. Vol. 14, 1815.
- Johnson, Loch K. *America's Secret Power: The CIA in a Democratic Society*. New York: Oxford University Press, 1989.
- . "On Drawing a Bright Line for Covert Operations." *The American Journal of International Law* 86, no. 2 (Apr. 1992): 284-309.
- . *Secret Agencies: U.S. Intelligence in a Hostile World*. New Haven: Yale University Press, 1996.
- . *The Threat on the Horizon: An Inside Account of America's Search for Security after the Cold War*. Oxford; New York: Oxford University Press, 2011.
- . *National Security Intelligence*. Cambridge: Polity, 2012.
- Jones, Andy, Gerald L. Kovacich, and Perry G. Luzwick. *Global Information Warfare: How Businesses, Governments, and Others Achieve Objectives and Attain Competitive Advantages*. Boca Raton, Fla.: Auerbach Publications, 2002.
- Kahn, David. "The Intelligence Failure of Pearl Harbor." *Foreign Affairs*, 1 December 1991.

- Kahneman, Daniel, and Amos Tversky. "Prospect Theory: An Analysis of Decision under Risk." *Econometrica* 47, no. 2 (1979): 263-91.
- Katyal, Neal Kumar. "Criminal Law in Cyberspace." *University of Pennsylvania Law Review* 149, no. 4 (2001): 1003-114.
- Kautalya, and L. N. Rangarajan. *The Arthashastra*. New Delhi; New York, N.Y., USA: Penguin Books India, 1992.
- Keeney, Michelle, Eileen Kowalski, Dawn Cappelli, Andrew Moore, Timothy Shumeall, and Stephanie Rogers. "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors." Washington, D.C.: United States Secret Service and Carnegie Mellon Software Engineering Institute, 2005.
- Keohane, Robert O. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton, N.J.: Princeton University Press, 2005.
- Keohane, Robert O., and Joseph S. Nye. *Power and Interdependence: World Politics in Transition*. Boston: Little, Brown, 1977.
- . *Power and Interdependence*. 4th ed. Boston: Longman, 2012.
- Klimburg, Alexander. "Mobilising Cyber Power." *Survival* 53, no. 1 (2011): 41-60.
- Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz. *Cyberpower and National Security*. 1st ed. Washington, D.C.: National Defense University Press: Potomac Books, 2009.
- Krekel, Bryan. "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation." Mclean, VA: Northrop Grumman Cooperation 2009.
- Kshetri, Nir. "Informationa Nd Communications Technologies, Strategic Asymmetry and

- National Security." *Journal of Information Management* 11 (2005): 563-80.
- Landler, M., and J. Markoff. "Digital Fears Emerge after Data Seige in Estonia." *New York Times*, 2007.
- Levy, Jack S. "Misperception and the Causes of War: Theoretical Linkages and Analytical Problems." *World Politics* 36, no. 1 (Oct. 1983): 76-99.
- Lewis, James Andrew. "Significant Cyber Incidents since 2006." Washington: Center for Strategic and International Studies, 2011.
- Lewis, James A., and Katrina Timlin. "Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization." New York: Center for Strategic and International Studies
- United Nations Institute for Disarmament Research, 2011.
- Libicki, Martin C. *What Is Information Warfare?* Washington, DC: Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University: For sale by the U.S. G.P.O. Supt. of Docs., 1995.
- Libicki, Martin C., and Project Air Force (U.S.). *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND, 2009.
- Lieberman, Joseph. "S. 3480 (111th): Protecting Cyberspace as a National Asset Act of 2010." edited by United States Senate. Washington, D.C., 2010.
- Lomsadz, Giorgi. "A Shovel Cuts Off Armenia's Internet." In, *The Wallstreet Journal* (2011). Published electronically 04/08/2011.
- Lonsdale, David J. *The Nature of War in the Information Age: Clausewitzian Future*. London; New York: Frank Cass, 2004.
- Lord, Kristin M. *The Perils and Promise of Global Transparency: Why the Information*

- Revolution May Not Lead to Security, Democracy, or Peace.* Albany: State University of New York Press, 2006.
- Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. 4th ed. Washington, D.C.: CQ Press, 2009.
- . *Intelligence: From Secrets to Policy*. 5th ed. Washington, DC: CQ Press, 2011.
- Lynn, William J., III. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89 (2010): 105.
- Markoff, John. "Ideas & Trends: Blown to Bits; Cyberwarfare Breaks the Rules of Military " *New York Times*, Oct, 17 1999.
- Martin, Fredrick Thomas. *Top Secret Intranet: How U.S. Intelligence Built Intelink--the World's Largest, Most Secure Network*. Upper Saddle River, N.J.: Prentice Hall PTR, 1999.
- Massachusetts Institute of, Technology. "The Future of the Electric Grid an Interdisciplinary MIT Study." Massachusetts Institute of Technology, http://web.mit.edu/mitei/research/studies/documents/electric-grid-2011/Electric_Grid_Full_Report.pdf.
- Mazanec, Brian M. "The Art of (Cyber) War." *The Journal of International Security Affairs* 16, no. Spring (2009).
- Mearsheimer, John J. *The Tragedy of Great Power Politics*. New York: Norton, 2001.
- Metz, Steven, Douglas V. Johnson, and Institute Army War College . Strategic Studies. *Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts*. [Carlisle Barracks, PA]: Strategic Studies Institute, U.S. Army War College, 2001.

- Moravcsik, Andrew. "Taking Preferences Seriously: A Liberal Theory of International Politics." *International Organization* 51, no. 04 (1997): 513-53.
- Nakashima, Ellen. "List of Cyber-Weapons Developed by Pentagon to Streamline Computer Warfare." In, *The Washington Post* (2011). Published electronically May 31.
- . "White House, NSA Weigh Cybersecurity, Personal Privacy." *Washington Post*, Feb 27, 2012.
- Nye, Joseph S. . "Cyber Power." Cambridge, MA: Havard Kennedy School of Government - Belfer Center for Science and International Affairs, 2010.
- Nye, Joseph S. *The Future of Power*. New York: PublicAffairs, 2011.
- Olson, James M. *Fair Play: The Moral Dilemmas of Spying*. Washington, D.C.: Potomac Books, 2006.
- Organski, A. F. K., and Jacek Kugler. *The War Ledger*. Chicago: University of Chicago Press, 1980.
- Owens, William A., Kenneth W. Dam, Herbert Lin, Warfare National Research Council . Committee on Offensive Information, Science National Research Council . Computer, Board Telecommunications, Engineering National Research Council . Division on, and Sciences Physical. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington, DC: National Academies Press, 2009.
- Pape, Robert A. "The True Worth of Airpower." *Foreign Affairs*, 1 March 2004.
- Pillar, Paul R. *Intelligence and U.S. Foreign Policy: Iraq, 9/11, and Misguided Reform*. New York: Columbia University Press, 2011.

- Pleming, Sue. "U.S. State Department Speaks to Twitter over Iran." In, *Reuters* (2009).
Published electronically 06/16/. <http://www.reuters.com/article/2009/06/16/us-iran-election-twitter-usa-idUSWBT01137420090616>.
- Potter, Richard, and Akihiro Nakao. "Mobitopolo: A Portable Infrastructure to Facilitate Flexible Deployment and Migration of Distributed Applications with Virtual Topologies." In *ACM SIGCOMM*. Barcelona: SIGCOMM, 2009.
- Press, Daryl. "The Myth of Airpower: The Persian Gulf War and the Future of Airpower." 5-44, 2001.
- Quiggin, John. *Generalized Expected Utility Theory: The Rank-Dependent Model*. Boston: Kluwer Academic Publishers, 1993.
- Reagan, Ronald. "Executive Order 12333-United States Intelligence Activities." edited by Office of the President. Washington: US Federal Register, 1981.
- Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* (2011).
———. "Think Again: Cyberwar." *Foreign Policy*, no. March/April (2012): 80-84.
- Rohde, David. "The Obama Doctrine: How the President's Drone War Is Backfiring." *Foreign Policy*, no. March/April (2012).
- Rothkopf, David J. "Cyberpolitik: The Changing Nature of Power in the Information Age." *Journal of International Affairs* 51, no. 2 (Spring98 1998): 325.
- Rumsfeld, Secretary of Defense Donald H. "DoD News Briefing - Secretary Rumsfeld and Gen. Myers." In, (2002). Published electronically Feb 12.
<http://www.defense.gov/transcripts/transcript.aspx?transcriptid=2636>.
- Russell, Bertrand. *An Outline of Intellectual Rubbish ; a Hilarious Catalogue of Organized and Individual Stupidity*. Girard, Kan.: Haldeman-Julius publications,

1943.

Samaan, Jean-Loup. "Cyber Command." *RUSI Journal* 155, no. 6 (2010): 16-21.

Sanger, David E. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York: Crown Publishers, 2012.

Savio, Jessica. "Browsing History: A Heritage Site Is Being Set up in Boelter Hall 3420, the Room the First Internet Message Originated In." *Daily Bruin*, 1 April 2011.

Shackelford, Scott J. "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law ". *Berkeley Journal of International Law* 27, no. 1 (2008): 191-251.

Shackley, Theodore, and Richard A. Finney. *Spymaster: My Life in the CIA*. Dulles, Va.: Potomac Books, 2005.

Shakarian, Paulo. "Stuxnet: Cyberwar Revolution in Military Affairs." In, *Small wars Journal* (2011). Published electronically April 15, 2011.

Shakespeare, William, and Alvin B. Kernan. *The Tragedy of Julius Caesar*. The Yale Shakespeare. Rev. ed. New Haven,: Yale University Press, 1959.

Sharma, Amit. "Cyber Wars: A Paradigm Shift from Means to Ends." *Strategic Analysis* 34, no. 1 (2010).

Simpson, J. A., E. S. C. Weiner, and Press Oxford University. *The Oxford English Dictionary*. Oxford; Oxford; New York: Clarendon Press ; Oxford University Press, 1989.

Singer, David J. "Reconstructing the Correlates of War Dataset on Material Capabilities of States, 1816-1985." *International Interactions* 14 (1987): 115-32.

Singer, David J., Stuart Bremer, and John Stuckey. "Capability Distribution, Uncertainty,

- and Major Power War, 1820-1965." In *Peace, War, and Numbers*, edited by Bruce Russett. 19-48. Beverly Hills: Sage, 1972.
- Stokes, Mark A., Jenny Lin, and L.C. Russell Hsiao. "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure." Arlington, VA: Project 2049 Institute, 2011.
- Strezhnev, Anton, and Erik Voeten. "United Nations General Assembly Voting Data." 2012.
- Thomas, Timothy L. "Cyber Mobilization: A Growing Counterinsurgency Campaign." Fort Leavenworth, KS: Department of Defense, 2006.
- Thornton, Rod. *Asymmetric Warfare: Threat and Response in the Twenty-First Century*. Cambridge; Malden, MA: Polity Press, 2007.
- Thucydides, Rex Warner, and M. I. Finley. *History of the Peloponnesian War*. Harmondsworth, Eng.; Baltimore: Penguin Books, 1972.
- Traynor, Ian. "Russia Accused of Unleashing Cyberwar to Disable Estonia." In, *The Guardian* (2007).
- <http://www.guardian.co.uk/world/2007/may/17/topstories3.russia>.
- Treverton, Gregory F. *Covert Action: The Limits of Intervention in the Postwar World*. New York: Basic Books, 1987.
- United States. Dept. of Homeland, Security. *National Infrastructure Protection Plan*. [Washington, D.C.]: U.S. Dept. of Homeland Security, 2006.
- Van Evera, Stephen. *Causes of War*. Ithaca (N.Y.): Cornell University press, 1999.
- Von Neumann, John, and Oskar Morgenstern. *Theory of Games and Economic Behavior*. Princeton, NJ: Princeton University Press, 1944.

- Waltz, Edward. *Information Warfare: Principles and Operations*. Boston: Artech House, 1998.
- Waltz, Kenneth Neal. *Theory of International Politics*. Reading, Mass.: Addison-Wesley Pub. Co., 1979.
- Warner, Michael. "Wanted: A Definition of "Intelligence"." *Studies in Intelligence* 46, no. 3 (2002).
- Wendt, Alexander. "Constructing International Politics." *International Security* 20, no. 1 (1995): 71-81.
- Wheeler, David A., and Gregory N. Larsen. "Techniques for Cyber Attack Attribution." 84: Institute for Defense Analyses, 2003.
- Williams, Phil, Timothy Shimeal, and Casey Dunlevy. "Intelligence Analysis for Internet Security." *Contemporary Security Policy* 23, no. 2 (2010): 1-38.
- Zelizer, Julian E. *Arsenal of Democracy: The Politics of National Security-- from World War Ii to the War on Terrorism*. New York, N.Y.: Basic Books, 2010.