The Case for Integration of Cyberwarfare and Cyberdeterrence Strategies into the U.S. CONOPS Plan to Maximize Responsible Control and Effectiveness by the U.S. National Command Authorities

Bellevue, Nebraska
M.S. in Cybersecurity Program
Cyberwarfare and Cyberdeterrence – DET 630
Final Course Project Presentation

William F. Slater, III

November 18, 2012

Agenda

- Introduction
- Threat Analysis
- Policy Appraisal
- Strategic Comparative Analysis
- Conflict Resolution
- Policy Generation
- Conclusion

INTRODUCTION

Introduction

- I am a student in Professor Matthew Crosston's class on Cyberwarfare and Cyberdeterrence
- I have been in Bellevue University's Cybersecurity program since August 2011
- I have been a career Information Technology (IT) professional since July 1977
- I started my IT career as a young computer systems staff officer in the United States Air Force supporting the command control information systems that provided real-time information to the Strategic Air Command Battle Staff
- I chose this topic to research and write about because as an IT professional in cybersecurity, a former U.S. Air Force officer, and a patriotic American, I am deeply concerned about the recent unfolding events of cyberattacks and cyberwarfare in cyberspace. I am also deeply concerned that the United States, with all its wealth, technology, and leadership as a nation advocating democracy and freedom, seems to be ill-equipped with the policies and cohesive ideas needed to properly address the issues related to cyberattacks, cyberwarfare, and cyberdeterrence.
- The two ironies at this moment in time, are 1) that most of the cyber technologies that now threaten us were invented here in the United States; and 2) that we have just reelected President Barack , who is arguably the most tech-savvy president ever to serve as president of the United States, to serve as our president until January 2017.

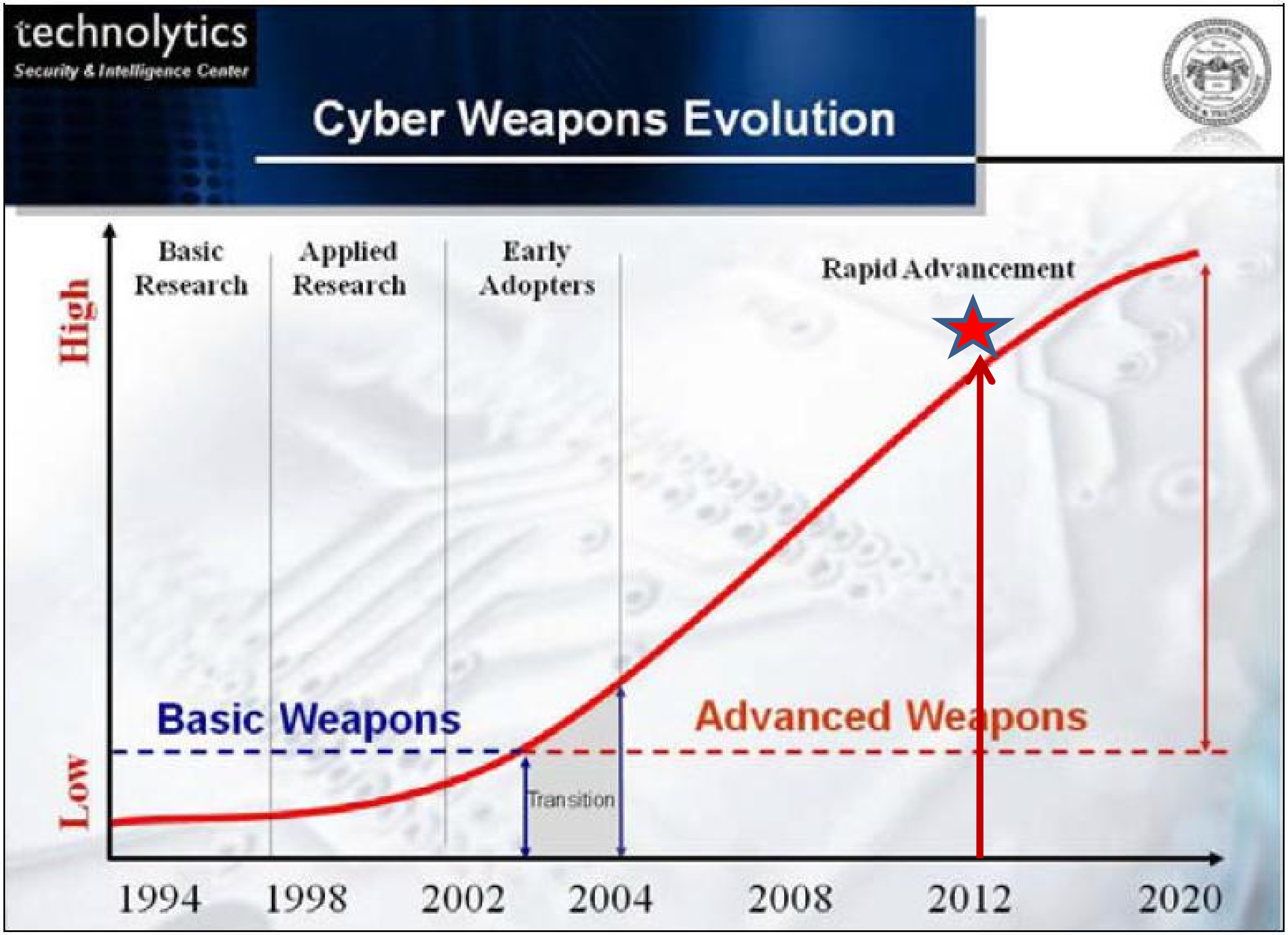
THREAT ANALYSIS

Threat Analysis

- The threat of cyberattacks and cyberwar are very real
- The quantity of cyberattacks and cyberwar incidents has increased dramatically since 2007, and it continues to increase daily
- The sophistication of cyberattacks and cyberweapons has grown dramatically since 2009
- There is now a dire need to incorporate strategies to deal with the threats of cyberattacks, cyberwarfare, and cyberdeterrence into the U.S. CONOPS Plan
- The lack of effective national plans and policies to effectively address cyberwarfare and cyberdeterrence constitutes a threat itself

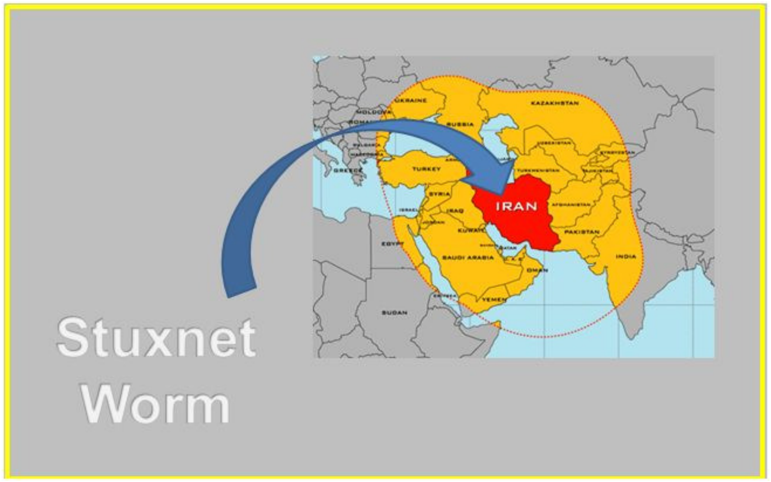
CYBERWAR AND CYBERATTACKS

Cyberweapon Evolution

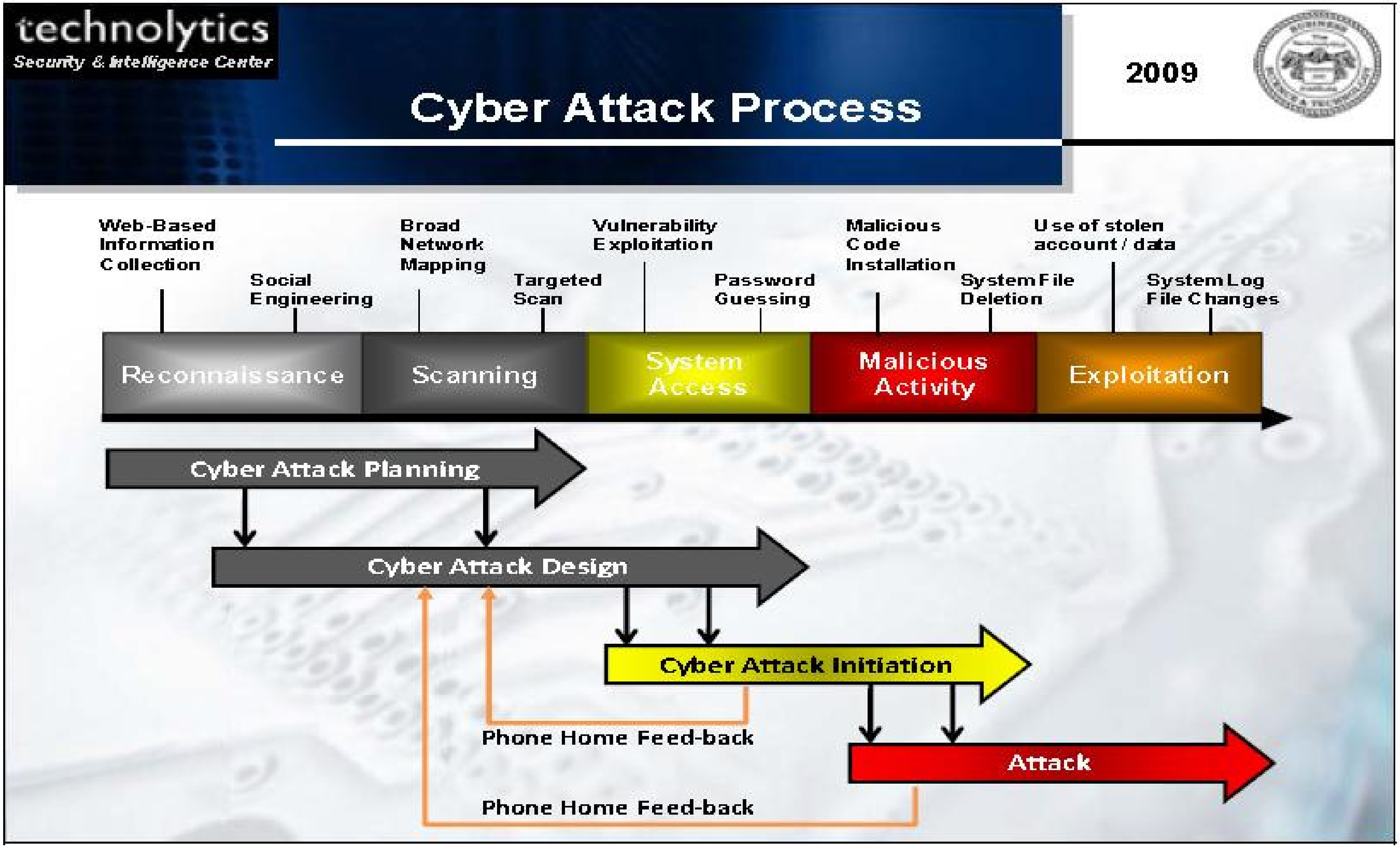


Some Notable Cyberattacks and Cyberweapons 2007 - 2012

- DDoS – Russia v. Estonia, 2007
- DDoS – Russia v. Georgia, 2008
- DDoS – Russian v. Kyrgyzstan, 2009
- Stuxnet – U.S. and Israel v. Iran, 2009 – 2010
- Flame - U.S. and Israel v. Iran, 2011
- Duqu - U.S. and Israel v. Iran, 2012
- Shamoon - 2012



Cyberattack Process



Cyberwar and Cyberattacks

- Dangers and incidents related to cyberattacks and cyberwar continue to increase at an alarming rate
- Compliance with security frameworks can help
- But… entire infrastructures, cities, and countries are at risk
- The Solutions will lie in National Policy, Regulation, preparation, and some form of deterrence

POLICY APPRAISAL

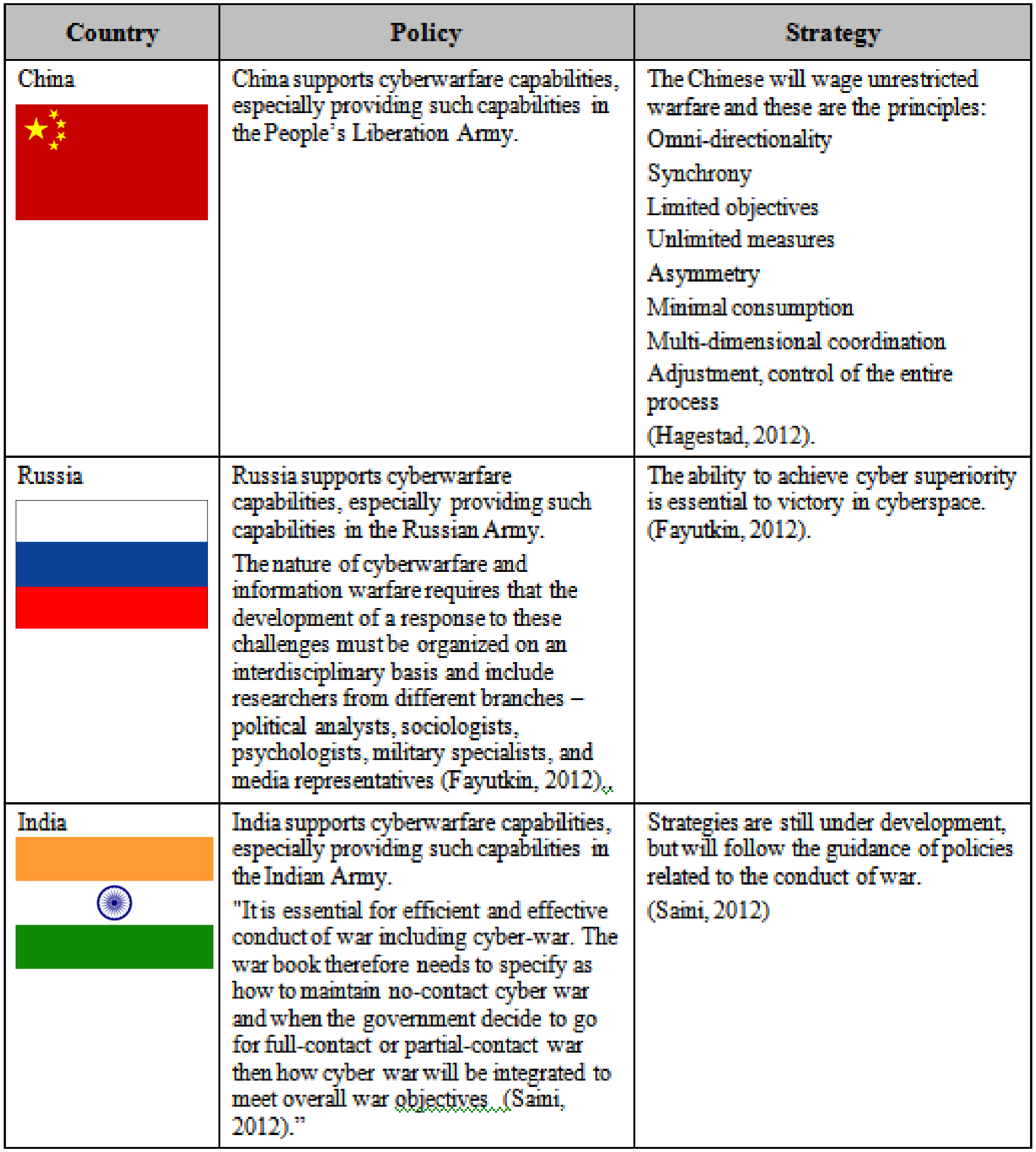
Policy Appraisal

- U.S. President Barack Obama is probably the most tech-savvy president ever elected
- Present U.S. public policies address the importance of cyberspace, and the importance of defending it for the U.S. and our allies.
- These policies have also provided for the creation and maintenance of military and government units that can provide cyber offensive and defensive capabilities
- But based on the rise of recent cyber attacks these present policies have not been effective enough

U.S. President Barack Obama

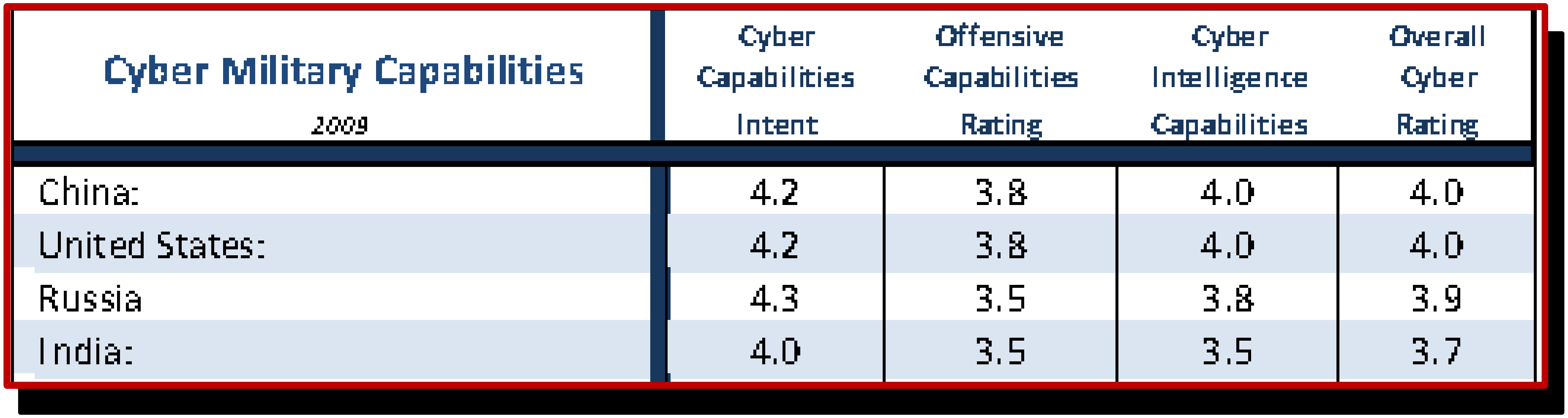
STRATEGIC COMPARATIVE ANALYSIS

Strategic Comparative Analysis



Country	Policy	Strategy
China	China supports cyberwarfare capabilities, especially providing such capabilities in the People's Liberation Army.	The Chinese will wage unrestricted warfare and these are the principles: Omni-directionality Synchrony Limited objectives Unlimited measures Asymmetry Minimal consumption Multi-dimensional coordination Adjustment, control of the entire process (Hagestad, 2012).
Russia	Russia supports cyberwarfare capabilities, especially providing such capabilities in the Russian Army. The nature of cyberwarfare and information warfare requires that the development of a response to these challenges must be organized on an interdisciplinary basis and include researchers from different branches – political analysts, sociologists, psychologists, military specialists, and media representatives (Fayutkin, 2012).,	The ability to achieve cyber superiority is essential to victory in cyberspace. (Fayutkin, 2012).
India	India supports cyberwarfare capabilities, especially providing such capabilities in the Indian Army. "It is essential for efficient and effective conduct of war including cyber-war. The war book therefore needs to specify as how to maintain no-contact cyber war and when the government decide to go for full-contact or partial-contact war then how cyber war will be integrated to meet overall war objectives. (Saini, 2012)."	Strategies are still under development, but will follow the guidance of policies related to the conduct of war. (Saini, 2012)

The Top Four Countries in Cyberwarfare Capability (as of 2009)



Cyber Military Capabilities 2009	Cyber Capabilities Intent	Offensive Capabilities Rating	Cyber Intelligence Capabilities	Overall Cyber Rating
China:	4.2	3.8	4.0	4.0
United States:	4.2	3.8	4.0	4.0
Russia	4.3	3.5	3.8	3.9
India:	4.0	3.5	3.5	3.7

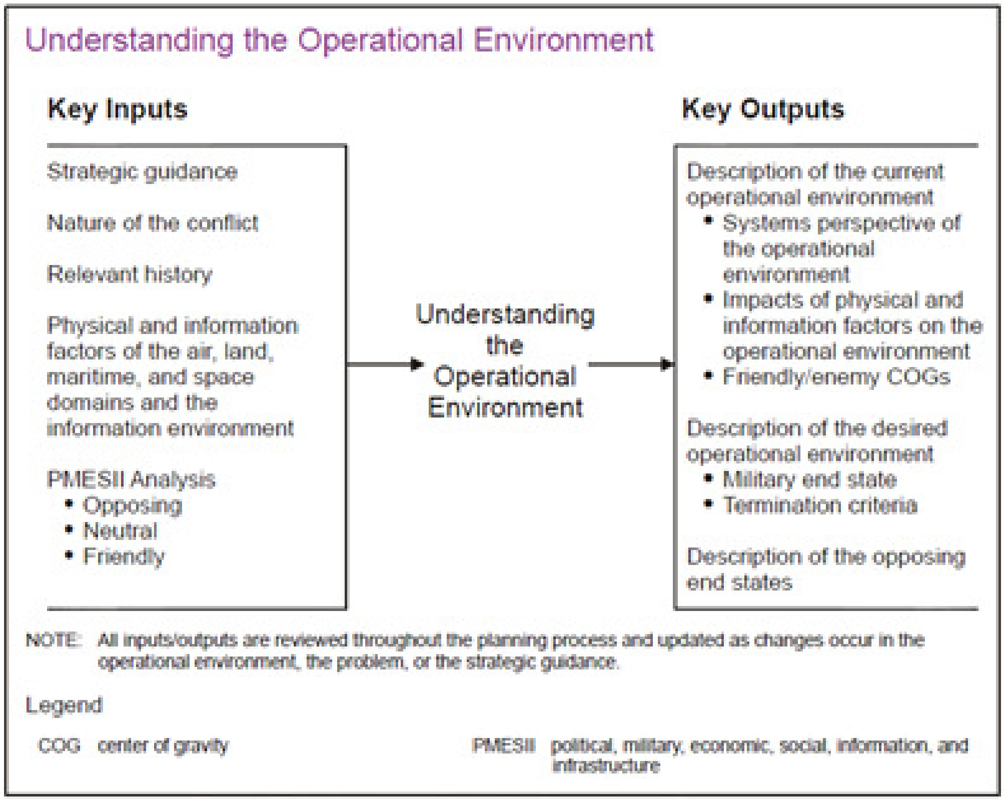
Table 1 – Country Cyber Capabilities Ratings (Technolytics, 2012)

CONFLICT RESOLUTION

Conflict Resolution

- The ability to resolve conflict in cyberspace requires:
  - A thorough recognition and understanding of the environment as an operational environment where there is potential for conflict
  - Understanding the interconnected nature of the realms related to the operational environment of conflict
  - Understanding the nature of the systems analysis is also essential for decision making and conflict resolution

The Operational Environment and Cyberspace



Understanding the Operational Environment

Key Inputs

- Strategic guidance
- Nature of the conflict
- Relevant history
- Physical and information factors of the air, land, maritime, and space domains and the information environment
- PMESII Analysis
  - Opposing
  - Neutral
  - Friendly

→ Understanding the Operational Environment →

Key Outputs

- Description of the current operational environment
  - Systems perspective of the operational environment
  - Impacts of physical and information factors on the operational environment
  - Friendly/enemy COGs
- Description of the desired operational environment
  - Military end state
  - Termination criteria
- Description of the opposing end states

NOTE: All inputs/outputs are reviewed throughout the planning process and updated as changes occur in the operational environment, the problem, or the strategic guidance.

Legend

COG	center of gravity
PMESII	political, military, economic, social, information, and infrastructure

Figure 2 – Understanding the Operational Environment

(U.S. DoD, JCS, 2006)

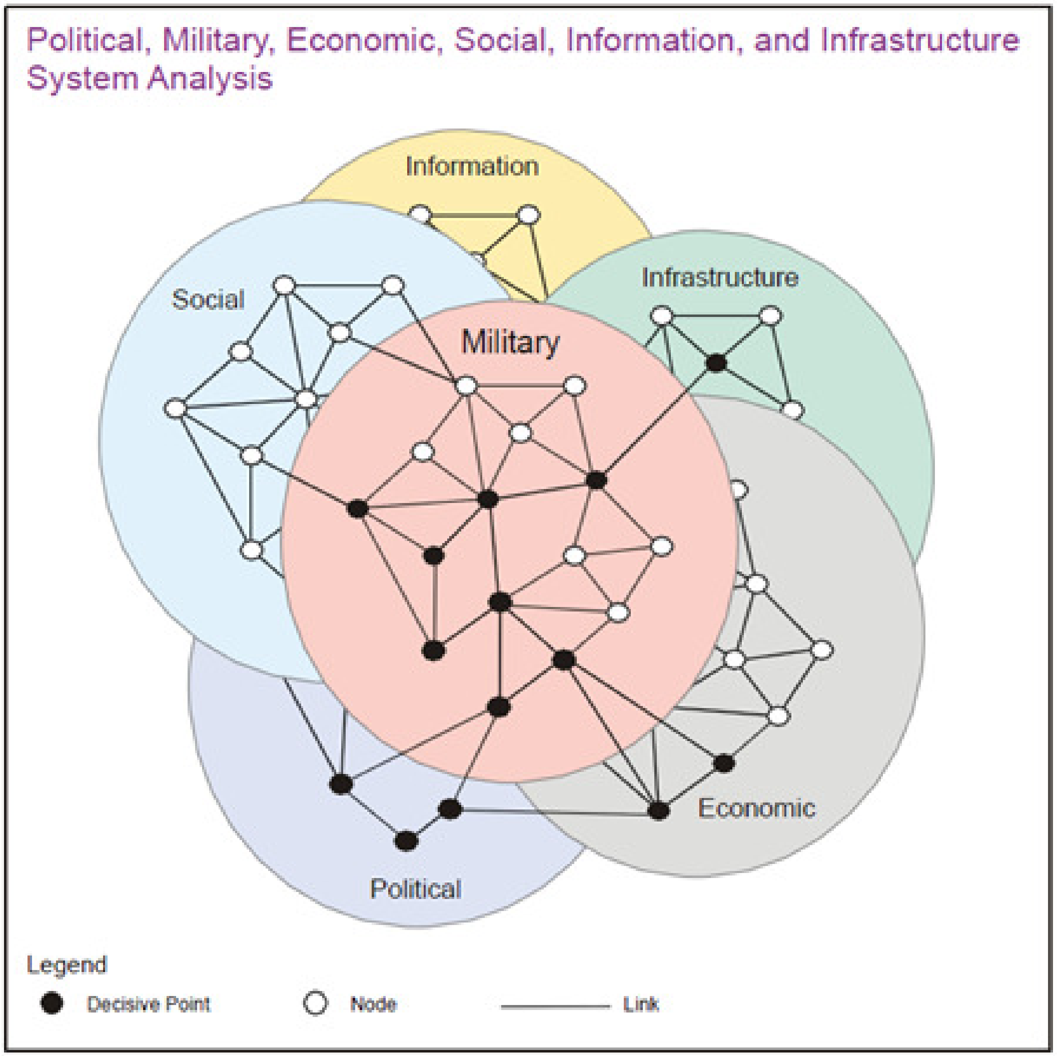
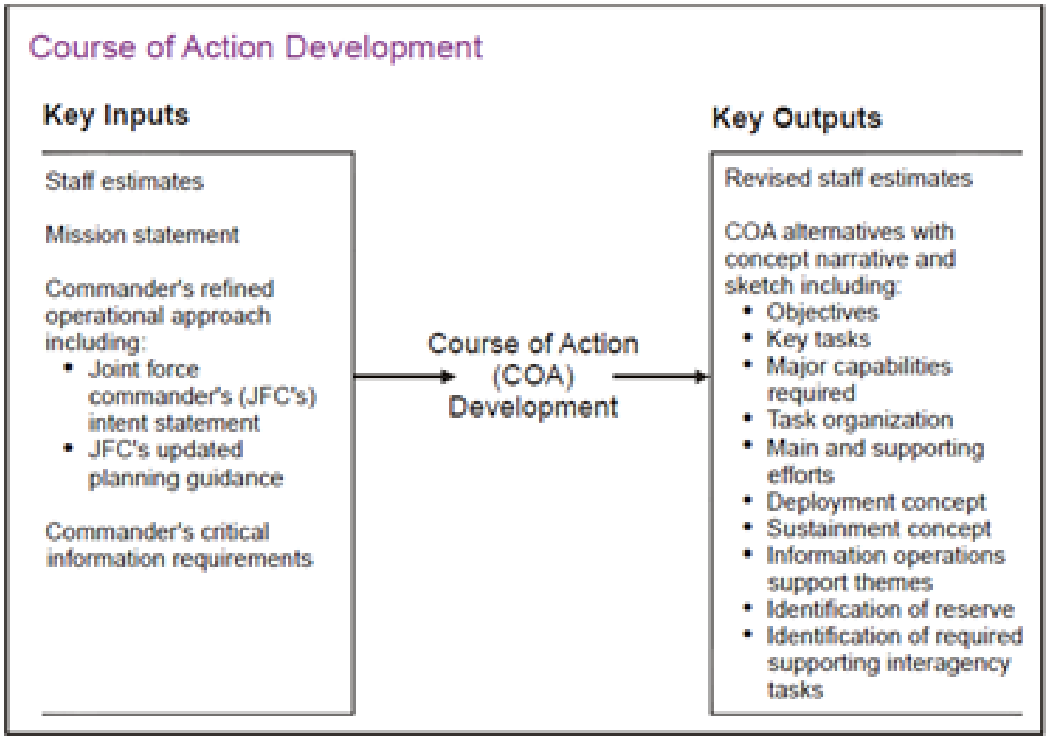


Figure 3 – Understanding the Interconnected Nature of the Realms Related to the Operational Environment of Conflict and the Nature of the Systems Analysis Required for Decision Making (U.S. DoD, JCS, 2006)

The Model Showing the Interconnected Nature of Cyberspace with Other Environments

The DoD Model Showing the Course of Action Development



Course of Action Development

Key Inputs

Staff estimates

Mission statement

Commander's refined operational approach including:
- Joint force commander's (JFC's) intent statement
- JFC's updated planning guidance

Commander's critical information requirements

Course of Action (COA) Development

Key Outputs

Revised staff estimates

COA alternatives with concept narrative and sketch including:
- Objectives
- Key tasks
- Major capabilities required
- Task organization
- Main and supporting efforts
- Deployment concept
- Sustainment concept
- Information operations support themes
- Identification of reserve
- Identification of required supporting interagency tasks

Figure 4 – Course of Action Development

(U.S. DoD, JCS, 2006)

The OODA Model (Observe – Orient – Decide – Act) for Analysis and Conflict Resolution

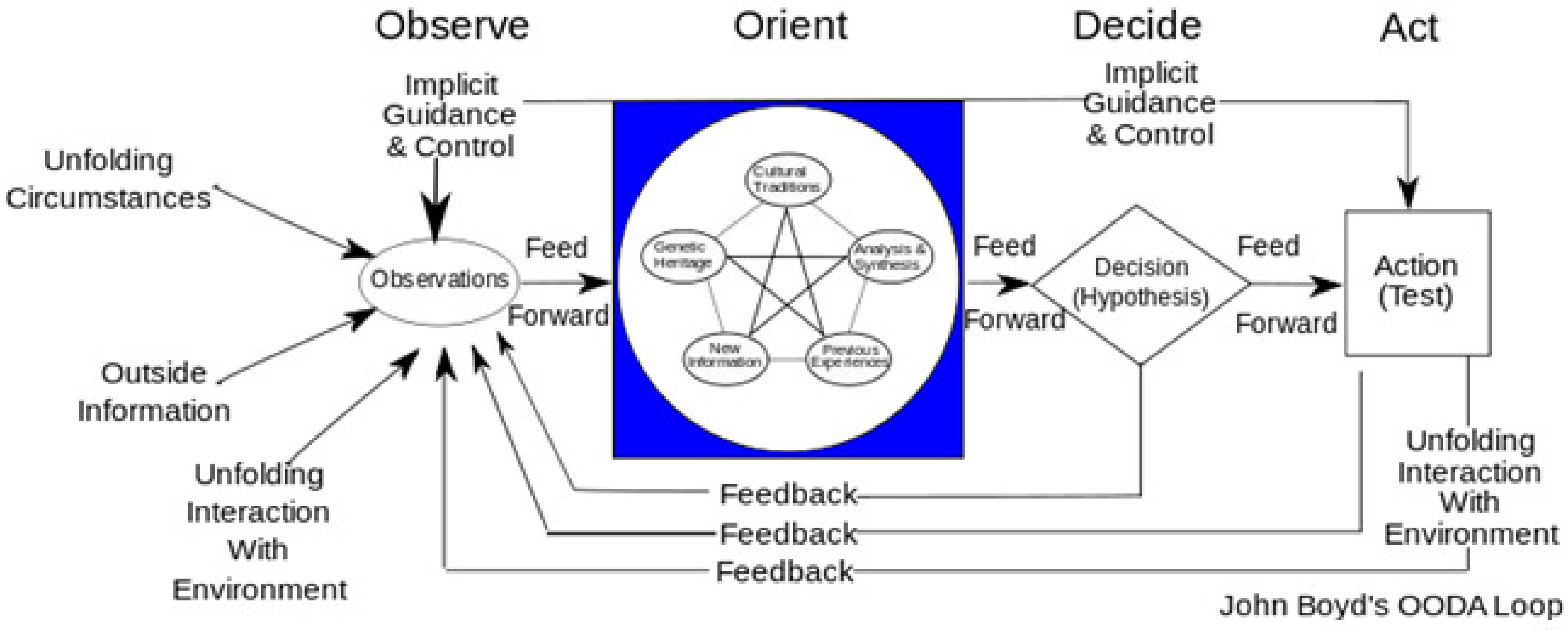
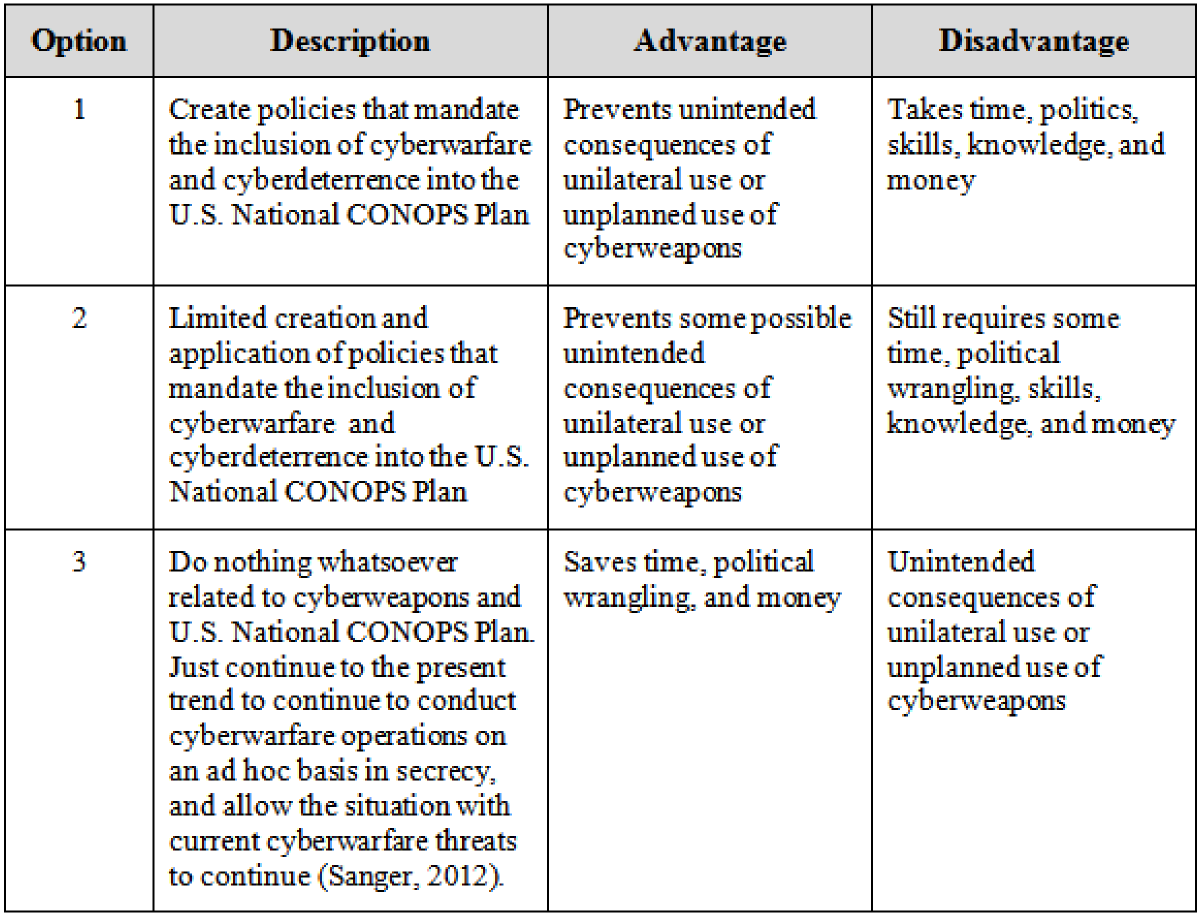


Figure 1 – Boyd's OODA Loop Model (Bousquet, 2009)

U.S. Options in Cyber Conflict



Option	Description	Advantage	Disadvantage
1	Create policies that mandate the inclusion of cyberwarfare and cyberdeterrence into the U.S. National CONOPS Plan	Prevents unintended consequences of unilateral use or unplanned use of cyberweapons	Takes time, politics, skills, knowledge, and money
2	Limited creation and application of policies that mandate the inclusion of cyberwarfare and cyberdeterrence into the U.S. National CONOPS Plan	Prevents some possible unintended consequences of unilateral use or unplanned use of cyberweapons	Still requires some time, political wrangling, skills, knowledge, and money
3	Do nothing whatsoever related to cyberweapons and U.S. National CONOPS Plan. Just continue to the present trend to continue to conduct cyberwarfare operations on an ad hoc basis in secrecy, and allow the situation with current cyberwarfare threats to continue (Sanger, 2012).	Saves time, political wrangling, and money	Unintended consequences of unilateral use or unplanned use of cyberweapons

Table 1 – Comparing Options for Incorporating Cyberwar and Cyberdeterrence Policies and Strategies into the U.S. National CONOPS Plan.

POLICY GENERATION

Policy Generation

- Present **challenges** to creation of policies
- Recommendations for **Cyberwarfare** policy creation
- Recommendations for **Cyberdeterrence** policy creation
- A framework for **Policy Generation**

Challenges to Policy Creation

Challenges
The lack of international definition and agreement on what constitutes an act of cyberwar (Markoff and Kramer, 2009).
The lack of the ability to clearly attribute the source of an attack (Turzanski and Husick, 2012).
The ability for non-state actors to conduct potent cyberattacks (Turzanski and Husick, 2012).
The inability to clearly define what the exact nature of critical infrastructure targets (Turzanski and Husick, 2012).
The massive proliferation and reliance on of ubiquitous, highly insecure, vulnerable systems based on SCADA technologies during the 1980s and 1990s (Turzanski and Husick, 2012).
The continually changing landscape of information technology including the vulnerabilities and threats related to systems that are obsolete, yet remain in operational use for several years past their intended useful life.

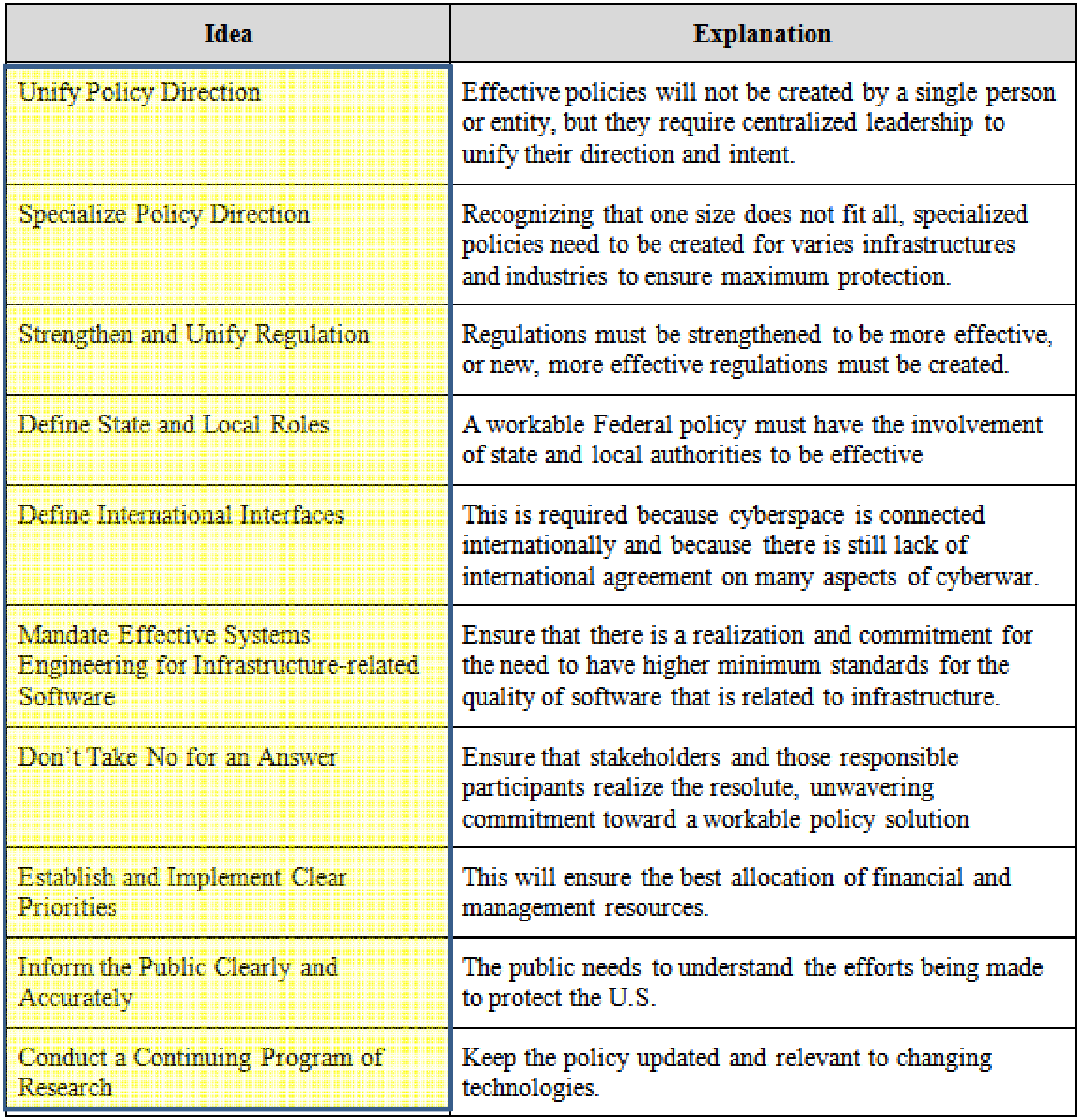
Recommendations for Cyberwarfare Policy Creation

Recommendations
Define the doctrines and principles related to cyberwarfare and the needs under which cyberwarfare would be conducted.
Create the policies that embody these doctrines and principles.
Conduct the intelligence gathering to accurately understand the landscape of the cyber battlefield.
Perform the analysis to create the strategy
Create the strategic plan and tactics
Conduct regular war games, at least twice yearly to test the strategic plan and tactics
Analyze and document the results of the cyberwarfare war games.
Refine the strategies and tactics for cyberwarfare and cyberdeterrence based on the results of analyzing the outcomes of the cyberwarfare war games

Recommendation for Creation of Cyberdeterrence Policies

Recommendations for Creation of Cyberdeterrence Policies
Continue to design, create, possess, and use offensive cyber warfare capabilities when necessary
Develop a defensive system for surveillance, assessment, and warning of a cyber attack. (I think such capability presently exists now)
A declaration that any act of deliberate information warfare resulting in the loss of life or significant destruction of property will be met with a devastating response (U.S. Army, 1997)
Include Crosston's idea of **Mutually Assured Debilitation** (Crosston, 2011).

Policy Generation Framework



Idea	Explanation
Unify Policy Direction	Effective policies will not be created by a single person or entity, but they require centralized leadership to unify their direction and intent.
Specialize Policy Direction	Recognizing that one size does not fit all, specialized policies need to be created for varies infrastructures and industries to ensure maximum protection.
Strengthen and Unify Regulation	Regulations must be strengthened to be more effective, or new, more effective regulations must be created.
Define State and Local Roles	A workable Federal policy must have the involvement of state and local authorities to be effective
Define International Interfaces	This is required because cyberspace is connected internationally and because there is still lack of international agreement on many aspects of cyberwar.
Mandate Effective Systems Engineering for Infrastructure-related Software	Ensure that there is a realization and commitment for the need to have higher minimum standards for the quality of software that is related to infrastructure.
Don't Take No for an Answer	Ensure that stakeholders and those responsible participants realize the resolute, unwavering commitment toward a workable policy solution
Establish and Implement Clear Priorities	This will ensure the best allocation of financial and management resources.
Inform the Public Clearly and Accurately	The public needs to understand the efforts being made to protect the U.S.
Conduct a Continuing Program of Research	Keep the policy updated and relevant to changing technologies.

A 10-step Remedy toward the Creation of National Policy (Kramer, et al, 2009)

Final Recommendations

- Create National Policies that clearly define the U.S.'s capabilities and intentions related to cyberwarfare and cyberdeterrence
- Based on the principles and philosophies described in these newly created national policies, it is imperative to modify the U.S. CONOPS Plan for war with strategies for cyberwarfare and cyberdeterrence
- Following these recommendations will probably make the U.S. and the world of cyberspace a bit safer

CONCLUSION

Conclusion

- In 2012, cyberattacks, cyberweapons, and cyberwarfare events are growing in number and sophistication
- The lack of clear U.S. national policies and strategies that deal with cyberwarfare and cyberdeterrence increases the probability of a massive cyberwar event
- This paper and presentation has reviewed the situation and proposed some answers
- The paper and this presentation with these answers will be sent to **President Barack Obama** for review and consideration by his National Security Team

REFERENCES

References

- Bousquet, A. (2009). The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity. New York, NY: Columbia University Press.
- Carr, J. (2012). Inside Cyber Warfare, second edition. Sebastopol, CA: O'Reilly.
- Crosston, M. (2011). World Gone Cyber MAD: How "Mutually Assured Debilitation" Is the Best Hope for Cyber Deterrence. An article published in the Strategic Studies Quarterly, Spring 2011. Retrieved from http://www.au.af.mil/au/ssq/2011/spring/crosston.pdf on October 10, 2012.
- Fayutkin, D. (2012). The American and Russian Approaches to Cyber Challenges. Defence Force Officer, Israel. Retrieved from http://omicsgroup.org/journals/2167-0374/2167-0374-2-110.pdf on September 30, 2012.
- Hyacinthe, B. P. (2009). Cyber Warriors at War: U.S. National Security Secrets & Fears Revealed. Bloomington, IN: Xlibris Corporation.
- Kramer, F. D. (ed.), et al. (2009). Cyberpower and National Security. Washington, DC: National Defense University.
- Libicki, M.C. (2009). Cyberdeterrence and Cyberwar. Santa Monica, CA: Rand Corporation.
- Markoff, J. and Kramer, A. E. (2009). U.S. and Russia Differ on a Treaty for Cyberspace. An article published in the New York Times on June 28, 2009. Retrieved from http://www.nytimes.com/2009/06/28/world/28cyber.html?pagewanted=all on June 28, 2009.

References

- Obama, B. H. (2012). Defense Strategic Guidance 2012 - Sustaining Global Leadership: Priorities for 21st Century Defense. Published January 3, 2012. Retrieved from http://www.defense.gov/news/Defense_Strategic_Guidance.pdf on January 5, 2012.
- Technolytics. (2012). Cyber Commander's eHandbook: The Weaponry and Strategies of Digital Conflict, third edition. Purchased and downloaded on September 26, 2012.
- Turzanski, E. and Husick, L. (2012). "Why Cyber Pearl Harbor Won't Be Like Pearl Harbor At All..." A webinar presentation held by the Foreign Policy Research Institute (FPRI) on October 24, 2012. Retrieved from http://www.fpri.org/multimedia/2012/20121024.webinar.cyberwar.html on October 25, 2012.
- U.S. Army. (1997). Toward Deterrence in the Cyber Dimension: A Report to the President's Commission on Critical Infrastructure Protection. Retrieved from http://www.carlisle.army.mil/DIME/documents/173_PCCIPDeterrenceCyberDimension_97.pdf on November 3, 2012.
- Articles at http://www.cyberwarzone.com
- Papers at http://billslater.com/writing

Questions?

Send e-mail to William F. Slater, III: slater@billslater.com

William F. Slater, III