ACHIEVING NATIONAL UNITY OF EFFORT IN CYBER

GRADUATE RESEARCH PROJECT

June 2011

Jonathan J. Frampton, Major, USAF

AFIT/ICW/ENG/11-04

DEPARTMENT OF THE AIR FORCE

AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/ICW/ENG/11-04

ACHIEVING NATIONAL UNITY OF EFFORT IN CYBER

GRADUATE RESEARCH PROJECT

Presented to the Faculty

Department of Electrical & Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master in Cyber Warfare

Jonathan J. Frampton, MA

Major, USAF

16 June 2011

AFIT/ICW/ENG/11-04

ACHIEVING NATIONAL UNITY OF EFFORT IN CYBER

Jonathan J. Frampton, MA

Major, USAF

Approved:

_____	_____
Michael R. Grimaila, PhD, CISM, CISSP (Chairman)	Date
_____	_____
Lt Col David Robinson, USAF (Member)	Date
_____	_____
Capt Jonathan Butts, USAF (Member)	Date

Abstract

Information is a foundation of power enabling national security, prosperity and cultural values for all nations. As such, significant national discussion is underway regarding the threats, risks and vulnerabilities of the national and global Cyber infrastructure, especially given recent events. Unfortunately, current U.S. national strategies regarding Cyber lack clarity on ways to achieve national goals. And, consequently, national U.S. efforts in Cyber suffer from a lack of focus and leadership. While the military is re-organizing its Cyber forces , the time has come to create a civilian led Federal Cyber Administration to focus national efforts, expand the National Security Administration authorities for the Federal Critical Infrastructure using the North American Aerospace Defense (NORAD) model, and create a National Cyberspace Safety Board.

Acknowledgements

I would like to thank my wife and daughters for their patience, understanding and love this year. They are the very reason I choose to serve.

- Jon

Table of Contents

Abstract v
Acknowledgements vi
Table of Contents vii
List Of Figures ix
I. Introduction 1

1.1 Motivation 1

1.2 Purpose 2
II. General Threats 3

2.1 General Threats 3

2.2 Weak and Failing States 4

2.3 Military Threats 5

2.4 Espionage Concerns 5

2.5 Economic Concerns 6

2.6 Cultural Concerns 6

2.7 Tempering the Cyber Threats 7

2.8. Assessment 7
III. Current National Efforts 9

3.1 General 9

3.2 National Goals 9
3.2.1 The National Security Strategy 9
3.2.2 The National Defense Strategy 10
3.2.3 The National Military Strategy 11

3.3 National Challenges 11
3.3.1 National and International Cooperation 11
3.3.2 Definition Agreement 12
3.3.3 Information Security 13
3.3.4 Attribution Challenges 14
3.3.5 National Monitoring 16
3.3.6 National Intelligence Discussion 18

3.4 Current Governance 19

3.5 Assessment 20
IV. EXISTING CONSTRUCTS 23

4.1 General 23

4.2 Federal Aviation Administration 23
4.2.1 A Brief History 23

Figure 4: U.S. Airway Routes[57] 24
4.2.2 An Operational Framework 25
4.2.3 A Regulatory Benchmark 27

4.2.4 A Commons Benchmark *30*
4.2.5 An Airspace Analogy *30*
4.3 North American Aerospace Defense (NORAD) 32
4.3.1 Brief History *32*
4.3.2 Monitoring and Surveillance *33*
4.4 National Transportation Safety Board (NTSB) 34
4.5 Discussion 35
V. A ROADMAP FORWARD 36
5.1 General 36
5.2 Federal Cyberspace Administration 36
5.2.1 Brief History *37*
5.2.2 Operational Framework *37*
5.2.3 Cyber Commons *39*
5.2.4 Segments *39*
5.2.5 Rules and Regulations *41*
5.2.4 Discussion *44*
5.3 National Security Agency 45
5.3.1 Mission *45*
5.3.2 Requirements *46*
5.3.3 Securing Others *46*
5.3.4 Discussion *46*
5.4 National Cyber Safety Board 47
5.5 Assessment 48
VI. CONCLUSION 49
6.1 Summary 49
6.2 Recommendations 49
6.3 Future Study 50
Appendix A: Lexicon 52
A.1 Threats, Vulnerabilities, and Risks *52*
A.2 Attack vs Exploit *52*
A.3 Warfare *53*
A.4 Cyber Domain *54*
A.5 Electronic Warfare *55*
A.6 Information *55*
Appendix B: Information as a Foundation of Power 56
B.1 Understanding Power *56*
B.1.1 Physical Dimension *57*
B.1.2 Cognitive Dimension *57*
B.1.3 Discussion *57*
Bibliography 59
Vita 65

List Of Figures

Figure 1: FBI Crime Statistics 15

Figure 2: Early-warning detection of attack signals 18

Figure 3: Internet Governance Organizations 20

Figure 4: U.S. Airway Routes 24

Figure 5: U.S. Traffic Density 25

Figure 6: Notional Flight Between Two Airports 27

Figure 7: Governance Comparison 31

Figure 8: Notional Message Flight Across Internet 38

Figure 9: Federal Cyberspace Segments 40

Figure 10: Foundations of Power Representation 56

I. Introduction

"If the people cannot trust their government to do the job for which it exists – to protect them and to promote their common welfare – all else is lost." ~ Barack Obama, 2006

1.1 Motivation

As outlined in Appendix B, information is a foundational element of power enabling national security, prosperity and values. In as much, nation states, non-state actors, businesses or other players leverage information to compete and interact on a daily basis. The spectrum of competition ranges from friendly exchanges between partners to hostile acts of war among enemies. In this competitive world, however, accurate information exchanges lie at foundation of efforts to achieve national goals. To build and maintain that power and achieve national goals, the open and accurate exchange of information is paramount.

In considering ways to achieve the U.S. national goals, understanding the relationships between power and information is important. Within U.S. strategy documents, discussions regarding leveraging a whole of government approach and power to achieve our national objectives abound. This really boils down to leveraging all U.S. organizations and tools synergistically to maintain competitive advantage. Thus, importance of information in achieving U.S. national goals cannot be understated, whether involving decisions to go to war, simple banking transactions among the citizenry, or social discussions between friends.

Traditionally when describing power, references to the Instruments of Power (IOPs) with the DIME construct (diplomacy, information, military, economic) have been used. Other expanded models exist (e.g. MIDLIFE) which include law/justice, intelligence, and finance (DIME + LIF).[1] Regardless, none of the models put the relationships between the instruments into context. These models insinuate

[1] US Army. (2004, Oct 1). Counterinsurgency Operations - Interim. *FMI 3-07.22* .

there is a central information office on par with the military, or there is one organization handling diplomacy or economics. This simply is not the case. However, where necessary, focused lead organizations have been built to govern issues of national significance (e.g. National Highway Administration, National Maritime Administration, or even the North American Aerospace Defense Command)

Additionally, the tools and capabilities to share information in Cyber have undergone significant leaps in capability in recent years. And, employment of these tools has not been without trade-offs between security, prosperity and values. Given these tools being deeply ingrained into society now, the need to balance security risks, prosperity and values in Cyber is paramount. Ultimately, trust in the confidentiality, availability and integrity (CAI) of information in Cyber is key to achieving U.S. national goals.[2]

1.2 Purpose

As such, significant national discussion is underway regarding the threats, risks and vulnerabilities of the national and global Cyber infrastructure, especially given recent events. Unfortunately, current national Cyber structures to govern Cyber suffer from a lack of focus, since we do not have a national administration to provide unity of effort. While the military is re-organizing its Cyber forces to address these concerns, the time has come to unify national efforts and provide clear leadership. Taken collectively, the need to unify national efforts in Cyber is a prescient step. Assuming government cannot do this alone, examining existing constructs is necessary to find a way forward.

Chapter 2 will assess the general threats to the U.S. in terms of information and Cyber. Chapter 3 will discuss current national efforts. Chapter 4 will explore existing constructs to benchmark. And, Chapter 5 will outline ways forward.

---

[2] Pipkin, D. L. (2000). Information Security: Protecting the Global Enterprise. Prentice Hall PTR.

II. General Threats

"An amazing invention – but who would ever want to use one?"

~ Rutherford B. Hayes, referring to the telephone

2.1 General Threats

In context of our national goals, some have laid out vulnerabilities to power generation, banking, industrial entities, etc. with dire apocalyptic warnings, stressing the national, state and local impacts due to the evolution of the Cyber Domain.[3] We have seen publically acknowledged events like STUXNET and Russia's Cyber attack on Estonia. The risks associated with these high impact, low frequency events are debatable. However, prudence and preparation are smart courses of action. We should address the vulnerabilities and adjust to the various tactics to reduce risks. And, we must examine our competitors to assess the potential threats or intent to prevent the U.S. from achieving its goals.

We have also seen a wide variety of activity inside U.S. networks by competitors with suspicious intent, to include theft of U.S. defense designs, Internet traffic diverted to China, and the WikiLeaks release.[4] Additionally, insurgents are using the Internet to organize and communicate. Organized crime is stealing millions via a wide array of means. And, individual criminals are committing a wide variety of acts. These daily acts of criminal activity are low impact, high frequency events.

A few years ago, Americans became cognizant of several discussions on-going within a rising China. Of note, a strategy called Shashoujian, or Assassin's Mace, laid out a process of stunning or subduing a more powerful enemy by using simpler, less costly tools in a multi-pronged approach.[5,6]

---

[3] Clarke, R. A. (2010). *Cyber War, The Next Threat to National Security and What to Do About It.* New York, New York: Harper Collins Publishers.

[4] Thomas, T. L. (2010, June 22). Google Confronts China's "Three Warfares". *Parameters* .

[5] Bruzdzinski, J. E. (2004). Demystifying Shashoujian: China's 'Assassin's Mace' Concept. In e. Larry Wortzel and Andrew Scobell, *Civil–Military Change in China: Elites, Institutes, and Ideas After the 16th Party Congress* (pp. 309-364). Carlisle, PA: Strategic Studies Institute, U.S. Army War College.

[6] Muniz, J. J. (2009). *Declawing the Dragon: Why the U.S. Must Counter Chinese Cyber-Warriors.* Fort Leavenworth, KS: U.S. Army Command and General Staff College.

Several Chinese writers noted the U.S. information advantages; and thus, proposed several means of attempting to cripple the U.S. advantage cheaply via jamming, anti-satellite capabilities, fiber cuts, and network intrusions in an attempt to temporarily blind and deafen an opponent. Additionally, another piece of work titled, *Unrestricted Warfare*, outlined moving beyond traditional armed conflict, or using all means at a nation's disposal, to beat an adversary.[7] Specifically, the discussion looks at economic, legal and other means of challenging competitors. Additionally, other comments by Russian figures include the concept of "*seizure of territory by means of information warfare presuming non-traditional occupation, controlling territory and resources without the victor's physical presence in territory of the vanquished."*[8] Tying these issues together has led to deep national discussions concerning a potential asymmetric advantage of world competitors or even from small criminal or insurgent organizations, due to network vulnerabilities of the Cyber Domain. While the academic threat from large, stable nation-states like China or Russia is to be considered, the real world actions must also be taken into account. Collectively, these discussions and activities lend credence to the dire apocalyptic warnings and fear-mongering some have written about in the event the competition turns hostile. As with any potential threat, counter measures must be considered, in the event of hostile actions, to ensure the U.S. can achieve national goals. As such, the American conversation has moved to ensuring U.S. security by leveraging a whole of government approach, especially in terms of Cyber.

2.2 Weak and Failing States

Other threats in today's environment include risks from weak and failing states, which recently has held much of the world's attention, blood and treasure.[9] Evolving events in weak and failing states are worth monitoring given the potential of those seeking power to leverage the cheap capabilities

---

[7] Liang, Q., & Xiangsui, W. (1999). *Unrestricted Warfare.* PLA Literature and Arts Publishing House.
[8] Thomas, T. L. (2010, July). Russian Information Warfare Theory: The Consequences of August 2008. *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald* . Carlisle, Pennsylvania: Strategic Studies Institute.
[9] Wyler, L. S. (2008, August 28). Weak and Failing States: Evolving Security Threats and U.S. Policy. *CRS Report for Congress* . Congressional Research Service: Library of Congress.

enabled by Cyber. Examining the 2010 U.S. National Security Strategy (NSS), we find physical threats based on terrorism as the "immediate threat." Threats are also outlined by global criminal networks against the international financial system, the grave threat of weapons of mass destruction, and large-scale cyber attacks. These issues are exacerbated by weak and failing states.[10] This means the risk in Cyber rises given those seeking power in weak and failing states are more apt to choose the cheaper Cyber option to cause problems. Given these complex issues, the DoD is undergoing a significant realignment to mitigate the risks. However, the national effort to coordinate Cyber policy seems unfocused.

2.3 Military Threats

From a militarily perspective, Cyber is also opening new capabilities due to processing and networking which threaten military systems beyond kinetic strikes. Covert communications, active and passive detection systems, multi-static radars, jamming technologies, space system threats, etc open a wide avenue of emerging capabilities, to which we must adapt.[11,12] Within the man-made Cyber Domain, the convergence of computer processing, network warfare, and spectrum warfare challenge information movement for forces operating within the natural Land, Sea, Air and Space Domains. Thus, the force we prepare to fight with will have to adapt to the rapidly changing technology in Cyber.[13]

2.4 Espionage Concerns

Espionage is enabling countries to develop technologies much faster than they ever would on their own (i.e. the theft of U.S. defense designs mentioned above). As such, the potential for competitors to rapidly close the U.S. technological advantage on the battlefield has caused deep reflection within

---

[10] Wyler, L. S. (2008, August 28). Weak and Failing States: Evolving Security Threats and U.S. Policy. *CRS Report for Congress* . Congressional Research Service: Library of Congress.

[11] Yue, T. (2001, November 30). *The Tech Online Edition (MIT).* Retrieved Dec 7, 2010, from The Tech Online Edition: http://tech.mit.edu/V121/N63/Stealth.63f.html

[12] Muniz, J. J. (2009). *Declawing the Dragon: Why the U.S. Must Counter Chinese Cyber-Warriors.* Fort Leavenworth, KS: U.S. Army Command and General Staff College.

[13] Echevarria II, A. J. (2010, September). Preparing for One War and Getting Another? Strategic Studies Institute.

National Security circles. While espionage has existed for millennia, information access in Cyber is changing methods.

2.5 Economic Concerns

A significant long-term challenge to the U.S. may lie in relative global economic power since China is forecasted to overtake the U.S. economy in 2025.[14] While these simplified linear forecasts are likely wrong, the U.S. must examine its competitive position. Taken in context, Congressional Budget Office projections show U.S. debt payments consuming a larger portion of the U.S. budget, constraining U.S. competitiveness.[15] Admiral Mullin has called this issue the "single biggest threat to national security."[16] Given the role of information in the global economy, lack of focus or weakness in security could directly impact U.S. competitiveness and prosperity.

2.6 Cultural Concerns

Other threat forecasts include a Russian named Igor Panarin predicting the U.S. would collapse into six pieces due to economic and moral issues.[17] Others, such as Buchanan, have forecasted U.S. balkanization due to cultural warfare, economic collapse, loss of power in a multi-polar world, and other reasons.[18] While these cultural scenarios are highly unlikely, we must be mindful of hostile attempts to leverage social information flows during cultural debates to cause discord and panic. This is not intended as a scare tactic. Rather, this is intended to show the need for accurate and openly debated information flows, which is a strength of American society.

---

[14] Hawksworth, J., & Cookson, G. (2008, March). Beyond the BRICs:. *The World in 2050: A Broader Look at Emerging Market Prospects* . Price Waterhouse Coopers.
[15] Congressional Budget Office. (2011, April 5). Long-Term Analysis of a Budget Proposal by Chairman Ryan.
[16] Carden, M. J. (2010, August 27). *U.S. Department of Defense.* Retrieved May 3, 2011, from News: http://www.defense.gov/news/newsarticle.aspx?id=60621
[17] Osborn, A. (2008, December 29). As if Things Weren't Bad Enough, Russian Professor Predicts End of U.S. *Wall Street Journal* . Moscow, Russia.
[18] Buchanan, P. J. (2007). *Day of Reckoning: How Hubris, Ideology, and Greed are Tearing America Apart.* New York: St. Martin's Press.

2.7 Tempering the Cyber Threats

Arguably, some of these challenges are nothing new. When the telegraph and telephone were introduced in the early 20th century, many people became anxious, fretting over the looming disasters based on perceived abilities to falsify information passed over the wires. The belief was bad actors would be able to bring down the entire U.S. economy, disrupt military operations, etc.[19] These dire warnings of the past sound eerily familiar to today's apocalyptic warnings. While these doomsday scenarios did not materialize, precautions were taken to mitigate the risks. And common sense indicates we must do the same today.

2.8. Assessment

The risks in competition are real and on-going, so we must adapt. We must consider the intersection of the threats, vulnerabilities and resources weighed against the probability of occurrence and potential impacts. Hostile armed conflict scenario probabilities among stable, rational state actors is likely low; however, responses via other means places the stability of any state at risk, and one for which any prudent actor must be prepared. Altogether though, militarization of Cyberspace or information security is not in line with U.S. history. And as such, we must find a way to properly govern these issues.

Probabilities of high impact, low frequency events require prudent steps to mitigate risks. And, proper attention must also be paid to low impact, high frequency events which occur daily in significant numbers. Some competitors have determined other ways, such as asymmetric or unrestricted warfare, are more desirable given their inability to directly compete militarily.[20] Hopefully, these academic statements are not promoting hostile competition, but exploring possible options in the event of hostilities. Even so, the U.S. must focus its efforts prudently. Additionally, we must all be cognizant non-state actors like terrorists and criminals may use hostile acts in Cyber as a means to raise their level of power.

---

[19] Lawson, S. (2011, January). BEYOND CYBER DOOM: Cyberattack Scenarios and the Evidence of History. Mercatus Center at George Mason University.

[20] Liang, Q., & Xiangsui, W. (1999). *Unrestricted Warfare.* PLA Literature and Arts Publishing House.

While vulnerabilities exist to physical infrastructures, the vulnerabilities to/from information security, especially within the Cyber Domain, arguably, pose greater risks to stability for a nation-state at all levels. These issues have brought forth various schools of thought brought forth military concepts like the information engineering, net-centric warfare, information warfare, and even Wisdom Warfare.[21,22,23] And, while we are adjusting U.S. capabilities to our perceived environment, we must be cognizant our competitors will review our work and adjust accordingly.

Collectively, the information problem in Cyber seems untenable. These issues challenge any nation-state seeking to maintain stability. Based on existing and emerging threats, the networked nature of today's world, and discussions of leveraging the power of the whole of government, some have discussed changing the National Security structure implemented in 1947.[24] Just as the U.S. has done in the past, we should examine the realignment of Departmental responsibilities in the modern world. From a national perspective to address some of these issues, current government and industry players are working to identify the critical infrastructures necessary to defend today.[25] However, the current collective effort is not sufficient.

[21] Wood, R. J. (1995, April). Information Engineering: The Foundation of Information Warfare. Maxwell AFB, AL: Air University.
[22] Vice Admiral Arthur K. Cebrowski, U. N. (1998). Network-Centric Warfare: Its Origin and Future. *US Naval Institute Proceedings* (p. 10). US Navy.
[23] Murphy, E. F. (1996, April). Information Operations: Wisdom Warfare for 2025.
[24] Goldgeier, J. (2010). *Reforming the National Security Process in a Globalized World.* Strategic Studies Institute.
[25] Alexander, K. B. (2010). Statement of Gen Keith B Alexander to Before the House Committee on Armed Services. (H. C. Services, Interviewer)

III. Current National Efforts

"I believe there are more instances of the abridgment of the freedom of the people by gradual and silent encroachments of those in power than by violent and sudden usurpations." ~ James Madison, 1788

3.1 General

This chapter seeks to examine current defined national goals and associated challenges. Given the importance of information to wielding power, we then next examine the ways the nation is currently working to ensure information CAI.

3.2 National Goals

3.2.1 The National Security Strategy

Strategy is defined in terms of Ends, Ways and Means [ends = ways + means]. The 2010 U.S. National Security Strategy's (NSS) four national interests are security, prosperity, values and international order with a central theme of stability.[26] The British NSS centers on the same theme.[27] And, we find the same theme in pronouncements from Chinese leadership and other countries.[28] A key question with respect to Cyber is how do we coordinate the complex national and international issues that affect so many nations?

For security, the NSS stresses strengthening security and resilience at home; disrupting, dismantling and defeating Al Qa'ida and its violent extremist affiliates; use of force (when necessary); reversing the spread of nuclear and biological weapons and securing nuclear materials; advancing peace, security and opportunity in the greater middle east; investing in the capacity of strong and capable partners; and securing cyberspace as the priorities to achieve our national goals. For prosperity, the NSS

[26] White House. (2010, May). National Security Strategy.
[27] Prime Minister. (2010). A Strong Britian in an Age of Uncertainty: The National Security Strategy. London, England.
[28] Yesui, Z. (2010). China's Concept Paper as presented to the UN. New York, New York.

stresses strengthening education and human capital; enhancing science, technology, and innovation; achieving balanced and sustainable growth; accelerating sustainable development; and spending taxpayers' dollars wisely. For values, the NSS pushes strengthening the power of our example; promoting democracy and human rights abroad; and promoting dignity by meeting basic needs. And for international order, the NSS stresses strong alliances, building cooperation with other 21st century centers of influence; strengthening institutions and mechanisms for cooperation; and sustaining broad cooperation on key global challenges. All of the ways discussed in the NSS have information security at their foundation. However, a deeper look shows the NSS outlines investing in people and technology and strengthening partnerships as the ways forward. But, how do we do this nationally?

3.2.2 The National Defense Strategy

In 2008, Secretary Gates issued the National Defense Strategy (NDS) with the goals of defending the homeland, winning the long war, promoting security, deterring conflict and winning the nation's wars. Just as we have with air, land and water, how do we begin to separate the civilian population from military activities on the Internet? More importantly, can we?

While the 2008 NDS is older than the 2010 NSS, the core language is very similar. The focus of the NDS ways are shaping the choices of key states; preventing adversaries from acquiring or using weapons of mass destruction; strengthening and expanding alliances and partnerships; securing U.S. strategic access and retain freedom of action; and integrating and unifying our efforts…. The ways outlined in the NDS are obviously focused to the department mission; however, we see again see information security as a key underlying linchpin. These goals outlined in the NDS, at deeper levels, talk around Cyber, but offer no insight into ways forward.[29] In fairness, the recent actions of the Services to re-organize their respective Cyber forces are critical steps for the Department to address its challenges.

[29] Department of Defense. (2008, June). National Defense Strategy.

3.2.3 The National Military Strategy

In 2011, Admiral Mullen issued the National Military Strategy (NMS) with the goals of countering violent extremism, deterring and defeating aggression, strengthening international and regional stability, and shaping the future force. As with the NDS, the same questions apply.

The NMS then focuses on countering violent extremism; deterring and defeating aggression; strengthening international and regional security; and shaping the future force. Information security is a key to maintaining stability, but must be balanced with the potential for prosperity and the power of sharing and collaboration. The NMS discusses developing deterrence principles, having STRATCOM collaborate with government agencies, training and exercising in degraded Cyber environments, and instructs focus on securing the ".mil" top level domain name.[30] While the military is addressing some of the needs internally, we still lack definition of any solid way forward nationally.

3.3 National Challenges

3.3.1 National and International Cooperation

The global reach of the Internet, a network of networks, leads some to assume it is ungovernable since it reaches beyond national borders. Similar challenges existed when we moved into the air and space domains. Regardless, some are pushing for State responsibilities for this growing problem.[31] Realistically in Cyber, the systems reside in some physical space within some country's jurisdiction. So does the information therein. Just as with the concept of a global commons, public facing Internet access can be traversed by anyone globally within milliseconds, presenting challenges to international cooperation. Just as we have rules and protocols for people, mail, air traffic, shipping, vehicles, patents, and property rights, so too must we consider how we govern Cyber internationally, nationally and locally. Given the threat is similar for all nation-states, the need for global cooperation on this topic seems logical,

[30] Department of Defense. (2011, February 8). National Military Strategy.
[31] Shackleford, S. J. (2010). State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. *Conference on Cyber Conflict Proceedings 2010* (p. 12). Tallinn Estonia: CCD COE.

even for hostile actors. However, we should start with cooperative partners if others do not want to act. This means building alliances to agree upon lexicon, establishing legal parameters, and sharing of information should remain high atop the priority list.

Since the threats expose all nation-states to a wide variety of risks, it is prudent to reach an international agreement on rules and protocols of Internet usage. Given the scope of the problem, it is reasonable to assume a partnership between government, industry and users is necessary. The answer cannot lie at the feet of government alone. Nor can we ask the industries, the Internet Service Providers (ISPs) and Content Providers (CPs), and other capability providers to handle the burden alone.

Higher impact national and insurgency threats are much less probable than organized and individual crimes. However, lower probability national events would have a much more significant impact. This is where a comprehensive, layered sensing approach similar to public health and defense in depth strategies between government, industry and users may be the best course of action, reducing, but not eliminating, risks in all discussed threat categories. [32,33,34]

3.3.2 Definition Agreement

It is prudent to reach international agreement on key Cyberspace definitions. And, we need to reexamine the language used in information and spectrum warfare to ensure common lexicon. Given the wide array of risks posed by electronic systems and the Internet, it is prudent to agree on what critical national infrastructures are to separate what nation-states or others deem legitimate attacks while performing due diligence to keep civilians relatively safe. Language ambiguity with phrases like Cyber Attack may cause inappropriate responses from nation-states, potentially raising issues of instability. These definitions also help nation-states determine who should respond, law enforcement or militaries,

---

[32] Bryant, M. D. (2008). Layered Sensing: Its Definition, Attributes, and Guiding Principles for AFRL Strategic Technology Development. Wright Patterson AFB, OH.

[33] Rice, M., & Butts, J. e. (2009). Applying Public Health Strategies to the Protection of Cyberspace. Tulsa, OK.

[34] Rice, M., & Butts, J. (2010). An Analysis of the Legality of Government-Mandated Computer Inoculations. *International Journal of Critical Infrastructure Protection* , p. 11.

and how nation-states respond to given threats on Internet systems. Definitions are important as we work to prevent crimes and attacks, negate their effects, and protect our critical infrastructures and citizens.

Determining a response to a particular Cyber event is challenging in the current international environment. Issues like Jus Ad Bellum, where UN Article 1 defines an act of aggression, UN Article 2 outlines the threat or use of force, and Article 51 defines an armed attack, and which collectively leave issues related to Cyber completely ambiguous. Jus In Bello lays out the Law of Armed Conflict defining necessity and proportionality, limitations, methods, and distinctions between combatants and civilians; however yet again, issues of Cyber remain ill defined. UN Article 58 directs nation-states to segregate civilians and associated objects from military targets to spare them from attack.[35] So the efforts to define and identify critical infrastructures and clarify other language are important, but must be done and agreed upon at a national and an international level. And, any nation's response must be based on some reasonable attribution of a given attack. So an international effort to agree on the rules and protocols of identification, authentication and monitoring become very important.

3.3.3 Information Security

A well-known hacker, Kevin Mitnick, stated anyone thinking there is a true solution to information security is buying into an illusion.[36] Many practices and technologies from the Information Security community have made getting information harder, but, generally, smart adversaries will figure out a way to get the information.[37,38] This is usually due to simple human errors of one degree or another.

One key factor to consider with information though is the relatively transient time value. For example, we may have information we absolutely do not want to share today, but, tomorrow, who cares who knows it. Sometimes the value of information is not in protecting it, but sharing it. A prime

[35] Kanuck, S. (2010). Sovereign Discourse on Cyber Conflict Under International Law. *Texas Law Review* , 27.
[36] Mitnick, K., & Simon, W. L. (2002, October 4). Controlling the Human Element of Security: The Art of Deception. John Wiley & Sons.
[37] Pipkin, D. L. (2000). Information Security: Protecting the Global Enterprise. Prentice Hall PTR.
[38] Skoudis, E., & Liston, T. (2006). Computer Hack Reloaded. Pearson Education, Inc.

example of this is the use of a simple modern cell phone. You can find your position, that of a friend, restaurants around you, social reviews of those restaurants, etc. all in a matter of seconds while talking with them about options for dinner. This simple example obviates situations on the battlefield and numerous other situations. As such, there is a fine line between the risks of sharing information and securing information.

In strict terms of securing information with network operations, typical responses involve building strong defensive capabilities similar to the middle age castles. The slow, plodding hack-patch cycle likely means a level playing field globally since most use very similar systems and software. Highly skilled practitioners excel in various areas, but the art and science of network operations challenges the best practitioner since what works today may not work tomorrow. The key difference in this battle-space lies in the level of training and experience of the operators and designers. Thus, the need to ensure proper training and certifications for those working in Cyber.

3.3.4 Attribution Challenges

Some posit we cannot provide attribution due to spurious actors falsifying authentication in the Cyber Domain. While true to a degree, this argument prevents us from taking any prudent action. As with FBI crime management, we will never eradicate crime. However, there are various methods or ways help drive the crime rate down to manageable levels. Figure 9 depicts the national crime rate in several areas.[39] The intent here is to show a declining rate of crime and actual number of events with an increasing population due to a variety of reasons (e.g. economic, law enforcement tactics). This daily, steady crime state is similar the continuous criminal events in Cyber. As such, we then must watch for spikes in activity in a given area to know where to focus our attention and resources. Persistent

[39] Derived from Federal Bureau of Investigation. (2009). *Federal Bureau of Investigation*. Retrieved March 23, 2011, from Crime in the United States: http://www2.fbi.gov/ucr/cius2009/data/table_01.html.

improvements in capabilities and techniques make it harder for low-level criminals to be effective, leaving a smaller pool of truly bad actors for authorities to focus on.

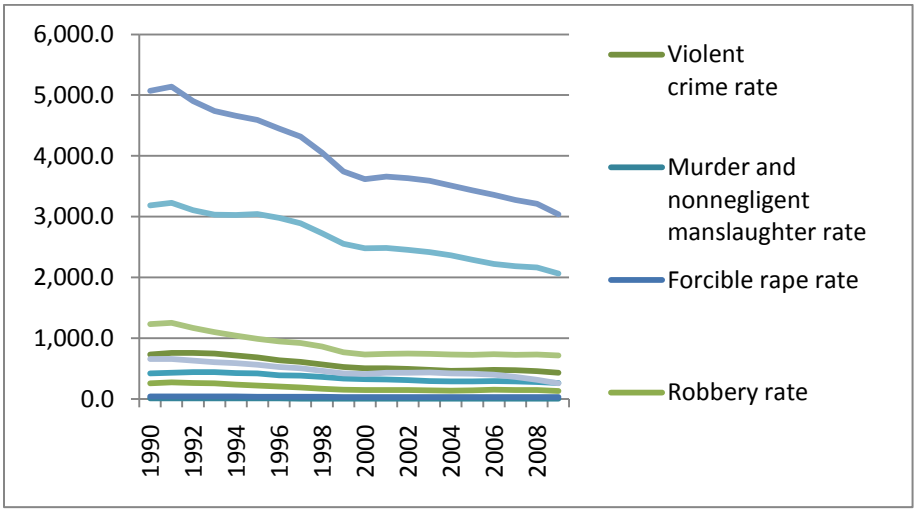


Figure 1: FBI Crime Statistics

The British have defined four Cyber threat categories: state-sponsored cyber attacks, ideological and political extremism, serious and organized crime and lower-level/individual crime.[40] Britain's four categories help categorize threats which helps clarify who should respond to an activity (e.g. criminal activity vs. nation-state attack).

To enable attribution, the technical means are available (e.g. fingerprinting computers, behavioral monitoring, stronger authentication/trust systems), but issues of costs, legalities and political concerns must be dealt with.[41] However, some techniques like fingerprinting and behavioral monitoring by government agencies may raise many questions among general Internet users, though these ways may be useful on more secure systems and critical infrastructures. Use of stronger identification and

[40] Cornish, P. R. (2009). *Cyberspace and the National Security of the United Kingdom, Threats and Responses.* London, England: Chatham House.
[41] Robinson, D. J. (2010). *Cyber Based Behavioral Monitoring.* Hanover, New Hampshire: Thayer School of Engineering.

authentication techniques do offer a way to reduce may issues we face on the Internet. However, Schneier argues the costs do not outweigh the benefits nationally.[42] Thus, there is a government wide effort to strengthen our intra-governmental trust relationships in Cyber by extending the Public Key Infrastructure using identification cards for critical infrastructures.[43] As Schneier argues out, however, every technology is eventually subverted. Thus, a policy promoting periodic evolution of software and technologies is warranted. While this evolution already occurs naturally in business cycles, there are many cases of very old technologies in vital organizations.

A debate in any government-industry-user alliance is who does what. Some lessons are available from telecom and airline examples from the past where government sets policy and regulation with industry providing the services to the users. There is also a fine line between government regulation, markets and innovation. Starting with a cooperative global approach on identification and authentication policy is good way to manage the daily criminal activity and other activity. We need to raise the standard for identification and authentication periodically to reduce overall risks. For the general Internet, this would likely be too onerous.

3.3.5 National Monitoring

Government monitoring raises the specter of Big Brother and police states, especially where issue like the Foreign Intelligence Surveillance Act (FISA) and privacy issues cross. Technologies like fingerprinting and behavioral monitoring would especially heighten this concern if implemented by the government.[44,45,46,47] However, this should not be the case for classified networks or critical infrastructures. For the general Internet outside of government and the Federal Critical Infrastructure,

---

[42] Schneier, B. (2008, February 23). *Bruce Schneier*. Retrieved April 20, 2011, from Bruce Schneier: Security at What Cost?: http://www.schneier.com/essay-207.html

[43] Temoshok, D. (2007). *Federal Identity Management and the Federal PKI*. Retrieved from www.kansas.gov/pki/clinic/presentations/federalPKI.ppt

[44] Joel, A. W. (2010). Choosing Both: Making Technology Choices at the Intersections of Privacy and Security. *Texas Law Review* , 15.

[45] Sales, N. A. (2010). Mending Walls: Information Sharing After the USA PATRIOT Act. *Texas Law Review* , 60.

[46] Graves, L. (2010). The Right to Privacy in Light of Presidents' Programs: What Project MINARET's Admissions Reveal About Modern Surveillance of Americans. *Texas Law Review* , 50.

[47] Banks, W. C. (2010). Programmatic Surveillance and FISA: Of Needles in Haystacks. *Texas Law Review* , 35.

these type activities are likely best managed by industry, in this case, the ISPs, given the scope of activity. Government should consider means of empowering industry, ISPs, CPs and others, to monitor and terminate unlawful activities. We should also strengthen the identification requirements for users setting up accounts. We see strong analogs to this today where UPS, for example, now requires photo identification to mail a package.

Regarding monitoring, some interesting science is emerging which could be beneficial in terms of security. However, there are serious legal issues to be addressed. Hamil and Trusov, et al effectively lay out the rationale for the communication links between people, meaning they found patterns in how people share information.[48,49] Drozdova and Samoilov found similar predictive capabilities when observing traffic flows within social networks. They found potential clues regarding threats, as shown in Figure 2, by noting an increase network chatter leading up to an event.[50] This predictive capability was also found by Gruhl, et al.[51] And as such, the potential to monitor network activity levels, without compromising privacy, may be of benefit to national security. However, these remarkable advances are not without complex legal challenges.

[48] Hamil, J. T. (2006). Analysis of Layered Social Networks. Air Force Institute of Technology.
[49] Trusov, M., Bodapati, A., & Bucklin, R. E. (2010). Determining Influential Users in Internet Social Networks. *Journal of Marketing Research* . Vol 47 (4), 643-658.
[50] Drozdova, K., & Samoilov, M. (2010). Predictive analysis of concealed social network activities based on communication technology choices: early-warning detection of attack signals from terrorist organizations. University of California.
[51] Gruhl, D., Guha, R., Kumar, R., Novak, J., & Tomkins, A. (2005). The Predictive Power of Online Chatter. *KDD-2005* .

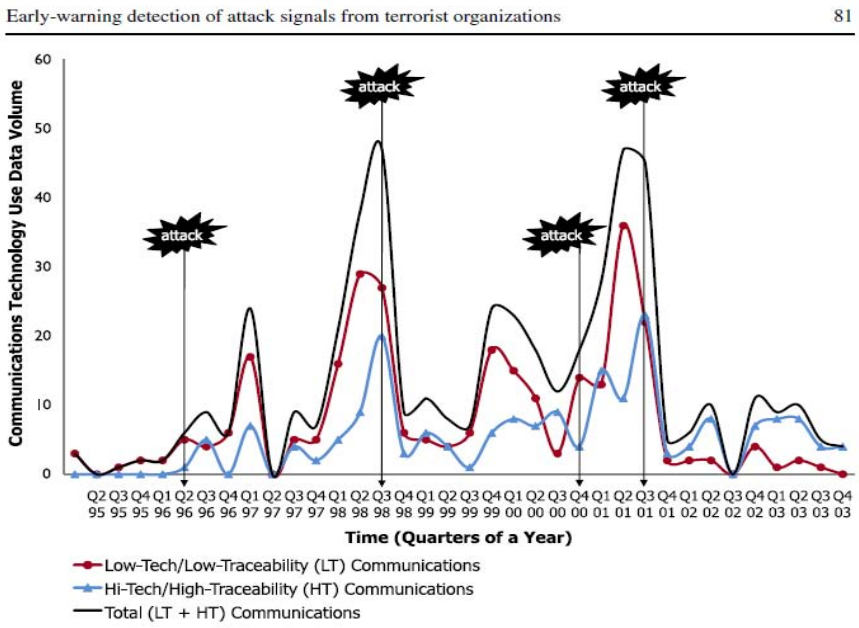


Figure 2: Early-warning detection of attack signals

3.3.6 National Intelligence Discussion

On the intelligence side, we have seen significant attempts at restructuring the intelligence apparatus, to include opening the sharing of intelligence and creation of a Director of National Intelligence. While some challenges have been posed to sharing information (e.g. WikiLeaks) the predominant impact has been overwhelmingly positive. This is evidenced by the lack of events in recent years upon U.S. soil. Additionally, there is great opportunity filtering and fusing related data obtained from space, air, surface, subsurface systems and computer network capabilities to support general reconnaissance, tracking, and identification of nefarious actors. However, there are legal and, in some cases, classification issues that must be addressed. Thus, we must consider if this must be done and, if so, how could it be done within constraints of U.S. law. Several of these issues arose with FISA and the Patriot Act. Given the U.S. is defining critical infrastructures; we should examine the value of sharing intelligence information regarding critical infrastructure by similar means.

3.4 Current Governance

Today, the Department of Homeland Security (DHS) per Homeland Security Presidential Directive 7 (HSPD – 7), *Critical Infrastructure Identification, Prioritization, and Protection,* leads federal Cyberspace efforts.[52] Within DHS, the National Protection and Programs Directorate oversees the Office of Cyber Security and Communications. And, therein is the National Cyber Security Division (NCSD). According to the NCSD website, the mission is to "work collaboratively with public, private and international entities to secure cyberspace and America's cyber assets." However, the two key objectives for NCSD are: 1) "to build and maintain an effective national cyberspace response system", and 2) "to implement a cyber-risk management program for protection of critical infrastructure."[53] NCSD oversees U.S. Computer Emergency Response Team (CERT), the National Cyber Alert System, and the National Cyber Response Coordination Group. Collectively, these entities analyze cyber threats, coordinate information, and coordinate national response efforts in the event of a major scenario.

The Department of Commerce has the National Institute of Standards and Technology (NIST) and the National Telecommunications and Information Administration (NTIA). The Department of Defense has reorganized recently with the creation of CYBERCOM while parting a fine line with the National Security Agency (NSA). There are also numerous applicable civilian agencies overseeing various aspects of Internet governance as described by Harold Kwalwasser in Figure 10.[54]

---

[52] White House. (2003, December 17). Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection.

[53] Department of Homeland Security. (n.d.). *National Cyber Security Division*. Retrieved 2011, from Department of Homeland Security: http://www.dhs.gov/xabout/structure/editorial_0839.shtm

[54] Kwalwasser, H. (2009). Internet Governance. In F. D. Kramer, S. H. Starr, & L. K. Wentz, *Cyberpower and National Security.* Potomoc Books, Inc.

ORGANIZATION	SUBJECT MATTER JURISDICTION
Internet Corporation for Assigned Names and Numbers, which includes functions referred to as the Internet Assigned Numbers Authority (ICANN)	Supervises the Domain Name System, allocates Internet protocol address space, and oversees the root zone servers that provide basic finding information for Internet traffic.
Internet Society and related organizations: Internet Engineering Task Force (IETF), Internet Engineering Steering Group, and Internet Architecture Board	Develops standards for operation of Internet and its overall architecture
World Wide Web Consortium	Develops standards for the World Wide Web
International Telecommunications Union (ITU)	Develops standards for telecommunications, including interface of Internet and telecommunications systems
Organization for Economic Cooperation and Development, European Union, Council of Europe, United Nations agencies	Ad hoc policy development on issues of critical interest to members
National governments acting individually or through joint agreements	Ad hoc policy development chiefly related to cyber crime, use, and commercial regulatory issues
Institute of Electrical and Electronic Engineers, International Electrotechnical Commission, International Organization for Standardization	Standards for projects and for manufacturing and testing processes (operations of these entities relate only peripherally to the operation of the Internet itself)

Figure 3: Internet Governance Organizations

3.5 Assessment

Today, Cyber plays a very strong role in the movement of information. The current and future economic opportunities offered by cyberspace systems leveraging information stagger the imagination. As with maritime trade, the path to future prosperity relies on open access, engagement and cooperation among friends and allies in the global cyberspace commons. Conversely, the growing U.S. dependence on these critical, yet vulnerable systems has led to discussions of dire national scenarios occurring with no strategic warning. Various actions (e.g. the Chinese anti-satellite test, Estonia, organized crime and espionage), while overly hyped, only serve to lend credence to the warnings.

Typically, the Federal Government manages national capabilities such as highways, railroads, pipelines, motor carriers, maritime, aviation, power, and energy with focused administrative agencies that develop minimum regulatory guidance, coordinate national and international policies, and develop standards for technology, training and certifications. Yet, government organization today appear to only focus on federal response issues without developing any real regulatory guidance.

While the military is taking prudent steps to address these concerns, the collective national effort, according to McCarthy, et al. in *Cyber Power and Critical Infrastructure Protection: A Critical Assessment of Federal Efforts*, suffers from irresolute and inconsistent leadership. Joeli Field supports this assertion by exploring several alternatives. One alternative was maintaining status quo. The challenges found include cultural biases and gaps, lack of coordination, absence of leadership and accountability, and low priority for cyber security. Field also references a 2009 GAO Report stating "independent efforts will not be sufficient" and "roles and responsibilities need to be assigned to eliminate duplication of effort". Other alternatives were explored including empowering an office within the White House and the creation of a national cyber security agency. After weighing the pros and cons, the creation of a national security agency to address the many issues was recommended as the best alternative.[55,56] However, this would unduly place emphasis on security over prosperity. As such, we must find a way to balance the needs of security and prosperity.

Since no single entity will ever control cyberspace, finding an appropriate model for a government, industry and users partnership is necessary. Given the myriad of issues, the time has come to create a national civilian agency, beyond a singular Cyber Czar or the current mix of national offices, to develop and coordinate national cyberspace efforts, regulatory guidance, standards, etc. Building upon

---

[55] Field, Joeli. (2010, September 8). *Cybersecurity: Division of Responsibility in the U.S. Government.* Retrieved May 13, 2011, from http://www.nsci-va.org/CyberReferenceLib/2010-09-18-Cybersecurity-Division of Responsibility in the US Government-Joeli Field.pdf

[56] Government Accountability Office. (2009). *President's Cyberspace Policy Review.* Retrieved Sep 4, 2010, from http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

McCarthy and Field, the need to explore a relevant construct to govern Cyber while balancing prosperity and security emerges. The complex challenges require focus and strong commitment to resolving them.

IV. EXISTING CONSTRUCTS

4.1 General

This chapter explores how the U.S. currently governs other complex constructs by providing an overview in analogous terms.

4.2 Federal Aviation Administration

Given the complexities of Cyber, it is assumed neither complete commercial control or government control is viable. The issue, then, becomes finding a useful construct to government, industry, user alliances. Interestingly enough, these models exist where commerce is heavily involved (e.g. in the air, land or maritime domains). There is the Federal Highway Administration (FHA), Maritime Administration, and several others. In as much, the Federal Aviation Administration (FAA) provides such a model, bringing together government, industry and users for infrastructure (e.g. air traffic control (ATC), aircraft, airports) and people (e.g. training, licensing and certification). Similarly, the International Civil Aviation Organization (ICAO) coordinates global policy and regulations.

4.2.1 A Brief History

The National Airspace System (NAS) has evolved today into approximately 690 ATC facilities providing tracking, monitoring, control and communications services. There are approximately 19,800 airports and 11,120 air navigation facilities. Collectively, FAA employees provide ATC, flight services, security, field maintenance, certification, system acquisitions, and other services. However, this complex system of systems did not just appear overnight. Various activities led to the Congress passing the Air Commerce Act of 1926, which was the government's initial hand in regulating civil aviation. The Department of Commerce was charged with setting rules and regulations, licensing, certifications and creating a system to ensure the safe movement of aircraft. As aviation evolved, Congress passed the

Federal Aviation Act of 1958 creating an independent Federal Aviation Agency, which was later aligned under the Department of Transportation in 1967.[57]

Similar to the evolution of Cyber, Figure 4 depicts the evolution of airways across the U.S. over the years. The irony of this visual is inescapable when one considers the development of the Internet. Due to the complexity of routing traffic along the airways, many rules, regulations and procedures were developed to separate aircraft from each other.

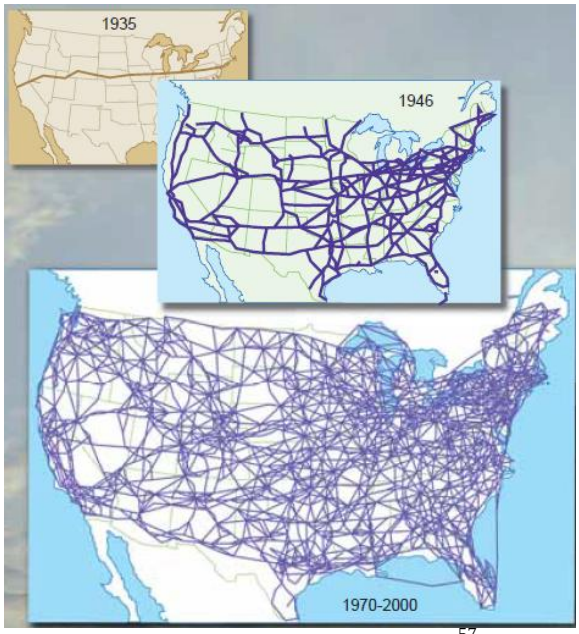


Figure 4: U.S. Airway Routes[57]

Today, one finds traffic densities as depicted in Figure 5. However, keeping so many aircraft separated and people safe is no easy task. A series of functions must happen to ensure government, commercial and private users to operate safely within the system. And, if there is a threat or emergency, authorities can track the issue, as necessary. The intent here is to show there are ways to depict national traffic densities

[57] Federal Aviation Administration. (n.d.). *IFR Operations in the National Airspace System.* Retrieved 2011, from http://www.faa.gov/library/manuals/aviation/instrument_procedures_handbook/media/CH%2001a.pdf

by sharing information from across the FAA's ATC facilities. These simple observations helps decision makers determine how to respond to weather phenomenon, emergencies or other issues.

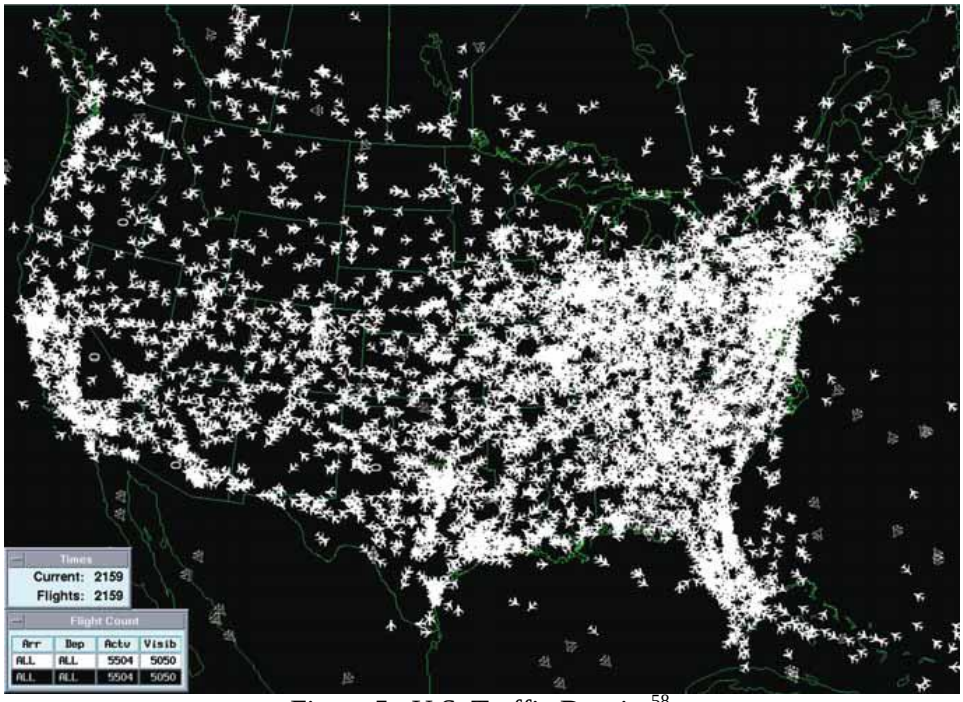


Figure 5: U.S. Traffic Density[58]

4.2.2 An Operational Framework

To provide various services to pilots operating in the ATC system, many different things must happen. It starts with the design of aircraft, airports and other support facilities, to include a certification process. People are trained and certified to various standards. And, there are many more facets of what could be deemed passive, defensive actions to ensure aviation safety.

[58] Federal Aviation Administration. (n.d.). *IFR Operations in the National Airspace System.* Retrieved 2011, from http://www.faa.gov/library/manuals/aviation/instrument_procedures_handbook/media/CH%2001a.pdf

There are service providers who provide active, defensive support to ensure safety, the air traffic controllers. Figure 6 depicts a notional flight between two airports. The purpose here is to very generally describe the services provided by air traffic controllers without complicated and lengthy details.

A pilot typically departs one airport under the control of the air traffic control tower. The tower controller transfers the pilot to a departure controller after a couple miles. This departure controller will guide the pilot for 20 or so miles, then possibly transfer the pilot to an en route control facility. Depending on the length of the flight, the pilot may be transferred between several en route controllers who may be working in different facilities. Once near an airport, the en route controller will then turn the pilot over to an arrival controller who monitors the pilots approach. Once near the airport, the arrival controller turns the pilot over to the destination tower. During this flight, the pilot likely flew through a variety of different airspace types discussed in 4.2.5. In each airspace segment, there were a variety of services provided and rules to operate therein. There were different infrastructure and equipment standards (e.g. radars, transponders, radios, aircraft), operational standards (communication requirements, identification codes, instructions), training standards (e.g. commercial pilot vs. visual flight rules only, instrument flight rules), and services provided (e.g. separation, routing around weather, traffic advisories). A look deeper exposes maintenance requirements, facility standards and a host of other minimum regulatory standards to ensure a common understanding for those operating the system and those using the services provided by the system. While aviation purists will likely see this as overly simplified example, most will wonder how this relates to Cyber. This is discussed in the next chapter to keep topics focused.

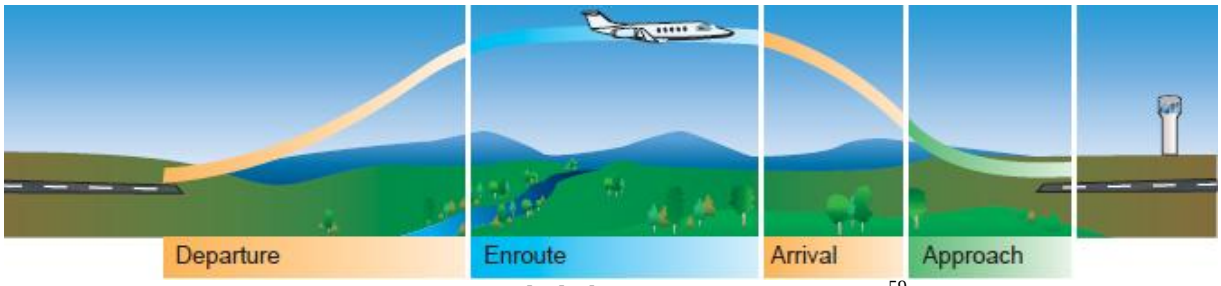


Figure 6: Notional Flight Between Two Airports[59]

4.2.3 A Regulatory Benchmark

Given the history of the FAA, many key components of regulation have been developed, providing analogous examples to consider as shown in Table 1. Stepping through Table 1's sample FAA Regulatory Titles, we find common ground with Subchapter A Definitions. Definitions, as discussed, are very contentious and vary widely just as they did at the beginning of aviation. Over the years, the definitions have solidified with modifications from time to time. But, there is a common reference nationally for people to use. Subchapter B is self-explanatory given basic procedures are outlined through which government, industry and users coordinate regulatory guidance. The need to establish rule-making guidance is necessary. Most government agencies leverage the Federal Register as a means to allow public comments prior to establishing rules. Subchapter C governs certification standards for aircraft. Depending on the level of operations and relative importance, various regulations are laid out to ensure overall safety. Subsection D governs the level of required training and certification to operate in the various segments of airspace. Subsection E is discussed in 4.2.5. Subsection F covers basic operating rules in the various segments of airspace, special air traffic rules, operating on instruments, and security control of air traffic. For example, ATC generally heavily monitors and controls pilots flying on

[59] Federal Aviation Administration. (n.d.). *IFR Operations in the National Airspace System.* Retrieved 2011, from http://www.faa.gov/library/manuals/aviation/instrument_procedures_handbook/media/CH%2001a.pdf

instruments regardless of where they are operating. This establishes what systems are required, how to operate and what services, in general, to expect. Subchapters G and H essentially establish minimum guidelines for commercial entities and schools. Subsections I and J establish rules to operate airports and navigational facilities.[60]

These regulations apply to government, commercial and private operators and users. Commercial and private entities provide the bulk of aviation service needs, thus a strong partnership between government, industry and private entities is essential and practical. A focused government administration, however, provides the necessary leadership nationally and internationally to coordinate with. While the FAA performs some security functions, several of the larger security issues reside with the Department of Homeland Security (DHS) and the Department of Defense (DoD). For example, DHS handles airport security. And, DoD operates the North American Aerospace Defense Command (NORAD).

[60] Adopted: http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?sid=cff1993aa3f46dd3752c9f90000e6d33&c=ecfr&tpl=/ecfrbrowse/Title14/14tab_02.tpl

Table 1: Code of Federal Regulations, Title 14, Aeronautics and Space, Chapter 1 Sample Titles[61]

Subchapter	Part	Title
A – Definitions	1	Definitions and Abbreviations
	3	General Requirements
B – Procedural Rules	11	General Rulemaking Procedures
	13	Investigative and Enforcement Procedures
C – Aircraft	21	Certification Procedures for Products and Parts
	23-35	Various Airworthiness Standards
	43	Maintenance, Preventive Maintenance, Rebuilding and Alteration
	45	Identification and Registration Marking
	47	Aircraft Registration
D – Airmen	61	Certification: Pilots, Flight Instructors, and Ground Instructors
	63	Certification: Flight Crewmembers other than pilots
	67	Medical Standards and Certification
E – Airspace	71	Designation of Class A, B, C, D and E Airspace Areas… Routes…Reporting Points
	73	Special Use Airspace
F- Air Traffic and General Operating Rules	91	General Operating and Flight Rules
	93	Special Air Traffic Rules
	95-97	IFR Altitudes and Standard Instrument Procedures
	99	Security Control of Air Traffic
G – Air Carriers and Operators for Compensation or Hire: Certification and Operations	110	General Requirements
	119	Certification: Air Carriers and Commercial Operators
	121	Operating Requirements: Domestic, Flag, and Supplemental Operations
	125	Certification and Operations…
	129	Operations: Foreign Air Carriers and Foreign Operators of U.S. Registered Aircraft Engaged in Common Carriage
	139	Certification of Airports
H – Schools and Other Certified Agencies	141	Pilot Schools
	142	Training Centers
	145	Repair Centers
	147	Aviation Maintenance Technician Schools
I – Airports	153	Airport Operations
	157	Notice of Construction, Alteration, Activation, and Deactivation of Airports
J – Navigational Facilities	170	Establishment and Discontinuance Criteria for Air Traffic Control Services and Navigational Facilities
	171	Non-Federal Navigation Facilities

[61] Adopted: http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?sid=cff1993aa3f46dd3752c9f90000e6d33&c=ecfr&tpl=/ecfrbrowse/Title14/14tab_02.tpl

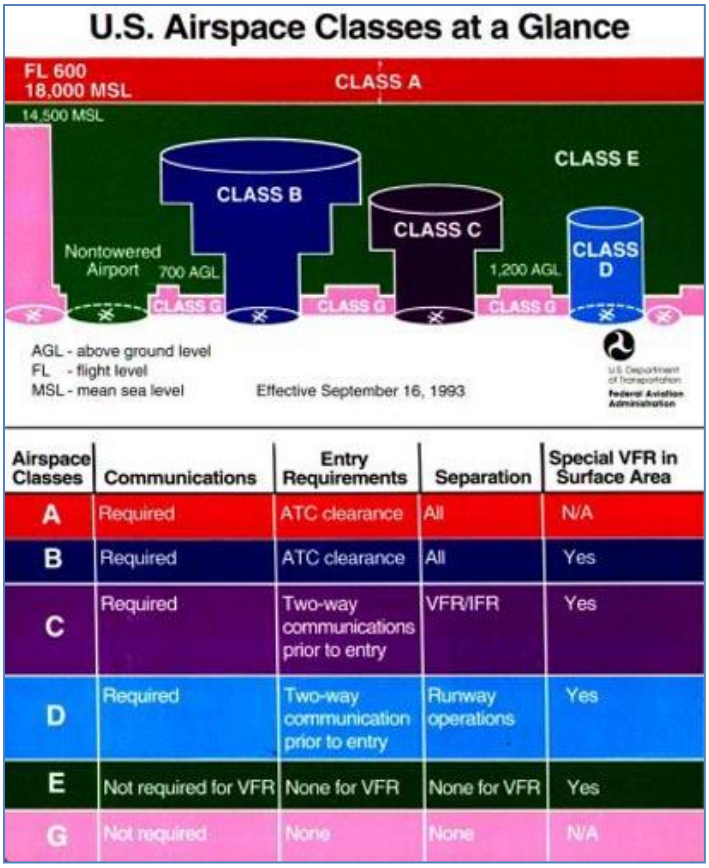
4.2.4 A Commons Benchmark

Jasper lays out a definition for the Global Commons used widely in air, maritime and space discussions. "The Global Commons are those areas that are used by multiple nations and private industries, and yet are not controlled by any single nation or private entity. They include international waters, international airspace, cyberspace and outer space. Since so many different actors operate within these shared spaces, including the U.S. military and its allies, regulation and protection of these areas becomes extremely complex." Within this definition, a state's territory over water and air extends up to 12 nautical miles from its shores; however, foreign entities are allowed innocent passage.[62] It is the phrase - allowed innocent passage - that is important as we move forward in the conceptual adaptation of a commons in cyberspace.

4.2.5 An Airspace Analogy

Given the vast expanse of air the FAA has to govern within the U.S., airspace is divided into segments as shown in Figure 7 below. Additionally, very similar rules have been adopted internationally, which are governed by the International Civil Aviation Organization (ICAO). In essence, there are different rules for identification, monitoring, training and certification, and equipment standards developed to balance operations (prosperity), security and safety in different segments. Different rules are built based upon different user groups. The issues faced in Cyber are similar to years ago when decision makers were trying to carve out rules for operating in the air.

[62] Jasper, S. (2010, March 15). Securing Freedom in the Global Commons. Stanford University Press.



Airspace Classes	Communications	Entry Requirements	Separation	Special VFR in Surface Area
A	Required	ATC clearance	All	N/A
B	Required	ATC clearance	All	Yes
C	Required	Two-way communications prior to entry	VFR/IFR	Yes
D	Required	Two-way communication prior to entry	Runway operations	Yes
E	Not required for VFR	None for VFR	None for VFR	Yes
G	Not required	None	None	N/A

Figure 7: Governance Comparison[63]

Figure 7 is a simple chart depicting the general rules to operate in national airspace. As a general rule, operations above 18,000 feet in Class A airspace are strictly governed, essentially requiring permission to be there, services are required, and adherence to stricter flying, equipment and training standards given the importance of activities in this airspace. Class E airspace has less stringent requirements, but services are available and not required unless flying on instruments. Class G airspace is

[63] Windsoar, D. o. (n.d.). *FAA Airspace Chart*. Retrieved April 28, 2011, from http://www.dukesofwindsoar.com/dukes.cgi?do=html&htmlfile=html/ppg_info/airspace_info.html

akin to the wild west, there are few, if any, rules. Moreover, with the FAA, there is Class B, C and D airspace with stricter rules around busier airports due to traffic densities and safety concerns.[64]

And, of course, the FAA also defines Special Use Airspace (not depicted on the chart), typically set aside for military or other purposes. There are prohibited, restricted, warning, alert and military operational areas established to alert general and commercial aviation users about places they cannot fly or should exercise extreme caution. Anyone trying to enter prohibited or restricted airspace is met with an appropriate response. In any case, these airspaces are monitored, when active. In some Special Use Airspace, the military is delegated responsibility for safety through a process called Military Assumes Responsibility for Separation or Aircraft (MARSA). Within the confines of this segment of airspace under these, the military is wholly responsible for safety and operations. However, if military traffic leaves this area civilian agencies provide services, as appropriate.[65]

4.3 North American Aerospace Defense (NORAD)

4.3.1 Brief History

On 16 Feb 1951, the DoD's Joint Chiefs of Staff approved a cooperative effort with Canada extending the Permanent Radar Net to consolidate the two control and warning systems into one system to provide for a common air defense. Through a variety of capability evolutions and activations, General L.S. Kuter began to advocate for the extension of the missile defense capability to detect threats from any direction to President Kennedy in 1962. In 1988, NORAD implemented a new Air Defense Identification Zone (ADIZ) around the periphery of North America. The ADIZ was an area of airspace where the ready identification, location and control of aircraft was required in the interest of national security. Presently,

---

[64] Federal Aviation Administration. (n.d.). *National Airspace System Overview.* Retrieved 2011, from http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/systemops/aaim/organizations/envir_programs/mase/media/ApxB_NAS_122805.pdf

[65] Federal Aviation Administration. (n.d.). *FAA Order 7110.65 Chapter 2, General Control.* Retrieved 2011, from http://www.faa.gov/air_traffic/publications/atpubs/atc/atc0201.html

NORAD is aligned under USNORTHCOM within the DoD and shares information with DHS in a partnership. With a long and distinguished history of protecting the U.S. and Canada, the current NORAD mission is:

> *In close collaboration with homeland defense, security, and law enforcement partners, prevent air attacks against North America, safeguard the sovereign airspaces of the United States and Canada by responding to unknown, unwanted, and unauthorized air activity approaching and operating within these airspaces, and provide aerospace and maritime warning for North America.*[66]

4.3.2 Monitoring and Surveillance

To accomplish this mission according to NORAD's website:

> *For the aerospace warning mission, the commander of NORAD provides an integrated tactical warning and attack assessment to the governments of Canada and the United States. To accomplish the aerospace control mission, NORAD uses a network of satellites, ground-based radar, airborne radar and fighters to detect, intercept and, if necessary, engage any air-breathing threat to Canada and the United States. In conjunction with its aerospace control mission, NORAD assists in the detection and monitoring of aircraft suspected of illegal drug trafficking. This information is passed to civilian law enforcement agencies to help combat the flow of illegal drugs into North America. The Command has developed an initial concept for implementing the new maritime warning mission.*[66]

This world-wide network of sensors provide NORAD an accurate picture of any airborne threat to Canada or the U.S. Some of the activities mentioned (e.g. drug trafficking monitoring) cause for very serious legal concerns based upon the Posse Comitatus Act of 1878, which limits the use of military forces in law enforcement on non-federal property unless specifically authorized by the constitution or Congress. The complexities of identifying friend from foe, monitoring missile launches from afar, and tracking inbound and outbound aircraft involve complexities that are hard to fathom. And, this is done with an integration of information feeds from a variety of sources.

---

[66] North American AeroDefense Command. (n.d.). *About NORAD*. Retrieved 2011, from http://www.norad.mil/about/index.html

4.4 National Transportation Safety Board (NTSB)

The mission of the NTSB is to promote transportation safety by:

- *maintaining our congressionally mandated independence and objectivity;*
- *conducting objective, precise accident investigations and safety studies;*
- *performing fair and objective airman and mariner certification appeals; and*
- *advocating and promoting safety recommendation.*[67]

The NTSB's history follows the same path of the FAA. However in 1974, Congress mandated creation of a completely independent agency to ensure objective and independent assessments. According to the NTSB website, this independence is a vital part of the balance of power between government and commercial activities and safety:

> *The NTSB's status as an independent federal agency sets us apart from other stakeholders in the transportation industry. Transportation companies are motivated by financial gain and many are ultimately accountable to their shareholders. Other government agencies, for example, the FAA, the Federal Railroad Administration (FRA), the Federal Highway Administration (FHWA), and the USCG have an official role in establishing and enforcing industry regulations. The NTSB has no such interests or obligations. Our most important stakeholder is the traveling public, and we are concerned with one principal objective, promoting transportation safety for the traveling public.*[67]

Insomuch, the NTSB has investigated over 132,000 aviation accidents to determine cause and assess any deficiencies in the system. Their recommendations are implemented, as possible, to improve the overall safety of the system.

[67] National Transportation Safety Board. (n.d.). *History and Mission*. Retrieved 2011, from NTSB: http://www.ntsb.gov/Abt_NTSB/history.htm

4.5 Discussion

What matters in this chapter is the conceptual understanding of how the U.S. governs its air domain with similar constructs developed internationally (e.g. ICAO). Where matters of prosperity appear to take precedence, the FAA works in close partnership with government, commercial and private entities to establish basic rules of the road. Where issues of national security take precedence, NORAD has been established to provide security. There are also other considerations such as passenger and infrastructure security at the airports provided by local authorities and DHS. And to balance the equation, the NTSB was created to provide critical, objective and independent assessments regarding the entire system. The real key is to understand significant leadership and unity of effort in the air domain has been enabled by focused organizations. McCarthy, Field and the GAO all concur, there is a need to provide leadership and focus in Cyber, but we must be careful not to place too much emphasis on security without providing balance.

V. A ROADMAP FORWARD

"The chief business of the American people is business. They are profoundly concerned with producing, buying, selling, investing, and prospering in the world." ~ Calvin Coolidge, 1925

5.1 General

This chapter explores a possible way ahead modeled on the existing FAA, NORAD and NTSB approach.

5.2 Federal Cyberspace Administration

We have reached a point where the development of a similar national construct to this existing FAA and ICAO partnership model makes sense for cyberspace governance. By carving out rules and regulations for given spaces on the Internet, it becomes much easier address the challenges. Various laws and regulations can be developed accordingly to address infrastructure, operational and training needs to ensure safe, innocent passage in Cyber. However, this still requires a national administration to coordinate the rules and regulations among government, industry, and people. This approach begins to resolve the national leadership challenges by providing a focused national organization to resolve national and international issues. Coordinating the economic partnerships between government, industry and users, nationally and internationally, requires focus. This focus is necessary when balancing the issues of prosperity and security needs regarding development of rules of engagement, neutrality agreements, customs and norms and other issues. As with the birth of the FAA, aligning the FCA with Commerce to promote prosperity may make the most sense. This would also help mitigate Big Brother concerns.

Arguments for creating a new organization under Commerce include the focus of mission, leadership and accountability, a central national office to coordinate national and international regulations including standards for certifications, training and operations in Cyber, and a focus on prosperity while

working with industry and users. And, a focused organization with trans-disciplined skills would foster innovative synergies for U.S. competitiveness.

Arguments against this approach include perceived risks to security given security is not the only focus of the organization and the time required for the organization to establish its culture and results.

5.2.1 Brief History

The National Cyberspace System (NCS), a notional term, has evolved today into an alliance of the willing from the commercial and private sectors with some governmental influence. Several civilian organizations outlined in Figure 3 have emerged to govern various aspects of the Internet. However, most government involvement in recent years has revolved around the Federal Critical Infrastructure construct. While HSPD – 7 moved the ball with respect to this particular topic, two key presidential directives have emerged. One is a 2004 National Security Policy Directive (NPSD) 38, *National Strategy to Secure Cyberspace*, and the other is 2008 NPSD 54, *Cyber Security and Monitoring*. Another key national document is the White House memo titled *The Comprehensive National Cybersecurity Initiative* of 2010.[68] Aside from several initiatives, DHS was assigned lead for coordinating national Cyber policy. This DHS focus would be like asking the FAA to only govern federal aviation assets, not the national needs.

5.2.2 Operational Framework

To provide various services to users operating in the cyber system, many different things must happen just as in the NAS. It starts with infrastructure issues (e.g. the design of computers, components, routers, switches, fiber, facilities), provided services (e.g. monitoring, security, tracking), people concerns

[68] Federation of American Scientist. (n.d.). Retrieved 2011, from http://www.fas.org/irp/offdocs/nspd/index.html

(e.g. training, certifications), and many other facets. The focus here is not to mandate training for general Internet users; however, users may operate in areas requiring training (e.g. Federal Critical Infrastructure, banking). And, there are many more facets of what could be deemed passive, defensive actions to ensure cyber safety.

ISPs and CPs to one degree or another try to provide active, defensive support to ensure safety. However, how this is done varies widely. Figure 8 depicts a notional Internet connection path a message must travel between a user and a given website.

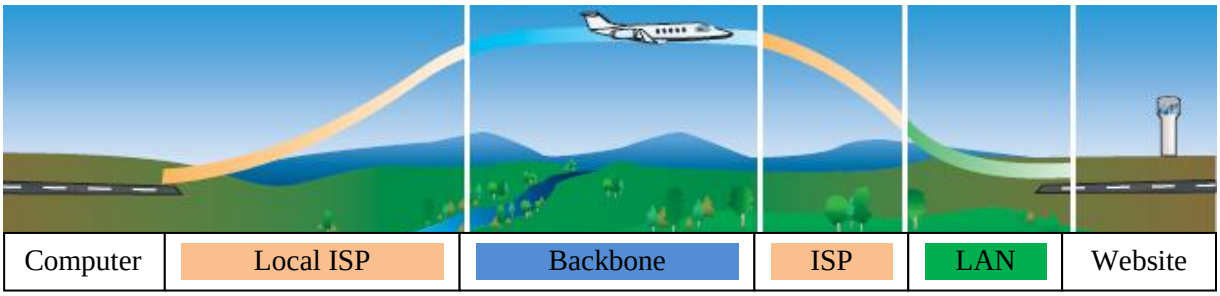


Figure 8: Notional Message Flight Across Internet

In very simplified terms referring to Figure 8, a computer user enters a web address (some CP) to visit. The computer translates this request into a given message or set of packets, which leave the home toward their local ISP. The local ISP forwards the message on to another service provider, likely a backbone provider (e.g. ATT, Sprint) who continues to move the message towards its destination. The CP's local ISP receives the message from the backbone provider and forwards the message onto the CP's Local Area Network (LAN) where the website resides. During this transit, the message packets likely traveled through several different segments of the Internet, passing through many different switches, routers, transmission media, etc. Each of those devices may be owned and operated by different providers. And, different services were provided along the way. In essence, there are different infrastructure, operational, and training standards necessary to make the system work. The rules for these different segments are discussed in 5.2.5. While this is a gross simplification, the same can be said about

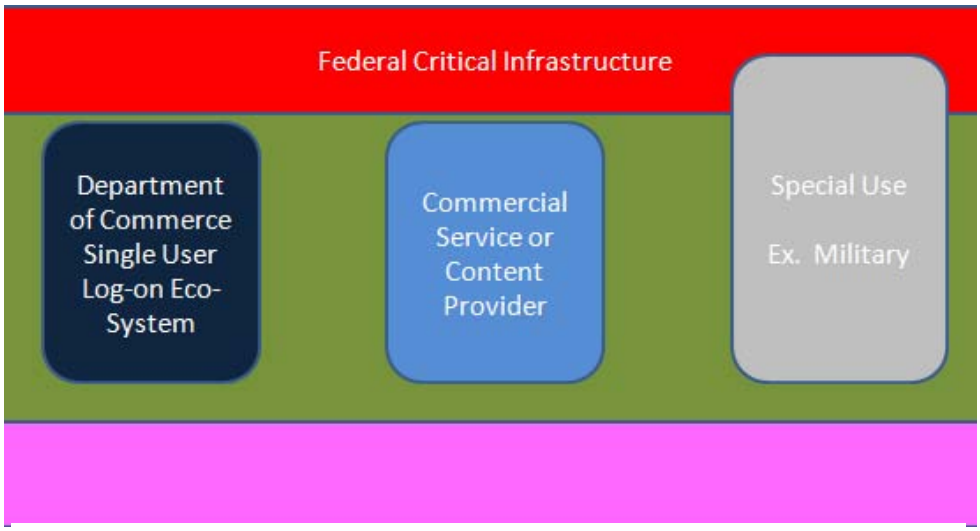
the ATC example. What is important is the concept. There are different functions performed along the way, requiring different rules. Today's rules efforts to provide security by the ISPs and CPs could, arguably, be described as a best effort approach.

5.2.3 Cyber Commons

The concept of a Cyber Commons is vague, but is not unlike the commons of the Air and Maritime Domains. This is another relatively simple, but complex issue requiring a good working definition due to global implications. The other domains leverage the word "commons" to mean places people can innocently travel within a nation's sovereign territory, but there are applicable rules. In Cyber, this concept is not unlike public and private Internet sites from a global perspective. People can navigate to public facing websites in seconds. However, they should not have access to the private servers or LAN providing that public web site beyond what was allowed. Public sites are made available to the public and are commonly available to any global user. However, many private sites are intentionally not available to global users. As such, people should not be navigating within those private websites, unless they have permission. Therefore, public websites are available to anyone globally for innocent access as a "commons". So taking into account attempts to segregate Federal Critical Infrastructures, banking, single user log-on efforts, military operations as private sites, the U.S. can begin to establish rules regarding required services provided and actions taken.

5.2.4 Segments

One of the significant challenges facing the Internet is how to govern. Since the Internet is by definition a network of networks, there are obviously places people can go and places they should not be, unless authorized. Adapting the way in which airspace was segmented, the following potential chart, Figure 9, is proffered.



	Type	Identification	Monitoring	Training and Certs	FWs, IDS, AV, etc
A	Federal Critical	High/Multi-factor	High	High	Enforced
B	Fed, State & Local	High	Med	Med	Enforced
C	Commercial	Med	As Ra'd	Med	Avail
E	Standard Internet	Low	As Ra'd	Low	Avail
G	Ungoverned	None	None	None	As Ra'd
S	Special Use	As Ra'd	As Ra'd	As Ra'd	As Ra'd

Figure 9: Federal Cyberspace Segments

Using a similar convention to FAA airspace segmentation, Federal Critical Infrastructure – Class A, is where standards for operating are highest. Those on these networks require a high degree of identification (e.g. multi factor) to gain access to the network. All users are subject to monitoring, are required to meet a higher threshold for training and certifications, and will have enforced firewalls, intrusion detection systems, anti-virus programs, etc. In other words, everyone is aware that operating in

this segment has much higher standards to operate. These monitoring and other services are provided or enabled by a NORAD-like agency, which is discussed later, given their critical importance. The Standard Internet – Class E would see relatively low requirements for identification, training and certifications with firewalls, etc. available as desired. Monitoring would be available upon request. However in these cases, monitoring would have to be provided by commercial or private concerns. Ungoverned – G segments are either not connected to the Internet or belong to various users who want to set up their own operations. There will always be situations where governance is not in the best interest of the overall system and freedom of activity is necessary. And, notional segments B and C begin to establish rule sets for government or commercial CPs or ISPs depending on the specifics and size of the operation (e.g. non-critical government web sites, banking).

Special Use segments would be like Special Use Airspace. These segments are established by the military for special purposes in coordination with the FCA, including training and war. There is, arguably, a need for prohibited, warning and alert areas. And, there is a need for military operations areas areas. This would be very similar to the military protecting and operating in the .mil domain, where through a similar construct potentially called Military Assumes Responsibility for Internet Security (MARIS). For example, users may navigate to the commons of public military web sites. Once navigating past the main site; however, users would be subject to military special use rules. On the other hand, users who have gained unauthorized access could be addressed appropriately since the requisite authorities would be established by federal rules.

5.2.5 Rules and Regulations

Just as in other domains, rules and regulations have been developed over the years to enable all to operate safely while also pursuing prosperity. This may be one of the biggest issues facing the Cyber Domain today. This is largely due to the lack of a mission focused organization with an accountable leader who is tasked to oversee these issues. As discussed in Chapter 3, there are several significant

challenges directly attributable to the lack of regulatory guidance. While industry has created many groups to address particular issues, many of the particular challenges we face nationally and internationally could be easily addressed by having a Federal Cyberspace Administration focus on the given issues by collaborating with existing commercial and private entities, just as we do with the FAA.

One basic need is creating clear national definitions regarding terms like cyber attack to discern acts of aggression and help resolve UN language regarding behaviors in Cyber. Another need is setting standards for production of various pieces of equipment. Manufacturers who fail to meet minimum standards would be exposing users and operators to many security risks. This would have to be done with close coordination with industry manufacturers. Training and operator certifications also need minimum standards to ensure competency in network operations. Commercial providers would also see minimum standards whether ISPs or CPs. While the specifics of regulatory guidance will be debated, there is a clear need to provide guidance for many reasons. And, a good forum for this necessarily open public debate should be in a Federal Register forum, just as with other processes.

Table 2: Potential Code of Federal Regulations, Title XX, Cyberspace, Sample Titles

Subchapter	Part	Title
A – Definitions	1	Definitions and Abbreviations
	3	General Requirements
B – Procedural Rules	11	General Rulemaking Procedures
	13	Investigative and Enforcement Procedures
C – Computers, Routers, Switches, Devices, Satellite, Wireless	21	Certification Procedures for Products and Parts
Formats, Messages, Interfaces	23-35	Various Standards
	43	Maintenance, Preventive Maintenance, Rebuilding and Alteration
	45	Identification and Registration Marking
	47	Registration
D – Operators	61	Certification: Engineers, Programmers, Designers, Security, Architects
	63	Certification: Maintenance, Installers, Administrators
E – Segments	71	Designation of Network Segments… Routes…Reporting Points
	73	Special Use
F- General Operating and Use Rules	91	General Operating and Use Rules
	93	Special Rules
	99	Security Control of Cyber
G – Commercial: Certification and Operations	110	General Requirements
	119	Certification: Backbone Providers, ISPs and CPs
	121	Operating Requirements: Domestic, Flag, and Supplemental Operations
	125	Certification and Operations…
	129	Operations: Foreign Providers
	139	Certification of ISPs and CPs
H – Schools and Other Certified Agencies	141	Schools
	142	Training Centers
	145	Repair Centers
	147	Maintenance Technician Schools
I – Content Providers	153	Operations
	157	Notice of Construction, Alteration, Activation, and Deactivation of Websites
J – ISPs	170	Establishment and Discontinuance Criteria for Federal Network Services and Facilities
	171	Non-Federal Services and Facilities

5.2.4 Discussion

Just as in 5.2.2., a user's request for a website from a CP will traverse various types of ISPs whether local or national providers. This is very similar to a pilot taking off from a local airport in Class G (min governed) airspace, flying through Class E (controlled) airspace, through Class A (instrument flying only), back to Class E (controlled), then to Class B (major airport). To take off from Class G, there are very few governing standards. Entering Class E, some basic rules exist for identification and other services are available upon request. However to enter Class A airspace, the controller has to positively identify the aircraft, provide mandatory services, and ensure a high degree of safety. On the way back to land at the major destination airport, there are higher standards for identification, communication, etc. to enter the airspace and land at the airport. Along the way, there were different standards for the equipment, training, services provided, etc. However, the pilot knew this and was prepared.

The corollary is a home user trying to go to a major website such as a bank. The user should start at their home device in Class G (minimally governed segment); the message travels through Class E (controlled general Internet) en route to a Class C (Commercial website) destination. While there are certain equipment, training and service standards and options along the way, to enter the commercial website requires a higher degree of authentication. In this case, the standard for access identification is higher. In addition, the CP has higher training and certification requirements to provide the banking service website to the public. Along the way, the message traffic is not allowed to traverse Class A – Federal Critical Infrastructure since the user did not meet the requirements to enter that protected segment. Due to clear rules, this is understood by all. As a reminder and as discussed in 3.3.4, Attribution, all crime will not be eradicated, but good practices can bring down the systemic issues, allowing authorities to focus on the truly bad actors. However, these clear boundaries enabled by clear rules and regulations set the stage for allowed monitoring and corrective action where necessary.

Along the way, the user encountered various ISPs (local and backbone) who were subject to various equipment manufacturing standards and certifications, installation and service standards, training

standards and certifications. The user knew what to expect and had reasonable assurances of safety. It is not difficult to surmise the legal community will soon determine ways to sue manufacturers, ISPs and CPs based on negligence to provide higher security capabilities. Thus, there is another need to get out in front of this issue.

5.3 National Security Agency

This organizational standard of the FAA also sets significant precedent regarding cooperation between DoD, DHS, Intelligence, and other agencies. For example, NORAD's command center in Colorado monitors civilian and military radars and other systems to build situational awareness regarding the security of the U.S. Multiple systems are employed by each organization, which share information. Normal traffic flows daily without incident. However if an air traffic event occurs, established rules, protocols and relationships enable appropriate response to a given event. Day to day, NORAD does not monitor particular aircraft or any other personal information. However if a threat is found, the information can be made available through established authorities. This would not be unlike current efforts to enable a NSA-like agency to monitor Federal Critical Infrastructure for terrorist threats. It is interesting to note the similarities and parallels between NORAD monitoring aircraft within the U.S. and missile threats and the need to monitor the U.S. for internal and external Cyber threats. The potential name for this organization should remain the National Security Agency, but the mission should be expanded. This would begin to address the security needs outlined by Field.

5.3.1 Mission

For Cyber, the potential mission statement would be:

> *In close collaboration with homeland defense, security, and law enforcement partners, prevent cyber attacks against the U.S., safeguard the Federal Critical Infrastructure of the United States by responding to unknown, unwanted, and unauthorized cyber activity approaching and operating within this segment, and provide cyberspace warning for the U.S.*

This notional mission statement could also be expanded to our partners and alliances as we have with Canada via NORAD and with NATO in Europe. However, this is an issue for State to initiate.

5.3.2 Requirements

The basic requirements set forth by the definition would include development and deployment of various sensors and capabilities to protect the Federal Critical Infrastructure. This expanded NSA, NORAD-like agency, then would have full authorities to monitor and actively secure Federal Critical Infrastructures. And, just as NORAD turns over appropriate information to law enforcement in light of Posse Comitatus laws, so too should the NSA, where appropriate.

5.3.3 Securing Others

The capability to defend all network users in the U.S. is impractical for any single organization to try and defend. As with the FAA example, many services are provided by industry to users and operators. For those users and operators outside the Federal Critical Infrastructure, industry would provide firewalls, anti-virus, and other monitoring services as desired. This is much the same way as services are provided today. However, the partnership between an expanded NSA and industry needs refined to share appropriate information concerning threats.

5.3.4 Discussion

The U.S. should explore the NORAD model to enable appropriate monitoring of traffic internal to the U.S. to find and react to internal threats to the Federal Critical Infrastructure. The challenges in this type of monitoring were discussed in 3.3.5.; however, monitoring without direct availability of privacy information could cross some of the legal hurdles in the same way they were resolved with NORAD. This will require strong partnerships with ISPs, CPs and existing governance entities to move forward. So the question becomes one of expanding NSA oversight nationally and building the relationships with

industry or building an entirely new organization. The latter is likely not cost effective or prudent given the NSA is becoming the Cyber equivalent of NORAD. Thus, limiting an expanded authority NSA to monitor Federal Critical Infrastructures and the .mil addresses only makes sense. And, enabling industry to provide monitoring and security services for other segments of the web makes sense also.

Arguments for this approach to security include limiting the reach of governmental monitoring to alleviate Big Brother concerns, a balanced approach between security and prosperity, leveraging existing organizations and models to move forward. This approach also enables industry to provide many security services to users on the network.

Arguments against this approach include the issue that the Federal Critical Infrastructure is not yet clearly defined and one organization is not handling all security matters since it is a partnership with industry. There are also legal issues which must be resolved.

5.4 National Cyber Safety Board

The National Transportation Safety Board (NTSB) is an independent and objective office to ensure safety by investigating incidents and accidents to determine root accident causes. The NTSB through analysis and studies also provides recommendations to improve the national system. The NTSB is also an important counter-balance to the perceived industry or governmental influence to FAA rules. Conceptually, a similarly independent office should be developed for cyberspace. The U.S. should create a National Cyberspace Safety Board akin to the National Transportation Safety Board, possibly modeled after or starting with US CERT, to provide safety recommendations and investigations.

Arguments for this approach include having a third party to independently and objectively report on issues regarding the balance between security and prosperity.

Arguments against this approach would include the creation of another organization and associated costs.

5.5 Assessment

While McCarthy, Field and the GAO have outlined significant issues regarding the lack of focused national leadership, the solution proffered by Field for a cyber security agency unduly places too much emphasis on security. The model provided by the FAA and associated structures provides a more balanced approach for the nation as a whole, which would improve security overall in the long run while continuing down the path of prosperity enabled by Cyber. By creating a FCA, national efforts to establish standards for training and system certifications in partnerships with industry and existing organizations set the stage for balance between security and prosperity.

With an expanded authority NSA focusing on Federal Critical Infrastructures and DoD interests similar to NORAD, security can be properly applied to vital national structures while mitigating Big Brother concerns with industry providing similar services at large. This is also the most practical step. Finally, an independent office called the Federal Cyber Safety Board would provide critical independent assessments regarding risks and threats to Cyber. The benefits of this approach far outweigh any issues regarding time, initial costs, etc. And, as Field argued, the details of implementation should be flushed out before enacting. However, this approach can be implemented in steps to preclude any arguments concerning security issues.

The benchmark by this approach is well founded with benchmark relationships between government organizations (e.g. military to civilian coordination). And, the same benchmark is there for commercial and private concerns to interact with a lead organization such as the FCA. Collectively, this approach enables a balance between security and prosperity while enabling an organization who can focus national efforts and provide leadership.

The notional constructs within this chapter exist to stimulate the necessary national dialogue. The exact makeup of any regulatory guidance, segment structures, and organizational efforts requires greater national discussion, but it is a necessary conversation.

VI. CONCLUSION

6.1 Summary

Weighing the possibilities in light of the threats and challenges to protecting information, the move toward a tiered system, or layered defense, based on a government-industry-consumer approach based on the NAS model (e.g. FAA, NORAD, and NTSB) is prudent and prescient. This means government sets the general minimum rules based on national and international agreements, leaving industry and consumers working cooperatively to comply. This means different rules are developed and applied for different areas (e.g. critical infrastructures, commercial needs, military/special use areas, federal ID programs, etc.)

The importance of protecting information in cyberspace cannot be understated. The current national structures and leadership dealing with these issues is insufficient, and must be addressed. Developing a non-military administration to be the national and international voice is required to focus our national efforts in pursuit of the U.S. national goals. This office should establish relationships with existing commercial entities as modeled by the FAA, NORAD and the NTSB to collectively govern the National Cyberspace System.

6.2 Recommendations

The need to provide effective national leadership in cyberspace is pressing. By far, the most significant recommendation nationally is to create a Federal Cyberspace Administration. In as much, the FCA must be charged with developing regulatory guidance in partnership with industry and the civilian population. The FAA model showing how government can partner with industry and the civilian population is an excellent analogy. While vulnerabilities and some threats exist, placing the FCA within the Commerce Department provides the right focus on the overall Internet with a strong eye on the economy. A strong economy is what enables the rest of U.S. power. In addition, the FCA should partner

with existing civilian organizations (e.g. ICANN, ITU, IETF and others) to establish minimum standards for the various operational need areas (e.g. Federal Critical Infrastructure, Military Special Use, Department of Commerce Single User Log-on and others) regarding training, certifications, and standards. The FCA can then also become the national voice supported by industry and others while coordinating the myriad issues nationally and internationally.

The Defense Department and Homeland Security should support the Commerce Department in defending the various layers. Those areas requiring higher security and monitoring (e.g. Federal Critical Infrastructure and Military Special Use) should be defended and have higher requirements established, as appropriate. Some facets of Cyber as conceptually outlined in Figure 9 require a high level of government monitoring (e.g. Federal Critical Infrastructure and military special use). This is where the concept of NORAD is key. Thus expanding the authorities of NSA to monitor these key structures is necessary. These same services could be offered to various other segments and users, if they desire. However, government cannot perform this function alone, requiring partnerships with industry and users. This is just like the concept utilized by the FAA where operations in various segments of airspace require certain levels of monitoring, contact, and system requirements, but the FAA does not run the entire system. As such, outside key infrastructure components, industry should provide these services.

Finally, creation of a Federal Cyber Safety Board is necessary to provide an objective source of investigations and recommendations to counterbalance the needs of prosperity and security.

6.3 Future Study

While the need for a focused organization to deal with the complex issues exists today, the exact organizational make-up, roles and responsibilities, relationships, and associated issues needs deeper analysis. This would likely drive future organizational evolutions after the organization is established. Likewise, the makeup of the various areas to be regulated requires analysis in partnership with the

affected entities as we move forward. Additionally, an international organization modeled after the ICAO should be explored to coordinate international issues.

Appendix A: Lexicon

A.1 Threats, Vulnerabilities, and Risks

Merriam-Webster stipulates a threat as an expression of intention to inflict evil, injury or damage. Merriam-Webster defines vulnerability as capable of being wounded or open to attack. However, just because something is vulnerable does not mean it will be exploited or attacked. Risk is also defined as the possibility of loss or injury. In general, this means risk is the intersection of vulnerabilities, threats and resources with the probability of occurrence and scope of potential impact accounted for. The probability increases significantly if someone has made a threat, whether overtly or covertly. Many vulnerabilities exist; however, balancing risks and threats is required to properly focus our attention.

A.2 Attack vs Exploit

An attack, as defined by Merriam Webster, uses the language of unfriendly and forcefully, but is generally loaded with emotion. Likewise, exploit means to make productive use of something. For purposes herein, language needs utilized when trying to determine a response to a particular event. As such, loose usage of the word attack fails to discriminate between crime, espionage, or a concerted nation-state effort to deny, destroy or disrupt national power structures.

From a national military perspective, the Vice Chairman of the Joint Chiefs of Staff (VCJCS) has put forth recent clarifying language defining the boundaries of a national cyber attack with the critical systems and infrastructures[9]. While this is helpful, vulnerabilities in the critical systems and infrastructures may still be exploited for espionage or criminal activities. The real issue is ascertaining the source and intent of a particular event. Was it a criminal or a nation-state intent on destroying the nation?

Assigning a specific definition to the word attack though may unnecessarily provide a bad actor bounds to act within and tie the hands of national leaders working to formulate a response. Any response formulation requires having an understanding of a malicious actor's origination and intent (i.e. did they make a threat and who are they aligned with?). Significant discussion regarding the UN definition of attack continues for this very reason. The key is to understand that not everything is an attack. Some things are espionage or some level of criminal activity. This is important given the emotion the word attack invokes. Thus, the word attack, in terms of Cyber, should be reserved for significant against critical systems and infrastructures. Otherwise, the word exploit should be used.

A.3 Warfare

Again, from Merriam-Webster, we discern warfare as the process or ways of open, declared war between hostile, opposing armed forces. Historically, warfare is organized into a campaign, or a designed series of battles, to exert physical influence on decision makers and/or the public to meet some ends. To win a war or competition, players focus on campaign maneuvers and battles to make the minds of decision makers and/or the public comply. We must be cognizant that hostile enemies may extend their strategies beyond traditional armed physical capabilities in today's world. Additionally, terms such as Cyber Warfare invoke some thinking akin to saying Sea, Air, Land or Space Warfare. While these terms invoke some mental imagery, the lack of precision only serves to confuse the issues. The use of a term like Warfare-in-Cyber, while a subtle difference, is important for clarity given it means hostile acts in a domain.

A.4 Cyber Domain

AFDD 3-12, Cyberspace Operations, now defines Cyberspace separately as a domain[69]. Competition exists in and through the man-made Cyberspace domain with friendly, neutral and hostile players. The Cyber domain is a medium or tool through which we transport information.

The Cyber Domain's definition has undergone a wide range of debate. In 2008, the DEPSECDEF issued a memo defining Cyberspace as "*a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers*[70]*."* While some interpret this domain to only include the Internet, desktop computers, personal devices, etc., a vast array of electronic systems in war-fighting platforms is arguably also included. Recently, the VCJCS provided clarification: *"…characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures.*[71]*"* This definition is supported by Franklin Kramer in *Cyber Power and National Security: Policy Recommendations for a Strategic Framework*[72]. However, some caution must be exercised as indicated by a recent White House memo defining Cyber as an integrated, not operational, domain not to be characterized as a warfighting, military or operational domain. Cyber domain should be replaced with Cyberspace whenever possible[73]. Various instruments of power (i.e., the military) may be forced to fight in and through Cyberspace, much like fighting in and through the air, sea or land. Importantly, no one entity owns Cyber. All share and operate in the domain. So the expanded definition, inclusive of the electromagnetic spectrum, is important as we move forward to enable the trans-disciplinary skills to emerge in Spectrum Warfare and Warfare in Cyber. And, the cautionary tone of the

---

[69] US Air Force. (2010, July 15). Air Force Doctrine Document 3-12. *Cyberspace Operations* .
[70] England, G. (. (2008, May 12). The "Definition of Cyberspace".
[71] Cartwright, J. (. (2010). Joint Terminology for Cyberspace Operations. *VCJCS Memo* .
[72] Kramer, F. D. (2009). Cyberpower and National Security: Policy Recommendations for a Strategic Framework. In F. D. Kramer, S. H. Starr, & L. K. Wentz, *Cyber Power and National Security* (p. 20). Washington D.C.: Potomoc Books, Inc.
[73] White House. (2011, March 14). Guidance Regarding The Use Of "Domain" In Unclassified Documents And Public Statements.

White House memo must be heeded at the national level to ensure open and free access to the Internet without militarizing this important national asset.

A.5 Electronic Warfare

For purposes of this paper, the phrase Electromagnetic Spectrum or Spectrum Warfare is used in place of Electronic Warfare.

A.6 Information

Joint Publication 3-13 defines information as a strategic resource[74]. Humans leverage information for decisions regardless whether the information arrived by human contacts or via Cyber. U.S Joint and Service language regarding Information Warfare has also caused several challenges within the Department. A myriad of competing and often confusing lexicon emerged as various communities vied to define their roles and responsibilities in this emerging battlespace. Information Warfare evolved into an eclectic grouping of Electronic Warfare (EW), Psychological Operations (PSYOPS) now known as Military Information Support Operations (MISO), Military Deception (MILDEC), Computer Network Operations (CNO) and Operations Security (OPSEC). Continuing down this path, the intelligence community put forth the cognitive, information and physical domains[75], which causes confusion. The joint community resolved this discrepancy by using the cognitive, information and physical dimensions[76]. However, an information dimension still causes confusion and should be clarified. As such, we start by exploring the role of information in terms of power.

---

[74] Department of Defense. (2006, February 13). Information Operations. *Joint Publication 3-13* .
[75] US Air Force. (2005, January 11). Air Force Doctrine Document 2-5. *Information Operations* .
[76] Department of Defense. (2006, February 13). Information Operations. *Joint Publication 3-13* .

Appendix B: Information as a Foundation of Power

B.1 Understanding Power

Figure 1 is a representation showing the relationships of power underpinning the thought process throughout this paper. On the left are the cognitive and physical dimensions used by the intelligence community. However, information is not used or described as a domain or dimension, though the information environment is retained[77]. A backdrop of knowledge is provided to allude to power being based not only in organizations, information, laws, etc, but also in the experience and education maintained.

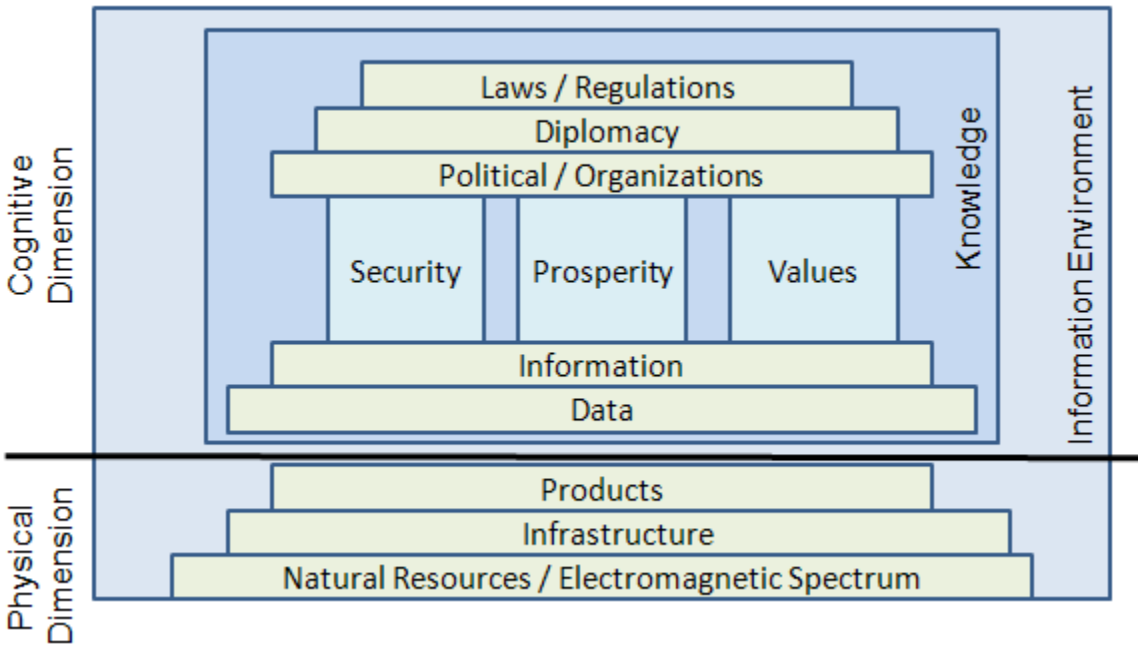


Figure 10: Foundations of Power Representation

[77] Department of Defense. (2006, February 13). Information Operations. *Joint Publication 3-13* .

B.1.1 Physical Dimension

In the Physical Dimension, natural resources including the electromagnetic spectrum are the physical foundation of power. At the next layer, infrastructures are built to provide various products.

B.1.2 Cognitive Dimension

In the Cognitive Dimension, data is a foundational resource just as natural resources are a foundation in the Physical Dimension. Likewise, information, or processed data, is a product and foundation. Next are the security, economic and cultural pillars, which were chosen given the 2010 National Security Strategy outlines power in terms of security, prosperity and values[78]. Differing from traditional IOP models, politics (how entities align themselves or organize themselves on various issues) cuts across the three pillars of power. Next, Diplomacy (the art of negotiation) also cuts across the pillars indicating the negotiations of politics. And on top are the laws, regulations or other agreements that emerge from various diplomatic efforts. Of note, data and information lie at the foundation of the cognitive dimension.

B.1.3 Discussion

The pillar of security is used given many organizations have a stake in providing security, whether physical security (e.g. armed forces, police), economic security (e.g. finances, retirement), cultural security (e.g. sense of belonging), or even information security. The economic pillar represents the goods and services provided by various organizations or individuals (e.g. businesses, banks, unions). And, the cultural pillar is used given the power of values is exerted through cultural means (e.g. Christians, Muslims, boy scouts, Masons, bike clubs). People align themselves to achieve unity of effort and power for a variety of reasons. People may join the political organizations (e.g. Democrats,

[78] White House. (2010, May). National Security Strategy.

Republicans), security organizations or any number of other organizations to join efforts at wielding power and influence.

There are, at times, competing goals in each of the pillars and foundations of power, which create tension (i.e. the goals of security often conflict with economic or cultural goals). For instance using a current example, the U.S. government has supported Egyptian President Mubarak, a purported dictator, for economic and security reasons while doing so is in direct conflict with the U.S. cultural values of freedom, democracy, etc. We also see the competing goals of this three-legged stool (security, economics and culture) play out in interactions with many nations (e.g. China and Russia). Ultimately, the organizations and associated alliances are built to wield power to one varying degree or another.

Bibliography

Alexander, K. B. (2010). Statement of Gen Keith B Alexander to Before the House Committee on Armed Services. (H. C. Services, Interviewer)

Banks, W. C. (2010). Programmatic Surveillance and FISA: Of Needles in Haystacks. *Texas Law Review* , 35.

Barabasi, A.-L. (2002). *Linked, The New Science of Networking*. Cambridge, Mass: Perseus Publishing.

Bockover, A., Lyon, B., Adai, A., & Voyles, J. (2005). *The Opte Project*. Retrieved from The Opte Project: http://www.opte.org/maps/

Brunnschweiler, C. N., & Bulte, E. H. (2009, January 28). Natural Resources and Violent Conflict: Resource Abundance, Dependence and the Onset of Civil Wars. CER-ETH Center of Economic Research at ETH Zurich, Switzerland.

Bruzdzinski, J. E. (2004). Demystifying Shashoujian: China's 'Assassin's Mace' Concept. In e. Larry Wortzel and Andrew Scobell, *Civil–Military Change in China: Elites, Institutes, and Ideas After the 16th Party Congress* (pp. 309-364). Carlisle, PA: Strategic Studies Institute, U.S. Army War College.

Bryant, M. D. (2008). Layered Sensing: Its Definition, Attributes, and Guiding Principles for AFRL Strategic Technology Development. Wright Patterson AFB, OH.

Buchanan, P. J. (2007). *Day of Reckoning: How Hubris, Ideology, and Greed are Tearing America Apart.* New York: St. Martin's Press.

Buys, J. R., & Clark, J. L. (1995, August). Events and Causal Factors Analysis. *SCIENTECH* . (J. Kingston-Howlett, Ed.) Great Britain: Aston University.

Carden, M. J. (2010, August 27). *U.S. Department of Defense*. Retrieved May 3, 2011, from News: http://www.defense.gov/news/newsarticle.aspx?id=60621

Cartwright, J. (. (2010). Joint Terminology for Cyberspace Operations. *VCJCS Memo* .

Clarke, R. A. (2010). *Cyber War, The Next Threat to National Security and What to Do About It.* New York, New York: Harper Collins Publishers.

College of Aerospace Doctrine, Research and Education. (2005). The Joint Air Estimate Planning Process. In R. M. Olienyk, *Joint Air Operations v4.1* (p. 34). Maxwell AFB, AL: Air Command and Staff College.

Congressional Budget Office. (2011, April 5). Long-Term Analysis of a Budget Proposal by Chairman Ryan.

Cornish, P. R. (2009). *Cyberspace and the National Security of the United Kingdom, Threats and Responses*. London, England: Chatham House.

Department of Defense. (2006, February 13). Information Operations. *Joint Publication 3-13* .

Department of Defense. (2009). *Initial Capabilities Document for the Joint Aerial Layer Network (FOUO).* Department of Defense.

Department of Defense. (2007, June 22). Joint Intelligence. *Joint Publication 2-0* .

Department of Defense. (2006, December 17). Joint Operations, Incorporating Change 2. *Joint Publication 3-0* . Department of Defense.

Department of Defense. (2008, June). National Defense Strategy.

Department of Defense. (2011, February 8). National Military Strategy.

Department of Defense. (2009, January 6). Space Operations. *Joint Publication 3-14* .

Department of Homeland Security. (n.d.). *National Cyber Security Division*. Retrieved 2011, from Department of Homeland Security: http://www.dhs.gov/xabout/structure/editorial_0839.shtm

Drozdova, K., & Samoilov, M. (2010). Predictive analysis of concealed social network activities based on communication technology choices: early-warning detection of attack signals from terrorist organizations. University of California.

Echevarria, A. J. (2010). *Preparing for One War and Getting Another.* Strategic Studies Institute.

Endsley, M. R. (2000). *Theoretical Underpinnings of Situational Awareness: A Critical Review.* (M. R. Endsley, & D. J. Garland, Eds.) Mahwah, NJ: Lawrence Erlbaum Associates, Inc.

England, G. (. (2008, May 12). The "Definition of Cyberspace".

Fadok, D. S., & Boyd, J. a. (1995). *Air Power's Quest for Strategic Paralysis.* Maxwell AFB, AL: Air University Press.

Federal Aviation Administration. (n.d.). *FAA Order 7110.65 Chapter 2, General Control.* Retrieved 2011, from http://www.faa.gov/air_traffic/publications/atpubs/atc/atc0201.html

Federal Aviation Administration. (n.d.). *IFR Operations in the National Airspace System.* Retrieved 2011, http://www.faa.gov/library/manuals/aviation/instrument_procedures_handbook/media/CH%2001a.pdf

Federal Aviation Administration. (n.d.). *National Airspace System Overview.* Retrieved 2011, from http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/systemops/aaim/organizations/envir_programs/mase/media/ApxB_NAS_122805.pdf

Federal Bureau of Investigation. (2009). *Federal Bureau of Investigation*. Retrieved March 23, 2011, from Crime in the United States: http://www2.fbi.gov/ucr/cius2009/data/table_01.html

Federation of American Scientist. (n.d.). Retrieved 2011, from http://www.fas.org/irp/offdocs/nspd/index.html

Field, J. (n.d.). *Cybersecurity: Division of Responsibility in the U.S. Government.* Retrieved May 13, 2011, from http://www.nsci-va.org/CyberReferenceLib/2010-09-18-Cybersecurity-Division of Responsibility in the US Government-Joeli Field.pdf

Gladwell, M. (2000). The Tipping Point. Little Brown.

Goldenberg, J. L. (2001). *Talk of the Network: A Complex Systems Look at the Underlying Process of Word of Mouth.* Netherlands: Kuwler Academic Publishers.

Goldgeier, J. (2010). *Reforming the National Security Process in a Globalized World.* Strategic Studies Institute.

Government Accountability Office. (2009). *President's Cyberspace Policy Review.* Retrieved Sep 4, 2010, from http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

Graham, D. E. (2007). Cyber Threats and the Law of War. *Journal of National Security Law and Policy* , 16.

Graves, L. (2010). The Right to Privacy in Light of Presidents' Programs: What Project MINARET's Admissions Reveal About Modern Surveillance of Americans. *Texas Law Review* , 50.

Gruhl, D., Guha, R., Kumar, R., Novak, J., & Tomkins, A. (2005). The Predictive Power of Online Chatter. *KDD-2005* .

Hamil, J. T. (2006). Analysis of Layered Social Networks. Air Force Institute of Technology.

Harmon, D., M. de Aguir, M. A., Chinellato, D. D., Braha, D., Epstein, I. R., & Bar-Yam, Y. (2010, August 26). Predicting Economic Market Crises Using Measures of Collective Panic.

Hawksworth, J., & Cookson, G. (2008, March). Beyond the BRICs:. *The World in 2050: A Broader Look at Emerging Market Prospects* . Price Waterhouse Coopers.

Jasper, S. (2010, March 15). Securing Freedom in the Global Commons. Stanford University Press.

Joel, A. W. (2010). Choosing Both: Making Technology Choices at the Intersections of Privacy and Security. *Texas Law Review* , 15.

Jones, K. M. (2010). *Cyberspace and the Electromagnetic Spectrum, Friend or Foe?* Maxwell AFB, AL: Air University.

Kanuck, S. (2010). Sovereign Discourse on Cyber Conflict Under International Law. *Texas Law Review* , 27.

Katzman, J. (1995, Mar 28). *Special Analysis: STRATCOM's 4-Star Blogger*. Retrieved from http://www.windsofchange.net/archives/006576.html

Kramer, F. D. (2009). Cyberpower and National Security: Policy Recommendations for a Strategic Framework. In F. D. Kramer, S. H. Starr, & L. K. Wentz, *Cyber Power and National Security* (p. 20). Washington D.C.: Potomoc Books, Inc.

Kwalwasser, H. (2009). Internet Governance. In F. D. Kramer, S. H. Starr, & L. K. Wentz, *Cyberpower and National Security*. Potomoc Books, Inc.

Lawson, S. (2011, January). BEYOND CYBER DOOM: Cyberattack Scenarios and the Evidence of History. Mercatus Center at George Mason University.

Liang, Q., & Xiangsui, W. (1999). *Unrestricted Warfare.* PLA Literature and Arts Publishing House.

Liles, S. (2010). Cyber Warfare: As a Form of Low-Intensity Conflict and Insurgency. *Conference on Cyber Conflict* (p. 11). Tallinn, Estonia: CCD COE Publications.

Lt Col Edward F Murphy, e. a. (1996). *Information Operations: Wisdom Warfare for 2025.* USAF.

McKitrick, J. (1995, September). The Revolution in Military Affairs. *Battlefield of the Future: 21st Century Warfare Issues* . Maxwell AFB, AL: Air University Press.

Mitnick, K., & Simon, W. L. (2002, October 4). Controlling the Human Element of Security: The Art of Deception. John Wiley & Sons.

Muniz, J. J. (2009). *Declawing the Dragon: Why the U.S. Must Counter Chinese Cyber-Warriors.* Fort Leavenworth, KS: U.S. Army Command and General Staff College.

Murphy, E. F. (1996, April). Information Operations: Wisdom Warfare for 2025.

National Transportation Safety Board. (n.d.). *History and Mission*. Retrieved 2011, from NTSB: http://www.ntsb.gov/Abt_NTSB/history.htm

North American AeroDefense Command. (n.d.). *About NORAD*. Retrieved 2011, from http://www.norad.mil/about/index.html

Osborn, A. (2008, December 29). As if Things Weren't Bad Enough, Russian Professor Predicts End of U.S. *Wall Street Journal* . Moscow, Russia.

Paul Cornish, R. H. (2009). *Cyberspace and the National Security of the United Kingdom, Threats and Responses.* London, England: Chatham House.

Pipkin, D. L. (2000). Information Security: Protecting the Global Enterprise. Prentice Hall PTR.

Porter, M. E. (2008, January). The Five Competitive Forces that Shape Strategy. *Harvard Business Review* .

Prime Minister. (2010). A Strong Britian in an Age of Uncertainty: The National Security Strategy. London, England.

Rice, M., & Butts, J. (2010). An Analysis of the Legality of Government-Mandated Computer Inoculations. *International Journal of Critical Infrastructure Protection* , p. 11.

Rice, M., & Butts, J. e. (2009). Applying Public Health Strategies to the Protection of Cyberspace. Tulsa, OK.

Robinson, D. J. (2010). *Cyber Based Behavioral Monitoring*. Hanover, New Hampshire: Thayer School of Engineering.

Sales, N. A. (2010). Mending Walls: Information Sharing After the USA PATRIOT Act. *Texas Law Review* , 60.

Schneier, B. (2008, February 23). *Bruce Schneier*. Retrieved April 20, 2011, from Bruce Schneier: Security at What Cost?: http://www.schneier.com/essay-207.html

Shackleford, S. J. (2010). State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. *Conference on Cyber Conflict Proceedings 2010* (p. 12). Tallinn Estonia: CCD COE.

Skoudis, E., & Liston, T. (2006). Computer Hack Reloaded. Pearson Education, Inc.

Stoessinger, J. G. (2008). Why Nations go to War. Michael Rosenberg.

Stover, C. M. (2010). Network Neutrality: A Thematic Analysis of Policy Perspectives Across the Globe. *Global Media Journal - Canadian Edition* , 11.

Temoshok, D. (2007). *Federal Identity Management and the Federal PKI*. Retrieved from www.kansas.gov/pki/clinic/presentations/federalPKI.ppt

Thatte, G. e. *Detection of Low Rate Attacks in Computer Networks.* Marina Del Ray, California: University of Southern California.

Thomas, T. L. (2005). *Cyber Silhouettes, Shadows Over Information Operations.* Fort Leavenworth, KS: Foreign Military Sales Office (FMSO).

Thomas, T. L. (2010, June 22). Google Confronts China's "Three Warfares". *Parameters* .

Thomas, T. L. (2010, July). Russian Information Warfare Theory: The Consequences of August 2008. *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald* . Carlisle, Pennsylvania: Strategic Studies Institute.

Trusov, M., Bodapati, A., & Bucklin, R. E. (2010). Determining Influential Users in Internet Social Networks. *Journal of Marketing Research* . Vol 47 (4), 643-658.

Tzu, S. (1971). *The Art of War.* (S. B. Griffith, Trans.) Oxford University Press.

US Air Force. (2002). AFDD 2-5.1 Electronic Warfare.

US Air Force. (2005, January 11). Air Force Doctrine Document 2-5. *Information Operations* .

US Air Force. (2010, July 15). Air Force Doctrine Document 3-12. *Cyberspace Operations* .

US Army. (2004, Oct 1). Counterinsurgency Operations - Interim. *FMI 3-07.22* .

USAF. (2010). *DTIC Online.* Retrieved 10 2010, from DTIC Online: http://www.dtic.mil/doctrine/jel/service_pubs/afd2_5.pdf

Vice Admiral Arthur K. Cebrowski, U. N. (1998). Network-Centric Warfare: Its Origin and Future. *US Naval Institute Proceedings* (p. 10). US Navy.

Watts, D. J. (2003). Six Degrees: The Science of a Connected Age. W.W. Norton and Company.

White House. (2011, March 14). Guidance Regarding The Use Of "Domain" In Unclassified Documents And Public Statements.

White House. (2003, December 17). Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection.

White House. (2010, May). National Security Strategy.

White House. (2010). The Comprehensive National Cybersecurity Initiative.

White House. (2010). US National Security Strategy 2010. Washington, DC.

Windsoar, D. o. (n.d.). *FAA Airspace Chart*. Retrieved April 28, 2011, from http://www.dukesofwindsoar.com/dukes.cgi?do=html&htmlfile=html/ppg_info/airspace_info.html

Wood, R. J. (1995, April). Information Engineering: The Foundation of Information Warfare. Maxwell AFB, AL: Air University.

Wyler, L. S. (2008, August 28). Weak and Failing States: Evolving Security Threats and U.S. Policy. *CRS Report for Congress* . Congressional Research Service: Library of Congress.

Yesui, Z. (2010). China's Concept Paper as presented to the UN. New York, New York.

Yue, T. (2001, November 30). *The Tech Online Edition (MIT).* Retrieved Dec 7, 2010, from The Tech Online Edition: http://tech.mit.edu/V121/N63/Stealth.63f.html

Vita

Major Jonathan Frampton enlisted in the Air Force in 1991 as an Air Traffic Controller. Following completion of a B.S. in Aeronautical Science, he was commissioned through Officer Training School in 1997. He has a Masters of Business Administration.

Maj Frampton is a Cyber Operations Officer. He was selected to attend Intermediate Developmental Education (IDE) in 2010 and is currently completing the IDE Cyber Warfare program at AFIT. Upon graduation, he will be assigned to the U.S. Strategic Command, Requirements Directorate.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
16-06-2011	Graduate Research Project	Jun 10 – Jun 11

4. TITLE AND SUBTITLE

Achieving National Unity of Effort in Cyber

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

Jonathan J. Frampton, Major, USAF

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
2950 Hobson Way
WPAFB, OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER
AFIT/ICW/ENG/11-04

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

N/A

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED

13. SUPPLEMENTARY NOTES

This material is declared a work of the U.S. Government and is not subject to copyright protection in the U.S.

14. ABSTRACT

Information is a foundation of power enabling national security, prosperity and cultural values for all nations. As such, significant national discussion is underway regarding the threats, risks and vulnerabilities of the national and global Cyber infrastructure, especially given recent events. Unfortunately, current U.S. national strategies regarding Cyber lack clarity on ways to achieve national goals. And, consequently, national U.S. efforts in Cyber suffer from a lack of focus and leadership. While the military is re-organizing its Cyber forces, the time has come to create a civilian led Federal Cyber Administration to focus national efforts, expand the National Security Administration authorities for the Federal Critical Infrastructure using the North American Aerospace Defense (NORAD) model, and create a National Cyberspace Safety Board.

15. SUBJECT TERMS

cyberspace, national leadership, unity of effort

16. SECURITY CLASSIFICATION OF: Unclassified\Releasable to Public			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
			UU		Michael R. Grimaila, PhD, CISM, CISSP michael.grimaila@afit.edu
REPORT	**ABSTRACT**	**c. THIS PAGE**		75	**19b. TELEPHONE NUMBER** *(Include area code)*
U	**U**	**U**			(937) 257-3636x4527