THE INTERNATIONAL

C2 JOURNAL

VOLUME 4, NUMBER 2, 2010–2011

Cyberspace: The Ultimate Complex Adaptive System

Paul W. Phister Jr.

CCRP
Focus
& Convergence
for Complex Endeavors

THE INTERNATIONAL C2 JOURNAL

About the Journal

The International C2 Journal was created in 2006 at the urging of an international group of command and control professionals including individuals from academia, industry, government, and the military. The Command and Control Research Program (CCRP, of the U.S. Office of the Assistant Secretary of Defense for Networks and Information Integration, or OASD-NII) responded to this need by bringing together interested professionals to shape the purpose and guide the execution of such a journal. Today, the Journal is overseen by an Editorial Board comprising representatives from many nations.

Opinions, conclusions, and recommendations expressed or implied within are solely those of the authors. They do not necessarily represent the views of the Department of Defense, or any other U.S. Government agency.

For more information

Visit us online at: www.dodccrp.org
Contact our staff at: publications@dodccrp.org

Cyberspace: The Ultimate Complex Adaptive System

Dr. Paul W. Phister Jr. (AF Research Laboratory, USA)

Approved for public release; distribution unlimited: 88ABW-2010-1968 dated April 9, 2010.

Abstract

Networks and information systems that are being constructed today are complicated. Integrating these networks together into a global Internet yields an extremely complicated environment. However, this cyber environment is beginning to exhibit traits of a complex adaptive system (CAS). It is the contention of the author that the cyber domain can be thought of as the ultimate complex adaptive system (e.g., the global Internet). Complex adaptive systems are those systems which have the additional important property of being adaptive—i.e., the structure and behavior of the system changes over time in a way which *tends* to increase its success. Within this complex cyber domain, two key aspects are discussed to illustrate that the cyber domain exhibits complex behaviors: 1) *Cyber awareness* (What? Where? When?), and 2) *cyber understanding* (Why? Who?). The cyber environment represents the interaction of complex events and how they relate to the mission being performed in the cyber domain namely: cyber stealth (operating as undetectable as possible); cyber terrain (traversing a series of networks and nodes); and, cyber path (traversing particular links and routers). Two future areas of research—knowledge awareness and understanding, and network science—are discussed as well as applicable technologies.

Introduction

At issue today is how to incorporate cyber operations into the Information Age's net-centric warfare philosophy. It is no surprise that cyber operations have become co-equal with other operations in importance and criticality. In 2006, the secretary of the Air Force added a third arm to the Air Force mission: that of cyberspace. Given the growing importance of the role of cyberspace within the Air Force, a sound strategy for achieving reliable, survivable, assured, and continuous cyber operations has become paramount within the 21st century. In fact, cyber operations have the potential to become an influential power provided by the Air Force. Cyber operations can be thought of as the third leg of a *command and control (C2) triad* (air and space being the other two). By adding this third leg, fundamental methodologies such as effects based operations (EBO) can be greatly enhanced.

The networks and information systems that are being constructed today are extremely complex. An adversary cyber attack against a network could have cascading and devastating effects on other portions of the information enterprise. To defend against a network wide attack, it is imperative that we know what is on our systems and their composition. We need to know what computers we have, what applications are running, what vulnerabilities exist and what networks are related to other networks. Only when armed with this type of information can we possibly adapt our countermeasures and protection procedures to counter an attack.

When considering cyber operations, military time lines will have to be reduced by several orders of magnitude in order to be able to keep pace with operations being conducted within a global cyberspace environment. Time lines to conduct a military operation have significantly been reduced from weeks-months to minutes-seconds. For example, in the mid-1990s, the then Chief of Staff of the Air Force General Jumper embarked on the goal of performing *sensor-to-shooter* operations in *single-digit-minutes*. This was no easy task. The

inter-relationships of data, information, awareness, understanding, and decision making along with the corresponding actions is quite complex. Imagine, conducting a sensor-to-shooter operation starting when a sensor detects a target (t^0) and ending when the target is neutralized (t^n), all occurring within single-digit-minutes or a maximum of 599-seconds. Since multiple entities[1] are involved, there are different time lines for each entity; thus to achieve shared awareness or shared understanding one has to wait for the slowest entity. Now consider 2009, where sensor-to-shooter in the cyber domain needs to be conducted in milliseconds-to-seconds-to-minutes. These are the fundamental issues when dealing with the network centric warfare construct.

What is Cyberspace?

DoD Definition (DoD Memorandum 2008) (RAND 2010, 3):

> **cyberspace:** *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.*

Cyberspace, taken as a whole is extremely complex and encompasses numerous elements as shown in Figure 1.

1. An entity can be an individual, a team, an organization, or a software algorithm, depending on the application.

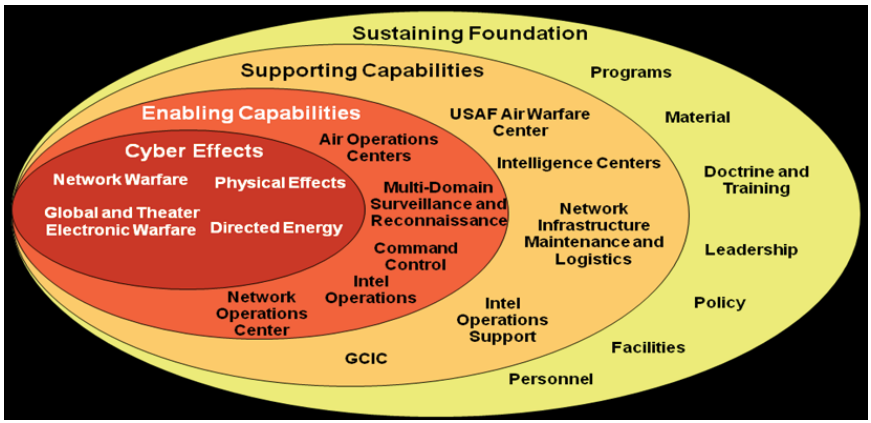

Figure 1. Elements of Cyberspace (AF Cyberspace Task Force 2007)

Cyberspace in the Context of Net-Centric Operations

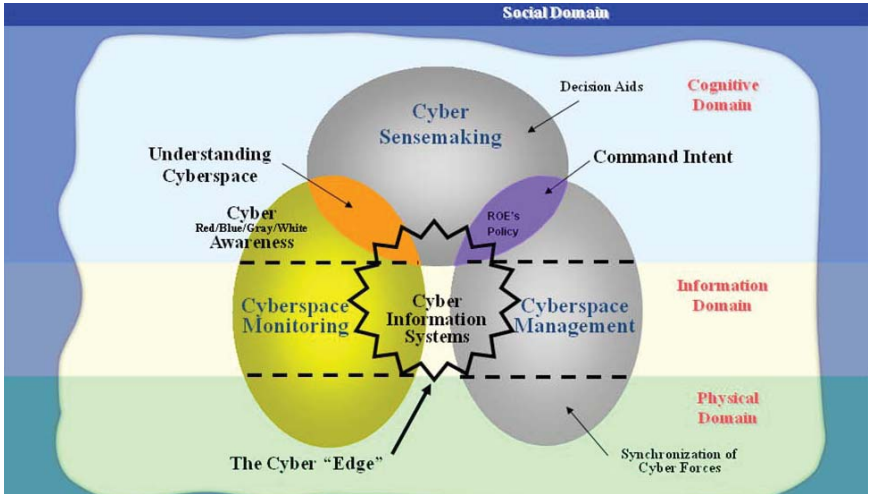

Figure 2. Net-Centric Operations Within Cyberspace (Alberts 2002, 146)[2]

2. ROE = Rules of Engagement, Red = Adversary, Blue = US/Allied, White = Neutrals, Gray = Unknown.

Describing *cyber C2* within a net-centric operations viewpoint is exactly as describing air C2 or space C2. Using Figure 2 as the backdrop, one can describe the various portions of net-centric warfare within a cyberspace context as follows:

Cyber Awareness

Cyber awareness (What? Where? When?) exists in the cognitive and social domains of net-centric operations. Cyber C2 covers red/gray/white as well as blue forces. Being able to capture and display this information provides the battlespace commander with a cyber awareness which can be folded into the entire battlespace awareness picture; therefore, cyber awareness is knowing what is in the cyber environment. Cyber awareness can be thought of as just another extension of the total battlespace awareness already provided by air and space forces. It takes place in the minds of key leaders and their supporting battlestaffs, not in computers. Awareness is achieved through a complex interaction of available information with prior knowledge and beliefs representing the experience and expertise of the battlestaff (Alberts and Hayes 2003, 13-36). Essentially, awareness relates to the operational situation as it currently is or was in the past with the human perception of the situation as it is and as it is becoming; with the goal of being able to totally document what is going on within the cyberspace environment.

Cyber awareness is essentially determining "What's going on?" within the total cyberspace environment[3] and seeks to determine ground-truth that is pertinent to the Commander and is situation dependent. One has to consider the total cyberspace because, unlike traditional military engagements, adversaries can be located anywhere and can engage from anywhere. In cyber awareness, one

3. The total cyberspace has to be considered because, unlike traditional military engagements, adversaries can be located anywhere and can engage from anywhere.

tracks links, nodes, IP-addresses, connections, and logons (to name a few) to build an awareness of interlocking, distributed entities. Cyber awareness can be thought of as just another extension of the total battlespace awareness provided by air and space forces. Table 1 illustrates some examples.

As with traditional C2, cyber awareness covers adversaries, neutrals, friendlies, non-government entities as well as blue forces; but, within the cyber domain of operations. Being able to capture and display this cyber information provides the battlespace commander with a more comprehensive awareness which can be folded into the entire battlespace awareness picture. The questions asked are: What is there? Who is there? How many? What configuration? What locations?

Cyber awareness has to answer the same questions as air and space awareness. By adding cyber awareness to the total battlespace awareness picture, a commander can obtain significant information not previously available by either air or space assets. Consider information on deeply-buried targets. The current air and space intelligence, surveillance, and reconnaissance (ISR) assets are limited to just the physical aspect of the surface terrain (e.g., buildings, cars, trucks, people) to determine activity. By adding the cyber domain to the equation, one can determine: operating systems, applications, number of workstations, number of active workstations, and links to other nodes. This added information would greatly improve courses-of-action (COA) analysis by the military planners.

Cyber Understanding

Also contained in the cognitive and social domains is the next step up, namely, *cyber understanding*. Cyber understanding (Why? Who?) is defined as the process state of drawing inferences about possible

consequences of the operational situation.[4] Cyber understanding is essentially making sense of the available awareness information. It is based on the ability of the battlestaff acting individually and collaboratively to predict possible future patterns of the battlespace. That is, whereas awareness deals with the battlespace as it was, understanding deals with the battlespace as it is becoming. Interpreting these patterns spatially, functionally, and temporally in the context of the goals/objectives, constraints, and planned courses of action envisioned for the operation, the battlestaff begins to identify potential threats and opportunities that demand a response change or decision from the command authorities. The goal is to understand adversarial intentions or to make sense out of seemingly disparate actions/information. Since cyber operations are more distributed than traditional engagements, the influence of friendly/neutral/coalition/civil forces could be significant. The questions asked here are: What does this mean? Why is this or that happening? Are all these seemingly disparate actions correlated? Are we therefore under attack?

Understanding is taking what is and recognizing what it may become. Understanding is defined as the process state of drawing inferences about possible consequences of the operational situation (i.e., anticipation) (Alberts and Hayes 2003, 13-36). It is based on the ability of the battlestaff acting individually and collaboratively to predict possible future patterns of the battlespace. That is, whereas awareness deals with the battlespace as it was, understanding deals with the battlespace as it is becoming. Interpreting these patterns spatially, functionally, and temporally in the context of the goals/objectives, constraints, and planned courses of action envisioned for the operation, the battlestaff begins to identify potential threats and opportunities that demand a response change or decision from the command authorities. Cyber understanding is essentially making sense of the

4. A more detailed discussion of understanding and its context to C2 can be found in Alberts and Hayes's book, "Power to the Edge," pages 13-36 and page 100.

awareness information. The goal is to understand adversarial intentions or to make sense out of seemingly disparate actions/information. Since cyber operations are more distributed than traditional engagements, the influence of gray forces could be significant. The questions asked here are: What does this mean? Why is this or that happening? Are all these seemingly disparate actions correlated? Are we therefore under attack?

Naturally, there will be new challenges and approaches with respect to cyber operations. Some examples being: 1) A cyberspace warrior[5] could be located anywhere and have the ability to disrupt military operations anywhere and at anytime; 2) cyber paths (links and nodes) are similar to traditional flight paths or sea-lane paths but can become extremely complicated to navigate; 3) cyber terrain is expressed in terms of hardware and software; 4) cyber stealth; and, 5) center-of-gravity (COG) location and implications. Currently, military operations COG determination has been largely defined in a physical sense. With the addition of cyberspace, the COG can be defined in an information sense. This is a significant change from traditional thinking. Consequently, this will be a significant challenge to overcome due to the complexity in determining the location and impact of these information COGs.

Within traditional C2, the air and space operations centers (AOCs) control physical entities (e.g., planes); however, when conducting cyber operations, the AOC needs to control information entities (e.g., intelligent agents). The strategies for acquiring information superiority and critical information infrastructure protection are inseparable. Capabilities providing for a superior defense of the United States' critical information infrastructure are required to *control the information space* (Phister and Plonisch 2003), these capabilities include:

- *Protecting* our own information space;

5. Cyber warrior could be either a civilian or military.

- *Detecting* intruders and anomalous conditions;
- *Denying the adversary* that same control;
- *Analyzing and correlating* information to understand attack sources and intent; and
- *Responding* to malicious intrusion attempts and determining courses-of-action, as well as other anomalous inconsistencies within the information environment.

Responding to an information warfare attack is critical. Today we see that it is difficult enough to detect an attack in a timely and accurate manner (i.e., cyber awareness). After an attack is detected and the particulars of the attack are analyzed (i.e., cyber understanding), a response to the attack must be carried out. The response can be as simple as shutting down a connection or prohibiting a specific Internet protocol (IP) address from accessing your network. Other responses may be more complex and include recovering a damaged information system or database, migrating critical processing to another node or network and verifying integrity of mission-critical information.

Cyber Environment

As discussed earlier, the cyber environment is similar to the air and space environments, in that a vehicle has to traverse the medium. Naturally, the context is different, but in all cases items such as location, speed, path to traverse the medium, and surrounding terrain have to be taken into account. Table 1 illustrates some characteristics and how they differ across the air, space and cyber domains. Table 2 illustrates the similarity between the physical and cyber environments.

Table 1. Sea, Ground, Air, Space versus Cyber Domains

Characteristic	Sea	Ground	Air Domain	Space Domain	Cyber Domain
Vehicles	Ships	Vehicles	Unmanned Aerial Vehicles (UAVs)	Space Vehicle (SV)	Network Protocols
Flight Medium	Air and surface	Surface	Air	Space	Physical wires and electromagnetic waves (Ground, Air, Space)
Weapons	Missiles, Bombs	Missiles, Bombs, Cannons, etc.	Missiles, Bombs	Directed Energy	Algorithms
Desired "Effect"	Destroy, Degrade, Deny, Disrupt (D4)	Destroy, Degrade, Deny, Disrupt (D4)	Destroy, Degrade, Deny, Disrupt (D4)	Destroy, Disrupt (D2)	Destroy, Degrade, Deceive, Deny, Disrupt (D5)
Control	Pilot (on-board or remote)	Driver	Pilot (on-board or remote)	Mission Ground Station	Network links that support enemy air, space, ground movements as well as vehicle on-board algorithms
Low Probability of Intercept	Stealth (Physical)	Stealth (Physical)	Stealth (Physical)	Stealth (Physical)	Stealth (Software)
Low Probability of Detection	Stealth (Large Ocean)	Terrain Masking	Terrain Masking	Stealth (Physical)	Network Masking
Home Base	Aircraft Carrier	Various vehicles + installations	Predetermined airfield	Keplerian Orbit	Any cyberspace portal
Logistics	Ranges from heavy/continual to light/infrequent	Ranges from heavy/continual to light/infrequent	Heavy, Continual	Minimal, Continual	Ranges from heavy/continual to light/infrequent

Table 2. Physical vs. Cyber Environments

Attribute	Physical Environment	Cyber Environment
Location	Latitude, Longitude	IP-Address
Speed	Air and ground in mph	Mbps or Gbps through communications links
Path	Roads, Rails, Flight Path, Sea-lanes	Links, Connections
Terrain	Hills, Valleys, Urban Canyons	Operating Systems, Disk Drives, Routers, Switches, Memory Devices, "thumb-drives"
Environment	Rain, Snow, Thunderstorms, Hurricanes	Condition of the links/nodes, protocols[12], speeds of the internet "highways", threats to existence

Cyber Stealth

As with aircraft conducting operations within the air domain, so must an intelligent agent operating within the cyber domain be as undetectable as possible. The concepts of low probability of intercept (LPI) and low probability of detection (LPD) still apply, but their *stealth* applications occur within software versus hardware. The ultimate goal, as with stealth aircraft, would be a software intelligent traversing a network and not be detected.

Cyber Terrain

As an intelligent agent traverses a series of networks, think of these networks as the *terrain*. In the air domain, the aircraft must contend with items such as: roads, bridges, buildings, and mountains. Within the cyber domain, the intelligent agent must contend with such items as routers, servers, computers, and communication links.

Additionally, types of operating systems (Microsoft, Apple, Linux, etc.) must be considered. Figure 3 shows a hypothetical example between the physical and cyber domains with respect to the terrain. As shown, the terrain for air is geographical (i.e., mountains) but the terrain for cyber is primarily hardware (i.e., switches, routers) and software (i.e., operating systems, protocols).

Figure 3. Terrains within Air and Cyber Domains

Cyber Path

Figure 4 illustrates some *paths* within cyberspace. Consider the buildings as various entities, such as routers, servers. The links on the backbone could be thought of as the communication links connecting the various entities. The intelligent agent would navigate this terrain in a similar manner in which one might navigate using Google-Earth. Given the "GPS coordinates" one might calculate such things as shortest path, safest path, and distance to the destination.

Figure 4. Illustration of Paths Within Cyberspace

What is Complexity?

Before we can discuss how cyberspace exhibits traits of a complex adaptive system, we need to discuss "What is complexity?" In most instances, there is confusion between what is complex and what is complicated.

Complicated systems are characterized by having many moving parts or actors and are highly dynamic (i.e., high levels of coupling), that is, the elements of these systems constantly interact with and impact upon one another. The cause and effect relationships within a complicated situation are generally understood which allows planners to predict the consequences of specific actions with some confidence. Complex systems, on the other hand, are characterized by circumstances in which relatively small differences in initial conditions or relatively small perturbations are associated with very large changes in the resulting patterns of behavior and/or strategic outcomes (Alberts and Hayes 2007, 11-15). Some complex situations develop into complex adaptive systems, which tend to exhibit "chaotic behavior" (naturally, not all complex situations are chaotic).

The relationship between complexity and Information Age warfare was discussed in "Complexity Theory and Network Centric Warfare" by James Moffat. One can take this analogy into the cyberspace domain as illustrated in Table 3. Professor Moffat provides a discussion on the differences between complexity and complication. He indicated that "…in complicated systems, the interactions are locally linear…they are locally independent, and their effect is additive (the effect is the sum of the parts)…for a complex system (with non-equilibrium order), the interactions are locally non-linear…the interactions are locally correlated, and the effect is thus more than the sum of the parts."

Table 3. Complexity Concepts as Applied to the Internet

Complexity Concept	Internet (Cyberspace) Domain
Non-linear interaction	Cyberspace as an enterprise is composed of a large number of non-linearly interacting parts.
Decentralized control	There is no centralized management dictating the actions of each and every entity within the cyberspace enterprise.
Self-organization	Local co-evolution induces long-range order.
Non-equilibrium order	Interactions within the cyberspace enterprise proceed far from equilibrium. Correlation of local effects is key.
Co-evolution	Entities must continually co-evolve in a changing environment.
Collectivist dynamics	Cascades of local effects ripple through the cyberspace enterprise.

There are many definitions of complexity ranging from very abstract and mathematical to descriptive and pragmatic. Precise definitions are often difficult to apply and justify, particularly at the boundaries (exactly what is or is not complex?), and different rigorous definitions may imply different boundaries. Moreover, formal approaches may seem obscure to the non-specialist and may not readily illuminate the salient features.

Therefore from a pragmatic point of view we adopt an operational approach—we consider a system to be complex when (Grisogono 2006):

1. *Causality is complex and networked:* i.e., simple cause-effect relationships don't apply—there are many contributing causes and influences to any one outcome; and conversely, one action may lead to a multiplicity of consequences and effects;

2. *The number of plausible options is vast:* so it is not possible to optimize (in the sense of finding the one best solution in a reasonable amount of time);

3. *System behavior is coherent:* there are recurring patterns and trends; but

4. *The system is not fixed:* the patterns and trends vary, for example, the "rules" seem to keep changing—something that "worked" yesterday may not do so tomorrow; and

5. *Predictability is reduced:* for a given action option it is not possible to accurately predict all its consequences, or for a desired set of outcomes it is not possible to determine precisely which actions will produce it.

Another way of putting it is that dealing with a complex system generally is a problem that has high task complexity—*a concept we define as the ratio of the number of ways of getting the wrong outcome to the number of ways of getting it right.*

Nominal Definition

The basic elements of a complex adaptive system are agents. Agents are semi-autonomous units that seek to maximize their fitness by evolving over time. Agents scan their environment and develop

schema. Schema are mental templates that define how reality is interpreted and determine appropriate responses for a given stimuli. These schemas often evolve from smaller, more basic schema. These schemas are rational bounded: they are potentially indeterminate because of incomplete and/or biased information; and they differ across agents. Within an agent, schemas exist in multitudes and compete for survival via a selection-enactment-retention process.

When an observation does not match what is expected, agents can take action in order to adapt the observation to fit existing schema. An agent can also purposefully alter schema in order to better fit the observation. Schema can change through random or purposeful mutation, and/or combination with other schema. When schema change it generally has the effect of making the agent more robust (it can perform in light of increasing variation or variety), more reliable (it can perform more predictably), or more capable in terms of its requisite variety (in can adapt to a wider range of conditions). The fitness of the agent is a complex aggregate of many factors, both local and global. Unfit agents are more likely to instigate schema change.

What is a Complex Adaptive System?

This term is used to describe those complex systems which have the additional important property of being adaptive—i.e., the structure and behavior of the system changes over time in a way which *tends* to increase its success.

This requires that:

1. There is a concept of 'success or failure', (technically known as *fitness*), for the system in the context of its environment;

2. There is a source of *variation* in some internal details of the system; and

3. There is a *selection process*, i.e., the system preferentially retains/discards variations which enhance/decrease its fitness, which requires…

4. Some way of evaluating the impact of a variation on the system's fitness—generally achieved through some kind of external *interaction and feedback*.

5. Thus over time the system generates and internalizes variations which tend to increase its fitness or success—amounting to incorporation of information into the system.

In the most general sense, such a system is interacting with aspects of its environment through taking in *inputs* or sensing, creating *outputs* or taking actions, and some kind of internal processing in between the sensing and the acting. The details of how these three basic functions operate change over time as a consequence of the system being adaptive. So a system which has the property of being adaptive is a system which is always changing by virtue of this adaptive process which is executing. We note that the process is a closed loop and that, because introducing variation will introduce harmful errors much more frequently than useful innovations, the selection process must serve two purposes: the elimination of fitness-decreasing variations most of the time, as well as the retention of the occasional useful fitness-enhancing variations. Complex adaptive systems has all the properties of complex systems, and in addition, displays some characteristic hallmarks of adaptivity (Grisogono 2006):

- "Intelligent" context-appropriate behavior – discovery and exploitation of advantages available in the system's environment, and recognition and appropriate response to threats to the system;

- Resilience – quick recovery from shocks and damage;

- Robustness to perturbations – core functionality is maintained;

- Flexible responses – the system has a range of different strategies towards any given end;

- Agility – rapid change of tack to more effective behaviors when needed;

- Innovation – leading to creation of new strategies and new structures; and

- The system learns from experience – relevant information about past contexts is incorporated.

Optimization of local fitness allows differentiation and novelty/diversity; global optimization of fitness enhances the CAS coherence as a system and induces long term memory. Schema defines how a given agent interacts with other agents surrounding it. Actions between agents involve the exchange of information and/or resources. These flows may be nonlinear. Information and resources can undergo multiplier effects based on the nature of interconnectedness in the system. Agent tags help identify what other agents are capable of a transaction with a given agent; tags also facilitate the formation of aggregates, or meta-agents. Meta-agents help distribute and decentralize functionality, allowing diversity to thrive and specialization to occur. Agents or meta-agents also exist outside the boundaries of the CAS, and schema also determines the rules of interaction concerning how information and resources flow externally (Dooley 1996, 2-3).

Complex adaptive systems involving humans are typically linked across a variety of arenas (DIME—diplomatic, infrastructure, military, economic) as well as the four domains recognized in net-centric warfare (Figure 2).

Additionally, when one views the Internet at the abstract level, some properties emerge to suggest traits of complex adaptive systems (Mitchell 2009, 12-13): 1) complex collective behavior (collective

actions of vast numbers of components that give rise to the complex, hard to predict, and changing patterns of behavior); 2) signaling and information processing (produce and use information and signals from both their internal and external environments); and, 3) adaptation (adapt through learning or evolutionary processes). Taking these traits into account, one can define a complex adaptive system as: "a system in which large networks of components with no central control and simple rules of operation give rise to complex collective behavior, sophisticated information processing, and adaptation via learning or evolution (Mitchell 2009, 13)."

Why is Cyberspace a Complex Adaptive System?

Over the past 10 years, the Internet has grown exponentially with no visible end in sight as to its size or complexity. The World Wide Web can be thought of as a self-organizing social system: individuals, with little or no central oversight, perform simple tasks: posting web pages and linking to other web pages. However, complex systems scientist have discovered that the network as a whole has many unexpected large-scale properties involving its overall structure, the way in which it grows, how information propagates over its links, and the co-evolutionary relationships between the behavior of search engines and the web's link structure, all of which lead to what could be called adaptive behavior of the system as a whole (Mitchell 2009, 10). Figure 5 illustrates a conceptual view of a pilot using the complexities of cyberspace to conduct a mission. Looking at this from a birds-eye viewpoint, one can envision an intelligent agent traversing this network maze (using its terrain, paths and taking into account the environment) to perform a particular mission (or set of missions). If LPI/LPD is an important consideration then the agent must be stealthy (or at least act in a stealthy manner).

Figure 5. Warfighter's Use of Cyberspace

Where the Cyber Domain exhibits most CAS traits is when one considers higher order functions being performed (i.e., knowledge). Referring to Figure 3 as to the major elements of net-centric operations, one can consider the fact that we are moving from net-centric to knowledge-centric operations (Phister and Plonisch 2004) (Phister and Cherry 2005). It is in this new set of operations that non-linearity plays a major role; hence complex adaptive systems.

One way of utilizing this new *network thinking* is to view cyberspace as a macro set of CAS relationships. First some definitions:

- *CAE (complex adaptive entity):* Represents the smallest unit (e.g., person, IP address);

- *CAS (complex adaptive system):* Represents a group of entities that make up a unit (e.g., team, COI);

- *CAS-of-CAS (complex adaptive system-of-systems):* Represents a group of complex systems that make up a unit (e.g., organization, metropolitan-area-network);

- *Family-of-CAS (family of complex adaptive system of systems):* Represents a multi-clustering of complex systems that make up a unit (e.g., global enterprise, global information grid-GIG);

- *COI-of-CAS (community of interest of complex adaptive systems of systems):* Represents the combination of Families of complex systems that combine/terminate at will (e.g., coalition, COI on GIG).

These relationships can be illustrated in Figure 6.

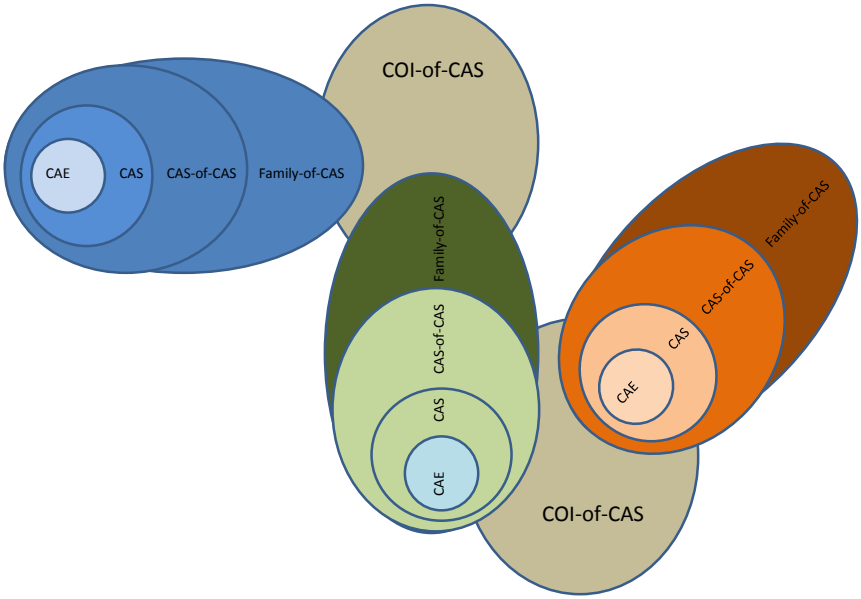

Figure 6. Complex Adaptive System Relationships

Potential Research Areas

Knowledge Awareness and Understanding

One of the most intriguing items when considering a complex adaptive system is that of knowledge. Relating to the previous discussion concerning cyber terrain and paths, this can be expanded into the knowledge domain as:

a. *Knowledge terrain:* This is the outside influences that help to increase/decrease knowledge. Picture it as an x-y-z plane with hills and valleys (similar to the left picture in Figure 3). Some areas are impediments to knowledge and others help gain knowledge.

b. *Knowledge paths:* The path you would take to increase knowledge. For example, in a typical organization, as you advance you typically increase your knowledge bases. A knowledge path follows the knowledge terrain (please note that this is not a unique path).

c. *Knowledge centers:* The closer you get to a center (e.g., air and space operational center) the more knowledge you would have. For example, in a classroom, the teacher would have the most knowledge; students would have lower knowledge on the particular topic of the class (and student knowledge will also vary according to the student).

One research area to explore is what can be called *cyber knowledge awareness*. This would be synonymous with cyber awareness, but one level up on the cognitive pyramid. This area would look at the whole cyberspace and look for areas of knowledge and determine their centers and inter-relationships. This is where the concepts of terrain, paths, centers, and environment can be analyzed to improve what has come to be called CYBINT (cyber intelligence).

Network Science

Over the past decade, a growing group of applied mathematicians and physicists have become interested in developing a set of unifying principles governing networks of any sort in nature, society, and technology. It is believed that a new way of thinking was needed to help make sense of the highly complex, intricately connected systems. This new thinking focuses on the relationships between entities rather than the entities themselves. This new thinking could have a large impact on our ability to engineer and effectively use complex networks, ranging from improved Web searches and Internet routing to controlling the spread of "cyberspace infections (Mitchell 2009, 233)." Within the net-centric warfare construct, the new age way of thinking—network-centric thinking—is similar to this new area of science (Alberts and Hayes 2007, 24).

Through this new *thinking* mentality, there has emerged a new field of science called *network science* (Mitchell 2009, 229-240); which is applicable to the study of cyberspace. Network science examines the interconnections among diverse physical or engineered networks, information networks, and biological networks, cognitive and semantic and social networks. This new field of science seeks to discover common principles, algorithms and tools that govern network behavior. This new theory is very similar to Isaac Asimov's "Psycho-History" outlined in his "Foundation Trilogy." Isaac Asimov took the current definition of psychohistory (according to the psychohistory website, this is defined as the science of historical motivations, which combines the insights of psychotherapy with the research methodology of the social sciences to understand the emotional origin of social and political organizations as well as nations, past and present) and applied it to his trilogy: "Psychohistory depends on the idea that, while one cannot foresee the actions of a particular individual, the laws of statistics as applied to large groups of people could predict the general flow of future events."

Therefore, one might want to explore the following psychohistory axioms as they are applied to cyberspace:

- *Axiom 1:* The actions of a group within cyberspace can be viewed and analyzed at the macro level; and,

- *Axiom 2:* Effective courses-of-action can be developed and implemented to effectively negate the actions of a group within cyberspace, given the indications at the macro-level.

Appendix 1 provides an example list of technologies that could be applied to implement the concepts discussed in this paper.

Summary

Given the growing importance of the role of cyberspace within the Joint Force, a sound strategy for achieving reliable, survivable, assured and continuous operations has become paramount within the 21st century. An adversary's attack against a friendly network could have cascading and devastating effects on other portions of the information enterprise. To defend against a network wide attack, it is imperative that we know what our systems are composed of and what is on our systems. Incorporating cyberspace C2 into the traditional C2 to form a C2 triad (combination of air-space-cyber) will significantly enhance military operations.

Providing that cyberspace can be treated as a complex adaptive system, there seems to be evidence to indicate that the theories of complex adaptive systems can be applied to studying (at the macro level) behaviors within cyberspace. The new research area (network science) seems like a promising area where numerous information technologies would be required. Some of the more important are: a) *physical domain* (e.g., robust intelligent networks, intelligent agents); b) *information domain* (e.g., publish-subscribe and query brokering); c) *cog-*

nitive domain (e.g., multi-intelligence information fusion, reasoning on desired/undesired effects); and, d) *social domain* (e.g., human behavior and cultural modeling).

These examples have become the *framework* or *model* within which cyber operational capabilities and future research directions can be articulated. Within this framework it is possible to identify currently assured capabilities and unaddressed vulnerabilities. The development of this comprehensive awareness and understanding, and the subsequent translation of it into a scientific discipline of information operations, becomes the basis for achieving information superiority within the cyber domain.

References

HQ USAF Cyberspace Task Force. May 15, 2007. "Mission and Challenges." Slide 23.

Alberts, David S., John J. Garstka, Richard E. Hayes, and David Signori. 2002. *Understanding Information Age Warfare*. Washington DC: CCRP.

Alberts, David S. and Richard E. Hayes. 2003. *Power to the Edge*. Washington DC: CCRP.

Alberts, David S., and Richard E. Hayes. 2007. *Planning: Complex Endeavors*. Washington DC: CCRP.

Dooley, Kevin. 1996. "A Nominal Definition of Complex Adaptive systems." *The Chaos Network* 8(1): 2-3.

Grisogono, Anne-Marie. 2006. "The Implications of Complex Adaptive Systems Theory for C2." Paper presented at the CCRTS, San Diego, California, June 20-22.

Mitchell, Melanie. 2009. *Complexity: A Guided Tour*. Oxford: Oxford University Press.

Phister, Paul W., Jr. and John D. Cherry. 2005. "Knowledge Centric Operations: Implications to Future Command and Control." Paper presented at the IEEE Aerospace Conference, Big Sky, Montana, March 5-12.

Phister, Paul W., Jr., Igor G. Plonisch, and Joseph V. Giordano. 2003. "Software Intelligent Agents: A Key Aerospace Vehicle in Cyberspace Environments." Paper presented at the AIAA Space Conference, Long Beach, California, September 23-25.

Phister, Paul W., Jr. and Igor G. Plonisch. 2004. "Knowledge Centric Warfare: Next Evolution of Network Centric Warfare." Paper presented at the 9th ICCRTS, Copenhagen, Denmark, September 14-16.

RAND Study. 2010. "Air Force Cyber command (Provisional) Decision Support."

Appendix 1: Applicable Technologies

To implement the concepts discussed in this paper will require new avenues regarding information technologies. To confront an enemy with the technical capabilities to conduct strategic, coordinated offensive information warfare attacks, and the national resolve to use them, will require more than just purely defensive measures. Future information systems require a variety of capabilities with active responses. They are more sophisticated in character to what might be called hacker style techniques in that they are intended for use as part of a large-scale strategic campaign of warfare designed to control the information lattice and achieve information superiority.

Using the four domains shown in Figure 2, some required information technologies would be:

Cognitive and Social Domains

- Advanced visualization
- High performance computing
- Organizational and human behavior modeling (e.g., cultural)
- Predictive models (e.g., pattern recognition, behavior estimation)
- Real-time, adaptive, and predictive simulations
- Distributed, virtual environments
- Multi-intelligence information fusion
- Information exploitation and understanding
- Knowledge reasoning

- Human behavior models
- Collaboration (distributed virtual environments)
- Real-time remote tasking
- Quality of service (QoS) – cognitive social domains

Information Domain

- Publish-subscribe and query brokering middleware
- Scalable real-time distributed systems
- Secure/survivable information systems
- Cross-domain information sharing (multi-level security, multi-domain security)
- Software wrappers
- Semantic interoperability
- Disadvantaged client services
- Quality of service (QoS) – information domain

Physical Domain

- Robust intelligent networks
- Intelligent agents
- Ultra-wideband and secure communications

- Information assurance (includes wireless)
- High performance computing
- Self-organizing/healing networks (survivability)
- Communications systems monitoring and management technology
- Information assurance
- Multi-domain (multi-national) network management allowing for the allocation of global situational information
- Quality of service (QoS) – physical domain