BRANDON VALERIANO | RYAN C. MANESS

CYBER WAR VERSUS CYBER REALITIES

CYBER CONFLICT IN THE INTERNATIONAL SYSTEM

Cyber War versus Cyber Realities

Cyber War versus Cyber Realities

Cyber Conflict in the International System

Brandon Valeriano

and

Ryan C. Maness

OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS

Oxford University Press is a department of the University of
Oxford. It furthers the University's objective of excellence in research,
scholarship, and education by publishing worldwide.

Oxford New York
Auckland Cape Town Dar es Salaam Hong Kong Karachi
Kuala Lumpur Madrid Melbourne Mexico City Nairobi
New Delhi Shanghai Taipei Toronto

With offices in
Argentina Austria Brazil Chile Czech Republic France Greece
Guatemala Hungary Italy Japan Poland Portugal Singapore
South Korea Switzerland Thailand Turkey Ukraine Vietnam

Oxford is a registered trademark of Oxford University Press
in the UK and certain other countries.

Published in the United States of America by
Oxford University Press
198 Madison Avenue, New York, NY 10016

Library of Congress Cataloging-in-Publication Data
Valeriano, Brandon.
Cyber war versus cyber realities : cyber conflict in the international system /
Brandon Valeriano, Ryan C. Maness.
pages cm
ISBN 978–0–19–020479–2 (hardback)
1. Cyberspace operations (Military science) 2. Cyberterrorism.
3. Technology and international relations. 4. Internet and international
relatins. I. Maness, Ryan C. II. Title.
U163.V36 2015
355.4—dc23
2014039240

9 8 7 6 5 4 3 2 1
Printed in the United States of America
on acid-free paper

Dedicated to John Vasquez and J. David Singer

CONTENTS

Preface *ix*
Acknowledgments *xiii*

1. The Contours of the Cyber Conflict World *1*
2. Cyber Power, Cyber Weapons, and Cyber Operations *20*
3. Theories of Cyber Conflict: Restraint, Regionalism, Espionage, and Cyber Terrorism in the Digital Era *45*
4. The Dynamics of Cyber Conflict Between Rival Antagonists *78*
5. The Impact of Cyber Actions: Cyber Events and the Conflict-Cooperation Nexus *109*
6. Stuxnet, Shamoon, and Bronze Soldier: The Impact and Responses to Cyber Operations *137*
7. Cyber Conflict and Non-State Actors: Weapons of Fear *164*
8. Cyber Rules: Encouraging a System of Justice and Proportionality in Cyber Operations *188*
9. Conclusion *209*

Appendix: Research Methods *229*
Notes *233*
References *249*
Index *259*

PREFACE

PROJECT BEGINNINGS

We started working in the cyber security field in 2010 when Derek Reveron invited one of us to a cyber security conference at the Naval War College. There were a lot of great and important minds in the room that day, but we were struck at how little theory, evidence, and logic were applied to the question of cyber conflict.

Lots of statements were made with no facts to back them up; the prevailing assumption was that cyber was the new threat, it was proliferating, and it would change the course of interstate relations. We were skeptical, but, more important, we wanted evidence and theory, and we wanted to move past the conjecture found on the proliferating news talk shows. The time since our first encounter with cyber security has only reinforced our view that rigorous analysis is needed regarding the topic.

To that end, this is a book about evidence and the nature of international threats. We have been influenced greatly by J. David Singer and John Vasquez. Singer created the Correlates of War project at the University of Michigan, which sought to empirically categorize and collect data on the origins of war. Vasquez used this data later to produce inductive theories regarding the nature of war in the system. Their goals were to explain what we know about the world, but also to do so in a scientific fashion.

We need evidence and rigorous data to guard against the tendency many have to make grand statements with little connection to actual processes. Singer taught us about the nature of data collection, the need for building a knowledge base through comprehensive data collection. Vasquez taught us about the nature of theory, induction, and the construction of threats in the international system. More often than not, threats and displays of power politics engender a response opposite to what is intended (often concession). These moves generally provoke counter-threats, escalation, and outright conflict. It is for this reason that the era of cyber security is dangerous; it needs rigorous analysis to counter the proliferating cyber hype motifs. We need to understand how cyber threats are constructed, who makes them, and the reactions to them in order to understand how to best respond to the developing arena of cyber military tactics.

MAKING PREDICTIONS

Marc Maron, on his popular WTF Podcast, made an offhand remark that he does not prepare for his comedy performances. He feels that preparing is for cowards, that you need to be ready and willing to fail in your work since there is a fine line between a unique achievement and total failure. Skirting this line led him to ruin many times in his career, but it has also led him to the transcendent place he is at now. He reached the heights of his field by putting it all on the line and risking total devastation in his Podcast, a new and untested medium in 2009. Now he has one of the most popular podcasts, a TV show, and is more popular than ever on the comedy circuit.

Maron's path to success reminds us that we need to think a bit about this frame in our own work. Are we really willing to fail? Are we cowards? Do we skirt that fine line between success and ruin?

We need to push for research that might encompass what we call political science without a net. This is how we characterize this research on cyber security. One massive global destructive cyber incident could invalidate our theory of restraint and regionalism in cyberspace. Of course, one case does not disprove a theory, but it can terminally harm it. The easy path would have been to articulate a frame of the future where cyber conflict dominates the system. We could write about the notion that we will see continued and constant netwar that will change how nations interact, rise and fall, and conduct strategy. These sorts of claims are easy to make, clouded by caveats and qualifications, and the frame can successfully be employed to describe one view of the cyber world or can even be applied to research about drones, airpower, and other frames of future war.

Frames that suggest massive changes to the system are largely inaccurate. We have failed to see cyberwar really proliferate in the decades since the ubiquity of digital communications. Russia has failed to use the tactic in Ukraine and Crimea, even after using it liberally, if in a restrained manner, during the Georgia invasion of 2008 and in Estonia in 2007. The United States rejected the widespread use of cyber tactics in Iraq (2003), Afghanistan (2002), and Libya (2011). Cyber terrorists and non-state actors use the tactic, but with little actual impact. Cyber technologies have changed our daily lives, but to argue that they have and will change our foreign policy and military strategy is too easy a claim and very difficult to prove wrong when articulated with unlimited time horizons. Taking a new weapon and arguing that it will change the world is a simple case to make; taking a new weapon and suggesting it is just more of the same, like ancient espionage practices, is difficult. In fact, it is important to take this position because arguing for the coming cyber threat risks provoking escalation and conflict. The frame becomes a self-fulfilling prophecy because the idea is so simple; people believe it to be true because it seems logical. Who does not feel vulnerable when they lose Internet access and cell phone service?

It sometimes feels as if our field of international relations is becoming stagnant. Not because we are not asking big questions or are not doing policy-relevant research, but often because we do not take big risks. Defying conventional wisdom is wonderful, even liberating. We need to insert more fear in our work; otherwise, as Maron says, we are cowards.

In this book, we make strong predictions about the future, using evidence from the recent past to outline the course of cyber conflict between states. We argue here that there is restraint in cyberspace, that cyber interactions are mainly regional on the international level, and that cyber terrorism is a limited tactic that will not change the course of international interactions. We make these predictions based on a large dataset of cyber interactions, and we use this data to test our theories. Finally, we outline the course of our possible cyber future. This is a future where offensive cyber actions are taboo and, hopefully, international institutions rise up to limit the dangers this domain might pose.

CYBER SECURITY RESEARCH

This is a crucial time for cyber security research, as the field has only just begun. We stake out a position in this debate that is counter to many that would seek to hype the cyber threat. The future is what states will make of it, but we hope that our perspective might add some much needed rationality to the field of cyber security.

We are under no illusions that we have described the entire past and future of cyber interactions. The future is in the process of being built. We can only make statements based on the evidence we have. Things are changing every day in the cyber security field; our statements here describe what we observe now. This entire effort is an early attempt to outline a path toward researching contemporary security developments with scientific standards of evidence and theory construction. As always, this project reflects our understanding of the cyber security landscape and conforms to our own intellectual biases.

We encourage others to use this work as a starting point to elaborate more on the cyber security field and how it is connected to international relations processes. There is much work to be done, and we hope others will help us move toward a greater understanding of the cyber security threat landscape.

Brandon Valeriano
April 20, 2014
In Glasgow coffee shops, on planes, and trains
Ryan C. Maness
April 20, 2014
At my desk at home, in my office, and in Chicago coffee shops

ACKNOWLEDGMENTS

There are many people to thank. This book was a long time coming and could not have been completed without the help of many interested parties and friends.

The University of Glasgow was instrumental in providing an institutional home and a future for Valeriano. The entirety of this book was written with the generous support the institution gives for its research faculty. The added normative context of this book was also inspired by the discussions and atmosphere of the UK, in particular with Cian O'Driscoll, Laura Sjoberg, Eric Heinze, and Caron Gentry. Within the University, Chris Carmen, Eamonn Butler, Myrto Tsakatika, and other members of the staff who attended various presentations provided key comments and encouragement that helped develop this work.

Derek Reveron's invitation to the Naval War College to attend a cyberwar conference in 2010 was important in starting this research. An early version of our ideas appeared in a book chapter in his edited volume, *Cyberspace and National Security*. Without him, and the comments of those who attended those important Naval War College talks, none of this work would have been possible.

Various institutions and organizations were important in providing a venue for discussion as this work progressed. The Air War College, Naval War College, University of Denver, Massachusetts Institute of Technology, University at Albany, Whiter College, Menlo Park College, and the University of Southern California all hosted invited talks. Other institutions such as the US Department of Defense, the US State Department, the Intelligence Community, Estonia's Lennart Meri Conference, the Up with Chris Hayes show on MSNBC, Scotland Herald, NBC Chicago, and the British Broadcasting Company all provided opportunities to share our ideas. Foreign Affairs ran an early version of our data, and the blogging collective the Duck of Minerva hosted many of our ideas as they were in development, as did the Atlantic Council.

There are many cyber scholars who were important for the development of this work. Nazli Choucri, Joseph Nye, Erik Gartzke, Jon Lindsay, Thomas Rid, Derek Reveron, Heather Roff, Emmet Touhy, Jason Healey, Jacob Mauslein, James Fielder, all provided comments. Other International Relations and Political Science scholars such as Doug Gibler, Stephen Saideman, Victor Asal, Patrick James, Dennis Foster, Melissa Michelson, Konstantios Travlos, Dan

Nexon, Fred Bergerson, Cullen Hendrix, and Samuel Whitt provided important comments and feedback.

Our own students have been important for comments and intellectual development: Rob Dewar, Sam Bassett (who was with us early, coding the dataset), Lauren Pascu, Stephen Powell, Signe Norberg, and Hugh Vondracek provided feedback, coding assistance, and editing help.

The Carnegie Trust for Universities of Scotland—Small Research Grant was helpful in completing this project. *The Journal of Peace Research* (2014) published an early version of Chapter 4 as "The Dynamics of Cyber Conflict between Rival Antagonists, 2001–2011," *Journal of Peace Research* 51 (3): 347–360.

And of course, there are our friends whom would we would like to thank. Valeriano thanks Jim Frommeyer, Victor Marin, Walther Pappa Catavi, Phillip Habel, and Richard Johnson. He would also like to thank his family. Maness would like to thank his parents, who are looking down on him with pride.

In particular, we would like to thank John Vasquez, whose style and ideas permeate everything we do.

All data can be found at brandonvaleriano.com, drryanmaness.wix.com/irprof, our book webpage www.cyberconflict.com.com.

An updated version of Chapter 5 is available in a forthcoming 2015 article in *Armed Forces and Society* titled 'The Impact of Cyber Conflict on International Interactions'.

Cyber War versus Cyber Realities

CHAPTER 1

The Contours of the Cyber Conflict World

INTRODUCTION

This is a book about cyber conflict and the process of international cyber interactions, a critical question given the climate surrounding the nature of the shifting international security landscape. We are guided by the division between what we call *cyber hype* and threat inflation, on the one hand, and the empirical realities of cyber interactions as they actually occur in the international system, on the other. These divisions are important because they represent the two dominating perspectives in the cyber security debate. The cyber hype perspective would suggest that we are seeing a revolution in military affairs with the advent of new military technologies. The moderate perspective is guided by careful consideration of what the real dangers are, as well as the costs of the overreaction. These two sides outline the perspectives of many in the emerging cyber security field.

Our concern is that fear dominates the international system. The contention is that harm is a constant factor in international life (Machiavelli 2003; Hobbes 2009); everything is a danger to all, and all are a danger to most. It is through this prism that the international affairs community approaches each technological development and each step forward, and it does so with trepidation and weariness. Because of the hype surrounding the development of cyber weaponry, the step toward what might be called cyber international interactions is no different. With the advent of the digital age of cyber communications, this process of fear construction continues to shape dialogues in international relations as cyberspace becomes a new area of contestation in international interactions. Old paradigms focused on power politics, displays of force, and deterrence are applied to emergent tactics and technologies with little consideration of how the new tactic might result in different means and ends. We argue that these constructed reactions to threats have little purchase when examined through the

prism of evidence or when judged compared to the normative implications of action. There is an advantage to bringing empirical analysis and careful theory to the cyber security debate.

The emerging fear that we seek to counter is the perspective that cyber weapons will come to dominate the system and will change how states and individuals interact.

In this book, we uncover how cyber conflict among international actors actually works by presenting an empirical account of these types of interactions since the turn of the century. We then use this data to uncover the foreign policy implications of this new domain of conflict and also examine how this type of conflict is being governed through international norms and regimes. Throughout, we develop theories of cyber conflict that seek to evaluate the nature of cyber fears and myths that dominate the debate on this ever important topic. We do not minimize the cyber security issue, but instead seek to analyze its dynamics in light of evidence, and we suggest a policy course in light of these findings.

CYBERSPACE AND CONFLICT

Currently, the cyberspace arena is the main area of international conflict where we see the development of a fear-based process of threat construction becoming dominant. The fear associated with terrorism after September 11, 2001, has dissipated, and in many ways has been replaced with the fear of cyber conflict, cyber power, and even cyber war.[1] With the emergence of an Internet society and rising interconnectedness in an ever more globalized world, many argue that we must also fear the vulnerability that these connections bring about. Advances and new connections such as drones, satellites, and cyber operational controls can create conditions that interact to produce weaknesses in the security dynamics that are critical to state survival. Dipert (2010: 402) makes the analogy that surfing in cyberspace is like swimming in a dirty pool. The developments associated with Internet life also come with dangers that are frightening to many.

In order to provide an alternative to the fear-based discourse, we present empirical evidence about the dynamics of cyber conflict. Often realities will impose a cost on exaggerations and hyperbole. We view this process through the construction of cyber threats. The contention is that the cyber world is dangerous, and a domain where traditional security considerations will continue to play out. A recent Pew Survey indicates that 70 percent of Americans see cyber incidents from other countries as a major security threat to the United States, with this threat being second only to that from Islamic extremist groups.[2]

This fear is further deepened by hyperbolic statements from the American elite. US President Barack Obama has declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation."[3] Former US Defense Secretary Leon Panetta has gone further, stating, "So, yes,

we are living in that world. I believe that it is very possible the next Pearl Harbor could be a cyber attack . . . [that] would have one hell of an impact on the United States of America. That is something we have to worry about and protect against."[4]

United States elites are not alone in constructing the cyber threat. Russian President Vladimir Putin, in response to the creation of a new battalion of cyber troops to defend Russian cyberspace, noted, "We need to be prepared to effectively combat threats in cyberspace to increase the level of protection in the appropriate infrastructure, particularly the information systems of strategic and critically important facilities."[5] The social construction of the cyber threat is therefore real; the aim of this book is to find out if these elite and public constructions are backed with facts and evidence.

First, we should define some of our terms to prepare for further engagement of our topic. This book is focused on international cyber interactions. The prefix *cyber* simply means computer or digital interactions, which are directly related to *cyberspace*, a concept we define as the networked system of microprocessors, mainframes, and basic computers that interact at the digital level. Our focus in this volume is on what we call *cyber conflict*, the use of computational technologies for malevolent and destructive purposes in order to impact, change, or modify diplomatic and military interactions among states. *Cyber war* would be an escalation of cyber conflict to include physical destruction and death. Our focus, therefore, is on cyber conflict and the manifestation of digital animosity short of and including frames of war. These terms will be unpacked in greater detail in the chapters that follow.

The idea that conflict is the foundation for cyber interactions at the interstate level is troubling. Obviously many things are dangerous, but we find that the danger inherent in the cyber system could be countered by the general restraint that might limit the worst abuses in the human condition. By countering what we assert to be an unwarranted construction of fear with reality, data, and evidence, we hope to move beyond the simple pessimistic construction of how digital interactions take place, and go further to describe the true security context of international cyber politics.

In this project we examine interactions among interstate rivals, the most contentious pairs of states in the international system. The animosity between rivals often builds for centuries, to the point where a rival state is willing to harm itself in order to harm its rival even more (Valeriano 2013). If the cyber world is truly dangerous, we would see evidence of these disruptions among rival states with devastating effect. Rivals fight the majority of wars, conflicts, and disputes (Diehl and Goertz 2000), yet the evidence presented here demonstrates that the cyber threat is restrained at this point.[6] Overstating the threat is dangerous because the response could then end up being the actual cause of more conflict. Reactions to threats must be proportional to the nature of the threat in the first place. Otherwise the threat takes on a life of its own and becomes a self-fulfilling prophecy of all-out cyber warfare.

Furthermore, there is a danger in equivocating the threat that comes from non-state cyber individuals and the threats that come from state-affiliated cyber actors not directly employed by governments. If the discourse is correct, non-state entities such as terrorist organizations or political activist groups should be actively using these malicious tactics in cyberspace in order to promote their goals of fear and awareness of their plight. If the goal is to spread fear and instability among the perceived enemies of this group, and cyber tactics are the most effective way to do this, we should see these tactics perpetrated—and perpetrated often—by these entities. This book examines how state-affiliated non-state actors use cyber power and finds that their actual capabilities to do physical harm via cyberspace are quite limited. This then leaves rogue actors as the dangerous foes in the cyber arena. While these individuals can be destructive, their power in no way compares to the resources, abilities, and capabilities of cyber power connected to traditional states.

The future is open, and thus the cyber world could become dangerous, yet the norms we see developing so far seem to limit the amount of harm in the system. If these norms hold, institutions will develop to manage the worst abuses in cyberspace, and states will focus on cyber resilience and basic defense rather than offensive technologies and digital walls. Cyberspace would therefore become a fruitful place for developments for our globalized society. This arena could be the place of digital collaboration, education, and exchanges, communicated at speeds that were never before possible. If states fall into the trap of buying into the fear-based cyber hype by developing offensive weapons under the mistaken belief that these actions will deter future incidents, cyberspace is doomed. We will then have a restricted technology that prevents the developments that are inherent in mankind's progressive nature.

Two themes dominate this analysis. The first is the goal to systematically account for international processes and the conduct of cyber security. We offer facts and evidence to help evaluate how cyber tactics have been used, will continue to be used, and will be used in the future. The world can be a dangerous place, but sometimes our reaction to threats is more detrimental than the nature of the threat. To that end, our second theme is that cyber conflict between states is rare, is restrained, and can be a tool in the domain of espionage rather than a demonstration of raw power. We analyze how states marshal cyber power, but we also place this evidence in the context of the development of strategy and doctrine. Understanding how cyber conflict actually occurs in reality is a key task in the field, and here we scope out the landscape of cyber interactions between states and state representatives. Our theory of cyber restraint depends on four processes: (1) the nature of the weapon and its reproducibility, making it a one-shot weapon of limited effectiveness; (2) the potential for blowback, given that initiating states are often weaker than the state they seek to infiltrate; (3) the natural potential of collateral damage in cyberspace since the technology is not limited to military space; and (4) the potential harm to civilians due

to these considerations. Because of these concerns, restraint dominates in the cyber realm.

In the rest of this volume we will describe the contours of conflicts in cyberspace, the theories that dictate the patterns of conflict, the dynamics of interstate interactions, and the developing norms in the system. In this examination of the past, present, and future of cyber political interactions, we hope to understand the greatest development in the twenty-first century thus far; the goal is to keep fear from dominating the discourse.

THE CHANGING SHAPE OF INTERNATIONAL RELATIONS

This project represents a view of international cyber conflict through the lens of the international relations field. The arena is mainly cyber conflict among states or directed toward states in the realm of foreign policy. The domain is clear; we cannot speak about the nature of cyber crime, but only about the nature of international interactions among states and their affiliates. There is a history and method of analyzing these events that feed directly into the nature of cyber conflict between international competitors.

To understand cyber conflict in the international relations realm, we must understand who uses the tactic, where, how, and for what ends. We therefore define cyber conflict as the use of computational technologies in cyberspace for malevolent and destructive purposes in order to impact, change, or modify diplomatic and military interactions between entities. We are speaking of cyber conflict as a foreign policy tool used by states or individuals against states.

In 2011, the US government declared that a cyber incident is similar to an act of war, punishable with conventional military means (White House 2011; Tallinn Manual 2013).[7] This is a significant step, because it allows the response to a non-physical malicious incident in cyberspace to be in the physical, kinetic form. Conflict then shifts from cyberspace to conventional forms. Rarely have we seen non-physical threats become the source of physical counter threats (Valeriano and Maness 2014). This represents a new direction in the way that threats and actions are interpreted in the international sphere.

The Department of Defense notes that "small scale technologies can have an impact disproportionate to their size; potential adversaries do not have to build expensive weapons systems to pose a significant threat to U.S. national security."[8] In 2013, a US private commission led by former US Ambassador to China John Huntsman and former Director of National Intelligence Dennis Blair went even further, suggesting that corporations would have the right to retaliate with cyber operations if other measures fail to deter cyber theft.[9] Here, the government would be removed from the process, thus allowing an international strike against an enemy by individuals and non-state actors. This is a significant and an unprecedented step in international relations, as an

individual could now respond to threats from a state, rather than just receive them. Huntsman, one of the drafters of the report advocating this strategy, noted, "China is two-thirds of the intellectual property theft problem, and we are at a point where it is robbing us of innovation to bolster their own industry, at the cost of millions of jobs. We need some realistic policy options that create a real cost for this activity because Chinese leadership is sensitive to those costs."[10] As the report documents, the "realistic" policy options are cyber operations.

To prevent a cyber intrusion in the first place, the Huntsman-Blair commission argues that we must be willing and able to launch a counter-threat, and it indicates that such a reaction is the responsibility of all of society: individuals, the state, and the military.[11] This argument blurs traditional foreign policy practices, because it enfranchises the responsibility of retaliation to individual or non-state actors, and leaves the state out of the process of its traditional role in international affairs. Going even further, the US government has also started to develop automated cyber capabilities known as "Plan X."[12] This program would find the source of the incident and automatically retaliate against the cyber perpetrator without the approval or oversight of human beings. Thus this step removes the individual and decision-maker from the process of policy and operational choices. It cannot be argued that cyber operations are not causing a shift in the way foreign policy is made; our contention is that this shift might be problematic in light of evidence.

In addition to cyber decision-making processes that shift how organizations and groups respond to threats, we also see cyber actions becoming part of the normal process of threat construction in international relations. Cyber operations, cyber crime, and other forms of cyber activities directed by one state against another are now considered part of the normal range of combat and conflict (Azar 1972; Valeriano and Maness 2014). It is now acceptable to respond to an incident in one domain, cyberspace, through another domain, the physical and conventional layer; thus these responses become the norm in international relations. Although the difference between the layers can be blurred, this is still an important and critical development. Perhaps there has been no greater shift in international dynamics since the end of the Cold War. The barriers between the hypothetical and the abstract have broken down due to the fears of the costs that the cyber world imposes in the physical world. As Clark and Knake (2010: xiii) argue, "cyber war may actually increase the likelihood of the more traditional combat with explosives, bullets, and missiles." The domains have blended together and have transformed into a new potential path to conflict.

According to proponents (Clarke and Knake 2010; Carr 2010; Kello 2013) who help construct the discourse of cyber politics in this debate, international interactions are shifting due to the advent of cyber technologies. The rising fear of cyber combat and threats has brought about a perceived reorientation of military affairs. Our entry into this debate is to first examine how cyber tactics are actually used from a macro perspective, and then to examine if these

potential leaps in logic are warranted given the evidence and analyses presented in this volume.

Clarke and Knake (2010: 32) frame the cyber debate as transformational, stating, "there is a credible possibility that such conflict [cyber] may have the potential to change the world military balance and thereby fundamentally alter political and economic relations." Further, even academics are making similar claims; Kello (2013: 32) declares that "[t]he cyber domain is a perfect breeding ground for political disorder and strategic instability. Six factors contribute to instrumental instability: offense dominance, attribution difficulties, technological volatility, poor strategic depth, and escalatory ambiguity. Another—the "large-N" problem—carries with it fundamental instability as well." The question we have is, what is the reality of this threat and prospect? We aim to return the debate on cyber conflict to a more nuanced approach based on empirics substantiating the actual dangers of cyber combat. While there is a real danger of cyber combat, one must remain prudent in relation to the actual threat, not the inflated threat presented by the imagination. Data and analysis allow us to make more accurate policy choices as to how to react, based on the current state of relations.

Often, cyber policy is made based on "worst case scenario" analyses. Analysts, the media, and governments ask what is the worst that can happen, and what can be done to respond to these situations. This is the issue brought up by commentators who suggest that corporations and individuals should be allowed to respond to cyber conflict through their own international actions, removing the state from the process due to the perceived extreme nature of the threat. Others point to the threat of a "Cyber Pearl Harbor," a theory that was given serious weight when mentioned by US Secretary of Defense Leon Panetta.[13] At the time of this writing, the term *cyber conflict* results in over one million hits on Google, which reveals the level of attention that it is receiving.

Basing policy and strategic advice on the worst possible case utilizes the straw man approach (Walton 1996) to design responses and capacity. Making a point based on a perceived extreme example of an event, which usually has little connection to the actual debate at hand—or, in many cases, to reality—is unhelpful. Here we demonstrate that international cyber interactions are typically benign communications that are removed from the security discourse. This is not to say that worst case analyses are never warranted; however, through our findings we assert that traditional security processes (where a threat is articulated, responded to, and then escalated by the opposing side in response to the newer threat) do not apply in the cyber domain. This then makes policy based on the worst case problematic, if not damaging, to international diplomacy. By securitizing cyberspace, there is the potential for the worst case to become the reality and the norm. To move beyond this process, we must examine how states and other international actors actually interact in cyberspace. We must examine the worst cases of abuse, the typical cases of abuse, and the normal day-to-day

interactions to understand the scope of cyber interactions. Through this process we can describe, shape, and develop arguments about cyber political interactions based on reality and empirical realities, rather than hyperbole and fear.

THE NATURE OF CYBER CONFLICT: CYBER REALITY

In this volume we present evidence that suggests that cyber incidents and disputes between states are seldom-used tactics that have not escalated to the possible doomsday propositions that many cyber security companies, pundits, and popular media outlets would have us believe.[14] We also present no evidence of cyber conflict escalating to more severe tactics anytime in the near future, although it is possible that this may happen (Valeriano and Maness 2012). In this book we explain and develop the logic for the current dynamics of cyber conflict. We also investigate the myths and suggestions brought on by what are deemed the most destructive cyber incidents that have occurred so far.

Using our explicit data collection procedures (fully explained in Chapter 4), we find that over an 11-year span, from 2001 to 2011, the dawn of the potential cyber era, rival states have undertaken 111 total cyber incidents within 45 larger cyber disputes. An incident is an isolated operation launched against a state that lasts only a matter of hours, days, or weeks, while a dispute is a longer-term operation that can contain several incidents. Only 20 out of 126 rival pairs of states have engaged in government-sanctioned and targeted cyber conflicts since 2001. We look at international rivals because they are the most conflict-prone dyads in the international system (Diehl and Goertz 2000); therefore, if cyber conflict is going to be used as a viable tactic against an enemy, it is most likely to be utilized between rivals. Furthermore, out of a severity scale from one to five, with five being the most severe, the highest recorded score for a cyber incident between rivals is three, which equates to a targeted operation on a state's national security strategy. In fact, there are only 14 examples of incidents that reach a severity ranking of three in our data. These incidents usually involve targeting military operations, such as sabotage of a nuclear weapons program or stealing stealth jet plans. This indicates that cyber conflict has remained at a low level for the past decade, and although the frequency of cyber incidents and disputes has increased over time, the severity level has remained constant and at a low level.

We also utilize our collected data (Chapter 5) to uncover the reactions that cyber conflicts provoke between states in the foreign policy realm. Surprisingly, our results demonstrate that the primary tactic evoking conflictual foreign policy responses from victimized states is the relatively benign distributed denial of service (DDoS) cyber method, which will be explained in more detail in the following chapters.[15] This is unexpected because the long-term damage done by these types of cyber incidents is minor to nonexistent. Furthermore, incidents and disputes launched by states where the goal is to attempt to change the national

security strategy of the target state will also lead to negative foreign policy responses. This is not surprising because states will usually escalate tensions with a source of coercive force (Vasquez 1993).

Our data also uncover a surprising number of regional state fights over territory motivating cyber conflict. Most rival dyads that engage in cyber conflict are neighbors; thus evidence of regionalism for cyber conflict is present. This finding is counterintuitive to the nature of cyberspace, which is global and instantaneous. Some say that cyber conflict transcends boundaries and borders. As Chansoria (2012: 1) notes, "Information Warfare (IW) especially in the digital ether of cyberspace has become a realm that defies borders, challenges state boundaries, and most significantly, provides the military of a nation to realize certain political goals, allowing for a more precise form of propaganda." Yet evidence presented here demonstrates that cyber conflicts are not disconnected from the typical international conflicts over space and place.

The research also demonstrates that nearly half of all cyber incidents in our data can be coded as theft operations, in which a government is attempting to steal sensitive information from another government. This alludes to cyber conflict just being the newest form of one of the oldest professions of the civilized world: espionage. Why put your human spies at risk by sending them to your enemy's territory to steal weapons plans when it is much easier and cost effective to steal these plans in cyberspace? This process is evident in the China-US rivalry; the Chinese have stolen Lockheed Martin plans and have also hacked into the Pentagon's secure network several times.

China is by far the most active state in the use of cyber tactics as a foreign policy tool; it is the most engaged and is the main initiator of cyber conflicts. The United States ranks second, and is the most targeted state. Other states include regional rivals in East and South Asia, the Middle East, and the former Soviet Union. Overall, cyber activity does not correlate with power, technology, or resources. Put simply, these tactics are part of a larger function of active foreign policy disputes between states. Low-severity cyber conflicts will likely make up the future normal relations range of low-level contentious actions between states and their proxies.

Regionalism is found to be prominent in what is usually thought of as a global issue and a global problem. Territorial disputes can lead to disagreements among rivals, and rivals who have territorial disputes will usually be neighbors (Vasquez and Leskiw 2001). Cyber tactics are then used because they are quick, easy, and can affect the rival's populace by inflicting pain on a large area swiftly. DDoS methods can shut down government websites. Vandalism methods can send propagandist messages through the Internet and affect the psyche of the enemy population. Cyberspace is therefore a perfect forum for low-level, widespread, and sometimes psychological threats to an enemy population.

Finally, each interactive cyber unit has unique dynamics; that is, not all cyber conflict is created equal. For example, China seems to initiate cyber espionage

or theft operations against states as a means to exert power, while India and Pakistan have been enmeshed in a propaganda war in cyberspace. Which states are involved with what targets, therefore, matters greatly when it comes to cyber conflict at the state level of interaction. The evidentiary context of cyber conflict is critical to the examination of how the tactic is used. Often analysts describe cyber initiators as nameless and faceless (Clarke and Knake 2010: 34; Carr 2010: 89). They often invoke the overstated and elusive attribution problem in cyberspace. Yet this is where international relations scholarship is so critical. We can know who is most likely to utilize cyber tactics against whom. Cyber incidents and their perpetrators are not mysterious given the targets. There are often real concrete issue disagreements that provide the proper context for cyber conflicts. We need to get to the root causes of conflicts in order to understand and eliminate dangerous cyber interactions.

EXAMPLES OF CYBER CONFLICT: FLAMBÉ AND THE GREATEST INTERNET ATTACK—EVER!

Most tomes examining cyber conflict approach the subject from the most devastating and damaging cyber incidents that have occurred in recent history. Stuxnet is often the center of the analysis. Stuxnet and other such incidents, like Red October, Titan Rain, and Flame, will not be ignored in this volume; we will spend considerable time examining the myths associated with these often cited major cyber incidents. Yet, the hypothetical tale that Clarke and Knake (2010: 67) lay out is typical of the cyber hype industry and is troubling for many reasons. This is a hyperbolic worst-case scenario that presents what could be possible in cyberspace if US relations soured with a cyber power such as China or Russia.

> Several thousand Americans have already died, multiples of that number are injured and trying to get to hospitals. There is more going on, but the people who should be reporting to you can't get through. In the days ahead, cities will run out of food because of the train-system failures and jumbling of data at trucking and distribution centers. Power will not come back up because nuclear plants have gone into secure lockdown and many conventional plants have had their generators permanently damaged. High tension transmission lines on several key routes have caught fire and melted. Unable to get cash from ATMs or bank branches, some Americans will begin to loot stores. Police and emergency services will be overwhelmed. (Clark and Knake 2010: 67)

Instead of taking the extreme and using it to justify the analysis, we must do more if we are covering the true scope of cyber interactions globally. It is critical and important to describe the shape of international cyber relations by examining the typical, the average, or the common cyber conflicts, and the

failures demonstrated by those who utilize cyber tactics. One of the most interesting cyber operations has been dubbed Flambé. A variant of the Flame virus, it is likely that cyber specialists utilized and repurposed the code of the Flame incident (that had plagued Iranian networks) for their own ends.[16] In May 2012, computers in the office of former French President Nicolas Sarkozy displayed evidence of malware. According to the French Press, "the attackers were able to get to the heart of French political power, harvesting the computers of close advisers of Nicolas Sarkozy and obtaining 'secret notes' and 'strategic plans.' "[17]

What is interesting is not the actual operation, but the method of the incident, as well as the weaknesses that were revealed. For one, the fact that the hackers utilized the basics of the Flame code demonstrates a typical problem with cyber weapons: once used and let out into the wild, anyone and everyone can then use them for their own ends. Weapons developed over years at vast expense can now be used by one's enemies to harm an ally. Due to this problem, is it therefore difficult to argue that major cyber weapons will not be released into cyberspace, which is public, because of how they may be used by others. In short, cyber weapons are not private and are challenging to contain, especially if the target does little to prevent the cyber incident.

Flambé is also interesting for the weaknesses it displays in the target. French policymakers were duped into accepting false Facebook "friends." These new friends then contacted members of the staff, according to their particular interest, who were then prompted to open seemingly harmless Word or PDF files that were infected with the Flame malware. This allowed hackers access to the French system, and the ability to access sensitive information.

Some might say that this demonstrates the ingenuity of the initiator, and this is true, but it also demonstrates that many successful cyber efforts can put the focus of failure in part on the target. That vital French systems were not "air gapped" and disconnected from the basic Internet, as well as Facebook, is seen as irresponsible, even shocking. That members of the staff of the French government would enter their security credentials in response to random Internet queries should be addressed, and protocols need to be adjusted or even created. There is great danger in cyberspace if such critical and responsible members of staff can be duped so easily. This suggests that we need to do a lot more than develop cyber weapons to protect a state; basic cyber hygiene or protocols on how to use one's personal computer in a secured network need to be applied.

More often than not, simple measures should be taken, for example updating software programs, providing for gaps between computer systems and the public, and giving basic training about Internet behavior to vital staff. Instead, many advocate more offensive methods, skipping past the banal and everyday types of efforts that Flambé lays bare. Flambé likely tells us much more about cyber interactions and cyber defenses than most realize. Flambé is not an outlier; most security professionals have many such stories of economic cyber conflict being

successful because of the failures of the target, rather than the brilliances of the infiltrator.

Another event important for the development of views on cyber conflict occurred on March 26, 2013. The *BBC, New York Times*, and other major news organization breathlessly promoted it as the greatest cyber attack ever.[18] Elsewhere it was dubbed the DDoS incident that "almost broke the Internet" by increasing traffic so much that normal processes would not work.[19] CNN noted, "It is the biggest attack we've ever seen."[20] In reality, a dispute between an e-mail spammer, Spamhaus, and an Internet protection force, CyberBunker, got heated and spilled over into the public sphere. A rise in Internet traffic would be indicative of the greatest cyber infiltration ever, but there was no evidence of such an increase. There were no Netflix outages, as the *New York Times* suggested. Internet news website Gizmodo noted, "why are the only people willing to make any claims about the validity or scope of the incident directly involved?"[21]

The key takeaway from this incident is that the public and elites often do not understand, or care to really investigate, the nature of cyber operations as they occur. They take the word of the state or a company at face value, while doing little research. This inflates the hype surrounding the tactic of cyber operations. How would one know if this was a great cyber operation—what evidence for this event was there that supported such reporting? Instead, the news media relied on a few selective and biased quotes to support their reporting.[22]

The corresponding issue is that the debate on the nature of cyber conflict is often led by—and benefits—self-interested Internet security firms. They have an interest in the escalation of cyber fear and the creation of a cyber weapons industrial complex. Fear has been good for business, as "the global cyber security industry is expected to grow an additional $7.2 billion in the next four years, according to projections."[23] Academics, scholars, and policymakers must recognize this and come to their own conclusions as to whether or not this hype is warranted. To truly understand the nature of cyber conflict, we must be able to analyze, predict, and explain how cyber incidents do occur, why, and by whom. In skipping this step, the foreign policy community has done a disservice to the international community, as they have skipped the step of examining the problem and have gone straight to the policy advice stage of the process. It is our goal to explain the actual nature of cyber conflict in the modern world in order to return debate on the issue to a more rational and considered perspective.

THE STAKES IN THE DEBATE AND CYBER VULNERABILITY

Some argue that cyber attacks could be considered acts of war (Stone 2012). With the increased digital connections between society, states, and individuals, some see a weakness that will be exploited through sheer probability and opportunity. McGraw (2013: 109) states "our reliance on these systems is a major factor