2015

University of North Carolina Wilmington

Master of Science in

Computer Science and Information Systems

Proceedings

https://csbapp.uncw.edu/mscsis

BUILDING A THEORETICAL BASIS FOR CYBER SECURITY BEST PRACTICES

Howard Kleinberg

A Thesis Submitted to the
University of North Carolina Wilmington in Partial Fulfillment
of the Requirements for the Degree of
Master of Science

Department of Computer Science
Department of Information Systems and Operations Management

University of North Carolina Wilmington

2015

Approved by

Advisory Committee

Jeffrey Cummings

Gene Tagliarini

Bryan Reinicke
Chair

Accepted By

Dean, Graduate School

TABLE OF CONTENTS

ABSTRACT

This thesis documents the creation of a theoretical basis for the Cyber Security field. While there is no shortage of experience-driven, practical guidelines for 'Best Practices' in Cyber Security, the Cyber Security field has no theoretical basis, per se. Without a theoretical framework, Cyber Security is ultimately hindered in its ability to describe, provide an overall and complete 'big picture' understanding of, and thus, how best to design and implement Cyber Security Best Practices. This thesis seeks to address this shortfall by introducing the theoretical framework of International Relations (IR) as the basis for generating a theoretical framework for the Cyber Security field. More specifically, this work will draw upon Technology and Security-specific IR theories to generate a framework that is then 'tailored' to describe, understand, clarify, and hopefully to predict the nature of Cyber Security. The goal of this work is clarify the threats, scope, and behavior of those threats, how they pertain to any operator of any size, and ultimately, how best to survive and thrive in cyberspace. Once this theoretical framework is established, it will then be 'validated' by comparing it with existing experience-based Cyber Security Best Practices, to determine how 'good a fit' there really is between the theoretically-predicted and industry-observed Best Practices. A longer-term goal of this Thesis is to offer this framework as a basis with which not only to more fully understand Cyber Security Best Practices, but also to seek out 'missing' best practices, whether in this thesis, or in other, future research.

LIST OF TABLES

LIST OF EQUATIONS

CHAPTER 1: INTRODUCTION

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." – Sun Tzu[1]

Cyber Security is, without a doubt, one of the most critical aspects of the computer information systems world today. However, questions inevitably arise as to how to go about providing Cyber Security. For instance, how does one know what to protect? How does one go about determining how to protect one's information and information assets? What kinds of measures, both technological and human, must be taken to safeguard both presence in and access to (and from) the internet? How does one even know where to begin to do so effectively yet affordably and manageably? In at least partial response to these "how to" questions, many standards and advisory bodies exist today. These organizations provide full 'bodies of knowledge' that enable organizations of almost any size and type to defend their information and systems, while also operating in the internet world, or 'cyberspace.' However, these bodies are all separate organizations, and thus, incorporate entirely separate systems of thought and operation, oftentimes embodied in large volumes of guidelines, standards, and recommendations. These numerous Cyber Security and/or assurance standards, and their sheer volume, raise the overarching question of whether any or all of these standards provide 'complete coverage' for anyone who properly implements them. Further, is there any way to distinguish what 'complete coverage' in the Cyber Security domain actually means? Perhaps most critically of all questions,

[1] Giles, Lionel, *Sun Tzu on the Art of War*, Luzan & Co., 1910, pg. 6, http://www.artofwarsuntzu.com/Art%20of%20War%20PDF.pdf

at least from the academic perspective, is: are any overarching theoretical perspectives for these standards and approaches to Cyber Security?

The answer to the latter question, and the subject of this thesis, is a resounding, and worrying, no: there is no theoretical body of thought that guides Cyber Security strategy and policy, only hard-won experience. As a result, one has to ask if it is even possible to have a theoretical basis with which to seek out a potentially fuller, clearer insight into the Cyber Security world; or, perhaps more simply, how to think about, cognize, and most critically of all, how to deal with Cyber Security, regardless of the size, nature, and expertise of the information operation, from the individual level, all the way up to the largest organization?

This paper addresses this latter issue of a theoretical basis for Cyber Security. This paper asserts that it is not only possible to provide a theoretical framework with which to understand Cyber Security, but that the underpinnings for such a body of theory already de facto exist elsewhere, in the form of International Relations (IR) theories. These theories come from the academic field of Political Science, which examines how people, groups, nation-states, and international alliances and organizations of nearly all kinds process information, plan and act in their own interests, whether individually and collectively. Furthermore, there is a subset of IR theories that already provides a framework for understanding how technologies play a role in, but are ultimately subject to, human behaviors and interactions in politics at any level, or scope, from the individual all the way up to the international or global scale. The purpose of this thesis is to apply these Technology and Security-specific theories to the Cyber Security world, to produce what may well be the Cyber Security world's first theoretical framework for Cyber Security, with all the perspective (and hopefully predictive) powers to be obtained thereby.

This thesis contains three main sections of effort. The first section examines IR theories pertaining to technology and security, and focuses these theories on Cyber Security, how it works, what it means for anyone operating in cyberspace (and hence, in the Cyber Security world,) to build a theory-set specific to Cyber Security. The second section examines published academic research work from the Cyber Security sector itself, to find a collective set of 'Best Practices' derived from the real-world-experience-based, pragmatism-derived perspective. The third and final section merges, compares and contrasts these two perspectives, to determine how well the IR-Theory-based perspective compares with the 'real-world' body of knowledge, whether the theoretical perspective helps to clarify the real-world Best Practices, and finally, whether or not the theoretical set provides further perspective and 'useful guidance' in the physical world of Cyber Security.

CHAPTER 2: REVIEW AND ANALYSIS OF CSBP LITERATURE & IR THEORY

This Chapter is comprised of three main sections. The first section lists the top results of a Literature Review of the most relevant and informative published articles found on the topic of Cyber Security Best Practices, or CSBPs. Next, the second section lists the top CSBPs found in this literature set, and then explores different ways to organize or group these CSBPs by both technological and sociological contexts. This is done to explore possible ways to bridge the existing cognitive gap between the current technology-based mindset in the Cyber Security field, and the individual and/or organizational aspects of CSBPs. Finally, the third section of this chapter introduces International Relations theories that pertain to the area of technology and national security, and then explores their potential applicability to Cyber Security overall.

Critically, the academic literature review found no articles, textbooks, or academic works that provided a theoretical framework for explaining or justifying the recommended CSBPs. All the material found in the literature review was based on empirical, experience-driven, real-world-proven recommendations and standards for how best to implement various facets of Cyber Security. While a wide variety of articles, textbooks, and sanctioning bodies exist that provide an oftentimes enormous array of CSBPs and how to transform them into a functioning system, none provide a theoretical framework for CSBPs. For instance, IBM's Posey et al's A Best Practices Guide to Cyber Security [2] cites no theoretical framework with which to derive, explain, or

[2] Posey, Clay, and Roberts, Tom L., and Courtney, James F., *A Best Practices Guide to Cyber Security*, IBM Center for the Business of Government, last accessed 05-24-13, http://www.businessofgovernment.org/sites/default/files/A%20Best%20Practices%20Guide%20to%20Information%20Security.pdf

otherwise justify these best practices. Similarly, Putvinsky's Cyber Security Series Part 1: Cyber Security Best Practices lists no theoretical framework upon which it based its recommendations.[3]

But why would one need a theoretical framework for CSBPs when there is such a plethora of standards and resources from which one can simply 'follow the recipe' and build the notionally 'best possible' Cyber Security system for one's information system? One can answer this question with a simple counter-question: how do you know whether any of these frameworks, no matter how widely renowned or reputable, or no matter how well-proven a record of success they may have, truly provides full, best-possible protection? How does one know, or begin to verify, the accuracy or completeness of any CSBP set, without a theoretical framework with which to explain why they are correct or complete? How does one even begin to cognize the otherwise overwhelming issues and facets of Cyber Security, unless one has a paradigm, a way of seeing and comprehending the issue with a clear and concise 'mental picture'? The answer to these questions is theory; however, a theory for CSBP does not yet exist. Fortunately, the foundation of a theoretical framework for CSBP is indeed possible, and is the very goal of this Thesis.

Section 2.1 Literature Review: Cyber Security Best Practices

This section lists all researched references from which all the best practices were extracted. These reference items used are listed in Table 1, below:

[3] Putvinski, Matthew, *Cyber Security Series Part 1: Cyber Security Best Practices*, Corporate Compliance Insights, 06-09-09, http://www.corporatecomplianceinsights.com/information-security-best-practices/

Table 1: Cyber Security Literature Review Research Articles

Item #	Research Article
1	Rambiesa, Barb, How to reduce IT security risk with IT asset management, "Information Security Magazine", TechTarget.com, May 2013, http://searchsecurity.techtarget.com/tip/How-to-reduce-IT-security-risk-with-IT-asset-management
2	Roman, Jeff, Developing IT Security Best Practices – NIST Analyzes Cybersecurity Framework Comments, BankInfoSecurity.com, 05-21-13, http://www.bankinfosecurity.com/developing-security-best-practices-a-5775/op-1
3	Saint-Germain, René, Information Security Management Best Practice Based on ISO/IEC 17799, The Information Management Journal, July-August 2005, http://www.arma.org/bookstore/files/Saint_Germain.pdf
4	Staff, Best Practices for Managing Information Security, Symantec.com, Feb. 2010, http://eval.symantec.com/mktginfo/enterprise/other_resources/b-best_practices_for_managing_information_security-february_2010_OR_2876547.en-us.pdf
5	Staff, 2013 Data Breach Investigations Report, Verizon RISK team, March 2013, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf
6	Whitman, Michael E., and Mattord, Herbert J., Management of Information Security, Third Edition, Course Technology – Cengage Learning, 2010, ISBN-13: 978-1-4354-8884-7, 'Security Management Models', Chapter 6, pg. 211-246.
7	Nicho, Matthew, An Information Governance Model for Information Security Management, from: Mellado, D; Sanchez, LE; Fernandez-Medina, E; and Piattini, M, "IT Security Governance Innovations: Theory and Research", Advances in Information Security Privacy and Ethics (AISPE) Book Series, 2013, ISBN: 978-1-4666-2083-4, pg. 155-185.
8	Johnston-Turner, Mary, Security Management Survey: ISO, ITIL and COBIT Triple Play Fosters Optimal Security Management Execution, BMSReview.com, 2012, http://www.bsmreview.com/security_best_practice_survey.shtml
9	Staff, Cyber Security Best Practices, InvenSys.com, June 2012, pg. 1, http://iom.invensys.com/EN/pdfLibrary/ServicesProfile_Invensys_CyberSecurityBestPractices_06-12.pdf
10	Eriksson, Johan, and Giacomello, Giampiero, The Information Revolution, Security, and International Relations: (IR)relevant Theory?, International Political Science Review. Jul2006, Vol. 27 Issue 3, p221-244, ISSN: 01925121, http://0-search.ebscohost.com.uncclc.coast.uncwil.edu/login.aspx?direct=true&db=a9h&AN=22177315&site=ehost-live

Importantly, while Reference #10 has no direct bearing on any of the CSBPs, it is nonetheless retained here, because it illustrates that there has heretofore been no successful effort in the academic published world to apply IR Theory to CSBP theory formulation. This, however, implies that the work of this Thesis, if successful, does indeed constitute original research.

Section 2.2 Grouping Cyber Security Best Practices for Correlation w. IR Theory

This section lists out and begins the process of grouping CSBPs for later comparison with the IR Theory derivations. Criteria and analytical processes are listed in the respective subsections below.

2.2.1 Criteria for Selecting CSBPs

The CSBPs chosen for further analysis were selected based on one simple criterion: to use a popular English-language phrase, "where the rubber meets the road." That is to say, what concrete, 'real-world', actionable, implementable and practicable steps can an individual, group, and/or organization actually do with, for, or to their information systems, that will best secure those systems against security breaches or data loss? Abstract, high-level guidelines and recommendations may be helpful in the longer run, but what concrete steps can anyone (of any social order of magnitude) actually take to protect themselves and their information, at least, based on the best practices as outlined in the referenced literature? The following section lists and analyzes these 'real-world actionable' best practices.

2.2.2 Experiments in CSBP Categorization Frameworks

This section focuses on generating and evaluating frameworks for collating the top Cyber Security Best Practices (CSBPs) found here. A framework is vital to provide a useable perspective or paradigm with which to formulate a theoretical basis for CSBPs that can thus generate CSBPs depending upon the size and nature of an IT organization.

Two conceptual frameworks are selected and tested for their 'level of fit' to the CSBP set. The first of these is more standard technology-based grouping. In this approach, the CSBPs are grouped by technological type. These proposed technological-grouping categories are: hardware (HW); software (SW); network (NW); antivirus and intrusion detection/prevention (AV); and, People, Policies and Procedures (P3). These categorizations are shown in Table 3, below.

The second of these frameworks is an altogether new one, one that attempts, for the first time, to correlate the list of CSBPs in a manner that is analogous to IR Theory's Three Levels of Analysis. This new correlation approach organizes the CSBPs by their Scale of Societal Effect (SSE); that is, by the scope or order of magnitude of the social grouping at which any given CSBP has most direct effect, demand, or impact. And, the SSE must have tiers that reflect the three levels of analysis of the IR Theories into which it is hoped that the CSBPs will fit, later on in this work. The proposed tiers are: Individual; Organizational (including bureaucratic and business/corporation); National; and finally, Global. Note that while Individual and Organizational groupings both fall under IR Theory's Sub-State level of analysis, this distinction is necessary here to provide the finer granularity at which operations can occur in cyberspace (individual vs. organizational actions and operations.) The four proposed levels of SSE are listed in Table 2 (below) alongside the analogous IR Theoretical Levels.

Table 2: Proposed Scales of Societal Effect (SSE) vs. their Counterparts in IR Theory Levels of Analysis

Proposed Scale of Societal Effect (SSE)	Analogous IR Theory Level of Analysis
Individual	Individual (Sub-State)
Organizational	Organizational (Sub-State)
National	State
Global	International

This 'first-pass' attempt to collate all CSBPs with any and all appropriate SSEs is incorporated in Table 3, below. All CSBPs were grouped with any and all SSEs that applied to them; for instance, CSBP #1, Inventory of Authorized and Unauthorized Devices, applies to both Individual- and Organizational-scale SSEs.

Table 3: CSBPs Categorized by Technology & Societal Scale

Item #	Best Practice	Tech Type	Indiv'l	Org'l	Nat'l	Global	Cites
1	Inventory of Authorized and Unauthorized Devices	HW	Y	Y			[1]
2	Inventory of Authorized and Unauthorized Software	SW	Y	Y			[5]
3	Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers	SW, HW, NW, P3	Y	Y			[1] [5]
4	Continuous Vulnerability Assessment and Remediation	SW, AV, P3	?	Y			[3][4] [5]
5	Malware Defenses	AV	Y	Y			[5]
6	Application Software Security	AV	Y	Y	Y		[1] [5]
7	Wireless Device Control	HW	Y	Y			[1] [5]
8	Data Recovery Capability	SW	Y	Y			[5][7]
9	Security Skills Assessment and Appropriate Training to Fill Gaps	P3	Y	Y			[1][5]
10	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	NW		Y	Y		[5]
11	Limitations and Control of Network Ports, Protocols, and Services	NW		Y			[5]
12	Controlled Use of Administrative Privileges	NW, P3		Y			[3][5]
13	Boundary Defense	NW		Y			[5]
14	Maintenance, Monitoring, and Analysis of Security Audit Logs	P3		Y			[5]
15	Controlled Access Based on the Need to Know	P3	Y	Y			[1] [5]
16	Account Monitoring and Control	P3		Y			[5]
17	Data Loss Prevention (DLP)	SW	Y	Y			[5]
18	Incident Response and Management	P3		Y			[3][5]
19	Secure Network Engineering	NW		Y			[5]
20	Penetration Tests and Red Team Exercises	AV, NW, P3		Y			[5]

Table 3 cont'd

Item #	Best Practice	Tech Type	Indiv'l	Org'l	Nat'l	Global	Cites
21	Information System Security Systems Design and Planning	HW, SW, NW, P3		Y			[3]
22	Top-Down Implementation is Essential	P3		Y			[3]
23	Physical Facilities Security	HW, P3		Y			[3][5]
24	"Combined-Arms Warfare": Most-Effective Implementations Combine all four Major Cyber Security Frameworks (ISO, ITIL, COBIT, SANS)	P3		Y			[7][8]
25	Centralized InfoSec Design, Planning & Implementation	P3		Y			[4]
26	InfoSec Department Separated from IT Department	P3		Y			[4]
27	InfoSec Department Reports Directly to CISO	P3		Y			[4]
28	Compliance with All Required or Applicable Regulations	P3		Y			[2][3] [6][8] [9]
29	InfoSec Implementation must be Consistent w. the Organization's Culture	P3		Y			[4][7]
30	Maximize Use of Automation in InfoSec Implementations	HW, SW, NW, P3		Y			[4]

2.2.3 CSBPs Grouped by Technology Type

In this subsection, the 30 CSBPs from Table 3 are grouped by Technology Type, as shown in Table 4 through Table 7, below:

Table 4: Hardware-Specific CSBPs

Item #	Best Practice	Tech Type CSBP Category	Cites
1	Inventory of Authorized and Unauthorized Devices	HW	[1]
3	Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers	SW, HW, NW, P3	[1] [5]
7	Wireless Device Control	HW	[1] [5]
21	Information System Security Systems Design and Planning	HW, SW, NW, P3	[3]
23	Physical Facilities Security	HW, P3	[3][5]
30	Maximize Use of Automation in InfoSec Implementations	HW, SW, NW, P3	[4]

Note: Table 4 contains 6 hardware-specific CSBPs.

Table 5: Software-Specific CSBPs

Item #	Best Practice	Tech Type CSBP Category	Cites
2	Inventory of Authorized and Unauthorized Software	SW	[5]
3	Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers	SW, HW, NW, P3	[1] [5]
4	Continuous Vulnerability Assessment and Remediation	SW, AV, P3	[3][4][5]
8	Data Recovery Capability	SW	[5][7]
21	Information System Security Systems Design and Planning	HW, SW, NW, P3	[3]
30	Maximize Use of Automation in InfoSec Implementations	HW, SW, NW, P3	[4]

Note: Table 5 (above) contains 6 software-specific CSBPs.

Table 6: Network-Specific CSBPs

Item #	Best Practice	Tech Type CSBP Category	Cites
3	Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers	SW, HW, NW, P3	[1] [5]
10	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	NW	[5]
11	Limitations and Control of Network Ports, Protocols, and Services	NW	[5]
12	Controlled Use of Administrative Privileges	NW, P3	[3][5]
13	Boundary Defense	NW	[5]
19	Secure Network Engineering	NW	[5]
20	Penetration Tests and Red Team Exercises	AV, NW, P3	[5]
21	Information System Security Systems Design and Planning	HW, SW, NW, P3	[3]
30	Maximize Use of Automation in InfoSec Implementations	HW, SW, NW, P3	[4]

Note: Table 6 (above) contains 9 network-specific CSBPs.

Table 7: P3-Specific CSBPs

Item #	Best Practice	Tech Type CSBP Category	Cites
3	Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers	SW, HW, NW, P3	[1] [5]
4	Continuous Vulnerability Assessment and Remediation	SW, AV, P3	[3][4][5]
9	Security Skills Assessment and Appropriate Training to Fill Gaps	P3	[1][5]
12	Controlled Use of Administrative Privileges	NW, P3	[3][5]
14	Maintenance, Monitoring, and Analysis of Security Audit Logs	P3	[5]
15	Controlled Access Based on the Need to Know	P3	[1] [5]
16	Account Monitoring and Control	P3	[5]
17	Data Loss Prevention (DLP)	SW	[5]
18	Incident Response and Management	P3	[3][5]
20	Penetration Tests and Red Team Exercises	AV, NW, P3	[5]
21	Information System Security Systems Design and Planning	HW, SW, NW, P3	[3]
22	Top-Down Implementation is Essential	P3	[3]
23	Physical Facilities Security	HW, P3	[3][5]
24	"Combined-Arms Warfare": Most-Effective Implementations Combine all four Major Cyber Security Frameworks	P3	[7][8]
25	Centralized InfoSec Design, Planning & Implementation	P3	[4]
26	InfoSec Department Separated from IT Department	P3	[4]
27	InfoSec Department Reports Directly to CISO	P3	[4]
28	Compliance with All Required or Applicable Regulations	P3	[2][3][6] [8][9]
29	InfoSec Implementation must be Consistent w. the Organization's Culture	P3	[4][7]
30	Maximize Use of Automation in InfoSec Implementations	HW, SW, NW, P3	[4]

Table 7 (above) contains 20 P3-specific CSBPs. Significantly, many P3-centric CSBPs cross-cut all technology types; this makes sense, given that P3 policies must often be implemented to protect the entire system in all its aspects against security breaches or loss of information.

2.2.4 CSBPs Grouped by Scale of Societal Effect (SSE)

In this subsection, the CSBPs are grouped by Scale of Societal Effect, as shown in Table 8 through Table 11, below.

Table 8: Individual-Scale CSBPs

Item #	Best Practice	Indiv'l	Org'l	Nat'l	Global	Cites
1	Inventory of Authorized and Unauthorized Devices	Y	Y			[1]
2	Inventory of Authorized and Unauthorized Software	Y	Y			[5]
3	Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers	Y	Y			[1] [5]
4	Continuous Vulnerability Assessment and Remediation	?	Y			[3][4] [5]
5	Malware Defenses	Y	Y			[5]
6	Application Software Security	Y	Y	Y		[1][5]
7	Wireless Device Control	Y	Y			[1][5]
8	Data Recovery Capability	Y	Y			[5][7]
9	Security Skills Assessment and Appropriate Training to Fill Gaps	Y	Y			[1][5]
15	Controlled Access Based on the Need to Know	Y	Y			[1] [5]
17	Data Loss Prevention (DLP)	Y	Y			[5]

Note: Table 8 (above) contains 11 Individual-Scale CSBPs.

Table 9: Organizational-Scale CSBPs

Item #	Best Practice	Indiv'l	Org'l	Nat'l	Global	Cites
1	Inventory of Authorized and Unauthorized Devices	Y	Y			[1]
2	Inventory of Authorized and Unauthorized Software	Y	Y			[5]
3	Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers	Y	Y			[1] [5]
4	Continuous Vulnerability Assessment and Remediation	?	Y			[3][4] [5]
5	Malware Defenses	Y	Y			[5]
6	Application Software Security	Y	Y	Y		[1] [5]
7	Wireless Device Control	Y	Y			[1] [5]
8	Data Recovery Capability	Y	Y			[5][7]
9	Security Skills Assessment and Appropriate Training to Fill Gaps	Y	Y			[1][5]

Table 9 cont'd

Item #	Best Practice	Indiv'l	Org'l	Nat'l	Global	Cites
10	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches		Y	Y		[5]
11	Limitations and Control of Network Ports, Protocols, and Services		Y			[5]
12	Controlled Use of Administrative Privileges		Y			[3][5]
13	Boundary Defense		Y			[5]
14	Maintenance, Monitoring, and Analysis of Security Audit Logs		Y			[5]
15	Controlled Access Based on the Need to Know	Y	Y			[1] [5]
16	Account Monitoring and Control		Y			[5]
17	Data Loss Prevention (DLP)	Y	Y			[5]
18	Incident Response and Management		Y			[3][5]
19	Secure Network Engineering		Y			[5]
20	Penetration Tests and Red Team Exercises		Y			[5]
21	Information System Security Systems Design and Planning		Y			[3]
22	Top-Down Implementation is Essential		Y			[3]
23	Physical Facilities Security		Y			[3][5]
24	"Combined-Arms Warfare": Most-Effective Implementations Combine all four Major Cyber Security Frameworks (ISO, ITIL, COBIT, SANS)		Y			[7][8]
25	Centralized InfoSec Design, Planning & Implementation		Y			[4]
26	InfoSec Department Separated from IT Department		Y			[4]
27	InfoSec Department Reports Directly to CISO		Y			[4]
28	Compliance with All Required or Applicable Regulations		Y			[2][3] [6][8] [9]
29	InfoSec Implementation must be Consistent w. the Organization's Culture		Y			[4][7]
30	Maximize Use of Automation in InfoSec Implementations		Y			[4]

Note: Table 9 (above) contains all 30 CSBPs!

Table 10: National-Scale CSBPs

Item #	Best Practice	Indiv'l	Org'l	Nat'l	Global	Cites
6	Application Software Security	Y	Y	Y		[1] [5]
10	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches		Y	Y		[5]

Note: Table 10 (above) contains only 2 National-Scale CSBPs. Importantly, the national level is another level above and beyond the 'usual' corporate/business/bureaucracy organizational level, as the nation-state encompasses all manner of organizations and individuals; however, that is a discussion for the IR Theory section to follow.

Table 11: Global-Scale CSBPs (none!)

Note: Table 11 is empty because there are no global-scale CSBPs in Table 3. None of the CSBPs are directed at or applicable to the global scale. The ramifications of this absence will be examined in greater detail later in this work.

2.2.5 Early Observations from CSBP Groupings by Technology and SSE

Table 12 lists counts for all CSBP groupings, both by technology and SSE, as generated in the prior sections:

Table 12: Counts for all CSBP Categorizations

Categorization	Count
Technology	
Hardware-Specific	6
Software-Specific	6
Network-Specific	9
P3-Specific	20
Societal-Scale-of-Effect	
Individual-Scale	11
Organizational-Scale	30
National-Scale	2
Global-Scale	0

There are some early observations from Table 12; for instance, the majority of Technology-focused CSBPs center on Networks and P3. Perhaps even more tellingly, the largest tech grouping is 20(!) P3-Specific CSBPs, which are ultimately not really technology-focused at all, but rather, are focused on societal factors (i.e., People, Policies and Procedures for people to follow) lending further, if indirect, credence to the SSE approach. Indeed, the majority of Societal-Scale of Effect CSBPs focus on individuals (11) and critically, on organizations (all 30 CSBPs), with precious few to be found at the national-scale (2), and none at all on the global scale.

Section 2.3 International Relations Theories & Cyber Security Best Practices

This theory-set is drawn from the academic fields of Political Science and National Security Studies. In more traditional IR analysis, only one level of analysis can be chosen at a time. In this work, all levels will be considered concurrently, both to evaluate each level and its theories for their applicability and potential predictive capabilities, and to remember that in cyberspace, the actions of a single individual can have global impacts and ramifications, full as much as those of any nation-state, blurring the traditional delineations of IR theory.

International Relations (IR) is divided into 3 ‘levels’ of study and paradigm analysis: 1) The International System level; 2) The National, or State, level; and, 3) The Sub-State level. In addition to these three ‘traditional’ levels of analysis, there is also a fourth, ‘All-Levels’ framework. This ‘All-Levels” framework crosscuts all three of the traditional levels, and is meant to understand and predict outcomes in specific circumstances: confrontations and conflicts. These three Levels of Analysis, and the theories that fit into them, are described in detail in the following sections.

2.3.1 Additional Thoughts and Factors Affecting IR Theory in Cyber Security

While these traditional levels are used for IR theory work, there are three factors that alter the way in which they might be applied to cyber security:

1) The internet is 'the great equalizer': one individual with a computer and sufficient knowledge and skill has the potential to challenge the cybersecurity of large organizations, businesses, and even nation-states.
2) Anonymity: since anyone can access any site, location, or indeed, individual device instantaneously via the internet, and since the attacker's identity can be masked (or at least, be made extremely difficult to find,) anonymity is the great 'force multiplier' and emboldener of actors in the internet. This undermines the usual boundaries or inhibitions of actors in the internet, far more than such individuals could have in the physical world.
3) Instant global access: the internet enables any individual, organization, or nation-state, to access any other point or region on earth, instantaneously. This means that any individual or government intelligence agency can find and attack any target (or target-set) almost anywhere on Earth, in real time. In many ways, the internet is instant global reach, awareness and effect, and all at nearly the speed of light.

These three factors tend to 'skew' or blur, but not eliminate, the usual boundaries separating the different 'layers' in the IR Theory model. That is, the combination of greater 'power' in cyberspace, combined with the vastly reduced threat of being discovered, yields a scenario in which many more people can and do 'go on the offensive' in cyberspace than would ever dare in the physical world. And this is just as true for nation-states and organizations just as it is for individuals. At the same time, the world's interconnectivity and virtual proximity mean

that the Internet is the most integrated of all existing embodiments of the International system as the unit of analysis.

The result of these factors is that all levels of analysis must be utilized, together, as appropriate, in order to understand and hopefully derive greater predictive power from these theories, with the goal of better securing ourselves from the threats of the internet. Where classical IR Theory demands that only one theory from one layer can be chosen and used at a time, this work instead examines all levels and theories together, not only for their usefulness in providing insights into the problems of cyberspace security, but to provide greater understanding of the interactions in the Internet Age.

Critically, cyberspace is ultimately just another operational medium for human endeavor and conflict. While it has its own unique attributes and properties that differentiate it from other media, it is, nonetheless, just another medium through which human beings can observe, communicate, and act. As a result, those theories of human interaction and security are arguably the best ones to draw upon for getting 'the big picture' in security in cyberspace.

2.3.2 IR Level 1: International-Level Theories

Nowhere else is the world today more heavily and thoroughly interconnected, interdependent, and thus, more vulnerable, than it is in cyberspace. In cyberspace, more than in any physical medium, the world is so interconnected by the internet and modern telecommunications that all the world's nations, and most of its population, are much 'closer together' than ever before in human history. National borders are heavily 'blurred' in cyberspace, and the power of states' sovereignty, or at least, their ability to 'enforce their borders' and assert their control over their territories are considerably diminished. And, the long-

standing IR Theory maxim that states that 'threats are proximal' is no longer valid, at least, not in cyberspace.[4]

In many ways, in cyberspace, the world effectively is 'one system' per the very definition of this highest level of analysis in the IR Theory domain (as will be described in more detail in the sections that follow). As a result, given that there is no central authority policing, controlling or (possibly even) monitoring the world's internet activities, the international system in cyberspace is most assuredly anarchic. And finally, as IR theorist Stephen Walt states, "No single approach can capture all the complexity of contemporary world politics. Therefore, we are better off with a diverse array of competing ideas rather than a single theoretical orthodoxy."[5] On that note, let us now examine the various approaches to world politics, and consider their applicability to cybersecurity.

Classical Realism – Description

This theory has four key assumptions: 1) states are the main actors in the system; 2) all states are rational, unitary actors; 3) all states pursue their own interests, i.e., power; and finally, 4) conflicts of 'interests', i.e., conflicts, are inevitable. This theory also has several key assumptions. States' "rationality" means that all states make calculations of goals, means and ends; goals are always internally consistent. "Unitary" means that each state has a single, coherent set of goals; internal processes are irrelevant. Further, there is no international order, i.e., anarchy; no central structure or authority exists to resolve inter-state disputes. Further to this

[4] In the physical world, "Because the ability to project power declines with distance, states that are nearby pose a greater threat than those that are far away."
From Walt, Stephen M., *Alliance Formation and the Balance of World Power*, International Security, Vol. 9, No. 4, (Spring 1985), pp. 3-43,
https://umdrive.memphis.edu/rblanton/public/POLS_7508_Fall_2012/walt_alliance_formation.pdf
[5] Walt, Stephen M., *International Relations: One World, Many Theories*, Foreign Policy, (Spring 1998), pg. 30,
http://faculty.maxwell.syr.edu/hpschmitz/PSC124/PSC124Readings/WaltOneWorldManyTheories.pdf

point, this paradigm holds that "Human nature is unchanging and evil." As a result, conflicts of interest are inevitable; thus, conflicts are inevitable.[6]

Offense-Defense Theory:

This sub-theory of Classical Realism points out that when offense has the advantage, conquests are easy, and there is little security or stability. By contrast, when defense has the advantage, and can be readily distinguished from the offensive, security is more plentiful.[7]

Classical Realism's Relevance for Cyber Security

The first point of classical Realism's relevance for cybersecurity is central: cybersecurity is OFFENSE-DOMINANT, at virtually all levels. What this means is that attacks in cyberspace are bound to be more common, more disruptive, and the most effective means of achieving one's interests, from self-defense through furthering one's own offensive goals. Defenses alone cannot guarantee security from cyber attack; sufficiently skilled attackers will inevitably find a way to penetrate a defended information system. And once they penetrate those defenses, attackers can wreak any and all manner of havoc. This is not to say that defenses are superfluous; quite the contrary, all possible defenses are vital, if only to reduce the frequency and extent of damage resulting from the ever-growing numbers, types, and severity of cyber-attacks, to 'slow down' an attacker, and to make the task of breaking in as 'expensive', i.e., as difficult, time-consuming, and risky as possible. A successful defender must thus have effective methods of intrusion

[6] Walt, Stephen M., *International Relations: One World, Many Theories*, Foreign Policy, (Spring 1998), pg. 30-31, http://faculty.maxwell.syr.edu/hpschmitz/PSC124/PSC124Readings/WaltOneWorldManyTheories.pdf
[7] Walt, Stephen M., *International Relations: One World, Many Theories*, Foreign Policy, (Spring 1998), pg. 31, http://faculty.maxwell.syr.edu/hpschmitz/PSC124/PSC124Readings/WaltOneWorldManyTheories.pdf

detection, tracking, defense in depth, and attribution, the latter of which must ultimately result in some form of countervailing actions (such as criminal charges, etc.)

Worse, the 'universal' accessibility of the internet can go far above and beyond any physical ability to access any point in the world; this means that any individual, organization, or nation-state can interact with (and thus, attack) any other individual, organization, or nation-state, in real time, and at any time. Such 'universal' accessibility only exacerbates the likelihood, frequency, and level of risk from attacks in cyberspace. This must thus affect the 'calculus' (strategies and tactics) used by organizations (and individuals) of all walks of life, in formulating, practicing, and improving their Cyber Security.

Overall, then, Classical Realism very much reflects the inherent nature of cyberspace: anarchy and offense-dominance. No one state can completely control the internet, or even a significant portion of it, only their own immediate networks, at best. Even more 'extreme' than classical realism and its global perspective, anyone anywhere in the world can 'go' anywhere in the world, and can have an effect limited only by his/her/their cyber 'hacking' skills, computing power, etc. The ability to have an effect in cyberspace goes to whoever has, and uses, the greatest skills and resources. Furthermore, this is true for all levels of the internet, from the nation-state, to the organization, down to the individual. Indeed, the anarchic, offense-dominant nature of the internet has profound ramifications for the threats facing any entity connected to and operating via the internet today.

Neorealism – Description

This theory has four key assumptions: 1) states are the main actors in the system; 2) all states are rational, unitary actors; however, 3) interests are defined by security, not power; and, 4)

power is the means to security, not the end goal itself.[8]

The central tenet of Neorealism is The Security Dilemma, which holds that one state's increased security decreases that of others. This compels other states to compete to 'keep pace,' e.g., via arms races, with an implicit long-term, pan-systemic pressure on states not to lead or lag the others. As a result, the international system's nature leads to states' general-power-matching behavior. Further, as with Classical Realism, the International system is anarchic, meaning that states must look to themselves to cope with both internal and external problems.[9] Also, all states are functionally similar, and thus, all states seek the same goal, namely, to maximize their security. Thus, when threats arise, states try to counter them by balancing, by either or both of two methods: 1) internal balancing, either via military and/or economic means; or, 2) external balancing (alliances.) External balancing (alliances) in particular, leads to the formation of international structures: 'don't seek too much power, or others will balance against you.'[10]

There are two types of alliances in Neorealism. The first of these is called Balancing, in which states join together to match a common threat (e.g. NATO.) This type of alliance is defensive in nature, and it results in a more stable system. The second type of alliance is called Bandwagoning, in which lesser states join with a greater power, firstly, to prevent being attacked by that greater power, and secondly, to benefit from the 'spoils' (such as conquests) of the greater power's successes. [11]

---

[8] Waltz, Kenneth N., *The Origins of War in Neorealist Theory*, Journal of Interdisciplinary History, Vol. 18, No. 4, (Spring 1988), pp. 615-628, http://sites.google.com/site/casaroes/Waltz-OriginsofWarinNeorealistTheory.pdf
[9] Walt, Stephen M., *International Relations: One World, Many Theories*, Foreign Policy, (Spring 1998), pg. 32, http://faculty.maxwell.syr.edu/hpschmitz/PSC124/PSC124Readings/WaltOneWorldManyTheories.pdf
[10] Waltz, Kenneth N., *The Origins of War in Neorealist Theory*, Journal of Interdisciplinary History, Vol. 18, No. 4, (Spring 1988), pp. 619, http://sites.google.com/site/casaroes/Waltz-OriginsofWarinNeorealistTheory.pdf
[11] Waltz, Kenneth N., *The Origins of War in Neorealist Theory*, Journal of Interdisciplinary History, Vol. 18, No. 4, (Spring 1988), pp. 620-623, http://sites.google.com/site/casaroes/Waltz-OriginsofWarinNeorealistTheory.pdf

Another factor that comes into play in this system is its Polarity: power accrues to the largest alliances, or primary political 'structures,' which become the 'poles' of overall power in the system. Polarity affects the likelihood of war or peace. Grimly, in this system, only great powers matter; weak states matter little. [12]

The international 'structure' with the greatest long-term stability is Bipolarity; in this system, there are only two powers to balance between; there is a decreased risk of miscalculations. While Unipolarity (one greatest power or alliance) is best of all, this is rare and short-lived; others will inevitably strive to balance against it. [13]

Neorealism's Relevance for Cyber Security

While Neorealism has some relevance to Cyber Security, as in the physical world, it has nowhere near as much relevance as Classical Realism. Neorealism also shares its primary real-world shortcomings in overlooking the ambitions of some nation-states, and actors, in the cyberspace realm. For instance, aside from limited assistance and protection provided by federal agencies such as the DOD, DHS and NSA, there is little active defense/protection of all US individuals and organizations from internet attack. The international system may be (but also questionably) unipolar, in that the US may be the most dominant power in cyberspace; however, there are significant challengers, both from other nation-states, and from organizations (cybercriminals, in particular) that threaten the US and its constituents of all sizes. Indeed, China,

[12] Waltz, Kenneth N., *The Origins of War in Neorealist Theory*, Journal of Interdisciplinary History, Vol. 18, No. 4, (Spring 1988), pp. 620-623, http://sites.google.com/site/casaroes/Waltz-OriginsofWarinNeorealistTheory.pdf
[13] Waltz, Kenneth N., *The Origins of War in Neorealist Theory*, Journal of Interdisciplinary History, Vol. 18, No. 4, (Spring 1988), pp. 620-623, http://sites.google.com/site/casaroes/Waltz-OriginsofWarinNeorealistTheory.pdf

Russia, Iran and North Korea are making significant efforts to undermine and take advantage of US cyberspace-based assets and vulnerabilities.[14]

Interestingly, one outstanding example of the fruits of international cooperation towards cyberspace security is STUXNET, a joint US-Israeli cyberwarfare program/operation carried out against Iran's Natanz and Isfahan nuclear-weapons development facilities, allegedly dating back to 2010.[15] However, this is a relatively isolated event in international cooperation; there is precious little else ongoing, at least, not in the open-source world. Tellingly, STUXNET was an offensive cybersecurity program and operation, supporting the previous assertions about the realist, anarchic, offense-dominant nature of cyberspace and Cyber Security operations. Nonetheless, STUXNET serves as a powerful example of the potential benefits of international cooperation in cybersecurity. Also, and more ominously, there is cooperation between Iran and Hezbollah, Iran's Lebanon-based terrorist proxy organization, in carrying out cyberwarfare operations against the US and elsewhere.[16] While this implies that there are at least some advantages to be obtained by 'balancing' or alliance-formation among states (and perhaps, all levels of entities within cyberspace) in Cyber Security, and that this IR Theory has at least some potential benefits to offer, Neorealism nonetheless holds little overall insight into the international system in cyberspace.

---

[14] Tadjdeh, Yasmin, *Fears of Devastating Attacks on Electric Grid, Critical Infrastructure Grow*, National Defense Magazine, October 2013, http://www.nationaldefensemagazine.org/archive/2013/October/Pages/FearsofDevastatingCyber-AttacksonElectricGrid,CriticalInfrastructureGrow.aspx

[15] Barnes, Ed, *Mystery Surrounds Cyber Missile That Crippled Iran's Nuclear Ambitions,* FoxNews.com, November 26, 2010, http://www.foxnews.com/scitech/2010/11/26/secret-agent-crippled-irans-nuclear-ambitions/?test=latestnews

[16] Staff, *Iran's global cyber war-room is secretly hosted by Hizballah in Beirut*, DEBKAfiles.com, 10-21-12 http://www.debka.com/article/22459

Neoliberal Institutionalism – Description

This theory has four key assumptions: 1) states are the main actors in the system; 2) all states are rational, unitary actors; 3) international cooperation (or Structuralism) is possible, even in an anarchic system; and, 4) international institutions and regimes enable international cooperation. Note that this latter feature is new to Neoliberal Institutionalism. International cooperation implies that: anarchy doesn't always mean self-reliance and competition; gains are measured in absolute, not relative terms; and, the Security Dilemma is not inevitable. [17]

International institutions/regimes can arise in such a system, and can facilitate cooperation among states, by monitoring and enforcing agreements, reducing uncertainty about other states' capabilities and intentions, extending out the "shadow of the future" (time horizons) among cooperating states, and finally, creating conditions for reciprocity, by linking issues.[18]

Game Theory and Cooperation under the Neorealist Security Dilemma

There are a number of game-theory-based analogs illustrating the nature of alliance-formation and stability under Neorealism. For instance, there is the "Stag Hunt" analogy: in this example, there are numerous hunters, ostensibly working as a group to hunt a large stag (the analog for international peace.) In this model, cooperation would help all participants, but self-interest leads to defections, which causes strife, and increases costs to the remaining alliance members. There is also the "Security Dilemma" analogy; in this parallel, increasing one state's own security decreases others', who then seek to raise theirs; this leads to arms races,

[17] Walt, Stephen M., *International Relations: One World, Many Theories*, Foreign Policy, (Spring 1998), pg. 32, http://faculty.maxwell.syr.edu/hpschmitz/PSC124/PSC124Readings/WaltOneWorldManyTheories.pdf
[18] Walt, Stephen M., *International Relations: One World, Many Theories*, Foreign Policy, (Spring 1998), pg. 32, http://faculty.maxwell.syr.edu/hpschmitz/PSC124/PSC124Readings/WaltOneWorldManyTheories.pdf

miscalculations, and wars. Next is the "Prisoner's Dilemma" analogy. In this parallel, two criminals (who are partners), are held prisoner; each prisoner is taken to a separate room with a separate interrogator. Each prisoner is then offered a deal to give up his partner, in exchange for freedom or a reduced sentence, along with the threat, 'if you're given up, you get the full sentence; so confess first, or suffer the worst of the consequences.' However, prior cooperation (via plans and/or rewards) is vital to the results of this scenario.[19]

Neoliberal Institutionalism's Relevance for Cyber Security

While there is global cooperation in technical terms (communications protocols, TCP/IP, connectivity standards, etc.) there is precious little international cooperation in terms of international cybersecurity. Indeed, as Whitman et al point out, "Because of the political complexities of the relationships among nations and cultural differences, currently few international laws relate to privacy and Cyber Security. Therefore, these international security bodies and regulations are… limited in scope and enforceability."[20] And frankly, international laws are only complied with, and enforced by, law-abiding states and organizations.[21] The risk here is that writing and enforcing laws will only hinder the law-abiding states and entities, give operational advantage and potentially superiority to cyberspace law-breakers. This problem is only exacerbated (and encouraged) by the innate anonymity, stealthiness and unaccountability of cyberspace. This theory, therefore, is of little to no practical help in understanding or furthering Cyber Security.

---

[19] Jervis, Robert, *Cooperation Under the Security Dilemma*, World Politics, Vol. 30, No. 2. (Jan., 1978), pp. 167-214, http://ic.ucsc.edu/~rlipsch/pol160A/Jervis.pdf

[20] Whitman, Michael E., and Mattord, Herbert J., *Management of Information Security*, Third Edition, Course Technology – Cengage Learning, 2010, pg. 442.

[21] Violations of a wide variety of arms control treaties cite non-democracies/rogue states, not Western democracies. From Staff, *Adherence to and Compliance with Arms Control, Nonproliferation, and Disarmament Agreements and Commitments*, U.S. Department of State, July 2010, http://www.state.gov/documents/organization/145181.pdf

Constructivism – Description

This theory has three key assumptions: 1) states are the main units of analysis; 2) international politics arise out of social constructs, i.e., "objective" relationships do not exist; and, 3) national identities drive national interests, such as social identities, norms, and elite beliefs. [22]

Constructivism's Relevance for Cyber Security

This theory has particular usefulness in identifying threat states, organizations and individuals. Arguably, if an entity (be it a state, organization or individual) is sufficiently antipathetic towards another entity, and has sufficient access to and/or skills with hacking, infiltration and/or espionage, then the hostile entity can and likely will become a threat to the targeted interests. In cyberspace at least as much as in the physical world, if an entity voices hatred, violence and destructive intentions towards another entity (or just practices illicit behavior,) then the former is a likely candidate for acting out its hostility/illegal behavior via cyberspace. Indeed, this theory is very useful in distinguishing between threatening states from non-threatening ones, for example, the threats to US cyberspace interests posed by Israel and France as compared to Iran, China, Russia, and North Korea.[23]

[22] Walt, Stephen M., *International Relations: One World, Many Theories*, Foreign Policy, (Spring 1998), pg. 33-34. 40-41, http://faculty.maxwell.syr.edu/hpschmitz/PSC124/PSC124Readings/WaltOneWorldManyTheories.pdf
[23] Reisinger, Don, *U.S. target of sustained cyber-espionage campaign*, CBS News, 02-11-13, http://www.cbsnews.com/news/us-target-of-sustained-cyber-espionage-campaign/

2.3.3 IR Level 2: State-Level IR Theories

Democratic Peace Theory (DPT) – Description

In this theory, democracies tend not to go to war with one another; hence, democracies are deemed to be the best form of government to have, to achieve overall peace. However, democracies may be more prone to wage wars vs. non-democracies. And more, democracies tend to wage shorter but more intense and destructive wars than do non-democracies. Worst of all, democratizing states may be the most war-prone of all, prime examples of which are post-WWI Germany and post-Cold-War Serbia.[24] [25]

There are two primary mechanisms of Democratic Peace: institutional constraints, and peaceful norms and values. Institutional constraints are comprised of elections, civilian control over the military, the rule of law, and checks and balances in the government structure; in this system, public opinion is vital. Peaceful norms and values translate into peaceful dispute-resolution with other states. Peaceful norms and values also generate a positive view of other democracies; as a result, it eliminates the security dilemma (at least, with other democracies.)[26] [27]

Democratic Peace Theory's Relevance for Cyber Security

At first glance, this theory does not appear to have as much traction in cyberspace as it does in the physical world. Indeed, two of our most notable problem-states in cyberspace, at least

---

[24] Walt, Stephen M., *International Relations: One World, Many Theories*, Foreign Policy, (Spring 1998), pg. 39-40, http://faculty.maxwell.syr.edu/hpschmitz/PSC124/PSC124Readings/WaltOneWorldManyTheories.pdf
[25] Levy, Jack S., *Domestic Politics and War*, Journal of Interdisciplinary History, Vol. 18, No. 4, (Spring 1988), pp. 658-662, http://fas-polisci.rutgers.edu/levy/1988%20Domestic%20Politics%20&%20War.pdf
[26] Walt, Stephen M., *International Relations: One World, Many Theories*, Foreign Policy, (Spring 1998), pg. 39-40, http://faculty.maxwell.syr.edu/hpschmitz/PSC124/PSC124Readings/WaltOneWorldManyTheories.pdf
[27] Levy, Jack S., *Domestic Politics and War*, Journal of Interdisciplinary History, Vol. 18, No. 4, (Spring 1988), pp. 658-662, http://fas-polisci.rutgers.edu/levy/1988%20Domestic%20Politics%20&%20War.pdf

in the cyber-espionage realm, are Israel and France (after China, that is.)[28] Worse, given that cyber-espionage can occur between two organizations in the same country (industrial espionage,) this theory clearly does not provide useful insights. How ironic, given that this theory is arguably the cornerstone of international policymaking from the perspective of the democratic nations of the world.

However, this theory actually provides great insight into where to look for cyberthreats at the highest levels: the world's most prominent non-democracies: China, Russia, Iran and North Korea, arguably precisely the same nation-states that pose most significant threats in the physical world today. Furthermore, this theory is widely considered to be the cornerstone paradigm driving US and Western foreign policy decision-making. Conversely, the great successes of Western modernity, both economically and militarily, make the West the recipient of hate, envy, rivalry, and targeting by ambitious, ruthless non-democracies (as well as non-state actors such as terrorist organizations.) As a result, this theory must be considered when seeking to understand where our greatest threats are emanating from.

Strategic Culture – Description

Different cultures, states, can also have different warfighting cultures. Thus, different states make different strategic choices.[29]

[28] Reisinger, Don, *U.S. target of sustained cyber-espionage campaign*, CBS News, 02-11-13, http://www.cbsnews.com/news/us-target-of-sustained-cyber-espionage-campaign/

[29] Levy, Jack S., *Domestic Politics and War*, Journal of Interdisciplinary History, Vol. 18, No. 4, (Spring 1988), pp. 653-658, http://fas-polisci.rutgers.edu/levy/1988%20Domestic%20Politics%20&%20War.pdf

Strategic Culture's Relevance for Cyber Security

This theory also provides some insight into where to look for threats in cyberspace, along similar lines to Democratic Peace Theory. That is, those cultures that are more warlike or hostile and ruthless, are even more likely to use cyberspace to carry out their 'missions', seek 'revenge', and carry out attacks on their enemies than they otherwise would in a much more visible and risky physical attack or combat operation. Cyberwar events such as Russia's 2007 attacks on Estonian government and banking institutions,[30] and the Palestinians' attacks on Israeli websites during the 2014 Israel-Gaza War[31], serve as examples of this. However, of the State-level theories discussed to this point, DPT (above) arguably provides more insight into identifying some of greatest cyberspace threats than does this theory.

Revisionism – Description

Under the Revisionism theory, there are two types of States. The first of these are Status-Quo States; these are satisfied with the existing international system, such as the U.S. The second type are 'pure' Revisionist states, that are unhappy with the existing international system, and want (and in some cases, strive) to change it. There are also several types of Revisionist states: the first of these are the Lambs'; these states are unhappy, but weak and timid. Next are the 'Jackals'; these states are unhappy, and risk-averse, but opportunistic. Finally, there are the 'Wolves'; these states are not only dissatisfied, but worst of all Revisionist states, they are also risk-eager, and will challenge the current order.[32] Contemporary examples of Revisionist

[30] Traynor, Ian, *Russia accused of unleashing cyberwar to disable Estonia*, The Guardian, 05-16-07, http://www.theguardian.com/world/2007/may/17/topstories3.russia
[31] Dunnigan, Jim, *Information Warfare: Iranian Hackers Step Up*, Strategy Page, 08-24-14, http://www.strategypage.com/htmw/htiw/articles/20140824.aspx
[32] Schweller, Randall, *Bandwagoning for Profit: Bringing the Revisionist State Back In*, International Security, Vol. 19, No. 1 (Summer, 1994), pp. 72-107, http://people.reed.edu/~ahm/Courses/Reed-POL-240-2012-S1_IP/Syllabus/EReadings/02.2/02.2.Schweller1994Bandwagoning.pdf

'wolves' are Iran, North Korea, China, and Russia.

Revisionism's Relevance for Cyber Security

This theory, perhaps even more than DPT itself, may serve to explain why we must be concerned about the manifold cybersecurity threats posed by Iran, North Korea, China, and Russia. All of these states share the Revisionist's 'hunger' for overturning the international system, for becoming great powers in their own right, and for displacing the U.S. from its current status as incumbent global superpower. Such displacement efforts can include direct and indirect means, both against the US as well as against its interests and allies worldwide. Indeed, all of these states (except North Korea) are former superpowers in their own right, the memory of which is very active in their history and collective cultures; and most importantly of all, they all 'want their empires back.'[33]

Importantly, this concept of a 'Revisionist' entity could also be extended 'downwards' in scale. in order to inform and warn us about other, lesser, sub-state and "non-state actors"[34] in the cyberspace system. This more flexible use of scale and scope enables the inclusion of the full spectrum of credible cyberspace threats, from nation-states all the way 'down' to and including groups and individuals with a similar drive to change the world order, or perhaps simply to act out a grudge or drive to defeat rival organizations (such as in the business world). This is the case because the internet is 'the great equalizer' in terms of an individual's ability to affect other entities in cyberspace.

---

[33] Mead, Walter Russell, *The Return of Geopolitics – the Revenge of the Revisionist Powers*, Foreign Affairs – Council on Foreign Relations, May-June 2014, http://www.foreignaffairs.com/articles/141211/walter-russell-mead/the-return-of-geopolitics

[34] Buse, Margaret, *Non-State Actors: Their Significance in the Global Picture*, James Madison University Center for International Stabilization and Recovery, Issue 5.3, December 2011, http://www.jmu.edu/cisr/journal/5.3/features/maggie_buse_nsa/maggie_buse.htm

2.3.4 IR Level 3: Sub-State-Level Theories

The essence of this level of analysis is the concept of 'Rationality.' Here, 'Rationality' refers to 'means-ends calculations.' 'Rationality' thus assumes that actors can logically identify all objectives and means, choose among them, and be consistent in their selections. However, 'rationality' is, in fact, affected by emotions, personal biases, misperceptions, miscommunications, uncertainty, and external opinion (whether it be elite, domestic, or foreign.) The decision-making process thus depends on the sub-structure in question.[35] The Three Primary Sub-State-Level Theories are Bureaucratic Politics, Organizational Politics; and Individual Politics.

Bureaucratic Politics – Description

In Bureaucratic Politics theory, there is no such thing as a state; rather, it is multiple bureaucracies that control the state's decision-making process. Policy is formed by bargaining processes that occur within and between the different bureaucracies. Policymaking is also driven by the nature of each bureaucracy.

Bureaucracies have a number of 'natural tendencies' worth noting. The first of these is that bureaucracies pursue their own interests (namely survival, growth, and power). Second, bureaucracies are hierarchical, meaning that subordinates follow their leader. Third, bureaucracies are an inherent characteristic of democratic politics. Fourth and finally, to understand a bureaucracy, there is lots of people-following to do (who are they, where they are, how important they are, what are their perspectives and agendas, etc.)

---

[35] Allison, Graham, *Conceptual Models and the Cuban Missile Crisis*, The American Political Science Review, Vol. 63, No. 3 (September 1969,) pp. 691-698, http://glennschool.osu.edu/faculty/brown/home/Public%20Management/PM%20Readings/Allison%201969.pdf

However, there are inherent problems in the information flow process within Bureaucratic Politics. The first of these is The Principal-Agent Problem: the flow of information, and the very control of that information, means power for whoever has or controls it. The second of these are Procedural Problems: whoever sets the agendas and decision-making rules also has power within the bureaucracy. The third of these is Psychological Problems referring to ways of thinking, understanding, framing and formulating problems and potential solutions to them, which can enable, constrain, or limit the bureaucracy and its members. The fourth and final problem considered here is Group-Think, in which all of a group's members either 'think alike', or fear to dissent. This problem can also enable, constrain, or limit the bureaucracy and its constituents.[36]

Bureaucratic Politics' Relevance for Cyber Security

In cyberspace, there effectively is no such thing as a nation-state: no or highly porous borders, few or no guards, and no military to be called in to protect and control or 'liberate' a nation's cyberspace at need. On the contrary, the most powerful actors in cyberspace tend to be individuals and organizations. As a result, the most powerful coherent entities operating in cyberspace may very well be government-funded and -sanctioned bureaucracies, or organizations. Such groups, especially groups of cyberspace-capable individuals equipped with superior resources, can not only protect themselves, but can also, impose their will in cyberspace by attacking other organizations or individuals via that medium. However, these organizations must ultimately answer to their governing states for their actions (at least, in the case of

[36] Allison, Graham, *Conceptual Models and the Cuban Missile Crisis*, The American Political Science Review, Vol. 63, No. 3 (September 1969,) pp. 707-715, http://glennschool.osu.edu/faculty/brown/home/Public%20Management/PM%20Readings/Allison%201969.pdf

government and commercial organizations); indeed, in many cases, they are directed by their government to do whatever they possibly can to achieve their government's goals in cyberspace. Such organizations as the US' NSA, CIA and USCYBERCOM, as well as China's PLA cyberwarfare units (and the 'volunteers' they oversee) are prime examples of this paradigm in action.

Organizational Politics – Description

The focus here is on limitations of organizational information processing, not bureaucratic structure; importantly, all organizations struggle with this. The demands of 'rationality' are too great; there is simply too much information and too many alternatives to process, to consider all the information and alternatives. As a result, each organization tries to formulate and follow its own decision-making process.

There are five methods for organizations to manage information problems:

a) Narrow the Range of Available Options: choose organization-selected solutions, or the first set of solutions found, for further processing.

b) "Satisfice:" find satisfactory and sufficient solutions; the solution selected for implementation is usually the first solution that meets the minimum subset of needs and minimum requirements.

c) Adopt "Standard Operating Procedures:" this helps to cope with uncertainty, sets methods for dealing with problems, and provides consistency.

d) Develop Missions and Cultures: This pan-organizational cultural approach shapes the behavior of individuals in the organization with time in the organization. It also focuses and narrows task-sets. However, this can also hinder information-flow and the range of possible solutions.

e) Resistance to Change: organizations tend to develop an inherent, unquestioned trust in the perceived effectiveness of their current methodology. There is also an inherent fear of, and unwillingness to invest in new methods. Thus, resistance to change in organizations can also hinder information-flow and optimal problem-solving.[37]

All of these inherent approaches limit the number of available options and their ultimate effectiveness. In addition, once an organization sets these information-processing 'habits' in place, they can be very difficult to break.

Organizational Politics' Relevance for Cyber Security

This aspect of IR Theory has great potential for cybersecurity theory. It is in organizations, subject to their culture, and both empowered to and also constrained by, their organization's culture, methods, capabilities, and limitations, that we can find perhaps the greatest insight into who 'they' are, what they want, are capable of, and thus, have done, are doing, and hopefully ultimately, predict what they will do. It is arguably at this level that a capable cybersecurity operator or group can have the greatest desired effect in cyberspace, and thus, out in the physical world. By 'banding together' with others of similar political, social, cultural and cyber-skills, the groups' collective intended effect can be best realized, particularly (though not only) if the organization is government-sanctioned and -supported. If the organization is governmental, particularly one such as the CIA, DHS or NSA, then both the organizational culture, operational nature, as well as policies and procedures, and resources of that organization, will be focused on their cybersecurity 'solutions' and operations writ large.

[37] Allison, Graham, *Conceptual Models and the Cuban Missile Crisis*, The American Political Science Review, Vol. 63, No. 3 (September 1969,) pp. 698-703, http://glennschool.osu.edu/faculty/brown/home/Public%20Management/PM%20Readings/Allison%201969.pdf

However, if the organization is in the private sector, then questions of motivation and skills become pan-societal; that is, the organization's members may well be there 'just for the job', and not at all necessarily motivated as cyber-operators by politics, culture or sheer skill-level. As a result, it will be up to either the individual employees themselves (not the best approach, organizationally) or the organization's leadership (much better) guiding and supervising the employees to incorporate and follow Cyber Security Best Practices per se as part of their assigned tasks.

Individual Politics – Description

This theory-set seeks generalizable psychological explanations for individual behaviors. It is not about 'psychological disorders;' rather, it focuses on the limits of the human brain to process all available information. Indeed, instead of processing all information and all possible outcomes, the human mind takes simplifying shortcuts, ignores trade-offs, makes inappropriate analogies, and makes premature closure. These limitations can be summarized as biases. As a result, the Individual Politics theory-set considers two types of biases, cognitive and emotional.
1) Cognitive Biases; several types exist. In Prospect Theory, people are risk-averse towards gains, but are risk-accepting towards losses. In Framing Effects, wording can affect understanding. In Coordination and Intent, people can misinterpret random and intentional events. In Attribution Errors, people can mistakenly believe that others think the same way as they themselves do (also known as "Mirror-Imaging.") In Clear Motives, people believe that their own motives are transparent and perfectly understood by others.
2) Emotional Biases: describe the difficulties of processing information under stress. For instance, Wishful Thinking means overestimating what we wish to see. Similarly, Bolstering

means investing in, and adhering to, a decision that isn't working. Selective Memory means putting either a positive or negative light on memory of events. And finally, Scenario Fulfillment means seeing only the desired evidence and results, while ignoring all contradictory evidence.

As a result, people tend to overestimate both their own reasonableness and the hostile intentions of others. And, these information-processing problems affect everyone; all must thus be cautious when dealing with others, both in terms of one's own perceptions and thought processes, as well as those of adversaries.[38]

The Power of Individual Leaders

In politics, and perhaps overall, a leader's personality can profoundly affect international politics. There is a list of hypotheses to factor this into international politics.
The first of these are Foundational Hypotheses, or how individuals affect what the state does, and how. The second hypothesis focuses on Personality Traits, or how risk-accepting/averse a leader is; risk-accepting leaders in particular, have more grandiose goals and are more likely to cause problems, conflicts, and wars. The third hypothesis is, simply, When Individuals Matter: that individuals matter more when power is concentrated at top of a structure (such as in an organization, company, or government.) The greater the concentration of power at the top, the greater the power and risk posed by the judgment of leadership. This hypothesis is even significant in a parliamentary democracy. This issue also becomes significant in inconclusive/fluid domestic or systemic pressures. Finally, one has to consider leaders' Interactions with Other Levels: individuals can shape the dynamics of a security dilemma; such greats as FDR, Churchill, and Gandhi set examples of this vital facet of history, and international

[38] Jervis, Robert, *War and Misperception*, Journal of Interdisciplinary History, Vol. 18, No. 4, (Spring 1988,) pp. 675-700, http://public.gettysburg.edu/~dborock/courses/Fall/p303/jervis%20war%20and%20misperception.pdf

relations. [39]

Individualism's Relevance for Cyber Security

Who becomes a cyber threat? An adventurer? A terrorist? An ideologue? A disgruntled current or former employee? Rival businesses/organizations? Terrorist organizations? A covert branch of a government seeking to gain information advantage, or the ability to defeat an enemy by paralyzing his internet and its dependencies? Add to all of this the fact that an individual can be far more emboldened and empowered (i.e., affective) by acting through cyberspace, and 'rationality' takes an entirely different and even more expansive meaning in Cyberspace. Indeed, an individual's 'power' can be enhanced by acting through cyberspace, endowing that individual with more 'leadership' capacity than might otherwise be the case in the physical world.

Vitally, it is individuals who comprise the building blocks of Cyber Security, of power in cyberspace. It is individuals who access, use, read, write, hack, defend, gather and exploit information in cyberspace. Individuals thus comprise the key components of power in cyberspace, and its greatest liabilities. Even more importantly, given the greater significance and sheer impact that an individual can have in the Cyber Security realm, the notion of an individual's 'cognitive' abilities, reasoning, intelligence, skills, and motivations, and chosen actions, all become vastly more significant, especially when a cyberwarfare-capable individual joins forces with others of like mind and purpose, arguably most of all, in an organization dedicated and resourced to carry out cyberspace-based operations. This level of analysis also thus has great potential explanatory power for CSBP theory-building.

---

[39] Byman, Daniel L., and Pollack, Kenneth M., *Let Us Now Praise Great Men: Bringing the Statesman Back In*, International Security, Vol. 25, No. 4, (Spring 2001), pp. 107-146, http://belfercenter.ksg.harvard.edu/files/bymanetalvol25no4.pdf

2.3.5 IR Level 4: 'All-Level' Theories

These 'All-Level' Theories encompass and integrate all levels of IR Theory discussed thus far. However, they are only applicable in the specific, limited circumstances of confrontation and conflict. The Types of interaction that are involved here are Coercion, Deterrence, and Compellence. [40]

Coercion – Description

'Coercion' means convincing an opponent to do something that the opponent might not otherwise want to do. It involves the use of force, threatened or actual with the goal of affecting an opponent's cost-benefit calculations. There is will involved, and not just relative capabilities.[41]

Deterrence – Description

'Deterrence' means preventing an opponent from taking actions against one's own interests, by making the costs of refusal outweigh the benefits to that opponent. It also involves the threat or use of armed aggression, escalation, etc.[42]

Compellence – Description

'Compellence' means convincing an opponent to undo actions that have already been taken by that opponent. This is achieved by the threat and/or use of armed aggression, escalation, etc. Importantly, compellence is much more difficult to achieve than deterrence, because it is

[40] Freedman, Lawrence and Raghavan, Srinath, "Coercion," Section 15, pg. 216-227; from, Williams, Paul D. (Ed.), *Security Studies – An Introduction*, London and New York: Routledge, 2008.
[41] Freedman, Lawrence and Raghavan, Srinath, "Coercion," Section 15, pg. 216-227; from, Williams, Paul D. (Ed.), *Security Studies – An Introduction*, London and New York: Routledge, 2008.
[42] Freedman, Lawrence and Raghavan, Srinath, "Coercion," Section 15, pg. 217-219; from, Williams, Paul D. (Ed.), *Security Studies – An Introduction*, London and New York: Routledge, 2008.

psychologically much harder to let go of something than to obtain it. Note: this is Prospect Theory in action (see above).[43]

The Four Requirements ("4 C's") of Successful Deterrence & Compellence

Four requirements or conditions must be met, for either deterrence or compellence to succeed. These four requirements or "Four C's" as they are colloquially known, are Capability, Credibility, Communication, and Calculation, [44] and are described in greater detail as follows:

1) Capability: the affecting party must have the capability to inflict (usually military) costs on an opponent.

2) Credibility: the opponent must take the affecting party and its capabilities seriously, if it's for something of value to the latter.

3) Communication: the affecting party must be clear in its communications regarding its goals, and what it will do if this doesn't happen. The affecting party must also ensure that its opponent verifies that the latter received and understood the message.

4) Calculation: the opponent must be making 'rational' cost-benefit calculations, for coercion to work. [45]

All-Level Theories' Relevance for Cyber Security

Arguably, a factor missing from the "4 C's" list is Attribution. In the international (and physical) realm, actors in warfare are generally identifiable, and can be held to account for their actions; however, this is never the case in cyberspace.

---

[43] Freedman, Lawrence and Raghavan, Srinath, "Coercion," Section 15, pg. 217-219; from, Williams, Paul D. (Ed.), *Security Studies – An Introduction*, London and New York: Routledge, 2008.
[44] Freedman, Lawrence and Raghavan, Srinath, "Coercion," Section 15, pg. 216-227; from, Williams, Paul D. (Ed.), *Security Studies – An Introduction*, London and New York: Routledge, 2008.
[45] Freedman, Lawrence and Raghavan, Srinath, "Coercion," Section 15, pg. 216-227; from, Williams, Paul D. (Ed.), *Security Studies – An Introduction*, London and New York: Routledge, 2008.

The All-Level Theories arose during the Cold War, in which the US and Soviet Union were both readily identifiable and targetable in the nuclear war threat. There were only really the two superpowers to contend with at the global, superpower level, and thus, for each their own reasons, these two nation-states kept the nuclear peace (if only barely) throughout that 70-year confrontation.

However, the relative simplicity and clarity of the major actors in the Cold War scenario, is absolutely not the case in cyberspace security. Visibility and identification of those committing probes, infiltrations, attacks, thefts, thwarted attempts, and successful destruction is virtually nonexistent in cyberspace, even by comparison with, say, a bank robbery, let alone a commando-raid on the Pentagon. And while the threat of being caught and prosecuted is doubtlessly a factor in keeping cyberspace from descending into total chaos, the number and severity of cyber attacks is ongoing and increasing in both sheer numbers and severity over time.[46] Deterrence is thus a minor factor in cybersecurity at best, and at worst, utterly effective at any level, certainly not at the international level, as we have seen from China's years-ongoing and ever-growing ravaging of the US' military, intelligence, and industrial base. As a result, these all-level theories are effectively irrelevant to Cyber Security at this juncture.

2.3.6 Two New Cyber-Security-Specific Extensions to IR All-Levels Theory

While the traditional all-level theories of deterrence, compellence and coercion have little bearing on Cyber Security, the All-Level Theories 'space' itself provides considerable ground for Cyber Security-specific IR theory extension, or additions. Indeed, given the instant-global-

[46] Herridge, Catherine, *NSA chief: cyber-attacks skyrocket, account for 'largest transfer of wealth' ever*, FoxNews.com, July 9, 2012, *http://www.foxnews.com/politics/2012/07/09/nsa-chief-cyber-attacks-skyrocket-account-for-largest-transfer-wealth-in/?test=latestnews#ixzz20BitOaGs*

access, borderless nature of cyberspace for all users of any scale, anywhere in the world, this all-level framework is arguably the best workspace of all for understanding and framing cyberspace and security, and with it, Cyber Security.

To that end, this section contains two proposed extensions to the 'standard' All-Levels Theories. These extensions would enable the existing IR Theory models to more accurately reflect the characteristics and nature of interaction in cyberspace from the security perspective. As a result, these extensions should better enable the existing pertinent IR Theory components to be integrated together better, increasing the collective theory model's analytical and predictive power.

All-Levels Theory Extension #1: Information and Money - The 'Atomic Model' of Cyberspace

There are arguably two essential 'atomic-level' components differentiating cyberspace entities: information and money. The more of either component an entity has, the more powerful it becomes. In addition, the more of either component an entity has the more of a target it becomes, for attack, theft, disruption, and outright destruction. And, the nature of the information contained in and used by an entity also determines not only its functionality and power, but also the types of adversaries it might attract. This means that an individual who uses a smartphone for online banking can become the target for cyberattack. And, given that this individual has money and a personal identity (information), both components become valuable targets for, say, cybercriminals. This is even more the case for financial institutions; the bigger, the more powerful they are, but also, the bigger the target they become. Similarly, the information

contained in the US DOD's computer systems makes it a target for a wide variety of adversaries, from individual extremists through the Chinese PLA.[47]

Another example of this principle are national infrastructure networks such as electrical power grids. While they do not generally contain financial information directly, it is the strategically vital electrical system it monitors and controls that makes it a target for political and military adversaries, such as Al Qaeda and the Chinese PLA. Indeed, the Director of the NSA recently announced that China could shut down the United States by attacking its electrical grids.[48] As a result, these two 'atomic-level' components, and the 'amounts' of each that an entity has, implies how much of each type of defenses or other Cyber Security Best Practices to draw upon, which levels of IR Theory to look at, and how much of each to use to determine the best security methods to use. 'How big you are' determines what threats you need to be cognizant of, and how much you need to do to defend yourself and/or further your own interests in cyberspace.

All-Levels Theory Extension #2: There are no Fixed National Borders in Cyberspace

Unlike in the physical domain, there are no fixed borders in cyberspace. At the very least, national borders are vastly more tenuous in cyberspace than they are in any other medium. Entities of all sizes, types and locations can see and interact with, and thus affect, any other entity, anywhere in the world, at any time. This has several consequences:

1) The international system and nation-states model is made more 'diffuse'.

[47] Staff, *FBI Warns Tech Companies of State-Sponsored Chinese Hackers*, Newsmax.com, 10-16-14, http://www.newsmax.com/SciTech/FBI-China-hackers-cybersecurity/2014/10/16/id/601162/

[48] Herridge, Catherine, and the Associated Press, *NSA Director: China can damage US power grid*, Fox News, 11-20-14, http://www.foxnews.com/politics/2014/11/20/nsa-director-china-can-damage-us-power-grid/

2) Nation-states' ability to exercise their sovereignty over their territory and to control entities' access to and effects upon and within their territory is much weaker than in any other medium.

3) The relative power of individuals, groups and organizations is much greater in cyberspace.

4) The vulnerability of all entities within a nation-state, and thus, of the nation-state itself, is increased greatly in cyberspace.

5) Nonetheless, the power of a nation-state (military and/or economic) can determine to a great extent the ability of its governmental organizations to develop and utilize cybersecurity measures, both defensive and offensive. This, however, also depends on the will of that nation-state to make such decisions and efforts, alongside the technological capability to enable its cybersecurity choices.

6) As with the IR Theory domain, 'size matters', be it a nation-state, a corporation, a government agency, or an individual… though not solely.

7) 'Size' in cyberspace depends on cyberwarfare competence as much as, if not more than, any other factor. All the computer processing power in the world will avail nothing unless it is harnessed and directed by one or more highly-capable and suitably-motivated 'hackers'.

Section 2.4 Summary of IR Theories and their Applicability to Cyber Security

In this section, all the levels of IR Theory, and all their respective theories, are compiled and considered for their applicability and ramifications to Cyber Security Best Practices. First, all four levels and theories of IR Theory are listed and summarized in Table 13, below:

Table 13: IR Theories and their Key Traits

Level	Theory	Key Traits
International	Classical Realism	1) States are the main actors in the system. 2) All states are rational, unitary actors. 3) All states pursue their own interests (power). 4) Conflicts of "interests" are inevitable. 5) International system is anarchic.
		Offense-Defense Theory (subset): 1) When offense has the advantage, conquests are easy, and there is little security or stability. 2) When defense has the advantage, and can be readily distinguished from the offensive, security is more plentiful.
	Neorealism	1) States are the main actors in the system. 2) All states are rational, unitary actors. 3) Interests are defined by security, not power. 4) Power is the means to security, not the end goal itself. 5) International system is anarchic.
		The Security Dilemma (central tent of Neorealism): 1) One state's increased security decreases that of others. 2) One state's increased security impels other states to compete to 'keep pace,' e.g., via arms races. 3) Implicit pressure not to lead or lag.
		Types of Alliances Under Neorealism: 1) Balancing: states joining together to match a common threat (e.g. NATO;) - defensive in nature; more stable system. 2) Bandwagoning: lesser states joining with a greater power; - prevent being attacked by the greater power; - benefit from the 'spoils' of the latter's success.
	Neoliberal Institutionalism	1) States are the main actors in the system. 2) All states are rational, unitary actors. 3) International Cooperation (i.e. Structuralism) is possible, even in an anarchic system. 4) International institutions and regimes enable international cooperation.
		International Cooperation implies that: - Anarchy doesn't always mean self-reliance & competition; - Gains are measured in absolute, not relative terms; - Security dilemma is not inevitable
	Constructivism	1) States are the main units of analysis. 2) International Politics come from social constructs: - "objective" relationships do not exist. 3) National Identities drive national interests: - e.g., social identities, norms, elite beliefs.

Table 13 cont'd

Level	Theory	Key Traits
	Cooperation Under the Security Dilemma - Game Theory	1) "Stag Hunt" analogy: - Cooperation would help all, but self-interest leads to defections; causes strife, added costs. 2) "Security Dilemma" analogy: - Increasing one's own security decreases others', who then seek to raise theirs. => leads to: arms races, miscalculations, wars. 3) Prisoners' Dilemma" analogy: pre-crisis planned cooperation is key.
State-Level	Democratic Peace Theory (DPT)	1) Democracies tend not to go to war with other democracies. 2) Best form of government to have, for overall international peace. 3) More prone to wage wars vs. non-democracies. 4) Tend to wage more intense & destructive wars than non-democracies. 5) Democratizing states may be the most war-prone of all.
		Two Primary Mechanisms: 1) Institutional Constraints; 2) Peaceful norms and values.
	Strategic Culture	- Different cultures, states, can also have different warfighting cultures. - Different states make different strategic choices.
	Revisionism	Two types of States: 1) Status-Quo States: - satisfied with existing international system); 2) Revisionist States: - unhappy w. existing international system; - want, and strive, to change it.
Sub-State-Level	Bureaucratic Politics	1) There is no such thing as a state. 2) Multiple bureaucracies control the state's decision-making process. 3) Policy is formed by bargaining processes going on within, and between, the different bureaucracies. 4) Policymaking is also driven by the nature of each bureaucracy. 5) Bureaucracies pursue their own interests (i.e., survival and growth/power.) 6) Hierarchical: subordinates follow their leader. 7) Inherent characteristic of democratic politics. 8) Lots of people-following to do.

Table 13 cont'd

Level	Theory	Key Traits
		5 Methods for organizations to manage information problems: a) Narrow the range of available options. b) "Satisfice" (choose 1st solution that is satisfactory and sufficient.) c) Adopt "Standard Operating Procedures." d) Develop missions and cultures. e) Resistance to change.
	Individual Politics	Human brain can't process all information: - takes simplifying shortcuts; - ignores trade-offs; - makes inappropriate analogies. - makes premature closure.
	Individual Biases	Two Types of Biases: 1) Cognitive Biases: - Prospect Theory; - Framing Effects; - Coordination and Intent; - Attribution Errors; - Clear Motives. 2) Emotional Biases: - Wishful Thinking; - Bolstering; - Selective Memory; - Scenario Fulfillment; Results: - Statesmen tend to overestimate their own reasonableness, and others' hostile intentions.
	Individual Leadership	The Power of Individual Leaders: 1) Foundational Hypotheses; 2) Personality Traits; 3) When Individuals Matter; 4) Interactions with Other Levels
All-Levels	Coercion	1) Convince an opponent to do something that the opponent might not want to do. 2) Use of force, threatened or actual. 3) Affect opponent's cost-benefit calculations. 4) Will involved, not capabilities alone.
	Deterrence	1) Prevent an opponent from taking actions against your interests, by making the costs of refusal outweigh the benefits. 2) Threaten/use armed aggression, escalation, etc.
	Compellence	1) Convince an opponent to undo actions already taken by that opponent. 2) Threaten, use armed aggression, escalation, etc. 3) Much more difficult to achieve than deterrence.

Table 13 cont'd

Level	Theory	Key Traits
	The Four Requirements ("Four C's") of Successful Deterrence and Compellence + Attribution ("C4A"?)	1) Capability: to inflict (usually military) costs on an opponent. 2) Credibility: opponent must take you and your capabilities seriously, if it's for something you value. 3) Communication: MUST be clear in your communications re. what you want, & what you'll do if you don't get it. - Must also verify receipt & comprehension. 4) Calculation: opponent must be making 'rational' cost-benefit calculations, for coercion to work. Note: additional Requirement in Cyberspace: 5) Attribution: ability to identify, locate and target an opponent; - Impossible to achieve in cyberspace, as in the physical world. * Note: not a standard component of the" Four C's", but implicit in the 4 Requirements

Second, all four levels and theories of IR Theory, and their respective relevancies to Cyber Security are summarized in Table 14, below:

Table 14: IR Theories and their Applicability to Cyber Security

Level	Theory	Relevance for Cyber Security
International	Classical Realism	Extreme; 1) National goals and ambitions are being acted upon with varying levels of effort, by various nation-states, on an individual-nation-basis. 2) Cyberspace is Offense-Dominant
	Neorealism	Helpful; More cybersecurity cooperation needed.
	Neoliberal Institutionalism	Very little; Would largely just 'get in the way.'
	Constructivism	Helpful; who are the aggressive states?
State-Level	Democratic Peace Theory (DPT)	Very helpful at generally distinguishing between friendly and unfriendly states.
	Strategic Culture	Somewhat helpful.
	Revisionism	Very Helpful at highlighting threat-states, and their respective threat-levels.
Sub-State-Level	Bureaucratic Politics	Extreme; Bureaucracies may well be the single most powerful entities in cyberspace.

Table 14 cont'd

	Organizational Politics	Extreme; provides guidelines for how to determine how much or well an organization can cope with or affect events in cyberspace.
	Individual Politics	Extreme; Individuals comprise the key components of power in cyberspace, or its greatest liabilities.
All-Levels	Coercion	~None
	Deterrence	~Little, if at all.
	Compellence	~None
Proposed Additions to All-Level Theories	Information & Money – the Atomic Model of Cyberspace	Extreme; Emphasizes those fundamental elements that are of critical importance in all aspects of cyberspace.
	There are No Borders in Cyberspace	Extreme; All Cyber Security entities must be aware of this, and act accordingly.

Some ramifications of these theories are considered in the following sections.

Section 2.5 Six IR Theoretical Conclusions and Directions for Cyber Security Best Practices

The following six items are observations and distillations of the prior IR Theory analyses, to guide Cyber Security Theory process and framing the CSBPs later on in this work:

1) Cyberspace is ultimately just an extension of physical reality; thus, Realism is the best, most timelessly applicable perspective to use to understand the nature of the world, and thus, of cyberspace itself.

2) The State has poor control over its cyberspace 'borders'; as a result, the State-Level and especially the Sub-State-Level theories have the greatest bearing on Cyber Security in terms of detailed implementation. Organizations, bureaucracies, and (sufficiently-talented and experienced) individuals and groups are the largest, directly-affective 'entities' in cyberspace.

3) However, the power (military/cyberwarfare, and financial) of states can be harnessed to affect the ultimate purpose, capability and results of some or all of these individuals and/or organizations.

4) How much Cyber Security is needed by an entity, from individual to state, depends on its 'size', in terms of the value of the finances and/or information it possesses. This is tempered by the fact that all entities of all sizes are exposed to all other risks and threats in the world via cyberspace. Nation-states can and thus must harness their internal cyberspace-capable entities to the interests of the state by helping the state and its constituents to cope with these threats, to achieve their own goals, and ultimately, to further the goals of the state itself.

5) In cyberspace, all threats are proximal, though they can be informed by proximity.

IR Theory holds that 'threats are proximal,' meaning that the threat that one state poses to another depends in large part on their geographical proximity. In cyberspace, however, this is not the case, since distance is essentially irrelevant, being dependent only on whether or not the attacking and target entities can be connected via the internet. 'Distance' in cyberspace is only as great as the number of internet 'hops' separating threat from target, and thus, physical-world distance matters little. Nor do national borders do much to hinder or keep intruders (that could be located anywhere worldwide) out of local, domestic networks and systems in cyberspace. As a result, this concept is not applicable to cybersecurity; or, in other words, all threats are proximal. Rather, threats are entirely proportional to their cyberwarfare capability and their intentions and goals.

6) Given the relative ease with which cybersecurity breaches are achieved by capable attackers, almost regardless of the scope and extent of the defender's defenses, and combined with the great and worsening consequences of such breaches, it is painfully obvious that cyberspace is an offense-dominant system. This has two consequences. The first consequence is that defenders must expect be prepared to suffer and survive ever-worsening information-system breaches. This is very much both standard cybersecurity policy and the currently state of affairs, and is reflected

in the current CSBP-set. Secondly, however, based on the offense-dominant nature of cyberspace, ongoing attacking threats can only be halted or eliminated via the use of offensive cybersecurity countermeasures. The ongoing national and global trend of worsening (more frequent and more severe) cyberattacks and breaches, can best be explained by, and indeed, blamed on, the absence of an offensive countervailing strategy in current CSBPs, and in current US law.

CHAPTER 3: INTEGRATION AND ANALYSIS OF IR-THEORY AND EXPERIENCE-DRIVEN CYBER SECURITY BEST PRACTICES

This chapter provides two major steps to complete the Cyber Security Theory. The first step integrates the two sets of information (CSBPs and Cyber-Security-focused IR Theories) produced in CHAPTER 2: REVIEW AND ANALYSIS OF CSBP LITERATURE & IR (above) into one table and set of insights for further analysis. The second step draws upon and encapsulates these tabulated and written insights into a testable theoretical framework, including a set of equations, as a means of using the theory to determine which practices to use, when, and not least of all, why they should be used. This, then, is the Cyber Security Theory: both a paradigm for understanding the nature and extent of security needed in cyberspace, and a means with which to determine which practical, real-world CSBPs any entity should use, as determined by the nature of that entity.

Section 3.1 Table Merge of IR Theories and CSBPs

The first step in this process of merging the two fields of thought (both figuratively and literally) is to integrate the three primary CSBP tables (Table 8: Individual-Scale CSBPs; Table 9: Organizational-Scale CSBPs; and Table 10: National-Scale CSBPs) into Table 14: IR Theories and their Applicability to Cyber Security. The CSBP tables are inserted as new columns to the right of (and one table-row below) their respective Levels of IR Analysis and level-specific theories. (Note that there are no Global-Scale CSBP entries to be made here, since Table 11: Global-Scale CSBPs (none!) has nothing to contribute to this process.) The result of this integration process is contained in Table 15: IR Theories' Applicability to Cyber Security, & Corresponding CSBPs, below:

Table 15: IR Theories' Applicability to Cyber Security, & Corresponding CSBPs

Level	Theory	Relevance for Cyber Security	CSBP Item#	Corresponding CSBPs
International	Classical Realism	Extreme; 1) National goals and ambitions are being acted upon with varying levels of effort, by various nation-states, on an individual-nation-basis. 2) Cyberspace is Offense-Dominant		
	Neorealism	Helpful; More cybersecurity cooperation needed.		
	Neoliberal Institutionalism	Very little; Would largely just 'get in the way.'		
	Constructivism	Helpful; who are the aggressive states?		
State-Level	Democratic Peace Theory (DPT)	Very helpful at generally distinguishing between friendly and unfriendly states.		
	Strategic Culture	Somewhat helpful.		
	Revisionism	Very Helpful at highlighting threat-states, and their respective threat-levels.		
			6	Application Software Security
			10	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
Sub-State-Level	Bureaucratic Politics	Extreme; Bureaucracies may well be the single most powerful entities in cyberspace.		
	Organizational Politics	Extreme; provides guidelines for how to determine how much or well an organization can cope with or affect events in cyberspace.		
			1	Inventory of Authorized and Unauthorized Devices
			2	Inventory of Authorized and Unauthorized Software
			3	Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers
			4	Continuous Vulnerability Assessment and Remediation
			5	Malware Defenses
			6	Application Software Security
			7	Wireless Device Control
			8	Data Recovery Capability
			9	Security Skills Assessment and Appropriate Training to Fill Gaps
			10	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
			11	Limitations and Control of Network Ports, Protocols, and Services
			12	Controlled Use of Administrative Privileges
			13	Boundary Defense
			14	Maintenance, Monitoring, and Analysis of Security Audit Logs
			15	Controlled Access Based on the Need to Know
			16	Account Monitoring and Control
			17	Data Loss Prevention (DLP)
			18	Incident Response and Management
			19	Secure Network Engineering

Table 15 cont'd

Level	Theory	Relevance for Cyber Security	CSBP Item#	Corresponding CSBPs

			20	Penetration Tests and Red Team Exercises
			21	Information System Security Systems Design and Planning
			22	Top-Down Implementation is Essential
			23	Physical Facilities Security
			24	"Combined-Arms Warfare": Most-Effective Implementations Combine all four Major Cyber Security Frameworks
			25	Centralized InfoSec Design, Planning & Implementation
			26	InfoSec Department Separated from IT Department
			27	InfoSec Department Reports Directly to CISO
			28	Compliance with All Required or Applicable Regulations
			29	InfoSec Implementation must be Consistent w. the Organization's Culture
			30	Maximize Use of Automation in InfoSec Implementations
Sub-State-Level (continued)	Individual Politics	Extreme; Individuals comprise the key components of power in cyberspace, or its greatest liabilities.		
			1	Inventory of Authorized and Unauthorized Devices
			2	Inventory of Authorized and Unauthorized Software
			3	Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers
			4	Continuous Vulnerability Assessment and Remediation
			5	Malware Defenses
			6	Application Software Security
			7	Wireless Device Control
			8	Data Recovery Capability
			9	Security Skills Assessment and Appropriate Training to Fill Gaps
			15	Controlled Access Based on the Need to Know
			17	Data Loss Prevention (DLP)
All-Levels	Coercion	~None		
	Deterrence	~Little, if at all.		
	Compellence	~None		
Proposed Extensions of All-Level Theories	Information & Money – the Atomic Model of Cyberspace	Extreme; Emphasizes those fundamental elements that are of critical importance in all aspects of cyberspace.		
	There are No Borders in Cyberspace	Extreme; All Cyber Security entities must be aware of this, and act accordingly.		

Now the correlations between the IR Levels and Theories and their corresponding CSBPs can be more easily.

However, there is still 'too much information' in Table 15: not all of the listed IR theories actually provide useful insights; those that are not useful can be removed from further consideration, for the sake of greater compactness, clarity, and efficiency. The next step, then, is to determine which IR theories to keep, and which to 'throw out.' The 'threshold of utility' that will be used here is that any IR theory categorized as 'helpful' or less ('little' or 'none at all') must be removed from the table before any further analysis is completed.

Culling the minimally-useful theories from Table 15 yields Table 16: Relevant IR Theories & Corresponding CSBPs, below:

Table 16: Relevant IR Theories & Corresponding CSBPs

Level	Theory	Relevance for Cyber Security	CSBP Item#	Corresponding CSBPs
International	Classical Realism	Extreme; 1) National goals and ambitions are being acted upon with varying levels of effort, by various nation-states, on an individual-nation-basis. 2) Cyberspace is Offense-Dominant		
State-Level	Democratic Peace Theory (DPT)	Very helpful at generally distinguishing between friendly and unfriendly states.		
	Strategic Culture	Somewhat helpful.		
	Revisionism	Very Helpful at highlighting threat-states, and their respective threat-levels.		
			6	Application Software Security
			10	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
Sub-State-Level	Bureaucratic Politics	Extreme; Bureaucracies may well be the single most powerful entities in cyberspace.		
	Organizational Politics	Extreme; provides guidelines for how to determine how much or well an organization can cope with or affect events in cyberspace.		
	Organizational Politics	Extreme; provides guidelines for how to determine how much or well an organization can cope with or affect events in cyberspace.		
			1	Inventory of Authorized and Unauthorized Devices
			2	Inventory of Authorized and Unauthorized Software

Table 16 cont'd

Level	Theory	Relevance for Cyber Security	CSBP Item#	Corresponding CSBPs
			3	Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers
			4	Continuous Vulnerability Assessment and Remediation
			5	Malware Defenses
			6	Application Software Security
			8	Data Recovery Capability
			9	Security Skills Assessment and Appropriate Training to Fill Gaps
			10	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
			11	Limitations and Control of Network Ports, Protocols, and Services
			12	Controlled Use of Administrative Privileges
			13	Boundary Defense
			14	Maintenance, Monitoring, and Analysis of Security Audit Logs
			15	Controlled Access Based on the Need to Know
			16	Account Monitoring and Control
			17	Data Loss Prevention (DLP)
			18	Incident Response and Management
			19	Secure Network Engineering
			20	Penetration Tests and Red Team Exercises
			21	Information System Security Systems Design and Planning
			22	Top-Down Implementation is Essential
			23	Physical Facilities Security
			24	"Combined-Arms Warfare": Most-Effective Implementations Combine all four Major Cyber Security Frameworks
			25	Centralized InfoSec Design, Planning & Implementation
			26	InfoSec Department Separated from IT Department
			27	InfoSec Department Reports Directly to CISO
			28	Compliance with All Required or Applicable Regulations
			29	InfoSec Implementation must be Consistent w. the Organization's Culture
			30	Maximize Use of Automation in InfoSec Implementations
Sub-State-Level (continued)	Individual Politics	Extreme; Individuals comprise the key components of power in cyberspace, or its greatest liabilities.		
			1	Inventory of Authorized and Unauthorized Devices
			2	Inventory of Authorized and Unauthorized Software
			3	Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers

Table 16 cont'd

Level	Theory	Relevance for Cyber Security	CSBP Item#	Corresponding CSBPs
			4	Continuous Vulnerability Assessment and Remediation
			5	Malware Defenses
			6	Application Software Security
			7	Wireless Device Control
			8	Data Recovery Capability
			9	Security Skills Assessment and Appropriate Training to Fill Gaps
			15	Controlled Access Based on the Need to Know
			17	Data Loss Prevention (DLP)
Proposed Extensions of All-Level Theories	Information & Money – the Atomic Model of Cyberspace	Extreme; Emphasizes those fundamental elements that are of critical importance in all aspects of cyberspace.		
	There are No Borders in Cyberspace	Extreme; All Cyber Security entities must be aware of this, and act accordingly.		

Section 3.2 Theory of Cyber Security Best Practices

To paraphrase the ancient warfare-strategist Sun Tzu, "If you know your enemy and know yourself, you need not fear the result of a hundred outcomes."[49] This maxim will be used as the backbone upon which to place the set of observations and resultant directives (inputs and outputs) specific to cyberspace security. The results of the tables and observations will be integrated here. 'Inputs' into the theoretical framework are to be each SSE, alongside the level and nature of any cyber-security-seeking entity, while the 'outputs' are to be the corresponding CSBPs to provide the best practices for that level of activity. In addition, gaps in the CSBPs by SSE, and any other issues found, will also be listed here. These selections and other conclusions will also draw upon the contents of the sections 2.3.6 Two New Cyber-Security-Specific Extensions to IR All-Levels Theory, and Section 2.5 Six IR Theoretical Conclusions and

[49] Giles, Lionel, *Sun Tzu on the Art of War*, Luzan & Co., 1910, pg. 6, http://www.artofwarsuntzu.com/Art%20of%20War%20PDF.pdf

Directions for Cyber Security Best Practices, (above.) This will form the basis of this Cyber Security Theory (CST).

3.2.1 "Know Yourself"

First, any 'entity' must determine its scope, be it an individual, organization, or nation-state. Second, the entity must identify its nature (private, financial, civil, national security, etc.) and its 'order of significance' (how much and what kind of money and/or information it has, has access to, or processes, and how valuable these are.)Third, in accordance with that 'order of significance,' the entity must implement all CSBPs that apply to all levels of its nature. However, any entity's level of cybersecurity must always, always, start with individual-level cybersecurity practices, all of which must be implemented for all individuals participating in the organization, whether the entity is an individual or millions of individuals. Furthermore, if the entity is of sufficient cyber 'power' (wealth or value of possessed/accessed information,) the level of cybersecurity implemented must merge up into the realm of the organization-level, even if the entity is 'just one' individual. For instance, senior members of any organization (military, government, corporate executives, etc.) should have all of their information technology secured to the highest standards of and secured by their organization's cyber security organizations, even at their personal residences.

Individual-Level CSBPs

Every individual who operates in cyberspace is not only an actor in cyberspace, but is also a potential target in cyberspace, as well. Next, each individual must understand that he or she is potentially visible to any and all hostile actors in cyberspace, anywhere in the world, at any given moment. Every activity an individual undertakes in cyberspace, whether shopping,

searching for and viewing websites, banking, or emails, entails additional risks to the individual's cybersecurity. Furthermore, an individual's role in an organization further amplifies the significance of that individual's cybersecurity practices, and inherent vulnerabilities. Finally, any individual has the potential to become an actor of global significance, whether deliberately so (for instance, Edward Snowden[50], Bradley Manning[51], or Kevin Mitnick[52]) or inadvertently, say, by a Lockheed Martin F-35 systems engineer innocently clicking on a hyperlink in an email that appears to be an authentic email from a co-worker, but is actually a Chinese cyberwarfare-unit-issued phishing scam, which then downloads malware onto his computer, exposing the entire corporation's computer systems, and all its classified information, to the Chinese PLA.[53]

The result of all this is a table containing all Individual-level CSBPs, by listing those CSBPs applicable to the Sub-State Level from Table 16: Relevant IR Theories & Corresponding CSBPs (above) and listed here for brevity and conciseness. Every individual, regardless of role or value, must implement all or as many of these Individual-level CSBPs as possible. These are tabulated in Table 17: CSBPs for Individuals, below:

Table 17: CSBPs for Individuals

Inventory of Authorized and Unauthorized Devices
Inventory of Authorized and Unauthorized Software
Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers
Continuous Vulnerability Assessment and Remediation
Malware Defenses
Application Software Security
Wireless Device Control
Data Recovery Capability
Security Skills Assessment and Appropriate Training to Fill Gaps
Controlled Access Based on the Need to Know

[50] Staff, *Edward Snowden: Whistleblower or double-agent?,* FoxNews.com, 06-14-13, http://www.foxnews.com/politics/2013/06/14/edward-snowden-whistleblower-or-double-agent/
[51] Staff, *Manning not guilty of aiding the enemy in Wikileaks case, stall may face 128 years in prison,* FoxNews.com, 07-30-13, http://www.foxnews.com/us/2013/07/30/bradley-manning-not-guilty-aiding-enemy-in-wikileaks-case-convicted-lesser/
[52] Greenberg, Andy, *Kevin Mitnick, Once the World's Most Wanted Hacker, is Now Selling Zero-Day Exploits*, Wired.com, 09-24-14, http://www.wired.com/2014/09/kevin-mitnick-selling-zero-day-exploits/
[53] Gertz, Bill, *Stolen F-35 Secrets Now Showing Up in China's Stealth Fighter*, Washington Free Beacon, 03-13-14, http://freebeacon.com/national-security/stolen-f-35-secrets-now-showing-up-in-chinas-stealth-fighter/

Data Loss Prevention (DLP)

Organizational-Level CSBPs

This same approach applies to organizations of any and all sizes, natures, resources, and purposes. Every organization, regardless of role or value, needs to implement all of both the Individual-level and Organization-level CSBPs from Table 16: Relevant IR Theories & Corresponding CSBPs (above.) This is to ensure that all 'base' CSBPs are implemented by all individuals, as well as those CSBPs needed for this level. However, since the Organization-level CSBPs encompass all 30 CSBPs, those CSBPs that are unique to the organization-level are listed at the top of the Table, followed by the Individual-level CSBPs at the bottom of the Table, for clarity's sake. The results are tabulated in Table 18: CSBPs for Organizations (below):

Table 18: CSBPs for Organizations

Limitations and Control of Network Ports, Protocols, and Services
Controlled Use of Administrative Privileges
Boundary Defense
Maintenance, Monitoring, and Analysis of Security Audit Logs
Account Monitoring and Control
Incident Response and Management
Secure Network Engineering
Penetration Tests and Red Team Exercises
Information System Security Systems Design and Planning
Top-Down Implementation is Essential
Physical Facilities Security
"Combined-Arms Warfare": Most-Effective Implementations Combine all four Major Cyber Security Frameworks
Centralized InfoSec Design, Planning & Implementation
InfoSec Department Separated from IT Department
InfoSec Department Reports Directly to CISO
Compliance with All Required or Applicable Regulations
InfoSec Implementation must be Consistent w. the Organization's Culture
Maximize Use of Automation in InfoSec Implementations
Inventory of Authorized and Unauthorized Devices
Inventory of Authorized and Unauthorized Software
Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers
Continuous Vulnerability Assessment and Remediation
Malware Defenses
Application Software Security
Wireless Device Control
Data Recovery Capability
Security Skills Assessment and Appropriate Training to Fill Gaps
Controlled Access Based on the Need to Know
Data Loss Prevention (DLP)

National-Level CSBPs

As with the Organization-level CSBPs of Table 18: CSBPs for Organizations (above) National-level CSBPs require all previous CSBPs from all previous lower levels, in addition to those national-level-specific CSBPs from Table 16. Also as with (above,) the National-level CSBPs are listed at the top of the Table, followed by the Organizational-level, then Individual-level CSBPs. The result is Table 19: CSBPs for Nations, below:

Table 19: CSBPs for Nations

Application Software Security
Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
Limitations and Control of Network Ports, Protocols, and Services
Controlled Use of Administrative Privileges
Boundary Defense
Maintenance, Monitoring, and Analysis of Security Audit Logs
Account Monitoring and Control
Incident Response and Management
Secure Network Engineering
Penetration Tests and Red Team Exercises
Information System Security Systems Design and Planning
Top-Down Implementation is Essential
Physical Facilities Security
“Combined-Arms Warfare”: Most-Effective Implementations Combine all four Major Cyber Security Frameworks
Centralized InfoSec Design, Planning & Implementation
InfoSec Department Separated from IT Department
InfoSec Department Reports Directly to CISO
Compliance with All Required or Applicable Regulations
InfoSec Implementation must be Consistent w. the Organization’s Culture
Maximize Use of Automation in InfoSec Implementations
Inventory of Authorized and Unauthorized Devices
Inventory of Authorized and Unauthorized Software
Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers
Continuous Vulnerability Assessment and Remediation
Malware Defenses
Application Software Security
Wireless Device Control
Data Recovery Capability
Security Skills Assessment and Appropriate Training to Fill Gaps
Controlled Access Based on the Need to Know
Data Loss Prevention (DLP)

Significantly, all 30 CSBPs are now sorted out in descending order of SSE magnitude, if only roughly.

Worryingly, while Table 19 lists all CSBPs at the National level for practical/tactical implementation, only two are specific to the national level. This observation is consistent with All-Levels Theory Extension #2: There are no Fixed National Borders in Cyberspace, and implies a shortage of national-level CSBPs, and with them, a lack of protection at the national level. The consequences of this observation are dire: all sub-national entities (individuals and organizations) operating in cyberspace must understand that they are effectively 'on their own' in seeing to their cyber-defenses. The nation-state is not doing enough to protect its constituent entities from cyberthreats writ large, certainly not in the way it can provide effective defenses against such physical-world threats as aerial-bombing or terrorist attacks. As a result, it is entirely the burden and responsibility of the individual and organization, not only to know all the threats facing it, but also to take the fullest possible set of precautions it can afford in order to defend against those threats as best as it can. This also means that individuals and organizations must know and effectively defend themselves against all the threats they are likely to face in the cyberspace world. Is this really an effective strategy for the nation, much less for all the individuals and organizations operating in cyberspace now? The current and unending trend of increasing numbers and severity of cybersecurity breaches and losses[54] clearly shows that this lack of a true national cybersecurity strategy is not working.

There is another dire implication from Table 19: while the listed CSBPs should be in place to protect the nation as a whole, to the best of the author's knowledge, there are no

[54] Herridge, Catherine, *NSA chief: cyber-attacks skyrocket, account for 'largest transfer of wealth' ever*, FoxNews.com, July 9, 2012, *http://www.foxnews.com/politics/2012/07/09/nsa-chief-cyber-attacks-skyrocket-account-for-largest-transfer-wealth-in/?test=latestnews#ixzz20BitOaGs*

implementations and enforcements of either cited national-level CSBP at the nation's border gateway systems. That this is not the case, then, is an important implication of this theoretical framework.

Global-Level CSBPs

As observed elsewhere in this work, there are no international or global-level CSBPs in place to secure the US or its allies. This is entirely in following with Classical Realism in IR Theory, which states that the international system is anarchic, and as a result, each nation pursues power for its own survival and success. However, IR Theory further implies that if nation-states were to form alliances in cyberspace as they ofttimes do in the physical world, then the benefits would be two-fold: first, the challenge and burden of tracking and learning from the full array of cyber threats faced by each ally nation-state would be lessened; and second, the allied nation-states could 'pool' their resources to achieve more coherent, effective, and ultimately, more powerful cyberspace defenses. This stratagem will be explored in greater detail later on in this work.

Theoretical Framework for "Knowing Yourself"

So, how does one go about generating a theoretical framework from all these observations? First, consider a 'bottom-up' assessment of the relevant IR Theories above; always start with the individual-level, and implement the corresponding CSBPs. Second, examine how 'far up' up the IR Theory levels the entity and/or its organization goes. Third, perform an 'intelligence assessment' of the entity's area of activities, responsibilities, industry or

government sectors, and learn the threats that exist for each of those areas. And fourth and finally, the higher up the entity and its organization (and corresponding areas of activity) go in this chart, the more of the corresponding CSBPs the entity needs to implement.

3.2.2 "Know Your Enemy"

The nature of the entity in question, be it an individual, organization, or nation, determines the threats that that entity will have to prepare to contend with cyberspace. For instance, private citizens are vulnerable to cybercriminals, both domestic and foreign, such as from Russian and Eastern Europe. Organizations are also vulnerable to the same threat-sets, only more so, and at a much greater scale of loss. Organizations must also be prepared to face cyber-espionage, in addition to cybercrime. Furthermore, individuals and organizations involved in high-value activities such as national security, politics, or other areas of significant, national interest (such as banking, energy, journalism, and so on) are also at risk of Chinese, Russian, Iranian and North Korean cyberthreats, i.e., from rogue-nation-state-backed cyber-threats. As if all these threats weren't enough, other hacker organizations exist, such as Anonymous[55] or the Syrian Electronic Army[56], seeking to achieve political (and sometimes monetary) goals via cyber-hacking.

Notably, nation-states can and do commit themselves to significant power and effect in cyberspace at the international level: witness the US' NSA[57] and the Chinese PLA's Unit

---

[55] Coleman, Gabriella, *Anonymous in Context: the Politics and Power behind the Mask*, Center for International Governance Innovation (CIGI) Online, 09-23-13, http://www.cigionline.org/publications/2013/9/anonymous-context-politics-and-power-behind-mask?gclid=CP30lOOuucACFSMV7AodbQoARA

[56] Staff, *What is the Syrian Electronic Army?,* The Guardian, 2014, http://www.theguardian.com/media-network/partner-zone-infosecurity/what-is-the-syrian-electronic-army

[57] Staff, *National Security Agency/Central Security Service – Defending Our Nation, Securing Our Future*, NSA.gov, 2009, https://www.nsa.gov/

61398[58] as examples. However, even these are, ultimately, just sub-state organizations, and they are primarily involved in cyber-espionage and cyber-operations (offensive, not defensive per se) and do not, and indeed cannot, provide effective real-time cyber-defense of their own national borders.

Theoretical Framework for Knowing your Enemy

All individuals, from private citizens to corporate and national-security executives, must consider all aspects of all of their activities in terms of All-Levels Theory Extension #1: Information and Money - The 'Atomic Model' of Cyberspace, and how much their activities extend into each area, for example, financial accounts and confidential information, information/access to either of which would be of great value to thieves and hackers. All individuals (and organizational leadership) must also compare all of their cyberspace activities and items of value found from All-Levels-Theory Extension #1 (above) with All-Levels Theory Extension #2: There are no Fixed National Borders in Cyberspace, to research and understand all types and levels of cybersecurity threats that may apply to them. For instance, financial institutions need to be on guard against Russian and Eastern European as well as US domestic cybercrime attacks, while defense-sector organizations such as government agencies and defense contractors must be on guard against Russian, Iranian, and Chinese cyber-espionage threats. And, these organizations must maintain continual track of all emerging and changing threats in cyberspace.

[58] Staff, *APT1 – Exposing One of China's Cyber Espionage Units*, Mandiant.com, 02-19-13, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

3.2.3 Prepare Both Defensive and Offensive Measures in Accordance with your Cyberspace Power and Value

Need for Offense as Part of Cyber Security Best Practices

All of the cybersecurity measures outlined above are entirely defensive in nature. This is in line with all of the CSBPs found in this work, as well as with current US law.[59] However, the harsh reality of cyberspace is that it is anarchic and offense-dominant, and that individuals and organizations are both more important and yet more vulnerable in cyberspace. This means that all US actors in cyberspace must be enabled and empowered to plan and implement offensive cybersecurity countermeasures (at least, as many and as far as are legal in their areas of operation,) over and above all of the defensive CSBPs cited in this work. Offensive cybersecurity practices will be vital to the long-term survival and success of all entities operating in cyberspace, particularly those that are of higher 'value' in cyberspace. Left unstopped, persistent threats will eventually get through even the best of defenses, and do damage. It may simply be a matter of time before some cyber-threat emerges that can and will do catastrophic damage. These threats need to be stopped, or they will cause irreparable or unsustainable damage to us, perhaps to civilization itself. The only way to achieve true cyber security is to eliminate persistent, serious threats, a step that can only be achieved through offensive measures, including offensive cybersecurity measures. This, too, is a logical consequence of the application of IR Theory to the reality of cyberspace security (or the lack thereof), the fact that offensive actions dominate defensive ones in cyberspace, and that in such a system, the only way to permanently end a persistent threat in cyberspace is to either counterattack or eliminate that threat, whether

[59] Whitman, Michael E., and Mattord, Herbert J., *Management of Information Security*, Third Edition, Course Technology – Cengage Learning, 2010, pg. 427-462

temporarily or (preferably) permanently. This can be implemented responsibly and effectively via the following three changes to US policy and law nationwide:

1) Implement effective national-level border defenses in cyberspace, in which the US' national strategic "choke points"[60] of cyberspace such as border gateway routers are effectively monitored and guarded to protect all domestic internet networks and sites from external attacks. The DOD, NSA and/or DHS should be jointly tasked to provide this security measure. And, whenever a server threat or attack is detected and identified or tracked down, these border defenses can counterattack against that threat, or at least, marshal counteroffensive systems from elsewhere in the nation.

2) Licensing or 'deputizing' of individuals and organizations to conduct offensive, or more specifically, counter-offensive, cybersecurity operations. This could be patterned after permits for private citizens to own firearms, but with these permits applied to the cyberspace realm, and 'safety course' training to suit.

3) Update current US laws prohibiting use of offensive cyberspace activities by anyone, de facto, which leaves domestic cybersecurity collectively much more vulnerable than necessary, especially in the anarchic system of cyberspace. This vulnerability is only growing increasingly costly and perilous with time, a trend that is both unnecessary and can be remedied.

Need for National-Level Border Defenses in Cyberspace

Missing from the CSBPs amassed in this paper are significant protections and policies that specifically define the creation and enforcement of national borders in cyberspace. Even the

[60] Daly, John, *Naval Choke Points and Command of the Sea*, 03-02-09, world Politics Review, http://www.worldpoliticsreview.com/articles/3378/naval-choke-points-and-command-of-the-sea

national-level regulatory requirements and laws such as HIPAA[61] or Sarbanes-Oxley [62] do nothing more than require all individuals and organizations in that medical industry to take all the required defensive measures to protect their data; they do not, by any means, protect the nation as a whole, much less its borders with the outside world. Once again, it is not only the responsibility of individuals and organizations to protect the nation's cybersecurity, but in the case of in the health and financial sectors, they are the ones who are being held legally accountable for it.

Cyberspace has often been referred to as a 'Wild West',[63] but even this is not an adequate analogy for the sheer order of magnitude of chaos in cyberspace today. Indeed, given the global and anonymous nature of the world wide web, a more accurate and ominous analogy is that cyberspace is a global-cybersecurity 'Dark Ages,' in which individuals and organizations, not nation-states, are the only practical entities in existence, and there are no states to enforce laws and borders. Lacking nation-states as self-protecting entities proper in cyberspace, their constituents (citizens and organizations of all kinds) are effectively 'on their own' in knowing their situations and threats, and constructing and implementing their defenses (and, in the West at least, no offenses to eliminate or deter their more persistent and fiercest threats.) This results in the large-scale weak, haphazard, and increasingly porous cybersecurity scenario that is currently the case nationwide. In addition, only national-scale organizations such as the DOD, DHS and NSA can collectively monitor, guard, and plan and mount large-scale defense and especially offshore offensive operations in cyberspace. It is these organizations that should be 'manning the border' gateways, watching for attacks, shutting them down and bringing countervailing

[61] Staff, *Health Information Privacy*, U.S. Department of Health and Human Services, last accessed 08-27-14, http://www.hhs.gov/ocr/privacy/
[62] Staff, *The Sarbanes-Oxley Act of 2002*, Addison-Hewitt Associates, 2006, http://www.soxlaw.com/index.htm
[63] Morriss, Andrew P., *The Wild West Meets Cyberspace*, The Freeman, 07-01-98, http://www.fee.org/the_freeman/detail/the-wild-west-meets-cyberspace

cyberattacks to bear; no one else can or should be performing this security cyber function at the national level.

Need for International Mutual-Defense Coalitions in Cyberspace

Also conspicuous by its absence from the amassed CSBPs is any reference whatsoever to global-level CSBPs of any kind. Equally absent are international mutual-cyberspace-defense coalitions or alliances along the lines of physical-world collective-national-defense coalitions such as NATO. The advantages of alliances have always been compelling, especially when all potential members are vulnerable. As proof of the historic value of coalitions at the global scale, the US-led Allied Powers of WWII is the greatest possible demonstration of what an effective pan-global international alliance can achieve: in this case, unconditional victory in the greatest global armed conflict in world history.[64]

In short, the US needs to ally itself and its defenses in cyberspace with its friends and allies in the physical world. Sharing of all things cybersecurity, from information on threats, their sources, and their nature, through shared and pooled cybersecurity (and cyberwarfare) skill-sets, problem-solving, countermeasures, computing power, and the ability to instantly come to the aid of any ally in need via cyberspace, are all compelling reasons for the US to form cybersecurity alliances with its allies. Interestingly, allies are never closer to come to each other's aid than they are in cyberspace. This alliance-formation strategy won World War II and the Cold War after that; it may well constitute the greatest single collective means for the US (and its allies) to obtain their collective cyber, and thus national, security.

---

[64] Overy, Richard, *World War Two: How the Allies Won*, The BBC, 02-17-11, http://www.bbc.co.uk/history/worldwars/wwtwo/how_the_allies_won_01.shtml

Section 3.3 Mathematical Representations of Theoretical Framework for CST and CSBP Generation

This section focuses on the analysis and development of mathematical representations for the relationship between the nature of any entity, and the level of cybersecurity and CSBPs it needs to implement. First, the underlying notions of cyberspace power and its constituent components are presented. Then, derivative concepts are presented to provide further insights into cyberspace security. In this section, the concepts of cyberspace power, entity conspicuity in cyberspace and entity vulnerability in cyberspace are proposed and described, and a CSBP Spectrum is also proposed and described.

3.3.1 Cyberspace Power

First, consider an entity's power in cyberspace, or, its ability to operate, survive and grow or perish in cyberspace: the greater the entity's cyberspace power, the greater its ability to both defend itself and to exert its will on its area of interest, potentially up to a global scale; conversely, the greater the entity's cyberspace power, the more conspicuous a cyberspace target it becomes. For instance, the more financial assets or national security/intelligence information that are accessible by or via the entity, the greater is its power in cyberspace, but also the more valuable and tempting a target it is for cybercrime and/or cyber-espionage. The following equation is proposed as a means of describing Cyberspace Power, based on several essential constituent components:

Equation 1: Cyberspace Power

Cyberspace Power = (average cybersecurity competence) * (numbers) * (resources) * (authorization level) * (will)

Where,

- average cybersecurity competence = the average competence of the individual or group comprising the entity in question, from a single individual up through all the individuals and groups that comprise a larger 'entity,' such as an organization or nation-state.
- numbers = the numbers of individuals or groups that comprise the entity itself.
- resources = the resources (financial, cyberspace equipment, software, systems, etc.) that are available within or to the entity in question.
- authorization level = how much authorization an entity has to conduct its cyberspace operations. This could be government permissions, clearances, licenses or those within an organization (for instance, positions of trust within a financial institution.) This ultimately means access to and organizational or governmental consent to use more sensitive and capable information and systems.
- will = the will or determination of the entity to achieve its goals in cyberspace, be they simple defense against intrusion/destruction, or to attack, infiltrate, or defeat other entities in cyberspace.

3.3.2 Entity Conspicuity (EC) in Cyberspace

Another concept introduced here is 'Entity Conspicuity,' or EC. This concept describes an entity's most critical role or significance within society, and is directly related to the entity's cyberspace power. The nature of the most affective role played by that individual in society (such as homemaker, sole proprietor, employee,) the level of importance of that role (local, state, national), and thus, the value of the information that is accessible to that individual (monetary, identity, national security clearance, proprietary, trade secrets, medical), determines that individual's cyberspace Entity Conspicuity. If an individual's greatest EC is high enough (for example, the Director of the NSA, President of Lockheed-Martin, the Bank of America, or State Farm,) then that individual's EC is as high as that of the entire organization for which he or she works. Importantly, this drives that individual's (as well as his/her organization's) EC up into the Organizational-Level, or even National-Levels of CSBPs needed to secure that individual, as well as the affiliated organization. And whether or not an individual has a spouse, family, investments, side-businesses, etc., the amount of EC, and thus, the level of CSBPs needed by that individual/entity, is determined by the highest level of responsibility for which that individual's involvement in any activity, and thus EC, takes him/her. Similarly, the level of EC of an organization is determined by the EC of its most significant activity.

Thus, while Equation 1 (above) describes an entity's cyberspace power overall, it does not describe the entity's conspicuity in cyberspace. That is to say, the more valuable an entity is (due to financial, intellectual property, personal identity, or national security information,) the more conspicuous it is, and thus, the bigger a target it is in cyberspace. Equation 2 (below) describes this relationship via the following derivation:

- From Equation 1 (above),

Cyberspace Power = (average cybersecurity competence) * (numbers) * (resources) * (authorization level) * (will)

Thus, an equation for an entity's cyberspace conspicuity is its cyberspace power (Equation 1) divided by its average cyberspace competence, which yields:

Equation 2: Entity Conspicuity in Cyberspace

Conspicuity in cyberspace = (numbers) * (resources) * (authorization level) * (will)

= Cyberspace Power/(average cybersecurity competence)

From Equation 2, then, the cyberspace conspicuity value is an expression of its cyberspace power, with the average cybersecurity competence factor 'stripped away.' Note that all the previous factors, such as 'numbers' and 'resources,' are retained in this equation, in order to reflect both an entity's overall significance in, the number of potential points of risk and scales of impact, as well as the all-important resources in play within the entity.

3.3.3 CSBP Spectrum: Entity Conspicuity vs. CSBPs Needed

As described previously, an entity's Entity Conspicuity, or EC (see also Equation 2, above) can be used to determine the level of CSBPs it needs to implement for effective cybersecurity. To make use of this value, the next step in this theoretical development process is to create a CSBP Spectrum. In this spectrum, an entity's EC can be rated as low, medium or high-level from Equation 2. From this corresponding EC level, the entity must then implement all of the corresponding CSBPs up to and including that level of conspicuity. Table 20 (below) encapsulates this proposed CSBP Spectrum. Importantly, each EC Spectrum Level includes all

CSBPs up to and including that point. For instance, individual-level CSBPs must be included in Organization-level CSBPs, and all of the former must be included in National-Level CSBPs.

Table 20: CSBP Spectrum – CSBPs Needed vs. Entity Conspicuity (EC)

Entity Conspicuity (EC) Spectrum Level	Level of CSBP	CSBPs Needed
High-Level	International-Level	
		(null)
	National-Level	
		Application Software Security
		Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
	Organizational-Level	
		Limitations and Control of Network Ports, Protocols, and Services
		Controlled Use of Administrative Privileges
		Boundary Defense
		Maintenance, Monitoring, and Analysis of Security Audit Logs
		Account Monitoring and Control
		Incident Response and Management
		Secure Network Engineering
		Penetration Tests and Red Team Exercises
		Information System Security Systems Design and Planning
		Top-Down Implementation is Essential
		Physical Facilities Security
		"Combined-Arms Warfare": Most-Effective Implementations Combine all four Major Cyber Security Frameworks
Entity Conspicuity (EC) Spectrum Level	Level of CSBP	CSBPs Needed
		Centralized InfoSec Design, Planning & Implementation
		InfoSec Department Separated from IT Department
		InfoSec Department Reports Directly to CISO
		Compliance with All Required or Applicable Regulations
		InfoSec Implementation must be Consistent w. the Organization's Culture
		Maximize Use of Automation in InfoSec Implementations
		Limitations and Control of Network Ports, Protocols, and Services
		Controlled Use of Administrative Privileges
		Boundary Defense
		Maintenance, Monitoring, and Analysis of Security Audit Logs

Table 20 cont'd

Entity Conspicuity (EC) Spectrum Level	Level of CSBP	CSBPs Needed
Medium-Level		Account Monitoring and Control
	Individual-Level	
		Inventory of Authorized and Unauthorized Devices
		Inventory of Authorized and Unauthorized Software
Minimum Level		Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers
		Continuous Vulnerability Assessment and Remediation
		Malware Defenses
		Wireless Device Control
		Data Recovery Capability
		Security Skills Assessment and Appropriate Training to Fill Gaps
		Controlled Access Based on the Need to Know
		Data Loss Prevention (DLP)

However, Column #2 of Table 20 ("Level of CSBP") can be removed for greater clarity, as can the previously-clarifying line-spaces; this yields

Table 21, below:

Table 21: CSBPs Needed vs. Entity Conspicuity (EC) Spectrum Level

Entity Conspicuity (EC) Spectrum Level	CSBPs Needed
High-Level	Application Software Security
	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
	Limitations and Control of Network Ports, Protocols, and Services
	Controlled Use of Administrative Privileges
	Boundary Defense
	Maintenance, Monitoring, and Analysis of Security Audit Logs
	Account Monitoring and Control
	Incident Response and Management
	Secure Network Engineering
	Penetration Tests and Red Team Exercises
	Information System Security Systems Design and Planning
	Top-Down Implementation is Essential
	Physical Facilities Security
	"Combined-Arms Warfare": Most-Effective Implementations Combine all four Major Cyber Security Frameworks
	Centralized InfoSec Design, Planning & Implementation
	InfoSec Department Separated from IT Department
	InfoSec Department Reports Directly to CISO
	Compliance with All Required or Applicable Regulations
	InfoSec Implementation must be Consistent w. the Organization's Culture

Entity Conspicuity (EC) Spectrum Level	CSBPs Needed
	Maximize Use of Automation in InfoSec Implementations

Table 21 cont'd

Entity Conspicuity (EC) Spectrum Level	CSBPs Needed
	Controlled Use of Administrative Privileges
	Boundary Defense
	Maintenance, Monitoring, and Analysis of Security Audit Logs
	Inventory of Authorized and Unauthorized Devices
	Inventory of Authorized and Unauthorized Software
Minimum Level	Secure Configurations for Hardware & Software on Laptops, Workstations, & Servers
	Continuous Vulnerability Assessment and Remediation
	Malware Defenses
	Wireless Device Control
	Data Recovery Capability
	Security Skills Assessment and Appropriate Training to Fill Gaps
	Controlled Access Based on the Need to Know
	Data Loss Prevention (DLP)

Table 21 represents the final and complete "Spectrum" of CSBPs needed versus EC-driven Levels of intensity. The thresholds were set as 'low' as possible (relative to the levels of organizational size), in order to drive an entity to implement as many CSBPs as are feasibly possible at that level. As a result, the minimum and even the medium EC thresholds are very low, relative to the number of CSBPs to be implemented. (Note, however, that these levels are a 'first pass' at this aspect, and could also be the subject of future research to clarify and better place them in the EC hierarchy.)

3.3.4 Cyberspace Vulnerability

One other facet to consider is an entity's vulnerability in cyberspace. This value describes how well-protected the entity is, relative to its conspicuity. That is, the more conspicuous the entity is, but the greater its cybersecurity competence, the less vulnerable it is in cyberspace. Conversely, the more conspicuous it is, but the lower its cybersecurity competence, the more vulnerable it is, and the greater is its need to bolster its cybersecurity strategy. Thus, this value

provides a measure of how well-defended the entity is in cyberspace, and whether these defenses need to be shored up/improved, or are effective in their efforts. This value is derived as follows:

Equation 3: Entity Vulnerability in Cyberspace
- From Equation 1,

Cyberspace Power = (average cybersecurity competence) * (numbers) * (resources) * (authorization level) * (will)

- And, from Equation 2,

Conspicuity in cyberspace = (numbers) * (resources) * (authorization level) * (will)

= Cyberspace Power/(average cybersecurity competence)

- Thus,

$$\text{Vulnerability in Cyberspace} = \frac{(\text{numbers}) * (\text{resources}) * (\text{authorization level}) * (\text{will})}{(\text{average cybersecurity competence})}$$

$$= \frac{\text{Conspicuity in Cyberspace}}{(\text{average cybersecurity competence})}$$

$$= \frac{\text{Cyberspace Power}}{(\text{average cybersecurity competence})^2}$$

3.3.4 Cybersecurity Competence – the New Literacy

One important observation from all the table integrations and equations derived above is just how vital average cybersecurity competence truly is for the survival and success of any entity in cyberspace; appropriately so, since it highlights the need for cybersecurity competence within and throughout any entity's activities, regardless of its role or roles in cyberspace or society. It further highlights the vital role that this factor plays in the overall cybersecurity of any entity, no matter 'small' or how powerful the entity might be. It also highlights how much of the cybersecurity burden truly rests on the shoulders of the individual to maintain overall personal,

organizational, and ultimately, national-level, cybersecurity. If an entity cannot at least defend itself adequately, much less carry out significant cybersecurity operations, it is very, even completely, vulnerable. The nature of average cyberspace competence also highlights how any weak link in the entity's overall cyberspace competence can prove to be that entity's undoing, especially at higher levels of cyberspace power, conspicuity and vulnerability. In other words, cybersecurity competence may well be the single most critical aspect of an entity's survivability and viability in cyberspace. And, the greater an entity's cyberspace power, the greater the need is for that entity, and all of its constituent members, to have the highest possible average cyberspace competence. These relationships can be expressed by Equation 4: Recommended Average Cyberspace Competence, below:

Equation 4: Recommended Average Cyberspace Competence

i) Recommended Average Cyberspace Competence $\propto$ cyberspace conspicuity

- similarly, for any entity,

ii) Recommended Average Cyberspace Competence $\propto$ Max. Level of CSBPs

Thus, cybersecurity training should, indeed must, be made a required skillset for all individuals in American society. Given the growing ubiquity of cyberspace in American society, when combined with both our growing dependency on and increasing vulnerability in cyberspace, this will become nearly as vital a life-skill as literacy and basic arithmetic. However, for this to become the case would, once again, require leadership, organization and implementation at the National level.

CHAPTER 4: CONCLUSIONS AND FUTURE WORK

This final chapter covers two final items. First, it outlines potential avenues for future research and developmental work using the research, concepts, theoretical frameworks and conclusions found in this work. Second, it provides a conclusion for this work and its results.

Section 4.1 Future Work

Some areas for potential future developments of this research are:

1) Revisit the applicability and derivations of IR Theories selected for Cyber Security.

2) Revisit the applicability and further development of the All-Levels Extensions of IR Theory.

3) Re-evaluate and extend the six concepts developed for IR Theoretical Conclusions for CSBPs.

4) Validate the 'rubber meets the road' framework chosen in this work to derive the list of CSBPs, and review and validate the final list of CSBPs selected in this work.

5) Review the SSE paradigm developed as a 'gluing' framework used in this work to merge the selected CSBPs with the CSBP-Optimized IR Theoretical observations.

6) Evaluate and quantify the Conceptual Equations for Cyberspace Power, Conspicuity, Vulnerability, and Competence.

7) Correspondingly, the CSBP Spectrum thresholds applied to Entity Conspicuity in Table 21 could be further investigated, refined and augmented with quantification and more numerically-driven, more detailed analysis.

8) Further investigation into adopting offensive cyber security best practices (OCSBPs) within a legal, moral, and strategically vital context, as found absent and necessary by IR Theory. Such precepts are the US' Constitutional Right to Bear Arms and the Judeo-Christian Tradition of Proportionate Response are powerful potential bases for legitimizing and defining OCSBPs.

9) Similarly, further investigation is also warranted into the kinds of locations and corresponding CSBPs needed to better secure the nation's borders in cyberspace, as a means of providing full and proper national-level cybersecurity now absent from CSBPs for the nation as a whole. Starting points for this research should begin with the nation's border gateway systems, treating these nodes as naval-strategy-derived "choke points" or "strategic nodes," through which most, if not all, of the nation's international internet traffic must pass. Similarly, SATCOM (satellite telecommunications) ground stations would need to be examined and better "fortified."

10) In addition, further investigation needs to be made into creating and utilizing international cyberspace-security coalitions to protect all allied nations' cyberspace and related systems, also as found absent and forecast to be necessary by IR Theory.

11) Further investigation needs to be made into the integration of cybersecurity best practices with other forms of defense along the lines of the military–strategic paradigm of "Combined-Arms Warfare," from both theoretical and practical perspectives.

12) Consider refining or altogether changing the definition of the critical variable 'average cyberspace competence.' Altering this variable to 'mean cyberspace competence' or 'minimum cyberspace competence' might better serve to illustrative an entity's true strength or weakness in cyberspace.

Section 4.2 Conclusions

This thesis began by producing a list of "rubber meets the road" real-world-applicable CSBPs drawn from scholarly references. Next, a list of IR Theories was selected as a basis for building a theoretical framework into which to integrate the CSBPs. The CSBP List was then prepared for integration into the IR Theory frame-set by organizing CSBPs according to their

Scale of Societal Effect, reflecting IR Theory's Three Levels of Analysis. This resulted in an integrated table of all CSBPs, alongside their corresponding cyber-security-optimized IR Theories. This list was further reduced, showing only the CSBPs and their corresponding levels of applicability.

The final step to construct a more complete predictive framework began by introducing the notion of 'power,' specifically, Cyberspace Power, representing an entity's capability for survival, growth or failure in cyberspace. This led to further concepts and descriptive equations, most notably, of Entity Conspicuity (EC), describing an entity's prominence in cyberspace. Notably, these equations used both technical and social variables common to all entities of any size operating in cyberspace, completing the integration of technological and social concepts from both academic fields of International Relations and Computer Science and Information Systems.

This led to the final table containing CSBPs, ranked by their order of effect (individual to organizational) alongside their relevant level of "EC Spectrum"; that is, the higher an entity's EC, the greater the portion of the CSBP 'spectrum' that entity must implement to remain secure in cyberspace. This work further derived an entity's Vulnerability, which compared its EC to its ability to protect itself. In addition, cyberspace competence was found to be critical to an entity's security in cyberspace, and an equation was derived to describe and drive that level. Importantly, the IR Theoretical work also found that there are a number of glaring vulnerabilities in existing CSBPs, such as national-level practices, international coalitions, and offensive cyber security practices.

Hopefully, this work will prove to be effective at providing a useful theoretical toolset to enable any entity to find and implement all the CSBPs it needs to operate securely in cyberspace.

It is also hoped that in the future, the concepts and equations derived in this work will be built upon, quantified, and thus better able to provide detailed and powerful CSBP predictive tools. Finally, the national-level, international-level, and offensive cybersecurity strategies currently (and dangerously) absent from present practices and policies, vitally needs future research and implementation.

REFERENCES

Textbooks:

Whitman, Michael E., and Mattord, Herbert J., Management of Information Security, Third Edition, Course Technology – Cengage Learning, 2010, ISBN-13: 978-1-4354-8884-7

Published Articles:

Eriksson, Johan, and Giacomello, Giampiero, The Information Revolution, Security, and International Relations: (IR)relevant Theory?, International Political Science Review. Jul2006, Vol. 27 Issue 3, p221-244, ISSN: 01925121, http://0-search.ebscohost.com.uncclc.coast.uncwil.edu/login.aspx?direct=true&db=a9h&AN=22177315&site=ehost-live

Nicho, Matthew, An Information Governance Model for Information Security Management, from: Mellado, D; Sanchez, LE; Fernandez-Medina, E; and Piattini, M, "Cyber Security Governance Innovations: Theory and Research", Advances in Cyber Security Privacy and Ethics (AISPE) Book Series, 2013, ISBN: 978-1-4666-2083-4, pg. 155-189.

Staff, 2013 Data Breach Investigations Report, Verizon RISK team, March 2013, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

Online Articles:

Barnes, Ed, Mystery Surrounds Cyber Missile That Crippled Iran's Nuclear Ambitions, FoxNews.com, November 26, 2010, http://www.foxnews.com/scitech/2010/11/26/secret-agent-crippled-irans-nuclear-ambitions/?test=latestnews

Bisson, Jacquelin, and Saint-Germain, Rene, White Paper: The BS 7799 / ISO 17799 Standard For a better approach to Cyber Security, Callio Technologies, Inc., last accessed 05-30-13, http://www.infodom.hr/calliosecura/materijali/White_Paper_ISO_17799_en%5B1%5D.pdf

Buse, Margaret, Non-State Actors: Their Significance in the Global Picture, James Madison University Center for International Stabilization and Recovery, Issue 5.3, December 2011, http://www.jmu.edu/cisr/journal/5.3/features/maggie_buse_nsa/maggie_buse.htm

Coleman, Gabriella, Anonymous in Context: the Politics and Power behind the Mask, Center for International Governance Innovation (CIGI) Online, 09-23-13, http://www.cigionline.org/publications/2013/9/anonymous-context-politics-and-power-behind-mask?gclid=CP30lOOuucACFSMV7AodbQoARA

Daly, John, Naval Choke Points and Command of the Sea, 03-02-09, world Politics Review, http://www.worldpoliticsreview.com/articles/3378/naval-choke-points-and-command-of-the-sea

Dunnigan, Jim, Information Warfare: Iranian Hackers Step Up, Strategy Page, 08-24-14, http://www.strategypage.com/htmw/htiw/articles/20140824.aspx

Eriksson, Johan, and Giacomello, Giampiero, The Information Revolution, Security, and International Relations: (IR)relevant Theory?, International Political Science Review. Jul2006, Vol. 27 Issue 3, p221-244, ISSN: 01925121, http://0-search.ebscohost.com.uncclc.coast.uncwil.edu/login.aspx?direct=true&db=a9h&AN=22177315&site=ehost-live

Gertz, Bill, Stolen F-35 Secrets Now Showing Up in China's Stealth Fighter, Washington Free Beacon, 03-13-14, http://freebeacon.com/national-security/stolen-f-35-secrets-now-showing-up-in-chinas-stealth-fighter/

Giles, Lionel, Sun Tzu on the Art of War, Luzan & Co., 1910, last accessed 22-11-13, http://www.artofwarsuntzu.com/Art%20of%20War%20PDF.pdf

Herridge, Catherine, NSA chief: cyber-attacks skyrocket, account for 'largest transfer of wealth' ever, FoxNews.com, July 9, 2012, http://www.foxnews.com/politics/2012/07/09/nsa-chief-cyber-attacks-skyrocket-account-for-largest-transfer-wealth-in/?test=latestnews#ixzz20BitOaGs

Herridge, Catherine, and the Associated Press, NSA Director: China can damage US power grid, Fox News, 11-20-14, http://www.foxnews.com/politics/2014/11/20/nsa-director-china-can-damage-us-power-grid/

Johnston-Turner, Mary, Security Management Survey: ISO, ITIL and COBIT Triple Play Fosters Optimal Security Management Execution, BMSReview.com, 2012, http://www.bsmreview.com/security_best_practice_survey.shtml

Mead, Walter Russell, The Return of Geopolitics – the Revenge of the Revisionist Powers, Foreign Affairs – Council on Foreign Relations, May-June 2014, http://www.foreignaffairs.com/articles/141211/walter-russell-mead/the-return-of-geopolitics

Morriss, Andrew P., The Wild West Meets Cyberspace, The Freeman, 07-01-98, http://www.fee.org/the_freeman/detail/the-wild-west-meets-cyberspace

Overy, Richard, World War Two: How the Allies Won, The BBC, 02-17-11, http://www.bbc.co.uk/history/worldwars/wwtwo/how_the_allies_won_01.shtml

Posey, Clay, and Roberts, Tom L., and Courtney, James F., A Best Practices Guide to Cyber Security, IBM Center for the Business of Government, last accessed 05-24-13, http://www.businessofgovernment.org/sites/default/files/A%20Best%20Practices%20Guide%20to%20Information%20Security.pdf

Putvinski, Matthew, Cyber Security Series Part 1: Cyber Security Best Practices, Corporate Compliance Insights, 06-09-09, http://www.corporatecomplianceinsights.com/information-security-best-practices/

Rambiesa, Barb, How to reduce IT Security risk with IT asset management, "Cyber Security Magazine", TechTarget.com, May 2013, http://searchsecurity.techtarget.com/tip/How-to-reduce-IT-security-risk-with-IT-asset-management

Reisinger, Don, U.S. target of sustained cyber-espionage campaign, CBS News, 02-11-13, http://www.cbsnews.com/news/us-target-of-sustained-cyber-espionage-campaign/

Roman, Jeff, Developing IT Security Best Practices – NIST Analyzes Cybersecurity Framework Comments, BankInfoSecurity.com, 05-21-13, http://www.bankinfosecurity.com/developing-security-best-practices-a-5775/op-1

Saint-Germain, René, Information Security Management Best Practice Based on ISO/IEC 17799, The Information Management Journal, July-August 2005, pg. 60-66, http://www.arma.org/bookstore/files/Saint_Germain.pdf

Staff, Adherence to and Compliance with Arms Control, Nonproliferation, and Disarmament Agreements and Commitments, U.S. Department of State, July 2010, http://www.state.gov/documents/organization/145181.pdf

Staff, APT1 – Exposing One of China's Cyber Espionage Units, Mandiant.com, 02-19-13, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Staff, Best Practices for Managing Information Security, Symantec.com, Feb. 2010, http://eval.symantec.com/mktginfo/enterprise/other_resources/b-best_practices_for_managing_information_security-february_2010_OR_2876547.en-us.pdf

Staff, Cyber Security Best Practices, InvenSys.com, June 2012, pg. 1, http://iom.invensys.com/EN/pdfLibrary/ServicesProfile_Invensys_CyberSecurityBestPractices_06-12.pdf (Note: link deprecated)

Staff, Edward Snowden: Whistleblower or double-agent?, FoxNews.com, 06-14-13, http://www.foxnews.com/politics/2013/06/14/edward-snowden-whistleblower-or-double-agent/

Staff, FBI Warns Tech Companies of State-Sponsored Chinese Hackers, Newsmax.com, 10-16-14, http://www.newsmax.com/SciTech/FBI-China-hackers-cybersecurity/2014/10/16/id/601162/

Staff, Health Information Privacy, U.S. Department of Health and Human Services, last accessed 08-27-14, http://www.hhs.gov/ocr/privacy/

Staff, Iran's global cyber war-room is secretly hosted by Hizballah in Beirut, DEBKAfiles.com, 10-21-12 http://www.debka.com/article/22459

Staff, Manning not guilty of aiding the enemy in Wikileaks case, stall may face 128 years in prison, FoxNews.com, 07-30-13, http://www.foxnews.com/us/2013/07/30/bradley-manning-not-guilty-aiding-enemy-in-wikileaks-case-convicted-lesser/

Staff, National Security Agency/Central Security Service – Defending Our Nation, Securing Our Future, NSA.gov, 2009, https://www.nsa.gov/

Staff, The Sarbanes-Oxley Act of 2002, Addison-Hewitt Associates, 2006, http://www.soxlaw.com/index.htm

Staff, Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines – Version 4.1, SANS and the Center for Strategic and International Studies, March 2013, http://www.sans.org/critical-security-controls/

Staff, What is the Syrian Electronic Army?, The Guardian, 2014, http://www.theguardian.com/media-network/partner-zone-infosecurity/what-is-the-syrian-electronic-army

Tadjdeh, Yasmin, Fears of Devastating Attacks on Electric Grid, Critical Infrastructure Grow, National Defense Magazine, October 2013, http://www.nationaldefensemagazine.org/archive/2013/October/Pages/FearsofDevastatingCyber-AttacksonElectricGrid,CriticalInfrastructureGrow.aspx

Traynor, Ian, Russia accused of unleashing cyberwar to disable Estonia, The Guardian, 05-16-07, http://www.theguardian.com/world/2007/may/17/topstories3.russia

Theoretical Framework – Research Articles

International-Level IR Theory References

Walt, Stephen M., International Relations: One World, Many Theories, Foreign Policy, (Spring 1998), pg. 29-46, http://faculty.maxwell.syr.edu/hpschmitz/PSC124/PSC124Readings/WaltOneWorldManyTheories.pdf

Walt, Stephen M., Alliance Formation and the Balance of World Power, International Security, Vol. 9, No. 4, (Spring 1985), pp. 3-43, https://umdrive.memphis.edu/rblanton/public/POLS_7508_Fall_2009/walt_alliance_formation.pdf

Waltz, Kenneth N., The Origins of War in Neorealist Theory, Journal of Interdisciplinary History, Vol. 18, No. 4, (Spring 1988), pp. 615-628, http://sites.google.com/site/casaroes/Waltz-OriginsofWarinNeorealistTheory.pdf

Jervis, Robert, Cooperation Under the Security Dilemma, World Politics, Vol. 30, No. 2. (Jan., 1978), pp. 167-214, http://ic.ucsc.edu/~rlipsch/pol160A/Jervis.pdf

State-Level Theories – References

Levy, Jack S., Domestic Politics and War, Journal of Interdisciplinary History, Vol. 18, No. 4, (Spring 1988), pp. 653-673, http://fas-polisci.rutgers.edu/levy/1988%20Domestic%20Politics%20&%20War.pdf

Ray, James Lee, Does Democracy Cause Peace? Annual Review of Political Science, (1998), 1: 27–46, http://www.mtholyoke.edu/acad/intrel/ray.htm

Schweller, Randall, Bandwagoning for Profit: Bringing the Revisionist State Back In, International Security, Vol. 19, No. 1 (Summer, 1994), pp. 72-107, http://people.reed.edu/~ahm/Courses/Reed-POL-240-2010-S3_IP/Syllabus/EReadings/03.1/03.1.Schweller1994Bandwagoning.pdf

Sub-State-Level Theories – References

Levy, Jack S., Domestic Politics and War, Journal of Interdisciplinary History, Vol. 18, No. 4, (Spring 1988), pp. 653-673, http://fas-polisci.rutgers.edu/levy/1988%20Domestic%20Politics%20&%20War.pdf

Allison, Graham, Conceptual Models and the Cuban Missile Crisis, The American Political Science Review, Vol. 63, No. 3 (September 1969,) pp. 689-718, http://www.rand.org/pubs/papers/P3919.html

Jervis, Robert, War and Misperception, Journal of Interdisciplinary History, Vol. 18, No. 4, (Spring 1988,) pp. 675-700, http://public.gettysburg.edu/~dborock/courses/Fall/p303/jervis%20war%20and%20misperception.pdf

Byman, Daniel L., and Pollack, Kenneth M., Let Us Now Praise Great Men: Bringing the Statesman Back In, International Security, Vol. 25, No. 4, (Spring 2001), pp. 107-146, http://belfercenter.ksg.harvard.edu/files/bymanetalvol25no4.pdf

All-Levels Theories – References

Williams, Paul D. (Ed.), Security Studies – An Introduction, London and New York: Routledge, 2008.

APPENDIX

A: Plan Followed to Complete Thesis: Cyber Security Theory (CST)

This Chapter lists the final planned steps taken to integrate and analyze the CSBPs and IR Theory-Set to complete development of the Cyber Security Theory set for this Thesis. These steps are described in the following sections.

Section A.1 Merged CSBPs with Cybersecurity-Optimized IR Theories

The approach taken to complete the work of this Thesis, and to produce Cyber Security Theory, can be described by the following conceptual 'equation':

Equation 5: Cyber Security Theory Basis Development

(CSBPs grouped by SSE) + (Cybersecurity-Optimized IR Theories) = Cyber Security Theory Basis

The following steps were taken to produce the IR-based theoretical basis for Cyber Security in Chapter 3:

a) Combined the analyses of Sections 2.2 (CSBPs) and 2.3 (IR Theory) for comparison and contrast, and further analysis. This de facto completed the data-processing portion of this Thesis, by combining the results contained in 2.2.4 CSBPs Grouped by Scale of Societal Effect (SSE) (in which all the CSBPs have already been regrouped by SSE), with the results contained in Section 2.3 International Relations Theories & Cyber Security Best Practices. Grouping the final set of CSBPs by SSE rather than by the more traditional framework of technology or

policy, lays the groundwork for this new approach of aligning the CSBPs with the various IR Theory-based paradigms for comparison, contrast, and ultimately, evaluation of the new Cybersecurity Theory-set. At their simplest, the various "Levels" of IR Theory (International, National, Sub-State, Individual, and All-Levels) can be thought of as SSEs, albeit ones focused on the interactions, behaviors, and consequences of IR at those levels. The final step of the 'data-processing' work of this paper was achieved by integrating the contents of the SSE-specific CSBPs (Table 8 through Table 11) into "Table 14: IR Theories and their Applicability to Cyber Security."

b) Once these two concept-sets were integrated into a single table (along with all relevant non-tabulated IS-specific IR observations, rules, etc.), all alignments, gaps and any other insights to be found in their amalgamation were observed, analyzed, and any and all possible CSBP consequences were evaluated. All of these observations, conclusions and recommendations for future cybersecurity best practices and possible avenues for further research were then summarized in Chapter 4.

Section A.2 Planned Schedule for Thesis Deliverables

(*Note: this timetable is 'obsolete,' having been written on 02-13-14.)

a) Complete Thesis Proposal and distribute to Committee members: 3-7 Feb., 2014.

b) Schedule Thesis Proposal Defense: 7 - 14 Feb., 2014.

c) Conduct Thesis Proposal Defense: 27 - 28 Feb. 2014.

d) Update Proposal to Thesis as directed by Committee members: 03/11/14 - 04/11/14

e) Distribute Thesis to Committee members: 14 Apr., 2014.

f) Schedule Thesis Final Defense: 14 Apr., 2014.

g) Conduct Thesis Final Defense: 21-25 Apr. 2014.

h) Make final revisions, submit Thesis as completed to CSIS Dept.: 04/28/14 – 05/11/14.

i) Doctors Reinicke and Cummings to modify Thesis into IS publication-ready format: Summer I, 2014.

Section A.3 Thesis-Derived Publication Results

The first Thesis-derived publication was achieved in November 2014, per the following references:

Kleinberg, Howard, and Reinicke, Bryan, and Cummings, Jeffrey, "Cyber Security Best Practices: What to do?", 2014 Proceedings of the Conference for Information Systems Applied Research (CONISAR), ISSN: 2167-1508 v7 n3309, Baltimore, MD, November 6-9, 2014, http://proc.conisar.org/2014/pdf/3309.pdf

Note: paper was given the Conference's "Best Papers: Meritorious Paper Award (top 15%)": http://proc.conisar.org/2014/bestpapers.html

The above-cited Thesis-derived paper achieved a second, Journal-level publication in the October 2015 issue of the Journal of Information Systems Applied Research, per the following reference:

Kleinberg, Howard, and Reinicke, Bryan, and Cummings, Jeffrey, "Cyber Security Best Practices: What to do?", Journal of Information Systems Applied Research, 8(2) pp 52-59. http://jisar.org/2015-8/ ISSN: 1946-1836, http://jisar.org/2015-8/n2/JISARv8n2p52.html