Week 09 – Writing Assignment 04

William Slater

DET 630 – Cyberwarfare and Cyberdeterrence

Bellevue University

Conflict Resolution in Cyberwarfare and Cyberdeterrence

Matthew Crosston, Ph.D. - Professor

October 28, 2012

Conflict Resolution in Cyberwarfare and Cyberdeterrence

This brief paper will present the ideas of conflict analysis and resolution as well as possible alternatives to solutions I have proposed related to cyberwarfare and cyberdeterrence policy and strategy issues.

Current Academic Research on This Threat Problem

Since 2007, as the existence of well-orchestrated cyberwar attacks such as the DDoS attacks on Estonia (2007), Georgia (2008), and Kyrgyzstan (2009), as well as the Stuxnet (2010), Duqu (2011), and Flame (2012) have all become known to the world through security researchers, their victims, and the media. As a result, it has become apparent most who are watching this area that cyberspace has now become the new realm onto which the field of international conflict has been extended, and that cyberwarfare is now no longer a theoretical issue that could one day threaten those participants and systems that rely upon connections to the Internet and Internet-connected networks. Unfortunately however, the present findings and research on cyberwarfare related events shows that the U.S. is playing catch-up and doing so badly (Turanski and Husick, 2012).

Intellectual Positions and Theoretical Explanations That Have Been Staked Out on This Threat Problem

As recently as the 2008 – 2009 timeframe, John Boyd's conflict model known as Observe – Orient – Decide – Act (OODA) began to be applied to analyze the ideas of "cybernetic warfare" and "net-centric warfare." The model itself has been analyzed for its ability to simply demonstrate the nature of the complexity of conflict, complete with factors of ambiguity, unpredictability, and so the model has also been used to define the nature of life itself. Yet, the

model is also impacted by the chaotic nature of life and reality. The further shows the similarity between actual cyberwarfare events and this model. Other characteristics of the OODA loop model are its continuous nature and the feedback loops that provide data on which to base some form (or forms) of decision and action. The OODA Loop model is shown in the diagram below:

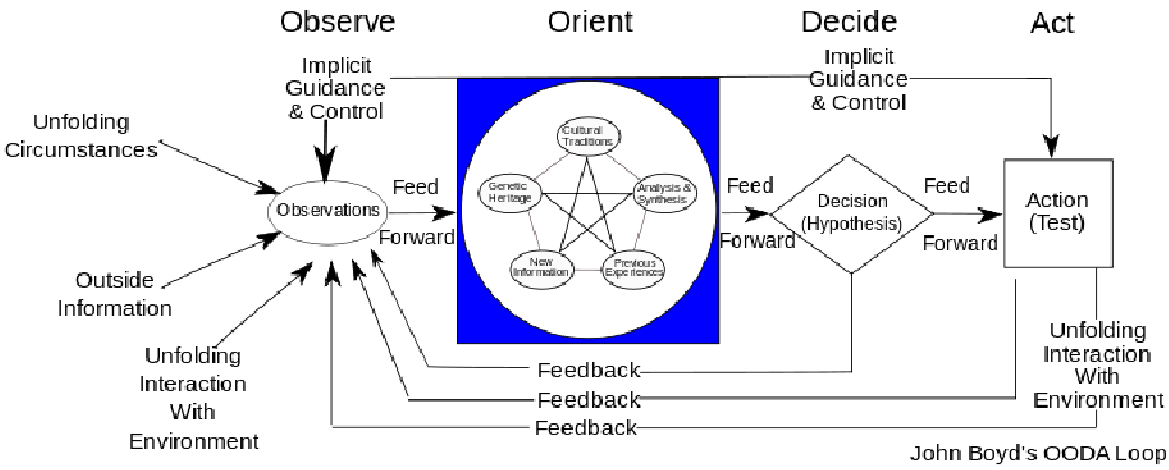

Figure 1 – Boyd's OODA Loop Model (Bousquet, 2009)

However, one key distinction between Boyd's OODA model and cybernetic warfare is Boyd's "focus on the conditions of emergence transformation of systems through information rather than merely the manner in which information is processed by a fixed organizational schema." Boyd would argue that Claude Shannon and others tend to overemphasize the view of information related to structure as opposed to information as a process (Bousquet, 2009).

Joint Publication (JP) 5-0, Joint Operation Planning

As recently as December 2006, the Joint Chiefs of Staff provided an inside look into how the U.S. National War Plan was created and maintained. In the document titled, Joint

Publication (JP) 5-0, Joint Operation Planning. While this publically available, 264-page, document is unclassified, it does provide an extraordinary look into the strategic military thinking, principles, and guidance of the Joint Chiefs of Staff and the National Command Authorities as they create policies and strategies that enforce the national strategic objectives of the United States. This document that was created during the Bush administration, is also significant because it is one of the first official publically known such documents that included cyberspace as part of the operational realm of conflict, along with air, sea, land, and space for conducting military operations (U.S. DoD, JCS, 2006). The high-level diagram below shows simply the concept of the inputs and the outputs that lead to understanding the operational environment of conflict, and it compares somewhat to the OODA figure shown earlier:

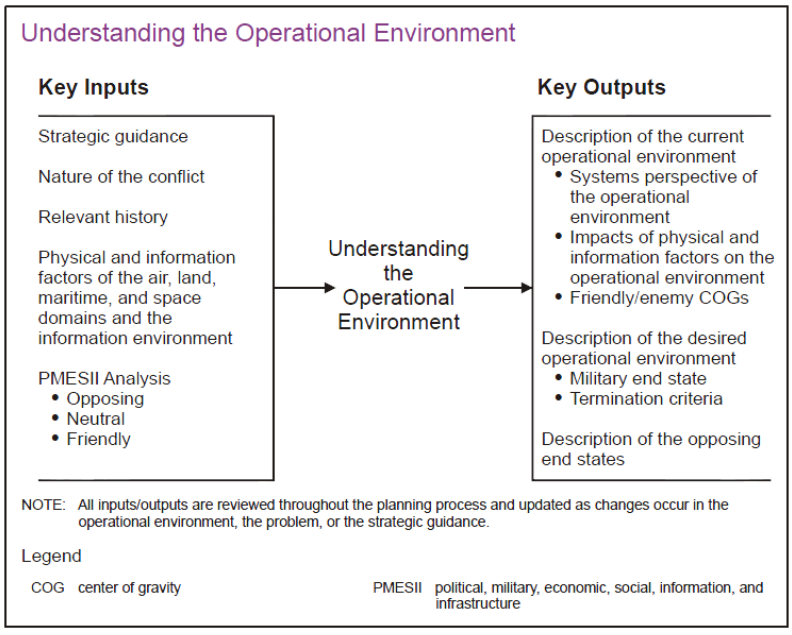

Figure 2 – Understanding the Operational Environment

(U.S. DoD, JCS, 2006)

To further illustrate the intent of the Joint Chiefs of Staff to the diagram below to visually explain the interconnected nature of the realms related to the operational environment of conflict and the nature of the systems analysis required for decision making.

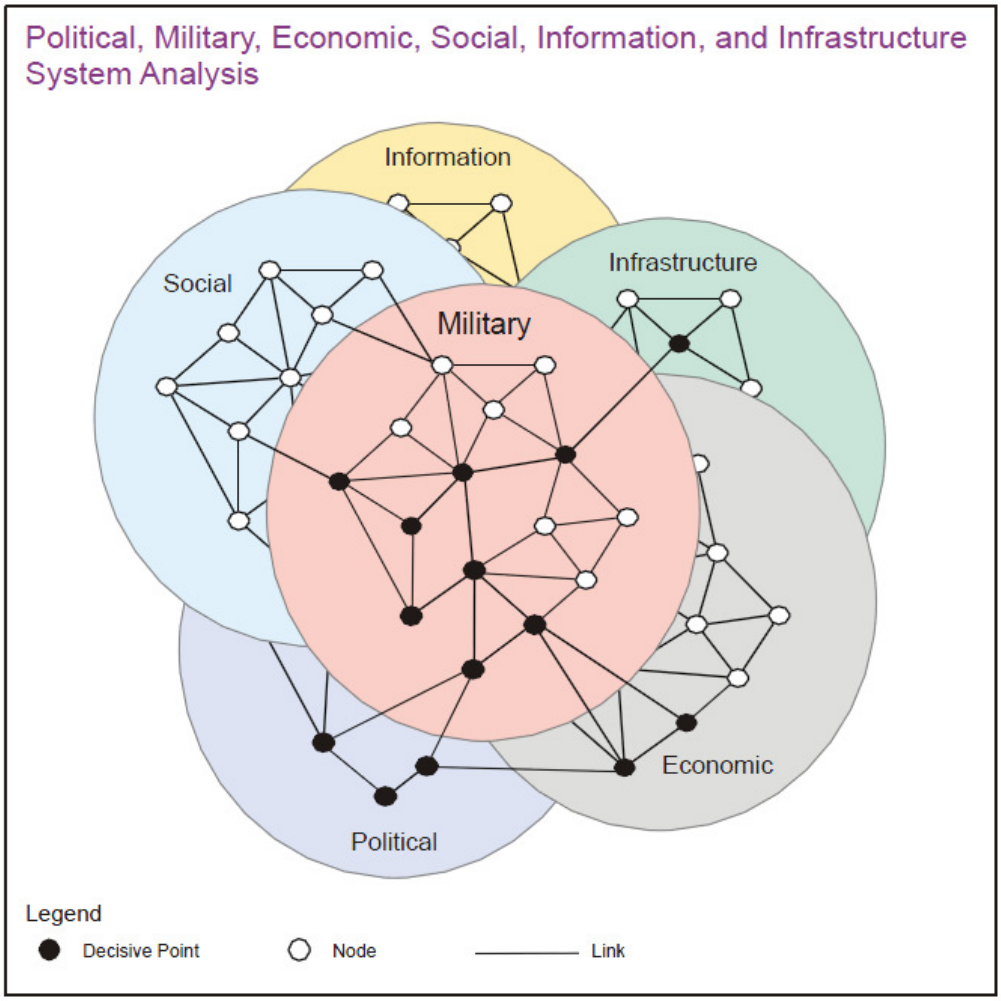

Figure 3 – Understanding the Interconnected Nature of the Realms Related to the Operational Environment of Conflict and the Nature of the Systems Analysis Required for Decision Making (U.S. DoD, JCS, 2006)

The JCS also described the environment of conflict as a place where simultaneity of operations would and this environment would include the information environment and cyberspace:

> "Simultaneity refers to the simultaneous application of military and nonmilitary power against the enemy's key capabilities and sources of strength. Simultaneity in joint force operations contributes directly to an enemy's collapse by placing more demands on enemy forces and functions than can be handled. This does not mean that all elements of the joint force are employed with equal priority or that even all elements of the joint force will be employed. It refers specifically to the concept of attacking appropriate enemy forces and functions throughout the OA (across the physical domains and the information environment [which includes cyberspace]) in such a manner as to cause failure of their moral and physical cohesion (U.S. DoD, JCS, 2006)."

Therefore, the JCS also created a Course of Action framework for determining the best courses of action in a conflict environment, and here again, cyberspace is included in that realm of options in which a course of action could and would be developed (U.S. DoD, JCS, 2006).

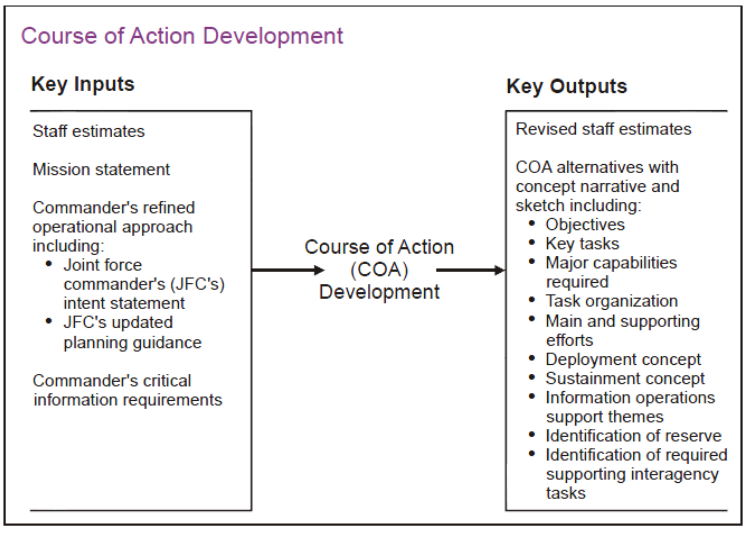

Figure 4 – Course of Action Development (U.S. DoD, JCS, 2006)

Options in Conflict

Based on the current state of where the U.S. stands with the lack of coherent and cohesive incorporated into its National CONOPSPLAN, and the potential for unintended consequences where the unilateral use of cyberweapons can and will occur, I see three possible options for the U.S., and each of these options has advantages and disadvantages.

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.

Conclusion

This paper has presented a brief look at the U.S. Military's recognition of cyberspace as an extension of the operational environment of conflict and a comparison of the options that exist for resolving the issues that threaten America's ability to create the coherent and cohesive policies and strategies that will define its ability to effectively conduct cyberwarfare and cyberdeterrence in the future.

References

Andress, J. and Winterfeld, S. (2011). Cyber Warfare: Techniques and Tools for Security Practitioners. Boston, MA: Syngress.

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.

Czosseck, C. and Geers, K. (2009). The Virtual battlefield: Perspectives on Cyber Warfare. Washington, DC: IOS Press.

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.

Mayday, M. (2012). Iran Attacks US Banks in Cyber War: Attacks target three major banks, using Muslim outrage as cover. An article published on September 22, 2012 at

Poltix.Topix.com. Retrieved from http://politix.topix.com/homepage/2214-iran-attacks-us-banks-in-cyber-war on September 22, 2012.

Saini, M. (2012). Preparing for Cyberwar - A National Perspective. An article published on July 26, 2012 at the Vivikanda International Foundation. Retrieved from http://www.vifindia.org/article/2012/july/26/preparing-for-cyberwar-a-national-perspective on October 14, 2012.

Sanger, D. E. (2012). Confront and Conceal: Obama's Secret Wars and Surprising Use of America Power. New York, NY: Crown Publishers.

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. Department of Defense, JCS. (2006). Joint Publication (JP) 5-0, Joint Operation Planning, updated on December 26, 2012. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf on October 25, 2012.