AIR WAR COLLEGE

AIR UNIVERSITY

CYBERDETERRANCE IN 2035: REDEFINING THE FRAMEWORK FOR SUCCESS

By

John W. Gloystein, Lt Col, United States Air Force

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements
Maxwell Air Force Base, Alabama

February 10, 2010

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

Illustrations

Page

Preface

Stories about the impact of cyberspace on military operations fill today's news, as United States' dependence on cyberspace continues to grow. While many expect a "cyber Pearl Harbor" to awaken the United States to potential vulnerabilities, there are other, more insidious, strategies for a potential adversary. Instead of highlighting the dangers cyberspace's vulnerability poses to US leadership, a nation may profit more by subtly controlling it. If a nation were able to realize this control, it could enjoy a greater advantage than just "reading the mail." It could influence the decisions made by leaders in the United States, possibly avoiding conflict altogether while achieving its strategic objectives. Most cyber deterrence focuses on preventing an adversary from coercing the United States. A more thoughtful adversary would simply shape the information the United States receives to make it think it was acting in its own interests.

I want to thank my paper advisor, Colonel Christopher "Scout" Kinnan, for all his patience and insight. I would also like to thank the instructors in the Center for Strategy and Technology (CSAT) and my classmates who participated in the 2010 Blue Horizons study. Our discussions were always interesting.

Most importantly, I would like to thank my supportive wife. Her perspectives and the inspiration of my children hopefully made this paper more digestible to a larger audience.

Abstract

Cyberspace has become a critical domain for enabling the United States to achieve its objectives. Claims of United States military missions to dominate cyberspace seem at odds with reality. In fact, cyberspace is a contested domain today and the situation is deteriorating. Several characteristics, such as non-attribution and operations at machine speeds combined with policies and laws that have not adapted to the changing realities within cyberspace, give the advantage to the attacker. These characteristics, combined with an increasing use of cyberspace for decision making, cast serious doubts on the ability of the United States to protect its strategic decision making apparatus in 2035.

By 2035, a cyber assistant or "familiar" will support most decisions. Without changes to the characteristics and trends in cyberspace, an adversary may influence US decision-making in the disputed cyberspace domain. This paper analyzes the impact of a cyber familiar using Graham Allison and Phillip Zelikow's decision-making frameworks as well as John Boyd's Observe, Orient, Decide and Act (OODA) loop.

This paper proposes modifications to an equation based upon John Mearsheimer's deterrence ideas, and examines how current cyberspace characteristics' affect variables in the model. Using a modified Mearsheimer deterrence equation as a reference, this paper recommends several policies that should increase the effects of options employed for cyberspace deterrence. These modifications should allow a future cyber familiar to assist leaders without an adversary influencing its processes.

Biography

Lieutenant Colonel John W. Gloystein was a distinguished graduate of the Air Force Academy in 1992. He was selected for a NASA flight sciences fellowship at NASA Langley where he completed a master's in Aeronautics and served as a flight test designer for the F/A-18 High Alpha Research Vehicle. Following undergraduate pilot training, he served two operational tours as an F-16 pilot, which included three deployments to Southwest Asia and a yearlong assignment in Korea. Selected for instructor duty, he flew with the 310th night-vision training squadron at Luke AFB. Lieutenant Colonel Gloystein attended USAF Test Pilot School and graduated as the top graduate. Following an F-16 developmental flight test tour at Eglin AFB, he attended Naval Command and Staff College. After attending the School of Advanced Air and Space Studies, Lt Col Gloystein was assigned to the Lemay Center for Doctrine Development and Education where he wrote Air Force Doctrine on Cyberspace Operations and served as Chief, Commander's Action Group.

Lieutenant Colonel Gloystein is a command pilot with 1700 hours, including 150 combat hours. A developmental test instructor pilot, he has flown 26 different types of aircraft. He has a bachelor's degree in aeronautical engineering, and master's degrees in Aeronautics, National Security and Strategic Studies, and Airpower Art and Science.

Introduction

April 1, 2035: Colonel Straightarrow, the Office of Special Investigation (OSI) agent barged into the AFRICOM commander's office. "Look boss, I know what VIPER (cyber familiar) is telling you about the situation in Nigeria, but it's wrong. I know Captain Pious, and he has been telling me that the crime bosses have been corrupting the information we have been getting over the net. In reality, the Chinese combined human-and-robotic forces have been trying to rid Nigeria of its corruption in an effort to build more oil infrastructure. They have been using nonlethal methods. Their robots cannot kill." The AFRICOM commander paused before he responded, getting an update piped directly into his brain from his familiar. "Look I just received Pious' psychological profile while you were talking. He is clearly unstable. Additionally, I simply cannot ignore the 23 other sources of information I have regarding the atrocities the Chinese and their robots are committing. I have to recommend to the President that he pursue sanctions against China unless they immediately leave Nigeria." The AFRICOM commander paused again, receiving another update, "Now, let's discuss the source behind ***your*** *large bank deposits over the last month…"*

Two recent trends in cyberspace and decision-making indicate this scenario, or something very similar, may play out by 2035. First, the United States increasingly depends on cyberspace. Second, leaders use cyberspace more and more to assist decision-making.

By 2035, leaders may have cyber "familiars" to assist with their decision-making processes. These machines can provide their "humans" relevant information regarding a major decision. In a contested cyberspace domain, an adversary, particularly a nation-state, may find the computers that assist United States' decision makers a desirable target as means to influence leadership decisions. This may range from targeting the United States' decision-making apparatus to destroy (least complicated), to disrupt, to distrust, and to deceive (most complicated) it. This potential reality elicits some questions.

Can the United States deter nation-states from using a contested cyber domain to influence the US decision-making apparatus in 2035? This question raises others. Is the United

States capable of cyberspace deterrence today? If the answer is no, what cyberspace characteristics make this so? What do current trends reveal about what cyberspace could be like in 2035? Finally, what policies can the United States adopt today that will shape the cyberspace domain in a manner that will allow the United States to effectively deter an adversary from attacking the national security decision-making apparatus?

This paper will attempt to answer these questions. First, it will define cyberspace and the information environment. After a review of the relevant characteristics of cyberspace, it will examine current trends and their implications for 2035. It will then discuss how future leaders might use cyberspace to make decisions in the future and the psychological implications that could result. This will alter the current paradigms for decision-making as well as man-machine interaction within the information environment. Specifically, Graham Allison and Phillip Zelikow's models for decision-making and John Boyd's *Observe, Orient, Decide, Act* (OODA) loop will explain the relationship between a decision maker and cyber familiar.

The paper will examine strategies an adversary might use to exploit this relationship. With the potential threat defined, the paper will develop a methodology for understanding deterrence in cyberspace based upon its unique characteristics. By modifying Mearsheimer's cost-benefit deterrence construct based upon realities in cyberspace, the paper will briefly explore why deterrence today has been ineffective. From this starting point, it will discuss policies that might alter future deterrence considerations. Finally, after a summary of key findings this paper will draw several conclusions. From these conclusions, the author will recommend policies, which might help deter a potential nation-state adversary.

Cyberspace Today and Tomorrow

> *From now on, our digital infrastructure -- the networks and computers we depend on every day -- will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient.*
>
> --President Barack Obama[1]

The President has serious concerns regarding the vulnerability of the National Information Infrastructure in cyberspace. With increasing dependence on cyberspace, deterring attacks, especially on national decision-making infrastructure, has become vitally important.

To date, deterrence against cyber-infiltration has been nonexistent. In July 2009, an *unknown entity* conducted scores of attacks against the White House, other government agencies, and commercial homepages. South Korea, also attacked, blamed the North Koreans, yet these attacks seemed to originate in South Korea.[2] Other attacks have stolen mountains of data from sensitive United States government and defense-contractor systems.[3]

Today cyberspace often resembles the American "Wild West"; the offense possesses a distinct advantage. Since these attacks take place at machine speeds, the first to shoot will often win the engagement. This, among other unique characteristics of cyberspace, presents new and complex deterrence challenges. These challenges coincide with increasing integration of cyberspace with human beings. Computers have become more portable, in many different forms, and used in ways never conceived by their creators. Given these cyberspace trends, President Obama's concerns about another nation influencing our vital decision-making systems have merit. From a historical perspective, President Obama is the *first BlackBerry president*. This and the advent of even more powerful cyber devices may be a turning point for senior leaders relying upon cyber assistance to support their decision-making.

President Obama *insisted* that he continue to use his BlackBerry, despite objections from security officers. The President, like many executives, views it as a valuable tool that enhances his leadership. At a recent World Health Care Congress meeting, 200 healthcare and hospital executives used "smart phones as tools to collect, analyze, and report data wirelessly, while at the conference."[4] National leaders and executives will increasingly use cyberspace to assist decision-making. By 2035, the United States' president and other senior leaders will have a wide variety of intelligent cyber-tools to assist them. As to what impact these tools might have on future leaders, one must clearly understand what cyberspace is and what it will become.

Definitions and Background

For purposes of analysis, cyberspace is "is 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."[5] The information environment is "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information."[6] Thus, cyberspace includes the *physical systems* that move information for individuals and organizations. In other (physical) domains, human senses can verify reality. However, in cyberspace, reality is measured and verified by *"the ones and zeroes"* that occupy and enable it. A nation that controls these bits can conceivably manage the perception of anyone using cyberspace. Although it contains physical components, many today view cyberspace as a "cloud."

Cloud computing "enables users and developers to utilize services without knowledge of, expertise with, nor control over the technology infrastructure that supports them. It is, almost literally, operating the service in a cloud."[7] As *The Economist* describes it, "Facebook runs what

is arguably the most successful cloud service, with more than 300 million registered users. It provides a platform for people to communicate, share information and collaborate online—all things that businesses want to do, too."[8] Facebook users access the software applications they need through the cloud. Thus, Facebook users can email their friends without having email software resident and licensed on their own computers.

Two relevant policy considerations derive from cloud computing. First, although it may not concern a user, everyone in the cloud is connected to a physical device or system of devices.[9] These computers and servers are located in a facility in *a nation's sovereign territory* and affect people and organizations within that nation. A country should govern the use of those systems.

Second, the cloud has logical relationships between users and systems. From a decision-making standpoint, one can view the logical relationships in cyberspace as a series of pipes where users access information from sensors to decision makers. The sensors, which are either human or machine, translate physical realities in other physical domains, such as land, sea, space, or air, into data bits for transport. Cyberspace transports the data, converts it (back) into information, and presents it to a user in a usable format.[10] Another way to view this idea is by dividing the information environment into dimensions.

The Information Environment

JP 3-13 divides the information environment into three dimensions: the *physical*, *information*, and *cognitive* (See Figure 1). Computers and sensors turn the physical reality into information, which the user can access. The user then processes the information and makes a decision in the cognitive dimension. Cyberspace exists primarily in the information dimension of the information environment. Cyberspace also has several sub-layers that one must understand to deter cyber attacks.

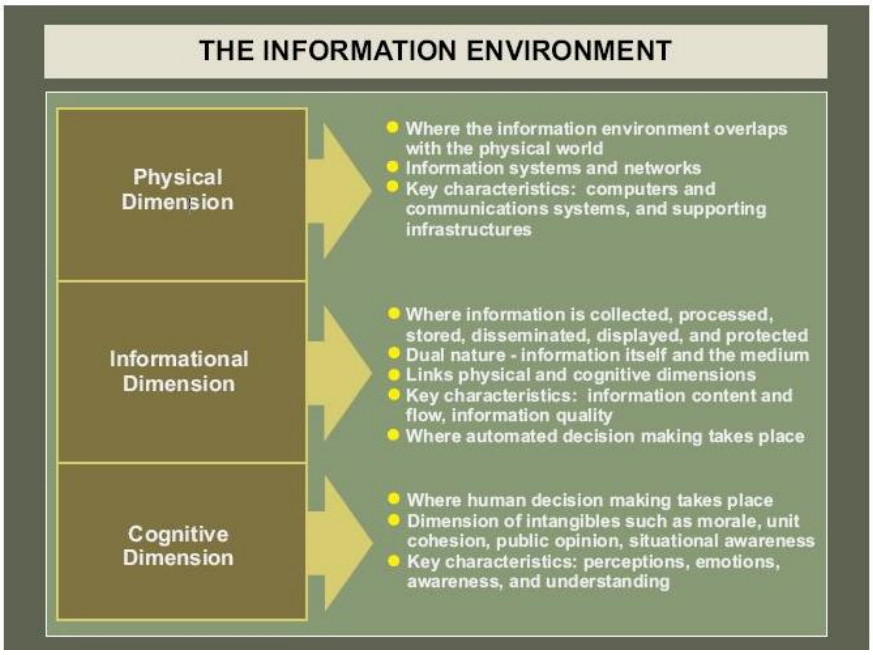

Figure 1: The Information Environment[11]

Cyberspace consists of three layers: the *physical* layer, a *syntactic* layer sitting above the physical, and a *semantic* layer resting on top.[12] Dividing cyberspace into these three layers makes it easier to visualize potential sources for deception in cyberspace. One method of deception might involve physically changing the system hardware. Another, currently used today by hackers, attacks the syntactic layer, potentially causing a system to fail to distinguish friend from foe. Finally, with good knowledge of where a decision support or other similar systems, receive input, one can deceive without disturbing a computer's internal workings.

The physical layer is what the users see on their desktop -- the wires, processors, and routers. Although computers today use silicon chips, this may not be the case in 2035. Advances in optical and quantum computing may change the "hardware." By 2035, the "physical" aspect of cyberspace may hardly be noticeable to each user. Advances in miniaturization and nanotechnology may make computers and processors nearly invisible to the unaided eye. Intel researchers claim that by 2020, people will control computers with their brain

waves.[13] These small computers, possibly imbedded in clothing, could then reach out to the cloud for various applications. Like today, an adversary who can access the physical component of cyberspace in 2035 will be able to deceive users and disrupt information. Physical access is not the only method of a cyber attack. As cyberspace becomes more interconnected, vulnerabilities in the syntactic layer will be exploited.

The syntactic layer controls how computers and networks interact with each other. It is where imbedded protocols allow communication between devices. There may be several protocols stacked upon each other, depending on the configuration of a particular system.[14] Cyber expert Martin Libicki of RAND Corporation states, "This is the level at which hacking tends to take place as human outsiders seek to assert their own authority over that of designers and users."[15] These layers would have no purpose without the semantic, or information, layer.

The semantic layer is where information exists. In *Cyberdeterrence and Cyberwar* Martin Libicki notes, "It is possible to attack computers solely at the semantic level by feeding them false information, like lighting a match under a thermostat to chill a room or creating a fake news source."[16] This may be an extremely useful attack vector in 2035, when cyber familiars autonomously mine information for their "master."

The "pipes" in cyberspace are physical realities and a nation that controls the layers within cyberspace can dictate the information presented. As Dr. Kamal Jabbour, chief scientist for the Air Force Research Laboratory's (AFRL) Information Technology Division stated, "I do not need to understand intent in cyberspace, the chess pieces are all on the board and I can see them all."[17] In other words, anyone controlling the physical and logical landscape inside cyberspace has the power to control the information passing through it. The mission to maintain control of that knowledge is information assurance.

Information assurance (IA) is the "measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities."[18] Achieving information assurance can be problematic due to several cyberspace characteristics.

Characteristics of Cyberspace

Two characteristics of cyberspace today are relevant to deterrence. First, operations within cyberspace occur at machine speeds. Operations must be preplanned or conducted by a machine or program matching a potential attacker's speed.

More importantly, it is difficult to identify attackers in cyberspace. The attacks against the United States and South Korea described previously appeared to emanate from South Korea. Additionally, for some with frequent system failures, it may be difficult to determine whether an actual attack occurred. Anonymity afforded in cyberspace today makes it difficult to deter "bad actors" since it is hard for defenders to attribute attacks to specific nations, groups and individuals. Without attribution, reprisal options for a punishment strategy are extremely limited, thus an attacker has little to fear. Martin Libicki makes the point that a defender may need to demonstrate to third parties that the attribution is correct.[19] A nation retaliating for a prior attack, which was likely invisible to the public, may appear as the aggressor. Additionally, cyber attacks on another nation may have second order effects beyond the intended target, especially since the world is growing more interconnected through cyberspace. For deterrence to be credible, the retaliating nation may be required to announce that it has attacked its aggressor in kind. What trends in cyberspace today may change these characteristics by 2035?

Trends in Cyberspace

Edward Skoudis, in *Cyberpower and National Security*, discusses cyberspace trends:

- Increases in computer and network power
- Proliferation of broadband connectivity
- Proliferation of wireless connectivity
- Transition from Internet protocol version 4 (IPv4) to IPv6[20]
- Increases in software complexity
- Enhanced capabilities for search both across local systems and Internet-wide
- Widespread virtualization of operating systems
- Convergence of technologies
- Increased noise in most aspects of cyberspace[21]
- Increased vulnerability due to advancement of computer and network attack and exploit methodologies
- Worldwide technological development, with different local emphases
- Rise in online communities, collaboration, and information sharing[22]

For the decision maker, these trends make cyber support tools abundant and increasingly useful. The 2008 Obama presidential campaign used Facebook and Twitter to further its message and receive immediate feedback from the electorate. During the campaign, the candidate's website was hacked several times, potentially divulging important campaign rally locations and timetables. Although the campaign staff recognized this, they apparently judged the benefit of direct communication outweighed the potential security threat. Then, *Senator* Obama stated his BlackBerry was vital for receiving current information and making decisions more quickly than any political adversary could.[23]

This information advantage is even more important to *President* Obama. Political events are fast moving and unpredictable; however, a politician can typically receive and assess information quickly and understand the implications in the domestic realm. With international situations, a president must often fight to get information within a more complex and dynamic environment. Thus, it is increasingly important to have devices capable of immediately

receiving and accessing information in order to have a faster decision cycle or OODA loop than a potential adversary. Moreover, the pace of development for information devices is increasing.

Today, many cyber-related applications are relatively autonomous. They adapt and reconfigure for each user. Google's new dashboard aggregates personal information for more than 20 services into one password-protected page.[24] This may increase productivity and efficiency in decision-making, but it is only the beginning. As G. Mark Hardy, President of National Security Corporation, said in a recent interview, "What comes after Facebook, MySpace and Twitter hasn't been invented yet, but two years from now it will have 20 million subscribers."[25] With advancements in artificial intelligence and increasing computational power, it is only a matter of time before independent, *intelligent* systems assist people. Intelligent systems will become necessary due to the increasing level of noise within cyberspace.

Cyberspace has become noisier, increasingly full of "apparently random data without meaning to most users or applications."[26] Because cyberspace is noisy and deterrence is often about sending messages, subtle signals may not be discernable.[27] "Without clear signaling, it is difficult to distinguish deterrence from aggression."[28] The increasing noise in the system allows bad actors to hide their activities, which creates less security.

Securing Cyberspace for the 44th Presidency, written by the Commission on Cybersecurity, categorizes the United States' cyberspace situation as similar to the Germans and their Enigma machine in World War II.[29] The Germans believed their Enigma machine codes could not be broken. However, the Allies were reading their communications, giving them a critical advantage. According to the report, the modern State Department has already lost "terabytes" of information.[30]

The report also claims the most sensitive US military communications are safe.[31] How can anyone know this? The report makes this claim without providing evidence. The claim is contrary to its compelling argument that United States' cyberspace systems, generally, are compromised. With current technologies, computer intrusion is detected only if the "intruder" leaves evidence behind – in other words, when he/she makes a mistake. However, what if there is no mistake? Can the United States government be certain that no infiltration has occurred? More importantly, because many actions are not attributable in cyberspace, people are learning to hack in a consequence-free environment.

Put another way, the Chinese and others are learning how to "ski cyberspace moguls" on US networks; they are only seen when they fall. According Dr. Jabbour, "adversaries have been using *unsophisticated* methods to infiltrate our systems and *they have been very successful* [emphasis added]."[32] These hackers are not just studying our defense systems, they are *testing our policies.* The growing use of cyberspace for decision-making and an increasingly contested cyberspace domain warrant reevaluation of deterrence policy. However, what will the United States deter in 2035 and how will potential attacks affect cyber familiars and decision-making?

The Cyber Familiar of 2035 and Implications for Decision Making

> *"By the late 2030's and 2040's, as we approach human body version 3.0 and the predominance of nonbiological intelligence, the issue of cyberwarfare will move to center stage. When everything is information, the ability to control your own information and disrupt your enemy's communication, command, and control will be a primary determinant of military success."*
>
> —Ray Kurzweil[33]

In some ways, Kurzweil's ideas are nothing new. Even Sun Tzu, 2,400 years ago, understood the importance of knowing your enemy and defeating his strategy. This section

discusses the characteristics of the cyber familiar in 2035 and the psychological ramifications of artificial intelligence (AI). It also examines the implications of artificial intelligences with two decision-making constructs: John Boyd's *Observe, Orient, Decide, Act*, (OODA) loop, and Graham Allison and Philip Zelikow's decision models. Finally, it proposes a modification to the OODA loop for machine-assisted decision-making.

As mentioned previously, by 2035, national leaders will likely possess AI systems, which will pass information and assist with decisions. These "cyber-familiars" will autonomously decide not only what information to present but *if and when to present it*. This independent operation will fundamentally change cyberspace. Instead of the physical dimension connected to the information dimension, which in turn is connected to the cognitive dimension, cyber familiars may occupy all three spaces simultaneously. They will be capable of independent thought and will quickly mine massive amounts of data. They may be empowered to make rudimentary decisions on behalf of their user based upon information preferences and relevance for a particular decision. For decision-making, the most important decisions a cyber familiar might make are where to get information and how to present it to its "master."

This may seem unrealistic to some, the sort of thing for a science fiction novel. In reality, the search engines people use today influence them. When one searches for something on Google, it shows the advertised sites first. Beyond this, programs make decisions, based on interpretation of what the program *thinks* the user wants to see. A recent traumatic event of a colleague provides an example.

An Airman was searching for a wooden model of an F-16 fighter aircraft to use for classroom instruction. He had heard that a company known as "Asian Imports" produced a quality wooden F-16 and typed their name into the search engine to locate the company website.

Immediately, several pornographic images corrupted his screen, which he quickly closed.[34] Violators of Air Force network protocols and inappropriate use of government computer systems can be punished.[35] After a short meeting with the squadron commander, the situation was resolved. In this case, the search engine, based upon the parameters of previous searches *decided* that the questionable web sites were actually what the user was attempting to locate. Search engines make finding information quicker and easier, however, as this example proves, they also determine what the user sees and therefore potentially influence him or her.

This effect would be magnified with powerful, intelligent cyber familiars. As *Joint Publication 3-13, Information Operations* states, "Targeting automated decision making, at any level, is only as effective as the human adversary's reliance on such decisions."[36] This reality will change by 2035, as most people will rely even more on cyberspace for daily decisions. The use of these familiars will not be limited to world leaders. Almost everyone will have some form of a cyber familiar, which may lead to several second order effects.

Psychological Implications

First, leaders (and the population, generally) will develop relationships with their familiars.[37] Indeed, a well-trained familiar will often gather the right information, deliver it at the right time, and present it in a way to make its "master" successful. The 2035 Chief of Staff of the Air Force (CSAF) may be attending intermediate developmental education today. This person probably owns an iPhone, a BlackBerry, or a similar PDA, and seeks the next better information gadget. This future CSAF will likely trust new generations of similar systems and may accept an advanced cyber familiar.

After using cyber familiars to handle crises earlier in their lives, leaders will perceive any new crisis in the same light and use all the tools at their disposal to respond. In fact, Jervis

argues that perceptions are strongest when people experience them firsthand and they derived important consequences for themselves.[38] If this is true, in the future, humans may trust machines more than they trust other humans, especially when users can mold cyber familiars in their own image. While this can enhance their ability to rapidly and effectively respond to crises, it can also lead to an unhealthy group dynamic.

Tailoring information passed from a cyber familiar to its master could lead to a new cyber/human form of groupthink. In this case, the cyber familiar becomes the guilty party as it searches and prioritizes information.[39] The user of the information makes a judgment about what is presented and not necessarily about what underlies the information they are evaluating. As Janis argues, "The more amiability and *espirit de corps* among the members of a policy making in group, the greater the danger that independent critical thinking will be replaced by groupthink."[40] Indeed, the leader will "train" the familiar daily for amiability and suitability. This trend may lead to a future where leaders trust and use cyber familiars with minimal consideration for the effect of the relationship.[41] These relationships have an effect on how people make decisions; therefore, it is appropriate to examine the decision-making constructs developed by Graham Allison, Philip Zelikow, and John Boyd.

Allison, Zelikow, and Boyd Applied to the Cyber Familiar

In *Essence of Decision: Explaining the Cuban Missile Crisis,* Allison and Zelikow use three models to describe decision-making. The Rational Actor (Model I) describes choices nations make as unitary rational actors. This model focuses on the logic of the action in terms of interests of the state.[42] The Organizational Behavior (Model II) describes "acts" and "choices" as output of organizations based upon organizational behavior.[43] This model refers to patterns, functions, and standard operating procedures for acquiring information and implementation. The

Governmental Politics (Model III) relates to actions as a "resultant of bargaining games among players in the national government."[44] Model III considers the key political players, their interests and perceptions, as well as the decision-making procedures.[45] Using Models II and III may more accurately explain certain governmental decisions and are the focus of this discussion.

Applying these models to decision-making in 2035, cyber familiars may provide insight into their effects on governmental decisions since they will affect Models II and III constructs. For the organizational behavior (Model II), cyber familiars may use their own standard operating procedures for acquiring information and may develop predictable patterns of behavior.

For the governmental politics model (Model III) the cyber familiar, as an artificial intelligence, may perform the role of a key player. While operating with a basic program, the familiar is trained by its master to bargain effectively and without any personal agenda. It may engender more trust from the decision maker than its human counterpart. Competing agendas among humans can become distracting, thus it is plausible a decision maker may perceive its cyber familiar as an honest broker. The leader may dismiss other people's input because of perceived bias. If the relationship between the decision maker and cyber familiar is significant, it bears further scrutiny. Examining the OODA loop, with the addition of the cyber familiar, complements our understanding of the effect the artificial intelligence has on decision makers.

Colonel John Boyd proposed the *Observe, Orient, Decide, Act* (OODA) loop as a way to understand decision making in a dynamic environment.[46] The most important step in this loop is *orient*. Boyd called orientation, "the interactive process of many-sided implicit cross-referencing projections, empathies, correlations, and rejections that is shaped by and shapes the interplay of genetic heritage, cultural tradition, previous experiences, and unfolding circumstances."[47] For Boyd, orientation shapes the way one interacts with the environment; therefore, it *shapes the way*

one observes, decides and acts.[48] Boyd also proposed that a faster OODA loop would generate a strategic advantage. This OODA loop interacts with the information environment (see Figure 2).

The *observe* step, for the human today, occurs in the physical and informational dimensions. The human uses his senses to physically experience an event or can experience it vicariously through a device (e.g., on a computer screen, etc.). *Orientation* takes place in the informational and cognitive domains. A senior leader may experience an operation entirely through cyberspace today.[49] *Decision* resides within the cognitive dimension then flows back into the informational dimension. Senior leaders give orders with some sort of electronic assistance. Finally, *actions* occur in the informational and physical domains.

The addition of a cyber familiar will change this relationship. Rather than depicting how the OODA loop operates in all three dimensions of the information environment, it may be more useful to describe the cyber familiar (previously, computer programs confined to the informational dimension) as a separate entity, which supports a senior leader.

Cyber familiars will assist human leaders by rapidly providing them the information needed to help them *observe* and *orient*. By assisting with decisions made at machine speeds some technology futurists forecast the OODA loop could shrink to a point. However, if the familiar is truly intelligent and autonomous, it will have its own OODA loop; one operating at machine speeds. It will provide information to its human user during its *act* step. Therefore, a machine-assisted decision loop does not shrink to a point; rather it appears as two complementary interlinked OODA loops (see Figure 3).[50] Such a symbiotic relationship could afford an adversary an opportunity to influence decision-making by affecting either the machine (which exists in cyberspace) and/or the human.

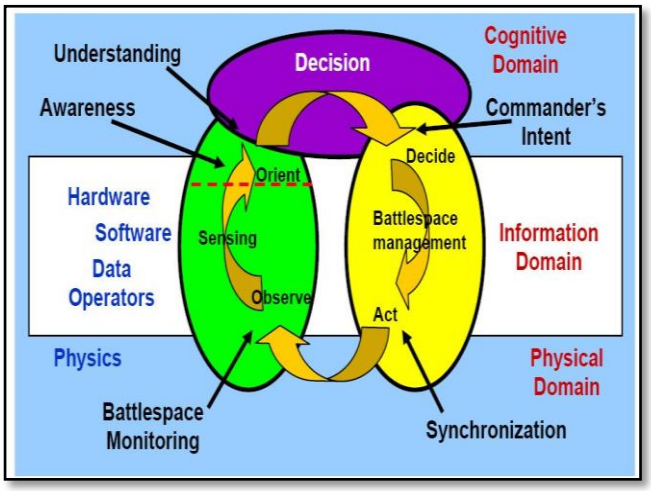

Figure 2: Information Environment[51]

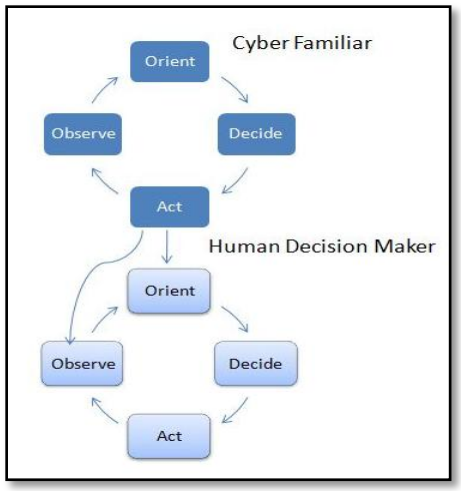

Figure 3: OODA Loop with Cyber Familiar[52]

For example, if an adversary knew the sources of a familiar's information, it could alter data and information at those sources and in a manner such that the familiar would likely change how (or even if) it presented the information to its user. In other words, it could cause the familiar to present information that could produce an inaccurate perspective. If the user normally relies on the familiar's input, this false perspective could fundamentally affect every decision. Significant errors in user judgment could, over time, threaten vital interests or cast doubt on the decision maker, decision processes, and the information used to formulate and execute decisions. It could theoretically slow the decision making process and extend the user's OODA loop. Therefore, an adversary could make decisions much quicker than the user. This is a recipe for mission failure.

This section described how cyber familiars might assist future leaders in decision-making. It also examined how these artificial intelligences interact with humans in the information environment and the overall strategic one. Because cyber familiars may be key players (Model II or III) and directly influence a senior leader's decision calculus (modified OODA), they may become a vulnerability, which an adversary in a contested cyberspace domain can exploit. The next section will explore methods the United States might employ to deter an

adversary from exploiting this potential vulnerability, assuming US decision makers use cyber tools for assistance.

A New Framework for Deterrence

This section will propose a strategy that an adversary might use to influence United States leadership decisions through cyberspace, offer ideas about how current deterrence calculations may be altered in cyberspace in the future, and then propose potential solutions.

In 2035, an adversary will likely use humans and independent cyber programs to influence other humans and programs that make decisions for and on behalf of the United States. Strategies needed to accomplish these difficult influence operations will require careful planning, sophisticated tools, and patience.

Any strategy to influence United States' decision-making must be subtle and coordinated over a long period. An adversary would likely want the United States to maintain its dependence on cyberspace and trust it as much as possible. In this case, for an influence operation to work, complete cyberspace control is not necessary. All an adversary must do is control information at the proper time and place.[53] Adversaries must determine how a cyber familiar acquires its information and how the familiar will process it. An example is the information presented to a Google user today. Although more relevant information sources may exist about a particular subject, organizations fill the page with their paid advertisements. While this is how Google pays the bills, an adversary could populate the cloud with several bogus sources of information at the right time and place if it knew where the cyber familiar typically acquired its information.

An adversary can affect United States' leaders along a continuum. They can move from simple techniques to disrupt, delay, and destroy information flow to more advanced techniques

to cause decision makers to distrust information systems. Such distrust could slow decision-making. There are several examples where this has been accomplished though other media.

In 1942, the British planted a dead body resembling a spy, with invasion plans in his briefcase. "Operation Mincemeat" deceived Hitler into believing the allies would conduct a two-pronged attack in Africa. Another example was when the KGB created the impression that the CIA was responsible for the assassination of President John F. Kennedy. Operation, ARLINGTON, as described by KGB defector Vasili Mitrokhin, detailed how the KGB used its knowledge of the United States' media to destroy confidence in the CIA.[54] Both of these examples proved effective because the deceivers had a thorough understanding of how information flowed to decision makers and the public.

In cyberspace in 2035, such attacks may not need to be as elaborate. An adversary can simply place the information directly into the system at the correct time and place. Additionally, if artificial intelligence exists, these cyber entities, the evolution of today's cyberbots, can autonomously attack the United States.[55] The development of intelligent systems will require not only a reevaluation of decision-making constructs, but also a reevaluation of deterrence itself.

Deterrence Revisited

Deterrence is "the prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction."[56] John Mearsheimer's deterrence ideas can be expressed as an equation to explain an adversary's decision calculus as a cost-benefit analysis. Mathematically, it is the probability of success times the value of the perceived reward and the probability of failure times the perceived consequences of failure.[57] If the former is greater than the latter, deterrence fails. Written as an equation, if $(P_{success}*Value_{success}) - (P_{failure}*Value_{failure}) > 0$, deterrence fails.

One must examine a deterrence strategy in terms of denial and punishment. In a denial strategy, sufficient countermeasures and defenses exist to deny an adversary options for an attack. This lowers the probability of success in Mearsheimer's deterrence equation. A punishment strategy may provide a potential adversary "powerful incentives to choose a particular way."[58] This either lowers the value of success or increases the value of failure depending upon one's point of view.

In cyberspace, such a cost-benefit analysis would change, as there may be several outcomes of an unsuccessful attack. First, an attack may not be classified as an attack (due to noise in cyberspace described earlier), or the target knows of the attack but cannot identify the attacker. This modifies the equation because there is no longer just success or failure. There is also a probability of non-attribution, or worse, false attribution. These variables are independent of whether the attack was successful or not. This increases the potential for attack and decreases deterrence. With this realization in cyberspace, Mearsheimer's deterrence equation becomes

$$[(P_{success}*Value_{success)} + P_{No\ Attribution} + (P_{False\ attribution}* Value_{False\ attribution})] - (P_{failure}* Value_{failure}) > 0.$$

This revision of Mearsheimer's deterrence equation enhances the understanding of potential strategies the United States can employ to affect an adversary's decision calculus and, if successful, deter them. As implied by the elements of this equation, the United States can implement policies to lower the probability of success, lower the perceived value gained from a success, increase the probability of failure and increase the perceived cost associated with failure. Most importantly, it can decrease the probability of non-attribution. Additionally, with an intelligent computer program, one that can act independently, one can arguably deter either the program or the human deciding to use it. With these realizations, this offers an opportunity to effect policies that could change the probable outcomes.

Deterrence Options

The high probability of non-attribution for a cyber attack today presents some challenges. As Libicki discusses in *Cyberdeterrence and Cyberwar*, although the odds of apprehending a cyber attacker are low, increasing the punishment may not successfully deter an adversary. This is true as "rare severe punishments tend to be perceived as disproportionate and hence less legitimate."[59] An adversary may view such a response as an act of escalation. Even worse, an attack may be falsely attributed to a third party, which the attacker might view favorably.

The United States *must completely redefine and reconfigure cyberspace* to ensure greater identification of users, decreasing the probability of non-attribution. Transition to IPv6 is only the beginning. The American public must revise its conceptions of cyberspace from a "cloud," where identities are hidden; to a mall or other "commons" where masked individuals are held in suspicion and may be interrogated by security personnel merely because of their attempt to conceal their identity.

While the United States already views cyberspace as a commons for trading goods and services, it does not apply laws to this medium as in other commons. Like the Transportation Security Administration at United States' airports, security should ensure that potential attackers do not bring weapons into these commons to inflict harm. This does not mean the United States government should invade personal privacy. There is a considerable difference between eavesdropping on a conversation and determining one's identity and searching for weapons. The United States has the right to determine identities within its sovereign cyberspace territory. So what constitutes United States' cyberspace?

Changes to make attribution a reality will require modifying the existing norms in the cyberspace, within United States territory and at every "border." As Mary Ann Davidson, the

chief security officer for Oracle, pointed out in her 18 November 2009 testimony before the House Homeland Security committee, "any new U.S. government framework for cyberspace should also respect the global nature and shared ownership of cyberspace by mapping policies to existing legal and societal principles in the offline world."[60] In other words, the United States should defend its cyber "turf" under the guise of a Monroe Doctrine for Cyberspace.[61]

For example, although searches require a warrant inside the United States, they are *not required* at the border.[62] The United States should search all incoming cyberspace transmissions as a general policy. This will require classifying physical portions of cyberspace as "border crossings." These would include satellite download stations, wireless networks near a physical border, and locations where fiber optic cables physically enter the United States. Of course, adjacent cyber territories with which the United States has had few problems will be treated differently than borders from which cyber attacks often emanate and this reality may form the basis for another policy, which can increase deterrence.[63]

If one knows the *physical location* associated with an IP addresses or the network that controls that address, networks can automatically slow traffic, to conduct a more thorough search, as cyber weapons enter the system from another network. This will have the effect of slowing networks from which trouble emanates. Users of these networks will either leave them or demand connectivity. Nations may not know who is attacking them, but systems will stand a good chance of identifying *the source of the physical attack.* Ideally, entry points into United States' cyberspace will cause minimal delay as data is screened and a threat determination is made. However, if attacks routinely come at a certain "border," defenders must employ more thorough and robust defenses.[64] These defenses must not focus on one layer of cyberspace.

The United States must also actively defend *all* layers of cyberspace – akin to a *defense in depth*. To date, most defensive efforts have been in the syntactic layer, however, as described above, the emergence of autonomous programs has blurred the lines between the layers of cyberspace. Therefore, the United States must search for potential vulnerabilities in each "band" of cyberspace. World War II provides an example of this. The Germans searched for evidence that the British were using radar prior to World War II, and although they found the radar station, they searched in the wrong frequency.[65] With a multispectral defense, the United States can ensure it is not looking "out of band" decreasing the probability of adversary success.

The battle for the destruction of British radars offers another important deterrence lesson. After the Germans attacked and destroyed a British radar site, the British mounted a transmitter atop one of the towers.[66] This gave the Germans, now listening in the correct frequency, the impression that despite all their efforts, the site was still operational.[67] Even in cyberspace, this "denial by deception" approach can serve to lessen an adversary's *perceived value of success*, as even a successful attack will only temporarily affect your opponent. This approach might prove useful in a virtual domain like cyberspace as it might deceive an adversary, thereby lowering the perceived probability of success.

Another possible method for securing the vital information is to place false data in the machines. A human could provide, after proper verification, a verbal cipher or mnemonic to make the information presented within cyberspace make sense. For a simple example, if the database contains coordinates, one could verbally instruct each user that all 3's in the left column were really 5's. Without knowing this fact, the data would appear corrupted to a would-be attacker. This can also lower the perceived value of success for an adversary because the information they are attempting to tamper with in cyberspace would not match physical realities.

The cyber familiar can also be "trained" to use multiple and random sources of input for its OODA loop. The more sources used could theoretically dilute the importance or effect of false or misleading information. In this way, attacks in the semantic (information) layer (remember the lighter under the thermostat example) become less effective. This reduces the *probability* of adversary *successfully* influencing the user's decision loop.

To summarize, this section provided several policy recommendations to enhance cyberspace deterrence. First, the United States must know the *identity* of every person operating within its cyberspace. Therefore, it must define United States' cyberspace and determine its borders. Second, it must automatically search all incoming cyberspace "transmissions" at every border. Third, it must punish connecting systems at these borders that have proven unable to prevent attacks, which freely transit their systems. Fourth, the United States must defend all layers of cyberspace. Fifth, the United States must not allow an adversary to know if it has been successful in a cyber attack. Sixth, to protect the most vital information, the United States should not place certain information in cyberspace that cannot be decoded without a "key." Finally, US decision aids should use random and multiple sources of information.

Traditional punishment strategies may not be effective in cyberspace. This is especially true for the United States today, as it is more dependent upon cyberspace than most of its potential adversaries. This may not be the case in 2035.[68] If the United States can convince other nations to adopt and follow a secure cyberspace regime, it may deter malevolent actions by changing the interests of other nations. This may be an indirect form of a punishment strategy because a nation understands its attacks may not only injure the United States, its attacks may also hurt itself. The United States may be able to create this situation through soft power.

Deterrence through Soft Power

Joseph Nye defines *soft power* as getting what you want through attraction.[69] It is about getting others to buy in to some of your values. They need not buy into all United States' values. Any shared interest may create soft power, and that power may be useful for deterrence. Shared interests are common; the difference with deterrence through soft power is that the shared interest is created by the soft or attractive power. Deterrence through soft power has the benefit of *lowering* the value of an adversary's success and raising the cost of its failure.

It lowers the perceived value of success because either interdependence directly injures the government, its economy, or lowers the governments standing with its own people. This may have more potential in what Thomas Friedman describes as the flat world of today—especially in cyberspace.[70] Cyberspace delivers US culture and values to more people than previous sources of media. As Friedman points out, cyberspace is drawing the US population closer to the Chinese people than to the Mexican people.[71] Thus, any action taken by China to disrupt that connection may hurt it economically as well as socially.

This is a punishment strategy, but not in the traditional sense. The act of attacking the United States also harms the attacker, without any explicit actions taken by the United States government. The destruction or disabling of Global Positioning satellites (GPS) provides a useful example. Although destroying the GPS will create significant problems for the United States economy and military, doing so will also significantly harm the attacker. Modern transportation, agriculture, medicine, communications, and other human services depend on the precision, navigation, and timing GPS provides. Thus, disabling or destroying CPS infrastructure could disrupt or disable the internet globally for a period. Thus, it is in the United States and China's best interests to ensure the GPS keeps functioning.

Another potential punishment inflicted on a would-be attacker is the effect on a third party. Even if North Korea does not value GPS, its trading partner, China, does. So long as China remains its principle trading partner and a guarantor of North Korean sovereignty and regime survival, this indirect form of deterrence will keep the North Koreans in check, with no immediate action required by the United States government.

Third parties may also react negatively to even a failed attack, raising the value of failure. The United States may not be the only nation that responds to an attack on the GPS constellation. An attack on GPS would injure several nations. Moreover, it would be clear to each nation affected *exactly how* this attack would damage them.

A potential strength of this strategy is its transparency. The target nation completely understands the nature of its symbiotic relationship with the United States. Therefore, it can accurately quantify its losses in the case of separation between itself and the United States.

This strategy will require proactive actions. If one assumes that China is a rising power, the soft power strategy might be effective against it.[72] Although there may be cultural differences between the United States and China, these are decreasing because of the internet. In fact, China possesses the most English speaking internet users today. Additionally, such a strategy does not include using hard power against the target. The target must perceive that the United States is acting in their interest. The United States can use hard power against third parties, but must carefully consider the target nation's perspective and frame any action in terms that nation would perceive benefits them.

Recent warnings from Google regarding shutting down its operations in China may provide an example of a potential application of a soft power deterrence strategy. Google, reacting to cyber attacks against its users and other companies, recently changed its operations in

China.[73] It will no longer filter searches in accordance with Chinese government wishes and threatened to pull out of the country altogether.[74] The economic symbiotic relationship for jobs and technical transfer to China combined with the potential social repercussions such as loss of connectivity between the United States and China might be enough to dissuade the Chinese government from continuing its cyber attacks. The US government did not need to threaten China, yet its goal of limiting cyber attacks emanating from China may be achieved through pressure brought by a commercial company. At the very least China will consider the financial implications of its cyber activities.

This section posited several policy options and introduced the concept of deterrence through soft power, the next section will summarize these policy options to make recommendations and draw conclusions.

Conclusions and Recommendations

> *Finally, the general unreliability of all information presents a special problem in war: where all action takes place, so to speak in a kind of twilight, which, like fog or moonlight, often tends to make things seem grotesque and larger than they really are.*
>
> --Carl von Clausewitz, *On War*

If, in the next 25 years cyberspace changes as rapidly as the previous quarter of a century, cyberspace strategists and policy makers will have to adapt quickly. While President Obama may have his BlackBerry today, future leaders will have informational assistants, like VIPER (the cyber familiar described at the beginning of the paper), that are much more powerful—and potentially more vulnerable. These assistants may *appear* to alter the reality that Clausewitz described. Deterrence against adversaries that seek to tamper with these systems must begin

today. It must begin with policies that can evolve as cyberspace "actors" do and it must shape the evolution of new actors. This section will summarize findings by answering the questions posed in the introduction, and provide concrete policy recommendations.

Can the United States deter nation-states from using a contested cyber domain to influence our decision-making apparatus in 2035? Yes, however, this will require United States' leadership to alter the cyberspace regime to deter potential adversaries and motivate other nations to support mutually beneficial uses of cyberspace.

Is the United States capable of cyberspace deterrence today? If the answer is no, what cyberspace characteristics make this so? Several cyberspace characteristics are responsible for this. First, there is a perception that everyone is connected to a ubiquitous "cloud," which has no borders. Second, operations within cyberspace occur at machine speeds. The defense against which must include preplanned actions (indicating one knew, *a priori*, the nature of an attack) or programs that have limited independence and capabilities to respond to an unforeseen event. Third, it is very difficult to attribute attacks in cyberspace and, even if attribution is possible, difficult to prove the identity of an attacker to a third party. Fourth, the "noise" level in cyberspace makes it difficult to detect an attack and makes signaling less clear. Each of these characteristics influences the variables in Mearsheimer's deterrence equation (See Figure 4)

$[P_{success}*Value_{success}+P_{No\ Attribution}+P_{\ False\ attribution}*\ Value_{\ False\ attribution}]-[P_{failure}*\ Value_{failure}]>0.$

What do current trends reveal about what cyberspace could be like in 2035? First, increasing artificial intelligence within cyberspace may change which entities are in the physical, informational, and cognitive dimensions of the information environment. These cyber familiars may or may not be able to discern the information from the noise in cyberspace. Without this information, it is difficult to determine the cyber familiar's influence on deterrence. Current

trends also indicate that future leaders will rely on cyber familiars more than they currently rely on programs and communications within cyberspace today. This reliance decreases the overall deterrence by increasing the perceived value of success.

Characteristic	Equation component affected	Probability of Deterrence Success
No borders	Increases Probability of No Attribution Increases Probability of False Attribution	Decreases
Machine Speeds	Increases Probability of Success	Decreases
Difficult to prove attacker's identity	Increases Probability of No Attribution Increases Probability of False Attribution	Decreases
High Noise Level	Increases Probability of Success Increases Probability of No Attribution Increases Probability of False Attribution Decreases Value of Failure	Decreases

Figure 4: Today's Cyberspace Characteristics Effect on Deterrence

Finally, what policies can the United States adopt today that will shape the cyberspace domain in a manner that will effectively deter an adversary from attacking the US security decision-making apparatus? This paper identified several policies, summarized in Figure 5.

Policy	Equation component affected	Probability of Deterrence Success
Claiming sovereign territory within cyberspace and insisting on knowing one's identity within US cyber territory	Decreases probability of nonattribution Decreases probability of false attribution	Increases
Searching all transmissions at the cyber border	Decreases probability of nonattribution Decreases probability of false attribution	Increases
Multispectral defense	Decreases probability of success	Increases
Restrict connectivity at "bad acting" cyber borders	Decreases probability of success Lowers perceived probability of success Lowers value of success	Increases
Denial by deception	Lowers perceived probability of success	Increases
False information in cyberspace	Lowers value of success	Increases
Multiple/ random inputs to cyber familiar	Lowers probability of success	Increases
Deterrence by soft power	Lowers value of success Raises value of failure	Increases

Figure 5: Proposed Policies Effect on Cyber Deterrence

These proposed policies can increase deterrence against an adversary; however, it is unlikely that policy implementation will affect the near term. These policies require the United States to lead a multinational effort to create a *new regime* within cyberspace, through bilateral

or multilateral treaties or through the World Trade Organization. The United States must prove to its partners that such a framework will serve their interests as well as its own.

The path to 2035 will be full of surprises; however, one thing remains certain. The United States cannot continue to view deterrence the way it has in the past. Mearsheimer's cost-benefit analysis may provide a good start, however the variables in it may change as cyberspace evolves. As cyber familiars become more important and more complicated, they may transition from linear, rational behavior to nonlinear, irrational behavior as Model II (Organizational Behavior) and Model III (Governmental Politics) decision-making constructs suggest. Additionally, understanding the implications of an OODA loop with a cyber familiar may provide insight into the causes for the aforementioned irrational behavior of the system.

It may never be possible to have perfect information; however, the United States should prioritize the fight to ensure it receives accurate and timely information through cyberspace. VIPER, the AFRICOM commander's familiar in the 2035 Nigerian scenario, should at least report that it could not draw a conclusion regarding the situation on the ground because it was not completely confident in its information. This paper serves as a warning that despite the promise of cyberspace and the tools within it offering *perfect knowledge* to a decision maker, the opposite may be true. Indeed, a wise adversary will continue to allow U.S. decision makers to believe they understand a situation completely, until a situation becomes a *fait accompli*, and the United States cannot do anything about it. Despite all the technological advances of the 20th century (and this paper argues, because of the technology), Clausewitz's notions of the fog of war may not have changed substantially.

Bibliography

Air Force Doctrine Document 2-5, *Information Operations*, 20 Sep 2002.

Allsion, Graham and Zelikow, Phillip. *Essence of Decision: Explaining the Cuban Missile Crisis*. New York: Addison-Wesley Educational Publishers, 1999.

Boyd, John. "A Discourse on Winning and Losing." Maxwell AFB Lecture. August 1987.

Clark, Richard. "War from Cyberspace." *The National Interest.* Washington D.C. 20 October 2009. http://www.National interest .org/ Article.aspx ?id =22340 (accessed 8 November 2009).

"Clash of the Clouds." *The Economist*, 15 Oct 2009. http: //www.economist.com/displaystory.cfm?story_id=14637206 (accessed 12 November 2009).

Danielson, Krissi. "Distinguishing Cloud Computing from Utility Computing." *EbizQ*. http://www.ebizq.net/blogs/saasweek/2008/03/ distinguishing _cloud_computing (accessed 12 November 2009).

Davidson, Mary Ann, Oracle Corporation, Testimony to the House Security Committee, http://homeland.house.gov/SiteDocuments/20090310143850-78976.pdf (accessed 18 November 2009)

Freedman, Lawrence. *Deterrence.* Cambridge: Polity Press, 2004.

Friedman, Thomas. *The World is Flat, A Brief History of the Twenty-First Century*. New York: Farrar, Stratus, and Giroux, 2005.

Gaudin, Sharon. "Intel: Chips in brains will control computers by 2020." http://www. computerworld.com/s/ article/9141180/Intel_ Chips_in_brains_will_control _computers_ by_ 2020 (accessed 14 November 2009).

Hardy, G. Mark. "Senior Leader Perspective." *Cyberpro Newsletter*, Volume 2, Edition 23. Smithfield, VA: National Security Cyberspace Institute, November 19, 2009.

Heater, Brian. "Analysis: Google's dashboard Tackles Transparency." *PC Magazine*. 5 Nov 2009. http://www.pcmag.com /article2 /0,2817, 2355490,00.asp (accessed 21 November 2009)

Jabbour, Kamal. Personal interview, 15 September 2009.

Janis, Irving. *Groupthink*. Boston, MA: Houghton Mifflin Company, 1982.

Jervis, Robert. *Perception and Misperception in International Politics*. Princeton NJ: Princeton University Press, 1976.

Johnson, T. J., Kaye, B. K., Bichard, and S. L., & Wong. "Every blog has its day: Politically-interested Internet users' perceptions of blog credibility." *Journal of Computer-Mediated Communication*, Vol *13*(1), article 6. http://jcmc.indiana.edu/vol13 /issue1 /johnson.html (accessed 14 November 2009).

Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 31 October 2009.

Joint Publication 3-13, *Information Operations*, 13 Feb 2006.
Kramer, Franklin, Starr, Stuart, and Wentz, Larry. *Cyberpower and National Security*. Dulles, VA: Potomac Books, 2009.
Kurzweil, Ray. *The Singularity of Near.* New York: The Penguin Group, 2005.
Langevin, James, McCaul, Micheal, Charney, Scott, and Raduege, Harry. *Securing Cyberspace for the 44th Presidency.* Washington D.C.: Center for Strategic and International Studies, December 2008.
Libicki, Martin. *Cyberwar and Cyberdeterrence*. Santa Monica, CA: RAND, 2009.
Lorber, Azriel. *Misguided Weapons*. Washington D.C.: Potomac Books, 2002.
Mearsheimer, John J. *Conventional Deterrence.* New York: Cornell University Press, 1983.
Mitrokhin, Vasili and Andrew, Christopher. *The Sword and the Shield.* New York: Basic Books, 1999.
Nakashima, Ellen. "U.S. plans to issue official protest to China over attack on Google." *The Washington Post*. http://www. Washington post.com/wp-dyn/content/article/2010/01/15/AR2010011503917.html (accessed 17 January 2010).
Nye, Joseph. *Soft Power*. New York: Public Affairs, 2004.
Obama, Barack. Interview on *The Today Show* with Matt Lauer, 3 February 2009.
Obama, Barack. "Remarks by the President on Securing out Nation's Cyber Infrastructure." http://www.whitehouse.gov/ the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure (accessed 10 January 2010).
Visiontree. "World Health Care Congress Attendees Use Palm Treo 700w Loaded with VisionTree For the First Time as Audience Response and Data Capture Tool." 10 April 2006. http://www.visiontree.com/index.cfm /fuseaction /newsevents .mediaalert (accessed 12 December 2009).
Wikipedia. "Cloud Computing." http://en. wikipedia .org/ wiki/File:Cloud_computing.svg (accessed 12 November 2009).
Wingfield, Thomas and Michale, James. "An Introduction to Legal Aspects of Operations in Cyberspace." Naval Postgraduate School, NPS-CS-04-005, 28 April 2004.

Notes

[1] Barack Obama, "Remarks by the President on Securing our Nation's Cyber Infrastructure," http://www.whitehouse.gov/ the_ press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure.

[2] Richard Clark, "War from Cyberspace," *The National Interest*, Washington D.C., 20 October 2009. http://www.nationalinterest.org/Article.aspx ?id =22340.

[3] These operations were codenamed Titian Rain" and "Moonlight Maze." From Richard Clark, "War from Cyberspace."

[4] *Visiontree*, "World Health Care Congress Attendees Use Palm Treo 700w Loaded with VisionTree For the First Time as Audience Response and Data Capture Tool," 10 April 2006, at http://www .visiontree.com/index.cfm /fuseaction /newsevents.mediaalert.

[5] Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001, 141.

[6] Joint Publication 3-13, *Information Operations*, 13 February 2006, page I-1.

Notes

[7] Krissi Danielson, "Distinguishing Cloud Computing from Utility Computing," *EbizQ*, http://www.ebizq.net/blogs/saasweek/2008/03/distinguishing_cloud_computing/
[8] "Clash of the Clouds," *The Economist*, 15 October 2009, http://www.economist.com/displaystory.cfm?story_id=14637206.
[9] In the 1960's and 70's this physical connection was through a central mainframe.
[10] It is important to differentiate information from data; information is "the meaning that a human assigns to data by means of the known conventions used in their representation." From Joint Publication 3-13, *Information Operations*, I-1.
[11] Ibid., I-1.
[12] Martin Libicki, *Cyberwar and Cyberdeterrence*, (Santa Monica, CA: RAND, 2009), 12.
[13] Sharon Gaudin, "Intel: Chips in brains will control computers by 2020," http://www. computerworld.com/s/ article/9141180/Intel_ Chips_in_brains_will_control _computers_ by_2020.
[14] IPv4 forms the basis for today's internet protocols.
[15] Martin Libicki, *Cyberwar and Cyberdeterrence*, 12.
[16] Ibid., 13.
[17] Dr. Kamal Jabbour, Senior Scientist for Information Assurance, Information Directorate, Air Force Research Laboratory, Interview, 15 September 2009.
[18] *Joint Publication 3-13, Information Operations*, II-5.
[19] Martin Libicki, *Cyberwar and Cyberdeterrence*, 41.
[20] "Incidentally, the IPng architects could not use version number 5 as a successor to IPv4, because it had been assigned to an experimental flow-oriented streaming protocol (Internet Stream Protocol), similar to IPv4, intended to support video and audio." I got this from CHIPS - The Department of the Navy Information Technology Magazine, http:// www.chips.navy.mil/archives/04_spring/web_pages/IPv6.htm.
[21] Degradation of the signal relative to the ambient noise.
[22] Franklin Kramer, Stuart Starr, and Larry Wentz, *Cyberpower and National Security*, (Dulles, VA: Potomac Books, 2009), 148.
[23] Barack Obama, Interview on *The Today Show* with Matt Lauer, 3 February 09.
[24] Brian Heater, "Analysis: Google's dashboard Tackles Transparency," *PC Magazine*, 5 November 2009, http://www.pcmag.com /article2/0,2817,2355490,00.asp.
[25] G. Mark Hardy, "Senior Leader Perspective," *Cyberpro Newsletter*, Volume 2, Edition 23, National Security Cyberspace Institute. Smithfield, VA., November 19, 2009.
[26] Franklin Kramer, Stuart Starr, and Larry Wentz, *Cyberpower and National Security*, 163.
[27] Martin Libicki, *Cyberwar and Cyberdeterrence*, 115.
[28] Ibid., 115.
[29] From James Langevin, Micheal McCaul, Scott Charney, and Harry Raduege, *Securing Cyberspace for the 44th Presidency*, (Washington D.C: Center for Strategic and International Studies, December 2008), 11.
[30]James Langevin, Micheal McCaul, Scott Charney, and Harry Raduege, *Securing Cyberspace for the 44th Presidency*, 12.
[31] Ibid., 12.
[32] Dr. Kamal Jabbour, Senior Scientist for Information Assurance, Information Directorate, Air Force Research Laboratory, Interview, 15 September 2009.
[33] Ray Kurzweil, *The Singularity of Near*, (New York: The Penguin Group, 2005), 335.
[34] In the tightly controlled Air Force network, every keystroke and site visited by all authorized users are catalogued and periodically reviewed by Air Force leaders at various levels.
[35] In this example, the system recorded an inappropriate use of a government system.
[36] Joint Publication, 3-13, *Information Operations*, I-9.
[37] Decision makers may see them as beloved pets that help get them to the top.
[38] Robert Jervis, *Perception and Misperception in International Politics*, (Princeton , NJ: Princeton University Press, 1976), 239.
[39] In this regard, the familiar is not the only guilty party; it has been trained by its master to behave in certain ways.
[40] Irving Janis, *Groupthink*, (Boston, MA: Houghton Mifflin Company, 1982), 13.

Notes

[41] A recent study found that bloggers trusted political blogs more than traditional media outlets . From Johnson, T. J., Kaye, B. K., Bichard, S. L., & Wong, "Every blog has its day: Politically-interested Internet users' perceptions of blog credibility," *Journal of Computer-Mediated Communication*, *13*(1), article 6, http://jcmc.indiana.edu/vol13 /issue1 /johnson.html.
[42] Graham Allsion and Phillip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis* (New York: Addison-Wesley Educational Publishers, 1999), 4.
[43] Ibid., 5.
[44] Ibid., 6.
[45] Ibid., *6.*
[46] Colonel Boyd studied the engagements of the MiG-15 versus the F-86 during the Korean War. Although the MiG-15 possessed an advantage in its ability to gain energy throughout the flight envelope, the F-86 was more maneuverable—it could reorient its flight path faster than the MiG. This ability to reorient faster than its opponent gave the F-86 an advantage, which led to a 12 to 1 kill ratio during the war.
[47] John Boyd, "A Discourse on Winning and Losing," August 1987, slide 216.
[48] John Boyd, "A Discourse on Winning and Losing," August 1987, slide 218.
[49] For example, the CFACC at the COAC may see air tracks, Predator video feeds, and data-linked target information through the computers and networks of the CAOC.
[50] This has been referred to as the "OODA snowman."
[51] Air Force Doctrine Document 2-5, *Information Operations*, 20 September 2002, 5.
[52] My adaptation of the OODA loop with a cyber familiar.
[53] In the Blue Horizons Failed State 2030 scenario for Nigeria, the crime bosses had to control critical information nodes and then inject information they wanted to target the key government officials, tribal leaders, individuals, and familiars in the decision tree. This succeeded in dividing a country with more than 400 ethnicities and accelerating the demise of governance.
[54] Vasili Mitrokhin and Christropher Andrew, *The Sword and the Shield*, (New York: Basic Books, 1999), 228.
[55] Although deterrence usually refers to human interactions, nature has its own form of deterrence in the animal kingdom. Bright colors, pungent odors, and "fake" large eyes on the back of butterfly wings serve as simple warnings to ward off potential predators. Are there analogous capabilities in cyberspace? Perhaps, if computer programs have learned to recognize what other programs are, they may understand which programs (other intelligences) to avoid. Thus, if systems that one hopes to protect *look* like traps or cyber predators (like the aforementioned butterfly), this appearance may serve to deter cyberbots.
[56] JP 1-02, p 161.
[57] John J. Mearsheimer, *Conventional Deterrence* (New York: Cornell University Press, 1983) 23.
[58] Lawrence Freedman, *Deterrence*, (Cambridge: Polity Press, 2004), 37.
[59] Martin Libicki, *Cyberwar and Cyberdeterrence*, 29.
[60] Mary Ann Davidson, Chief Security Officer, Oracle corporation, http://homeland.house.gov / SiteDocuments /20090310143850-78976.pdf.
[61] Ibid. The Monroe Doctrine said that further efforts by governments to interfere with states in North and South America would be viewed by the United States as acts of aggression.
[62] Thomas Wingfield and James Michale, "An Introduction to Legal Aspects of Operations in Cyberspace," (Naval Postgraduate School, NPS-CS-04-005, 28 April 2004), 5.
[63] This does not mean that the United States will not have security at these cyber "border crossings," only that the security will be less intrusive as a general rule. As may be pointed out, the attackers on 9/11 traveled to the United States from Saudi Arabia.
[64] These may many methods, including air gaping with data recreation or simply only allowing text of emails.
[65] Azriel Lorber, *Misguided Weapons*, (Washington D.C.: Potomac Books, 2002), 61.
[66] Ibid., page 63.
[67] Ibid., page 63.

Notes

[68]Other nations may become more dependent upon cyberspace because they either forgo or lack the resources to build an industrial-age telecommunications infrastructure as the United States did in the 20th century.
[69] Joseph Nye, *Soft Power*, (New York: Public Affairs, 2004), 5.
[70] Thomas Friedman, *The World is Flat, A Brief History of the Twenty-First Century* (New York: Farrar, Stratus, and Giroux, 2005).
[71] Ibid., 310.
[72] It is important to remember that the United States had Plan Red, one of the Rainbow Plans, scripted for an attack on England until 1921. Military planners saw the potential for fights over scarce resources and were concerned with British Imperial designs in the Atlantic. Nevertheless, a common culture, reinforced through faster travel across the Atlantic, brought these nations together. Today, through cyberspace, a similar outcome can occur with China and other emerging great powers (Brazil, Russia, and India).
[73] Ellen Nakashima, "U.S. plans to issue official protest to China over attack on Google," *The Washington Post*, http://www.washingtonpost.com/wp-dyn/content/article/2010/01/15 /AR2010011503917.html.
[74] Ibid.