Towards an Evolving Theory of Cyberpower

Dr. Stuart H. STARR[1,a]
[a] *Center for Technology and National Security Policy (CTNSP)*
National Defense University (NDU)

Abstract. In the 2006 Quadrennial Defense Review, a request was made to have the Center for Technology and National Security Policy (CTNSP), National Defense University (NDU), develop a theory of cyberpower. It was noted that there was a need to develop a holistic framework that would enable policy makers to address cyber issues in proper perspective.
To satisfy that tasking, CTNSP convened five workshops, drawing on experts from government, industry, academia, and think tanks. Those workshops addressed a broad set of issues related to the evolution of cyberspace, cyberpower, cyberstrategy, and institutional factors that influence those factors (e.g., governance, legal issues).
To develop the desired theory, this paper systematically addresses five key areas. First, the paper *defines* the key terms that are associated with cyber issues. Particular emphasis is placed on the terms "cyberspace", "cyberpower", and "cyberstrategy". Second, the paper *categorizes* the elements, constituent parts, and factors that yield a framework for thinking about cyberpower. Third, the paper *explains* the major factors that are driving the evolution of cyberspace and cyberpower. To support that effort, the paper presents strawman principles that characterize major trends. Fourth, the paper *connects* the various elements of cyberstrategy so that a policy maker can place issues in proper context. Finally, the theory *anticipates* key changes in cyberspace that are likely to affect decision making.
In view of the dramatic changes that are taking place in cyberspace, it is important to stress that this effort must be regarded as a preliminary effort. It is expected that the theory will continue to evolve as key technical, social, and informational trends begin to stabilize.

Keywords: cyberspace, cyberpower, cyberstrategy, cyber institutional factors

Introduction

This white paper represents a continuing effort to evolve a theory of cyberpower. The white paper begins by characterizing the components of a "theory of cyberpower". Consistent with that characterization, we identify key terms and put forth straw man definitions of those terms. We then identify the specific objectives that will be addressed in this theory. In

[1] **Disclaimer:** The views expressed in this article are those of the author and do not reflect the official policy or position of the National Defense University, the Department of Defense or the U.S. Government. All information and sources for this paper were drawn from unclassified materials.

accord with those objectives, we present a holistic framework to categorize and discuss key categories. Within this holistic framework, we discuss the intellectual capital required to address these issues.

Subsequently, we discuss theoretical dimensions of the key categories: cyberspace, cyberpower, cyberstrategy, and institutional factors. In addition, we discuss the challenges associated with connecting across these categories and anticipating the future cyber activities and issues of interest.

We conclude the white paper by summarizing major findings and identifying the next steps that should be taken to refine this evolving theory of cyberpower.

1. 1. Context

To provide context for this white paper, this section discusses elements of a theory, objectives, approach, structure, key definitions, and required intellectual capital.

1.1. Elements of a Theory

A theory of warfare should address five key issues [1]. First, it should introduce and **define** the key terms that provide the foundation of the theory. Second, it should give structure to the discussion by **categorizing** the key elements of the theory. Third, it should **explain** the elements in these categories by summarizing relevant events and introducing key frameworks or models. Fourth, it should **connect** the various elements of the subject so that key issues can be treated comprehensively. Finally, it should seek to **anticipate** key trends and activities so that policy can be germane and useful.

This framework for a theory raises one immediate issue. There is interest in the ability to predict, rather than anticipate, key activities. However, as described below, the cyber problem is in the midst of explosive, exponential change. In the midst of this exceptional uncertainty, it is infeasible to make reliable predictions. Thus, we have adopted the less challenging task of "anticipating" key trends and activities.

Finally, it is important to stress the following caveat: since this is an evolving effort to develop a theory of cyberpower, the emerging theory will **not** be complete. Furthermore, as discussed below, early efforts to develop a theory for a discipline have inevitably been somewhat **wrong.**

To provide some context for theoretical developments, it is useful to note the challenges that the theories associated with physics have faced in its evolution. Contemporary physics theory has evolved over hundreds of years, dating back to the seminal contributions of Galileo and Newton. In this discipline, there is a common base of knowledge, although there are significant variants for specific sub-areas (e.g., quantum mechanics, classical dynamics, relativity). In addition, there are strong links to other "hard science" disciplines (e.g., math, chemistry, biology). Although the definitions of key terms and concepts are generally established, it should be noted that there were many false starts (e.g., a hundred years ago, physicists had (incorrectly) postulated the existence of an ether through which electromagnetic waves propagated as they traversed a vacuum). Even in

contemporary times, discussions still persist about the fundamental definitions of matter (e.g., quarks with a variety of properties).

Within the sub-areas of physics, there is broad agreement about key categories (e.g., solid, liquid, and plasma physics). In these key sub-areas, mathematical models have generally been developed drawing on experiments and observations. Many of these mathematical models have proven to be extremely accurate and precise in explaining and predicting outcomes. However, there are still efforts underway to connect many of the key sub-areas of physics. For example, there is considerable work underway in the area of "string theory" to develop a unified understanding of basic phenomena, although some critics have argued that this is likely to be a dead end [2].

To highlight the challenges facing the "cyber theorist", it is useful to contrast the discipline of physics with that of cyberspace. The cyberspace of today has its roots back in the 1970s when the Internet was conceived by engineers sponsored by ARPA. Detailed analysis of cyberspace issues often requires even broader cross-disciplinary knowledge and skills than physics. These include, *inter alia,* computer scientists, military theorists, economists, and lawyers. Each of these disciplines has its own vocabulary and body of knowledge. Thus, it is quite challenging for these stakeholders to communicate effectively. This is manifested in debates about the most basic of terms (e.g., "cyberspace") where key definitions are still contentious. Consistent with the heterogeneous nature of the problem, it is not surprising that prior efforts to characterize this space have not been successful. At present, there is no agreed upon taxonomy to support a comprehensive theory.

As noted above, key attributes of a theory include its ability to explain and predict (or at least, to anticipate). There are many reasons why prior theoretical cyber efforts have foundered. These include the facts that key facets of the field are changing exponentially, there is little or no agreement on key frameworks, and the social science element of the discipline (e.g., understanding of cognition, human interactions in virtual societies) makes it very difficult to develop models that reliably explain or anticipate outcomes. Finally, we are unable to connect the disparate elements of the field because a holistic perspective of the discipline has not yet been created.

1.2. Objectives

This white paper addresses the five elements of a military theory: define, categorize, explain, connect, and anticipate. In the areas of "explain" and "anticipate", the focus is on identifying and characterizing key "rules of thumb" and principles for cyber elements.

The scope of the white paper is restricted in two key areas. First, we focus attention on the national security domain. Changes in cyberspace are having a major affect on social, cultural, and economic issues, but we address them only tangentially. Second, we limit attention to the key cyberpower issues that are confronting the national security policy maker. Thus, there is no attempt to generate a comprehensive theory of cyberpower that touches on broader issues.

1.3. Approach

The preliminary theory of cyberpower emerged from three initiatives. First, we drew insights from observations of cyber events, experiments and trends. Second, we extrapolated from prior national security methods, frameworks, theories, tools, data, and studies, which were germane to the problem. Finally, we formulated and hypothesized new methods, frameworks, theories, and tools to deal with unexplained trends and issues.

Subsequently, the theory has evolved based on two activities. First, over the past year, several conferences and workshops have been convened that focused on three key issues: cyber-deterrence, risk management, and international perspectives on cyber issues. Second, a number of papers have been generated that focused on assessing cyber policy issues and the US government's use of social networks. Accordingly, the preliminary theory has been evolved to reflect the insights that emerged from those activities.

1.4. Structure

This white paper has adopted the holistic cyber framework depicted in Figure 1. This framework is patterned after the triangular framework that the military operations research community has employed to decompose the dimensions of traditional warfare. In that framework, the base consists of systems models, upon which rests more complex, higher orders of interactions (e.g., engagements, tactical operations, campaigns).

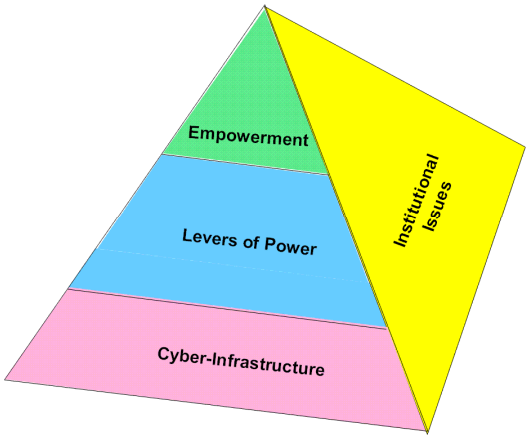

Figure 1. Broad Conceptual Framework

By analogy, the bottom of the pyramid consists of the components, systems, and systems-of-systems that comprise the cyber-infrastructure. The output from this cyber-infrastructure enhances the traditional levers of power: political/diplomatic, informational, military and economic (P/DIME). These levers of power, in turn, provide the basis for empowerment of the entities at the top of the pyramid. These entities include, *inter alia,*

individuals, terrorists, trans-national criminals, corporations, nation states, and international organizations. Note that while nation states have access to all of these levers of power, the other entities generally have access to only a sub-set of them. In addition, initiatives, such as deterrence and treaties, may provide the basis for limiting the empowerment of key entities.

The pyramid suggests that each of these levels is affected by institutional factors. These include factors such as governance, legal considerations, regulation, sharing of information, and consideration of civil liberties.

It must be emphasized that this framework is merely one of many frameworks that could be constructed to conceptualize the cyber domain. However, it has proven useful in decomposing the problem and developing subordinate frameworks to address key cyber issues.

1.5. Key Definitions

As noted above, there is a continuing discussion about the appropriate definitions for key cyber terms. In the definition posed by William Gibson, in his 1984 book "Neuromancer" [3] cyberspace was characterized as: "A consensual hallucination… A graphic representation of data abstracted from banks of every computer in the human system."

For the purposes of this theory, this white paper has adopted the formal definition of cyberspace that the Deputy Secretary of Defense formulated: "…the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries" [4]. This definition does not explicitly deal with the information and cognitive dimensions of the problem. To deal with those aspects explicitly, we have introduced two complementary terms: cyberpower and cyberstrategy.

This white paper has adopted the following definition for the term "Cyberpower". It is "the ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power." In this context, the instruments of power include the elements of the P/DIME paradigm. For the purposes of this evolving theory, primary emphasis will be placed on the military and informational levers of power.

Similarly, the term "Cyberstrategy" is defined as "the development and employment of capabilities to operate in cyberspace, integrated and coordinated with the other operational domains, to achieve or support the achievement of objectives across the elements of national power." Thus, one of the key issues associated with cyberstrategy deals with the challenge of devising "tailored deterrence" to affect the behavior of the key entities empowered by developments in cyberspace.

One of the major issues associated with cyberspace is the question of whether it is "…an operational domain…". To explore this issue, note that the term "domain" is not defined formally in key national security and military products. However, it is cited in selected policy documents. For example, the 2004 National Military Strategy [5] states that "The Armed Forces must have the ability to operate across the air, land, sea, space, and

cyberspace domains of the battlespace". Furthermore, in the 2006 Quadrennial Defense Review (QDR), it notes that "The DoD will treat cyberspace as a domain of warfare".

Joint Publication 3-0 [6] identifies several key features of a domain: it can be described physically; there are distinctions in means, effects, and outcomes; and military and combat operations can be conducted in and through the domain.

One can make the argument that cyberspace is a domain through the following logic. It is widely accepted that (outer) space is a domain. In comparison to "space", "cyberspace" has the following bounding attributes that suggest that it is a military domain. It is subject to ongoing levels of combat; it is characterized by greater ease of access; and it is more difficult to identify and track military operations within it.

If cyberspace is a domain, it has significant practical implications. It will require the allocation of resources to support organization, training, and equipping of "cyber-forces". It implies the need to develop a culture that is consistent with cyber activities. Finally, it has implications in the development of a professional cadre and establishment of a structured career progression. Thus, for the purposes of this evolving theory, it will be assumed that cyberspace is "an operational domain".

Consistent with this white paper's definition, the elements of the holistic framework can be recast as depicted in Figure 2.

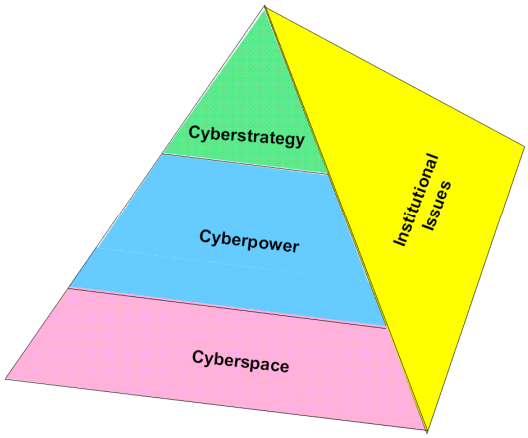

Figure 2. Cyberspace, Cyberpower, Cyberstrategy, and Institutional Factors

1.6. Required Intellectual Capital

To deal with the rich array of cyber policy issues that confront senior decision makers, it will require a diverse set of intellectual capital. Figure 3 suggests the differing types of knowledge that will be required to address issues within and across the categories of interest.

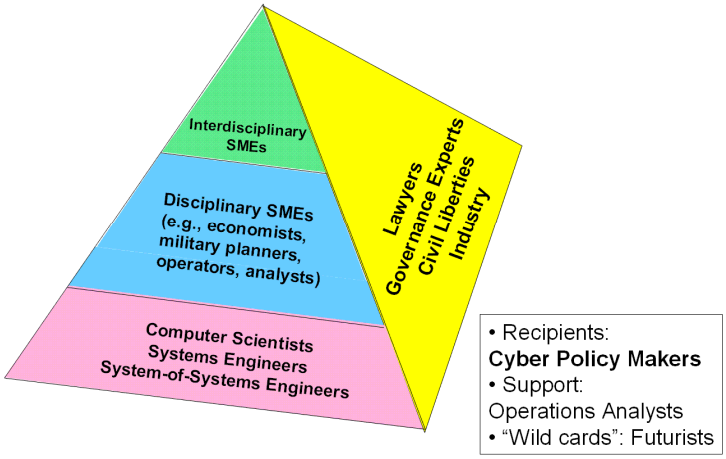

Figure 3. Required Intellectual Capital

For example, in the realm of cyberspace, there is a need for physicists, electrical engineers, computer scientists, systems engineers, and system-of-system engineers. These professionals will play key roles in developing the hardware components (e.g., microprocessors, hard drives), software protocols and standards (e.g., implementing Internet Protocol version 6 (IPv6)), applications and services, and the systems that exploit this hardware and software (e.g., command, control, and communications systems).

In the realm of cyberpower, there is a need for subject matter experts (SMEs) that are qualified to deal with issues of Politics, Diplomacy, Information, Military, and Economics. This implies extensive reliance on economists (both micro- and macro-) and social scientists with training in such diverse fields as sociology, cultural anthropology, psychology, and demographics.Furthermore, in the area of military knowledge, there is a need for participation by military planners, operators, and analysts.

In the realm of cyberstrategy, there is a need for interdisciplinary experts who are able to deal with the full range of political, military, economic, social, informational, and infrastructure (PMESII) issues associated with entities that are empowered by changes in cyberspace. In particular, analysts are needed who have had experience in addressing deterrence among these entities.

Finally, in the realm of institutional factors, the key skills required are legal, governance, civil liberties, and industrial experience.

It is anticipated that one of the main users of this intellectual capital will be cyber policy decision makers. They will also need operations analysts to help them orchestrate and harness this heterogeneous intellectual capital, and futurists to help them conceptualize possibilities that require unfettered imaginations.

2. Theoretical Perspectives

Three of the major objectives of a theory of cyber are to help **explain, connect,** and **anticipate** key aspects of the problem to the decision maker. To do so, it will require the formulation of conceptual models for the various categories introduced above. In formulating these conceptual models, it is useful to recall the famous epithet from the statistician George Box: "all models are wrong; some are useful" [7]. The challenge for the theorist is to suggest and apply appropriate models that are useful for the decision maker, and to delineate the range of their utility.

This section systematically introduces a variety of conceptual models that are germane to the many policy questions associated with cyber issues. Structurally, we will pursue a "bottom-up" approach and address cyberspace, cyberpower, cyberstrategy, and institutional factors. For each area, we will introduce a variety of models and frameworks that will help the decision maker explain key observables and conceptualize the issues of interest. This will be followed by articulating key "rules of thumb" and principles that highlight major issues of interest.

2.1. Theoretical Aspects of Cyberspace

This section of the white paper identifies key trends in cyberspace and discusses cyberspace "rules of thumb" and principles.

2.1.1. Key Trends

This section of the white paper briefly explains key trends in cyberspace. Trends are introduced in five key areas: growth in users, features of key components (e.g., microprocessors, hard drives), architectural features (e.g., Internet Protocols), and military systems-of-systems.

2.1.1.1. Growth in Users

The most remarkable aspect of the Internet has been the exponential growth in users, world-wide. Figure 4 illustrates that growth over a thirty-three year period. It can be seen that the user population increased from approximately 1M users in 1992 to 1,200M users in 2007. It is projected that the Internet will have 2B users by 2010. This number is projected to grow substantially if the One Laptop Per Child (OLPC) project is brought to fruition. That project aims to get many millions of low-cost laptops in the hands of children in under-developed countries.

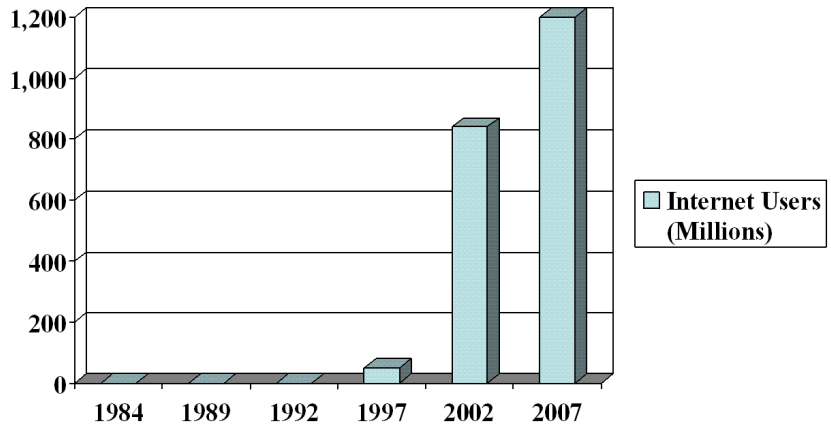

Figure 4. Number of Internet Users (Millions)

The Navy's Special Studies Group depicted this growth from another perspective. They used 50M users as a benchmark for penetration of a mass medium. That level was achieved by radio in 38 years, television in 13 years, and the Internet in 6 years (beginning with the introduction of the World Wide Web).

Another key element of cyberspace is cellular telephony. As a point of reference, the first cell phone call was made in 1973. It is estimated that today, thirty five years later, approximately 3.3B cell phones are in use, world-wide.

Two other benchmarks serve to calibrate the problem. It is estimated that around 210B e-mails were sent every day in 2008. That is equivalent to 2M e-mails sent every second. It is estimated that on the order of 70 percent of these e-mails may be spam or viruses.

2.1.1.2. Components

From a theoretical perspective, the physics of the hardware that supports cyberspace has a significant impact on its performance. This is particularly manifested in the design of microprocessors and hard drives.

2.1.1.2.1. Microprocessors

Clock cycles of modern microprocessors exceed 4 GHz. Therefore, under ideal circumstances, electrons can move a maximum of 0.075 meters in a single processor clock cycle, nearing the size of the chip itself. With clock cycles going even higher[2], electronic signals cannot propagate across a chip within one clock cycle, meaning elements of the chip cannot communicate with other elements on the other side of the same chip. Thus, this

[2]As a bounding case, note that in 2008 the fastest US computer, Roadrunner (built by IBM and Los Alamos National Laboratory), was capable of more than 1 petaflop (i.e., 1 quadrillion floating point calculations per second) [8].

limitation maximizes the effective size of a single integrated microprocessor running at high clock speeds. Addressing this limitation is one of the reasons that various processor manufacturers have moved chip architectures toward multi-core processors, where multiple, semi-independent processors are etched on a single chip. Current chips typically have two or four cores although there are instances where 1000 to 4000 cores are a single die.

2.1.1.2.2. Hard Drives

Figure 5 depicts computer hard drive storage capability (in gigabits per square centimeter) over the last twenty five years. It is notable that the improvement in memory was marginal for the first twenty years until IBM engineers applied the phenomenon of giant magnetoresistance[3]. Currently, improvements in memory are manifesting exponential improvement, making it feasible to create very portable devices, such as iPods, with extremely high storage capability.

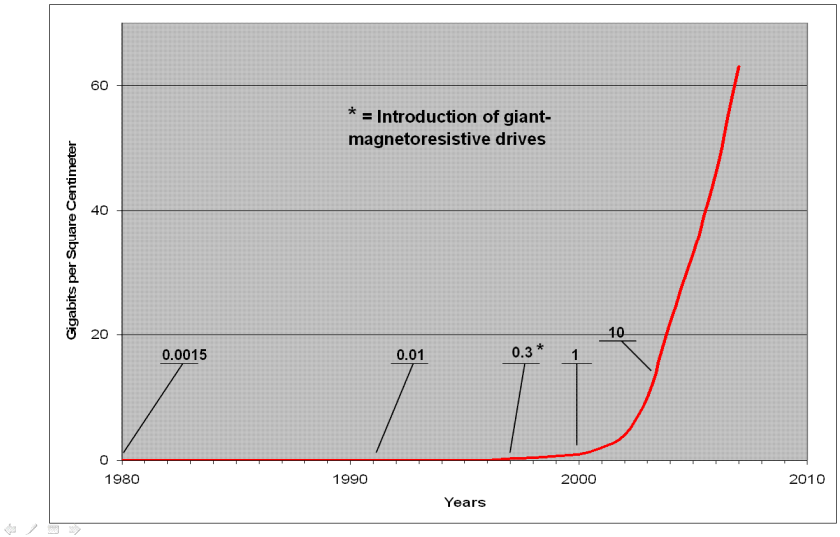

Figure 5. Hard Drive Capacity

These two examples suggest that a careful technology assessment is needed to assess if and when bottlenecks in technology will be overcome that limit current performance.

2.1.1.3. Architectural Features

Figure 6 schematically depicts the architecture of the existing Internet. The key innovations of this architecture revolve around the key protocols and standards instantiated in the

[3] The Nobel Prize in Physics for 2007 was awarded to Albert Fert, France, and Peter Grunberg, Germany, who independently discovered this phenomenon.

Transmission Control Protocol/Internet Protocol (TCP/IP) stack and the use of a router to transmit packets from the sender to the user.

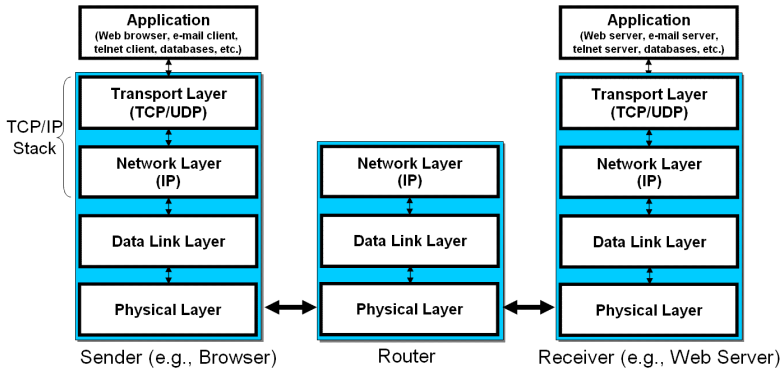

Figure 6. Protocol Layering and Routing Packets Across a Network

Originally, this architecture was devised by a group of colleagues for whom security was a secondary issue. Thus, the primary emphasis was to implement an architecture that facilitated the interoperability among heterogeneous networks. In addition, a decision was made to implement IP addresses that consisted of 32 bits (or approximately 4 billion addresses).

These two decisions have led to several major limitations in the current architecture. In light of the security shortfalls in the existing architecture, there is interest in alternative architectures that are designed around different priorities (e.g., highest priority: security; second priority: connectivity among highly mobile users). Consistent with those revised priorities, new architectural efforts are underway at the National Science Foundation and DARPA.

Second, the constraint on IP addresses (as well as concern about enhanced security and mobility) has led to the adoption of IPv6. Since it allocates 128 bits to IP addresses, it will give rise to an extraordinarily large number of IP addresses[4].

Both of these innovations pose a problem to the cyberspace community: how can one transition from the current architecture to an alternative architecture, efficiently and effectively, without creating new security vulnerabilities? This is an on-going challenge that the computer science community must confront over the next decade.

2.1.1.4. Military Systems-of-Systems

The military community has embraced the underlying computer science principles associated with the Internet, although they have enhanced security for classified systems by

[4] IPv6 will provide 2^{128} addresses. This would provide $5x10^{28}$ addresses for each of the 6.5B people alive today. Alternatively, our sun converts $3.4e^{38}$ hydrogen nuclei to helium nuclei each second. Each hydrogen atom could have its own IPv6 address.

developing “air gapped” networks (e.g., Secure Internet Protocol Router Net (SIPRnet), Joint Worldwide Intelligence Communications System (JWICS)). Figure 7 provides a cartoon of that implementation for the notional Global Information Grid (GIG).

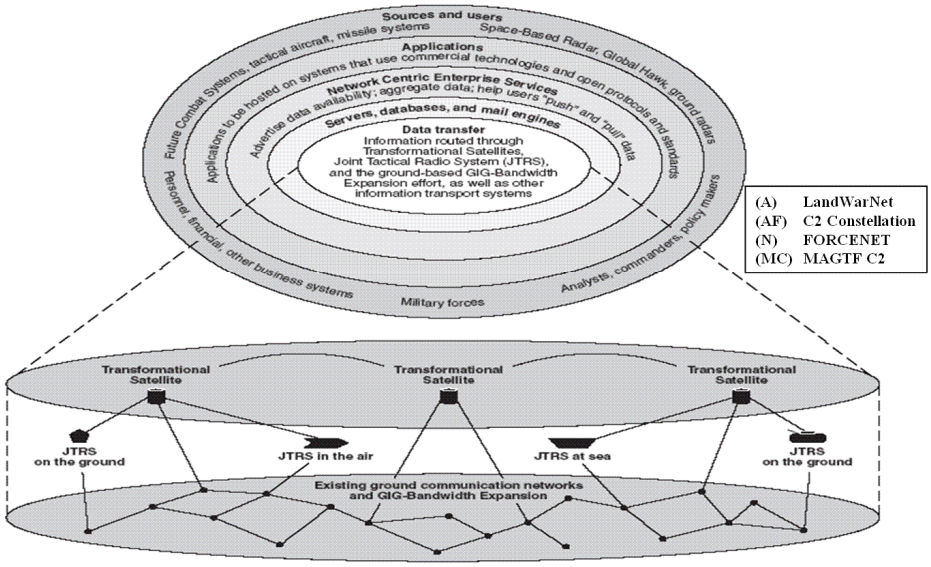

Figure 7. A Framework to Characterize the GIG

There are several distinctive aspects of the evolving GIG. First, for the transport layer, the plan is to employ a heterogeneous mix of satellite (e.g., Advanced Extremely High Frequency), airborne (e.g., selected Joint Tactical Radio Systems (JTRS)), and surface (e.g., fiber optic) telecommunications media. As a side note, the military is finding it difficult to develop many of these elements within acceptable levels of performance, schedule, and cost.

Second, there is interest in employing a Service Oriented Architecture (SOA) to provide loose coupling among key systems. Third, they have developed Communities of Interest to address the challenges associated with the data that will flow through the systems (e.g., specify metadata; deal with issues of pedigree). It has been articulated that they wish to transition from the principle of “need to know” to “need to share”. Finally, they hope to assimilate the Services’ visions of future systems into the GIG (e.g., USA LandWarNet; USN ForceNet; USAF C2 Constellation).

In order to achieve this vision it will require the concerted efforts of the military’s system-of-systems engineers [9].

2.1.2. Cyberspace "Rules of Thumb" and Principles

To help explain the various trends in cyberspace, one can provide several "rules of thumb" and strawman principles. Several "rules of thumb" are employed in the community that are incorrectly characterized as "laws". For example Moore's "Law" indicates that the number of transistors on a chip approximately doubles every 18 months[5]. This has contributed to the production of devices that have decreased cost, enhanced computational power, and decreased size. Although this trend is generally representative of past behavior, there is concern that it may be extremely difficult to sustain that trend in the indefinite future without a fundamental, expensive change in the underlying technology (e.g., transition to nanotechnology). Second, as noted above in Figure 5, recent break-throughs in physics have put the growth in hard drive capacity on an exponential curve, vice a conservative linear curve.Ultimately, this curve will reach a level of saturation (an "S-curve") that is representative of a mature technology. Lastly, the current limitation in IP addresses will be dramatically overcome once the transition to IPv6 is implemented.

Based on prior cyber research activities, several strawman cyberspace principles can be articulated. First, the offensive has the advantage. This is due, in part, to the "target rich" environment that an adversary faces. This makes it difficult for the defense to prioritize and defend selected targets. In addition, the existing architecture makes it very challenging to attribute an attack if an adversary seeks to be anonymous. If cyberspace is to be more resistant to attack, it will require a new architecture that has "designed in" security. However, it will be a challenge to transition, effectively and efficiently, from the current legacy system to a more secure objective system.

2.2. Theoretical Aspects of Cyberpower

This section of the white paper briefly explains key trends in the military and information dimensions of cyberpower. It focuses on changes in environmental theories of power and risk, net-centric operations (NCO), and the mission-oriented approach to influence operations.

2.2.1. Environmental Theories of Warfare

In the discussions that led to this study, it was observed that the naval theories of Alfred Mahan played a major role in shaping the US perspectives and strategies on naval power. It was suggested that cyber power needed a comparable perspective to shape its strategy in cyberspace.

Consistent with that interest, this study re-evaluated the various environmental theories of power. These included analyses of land power (Mackinder [11]), naval power (Mahan [12]), airpower (Douhet [13]), and space power (Gray and Sloan [14]). Based on these analyses, four common features of environmental power theories were identified:

[5] To put this change in context, note that in 1971, processor speeds were on the order of $4x10^5$ Hertz (or 400 KHz) and the cost of 1 MB of Dynamic Random Access Memory (DRAM) was approximately $400 (in 2006 dollars). By 2006, commercial processor speeds were on the order of $4x10^9$ Hz (or 4 GHz) and the cost of 1 MB of DRAM was $0.0009 [10].

technological advances; speed and scope of operations; control of key features; and national mobilization.

Consistent with each of these features, the following implications were drawn for a theory of cyberpower. With respect to technological advances, it was observed that dependency on cyberspace has given rise to new strategic vulnerabilities. This vulnerability has been dramatized by the specter of a "cyber Pearl Harbor" and the realization that the existing cyberspace is vulnerable to a variety of adversary attacks (e.g., denial of service attacks, exfiltration of sensitive but unclassified information; potential corruption of sensitive data). In addition, due to the diffusion of low cost cyberspace technology, the power of non-states (e.g., individuals, terrorists, transnational criminals, corporations) has been greatly enhanced (see below).

Improvements in cyberspace have also served to enhance the speed and scope of operations. This is manifested in the speed at which global operations can be conducted (e.g., the ability to successfully engage time sensitive targets, any where in the world). In addition, it has led to improvements in the ability to automate command and control, dramatically decreasing the classic Observe-Orient-Decide-Act (OODA) loop process.

In the environmental theories of power, emphasis was placed on controlling key features. For example, in naval theories this entailed the control of key "choke points" (e.g., the Straits of Malacca), while in space power, there was interest in controlling key geosynchronous orbit locations. In the case of cyberspace, the key features of interest are man-made. Thus, for example, there is interest in defending "cyber hotels" where key information and communications technology (ICT) systems are concentrated. In addition, while the choke points in the physical world tend to be immutable, they may change relatively rapidly in cyberspace (e.g., location of extensive server farms).

Finally, national mobilization is a key measure of cyberpower. To ensure that it is available when needed, it is vital to ensure that the US has access to a cadre of cyberspace professionals. This argues for re-examining career progression for cyberspace professionals in the military Services. In addition, it is important to establish links to the private sector where the bulk of cyberspace professionals reside. This suggests that a reservoir of reservists should be established to provide access to this intellectual capital in the event of national need.

It is argued in this white paper that the US Government (USG) has tended to focus on the opportunities offered by changes in cyberspace, rather than the risks that we are assuming. To summarize that dichotomy, Table 1 identifies the opportunities and risks associated with military activities at the strategic, operational, and tactical levels.

As can be seen in Table 1, the risks at the strategic level include loss of technical advantage (due to the diffusion of cyberspace technology), potential rapid change in the operating environment (e.g., possibility that nations such as China could "leap-frog" the US by transitioning rapidly to IPv6), and the vulnerabilities associated with military dependence on key systems (e.g., the GIG). At the operational level, the diffusion of cyberspace technology could result in the US loss of advantage in operational pace. Finally, at the tactical level, advances in cyberspace could generate a new front for adversaries to build resources. These observations suggest that the USG might be assuming significant, unknown risks by failing to take a balanced perspective of key cyberspace trends. It also

implies the need to undertake more extensive risk assessments to understand the potential "down-side" of key dependencies.

Table 1. Military Opportunities & Risks in Cyberspace

Level	Opportunities	Risks
Strategic	• NCW-enabled • New "Center of Gravity" opportunities (e.g., deterrence; "virtual conflict")	• Loss of technical advantage • Rapidly changing operating environment • Military dependence on key systems (e.g., GIG)
Operational	• Phasing of operations • Enhanced force structure mix (e.g., cheaper, more precise)	• Loss of advantage in operational pace
Tactical	• Discover and track adversaries using cyberspace	• New front for adversaries to build resources

To begin to deal with these risks, steps should be taken at the strategic, operational, and programmatic levels. At the strategic level, steps should be taken to ensure the resilience of supporting critical infrastructures (e.g., electric power generation and transmission). At the operational level, it is vital to plan to conduct operations against an adversary that is highly cyberwar-capable. This should include the creation of a highly-capable Opposing Force (OPFOR) that would be employed extensively in experiments and exercises. Finally, at the programmatic level, emphasis should be placed on addressing cyberspace implications in the development process. This should include placing higher priority on the challenges of Information Assurance. Overall, an improved analytic capability is required to address each of these issues.

2.2.2. Net-Centric Operations (NCO)

As one aspect of the analytic capability, work is needed to enhance and apply the existing conceptual framework for NCO. As illustrated in Figure 8, the NCO process involves consideration of the interactions among the physical, information, cognitive, and social domains[6]. There is a need to develop better analytic tools for all aspects of this process, particularly in the cognitive and social domains. One potential source of intellectual capital is the ongoing initiative by the Director, Defense Research and Engineering (DDR&E), OSD, to improve human, social, cultural behavior (HSCB) models and simulations.

[6] Note that the figure does not explicitly depict the social domain.

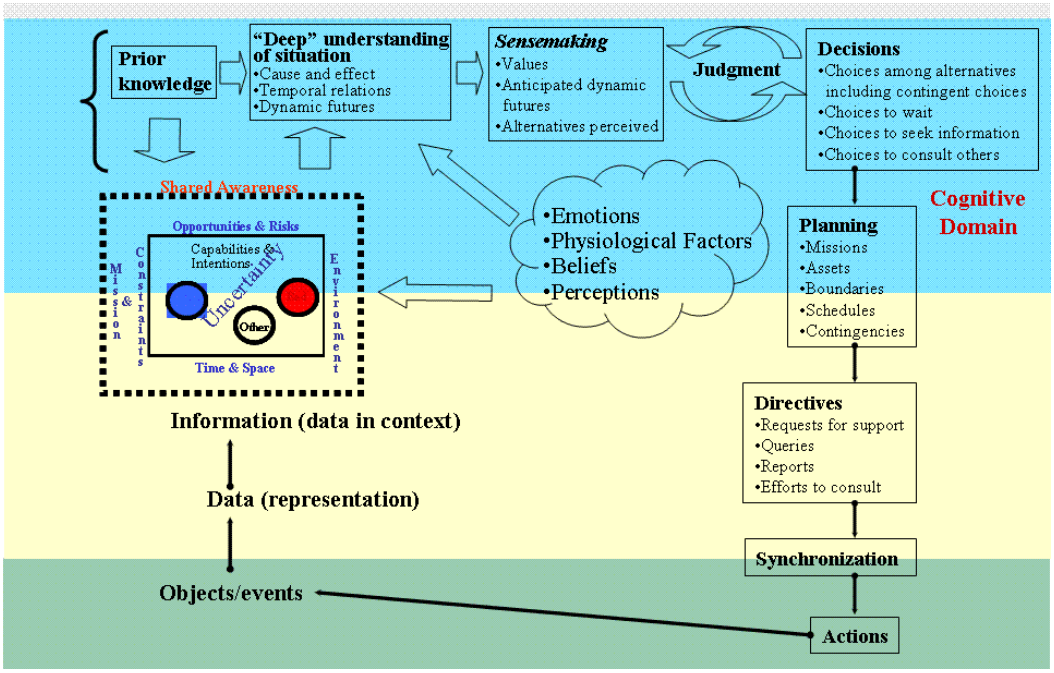

Figure 8. Conceptual Framework for NCO

2.2.3. Mission Oriented Approach to Influence Operations

In the area of influence operations, a strawman framework has been developed to help the community plan for and implement influence operations (Figure 9). This framework represents an extension of the Mission Oriented Approach to Command and Control (C2) that was developed and applied to a variety of C2 issues in the 1980s [16].

This approach begins with the articulation of the nature of the problem of interest. It then poses a sequence of questions. First, what is the operational objective of the operation? A reasonable objective may be to establish a trust relationship with the indigenous population (vice "winning their hearts and minds") [17]. Second, how should this operational objective be accomplished? Again, a decision was made to work with surrogate audiences in order to reach the undecided population. These surrogate audiences included the local media, religious leaders, educational leaders, political leaders, and tribal leaders. Consistent with those surrogate audiences, organizations and processes were established to reach out to them effectively. At this point, one can characterize the existing Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF) activities and compare them to the operational needs. This will give rise to DOTMLPF shortfalls and the articulation of options to mitigate them. It may also prompt the operator to re-evaluate the operational goals and the operational activities to support them.

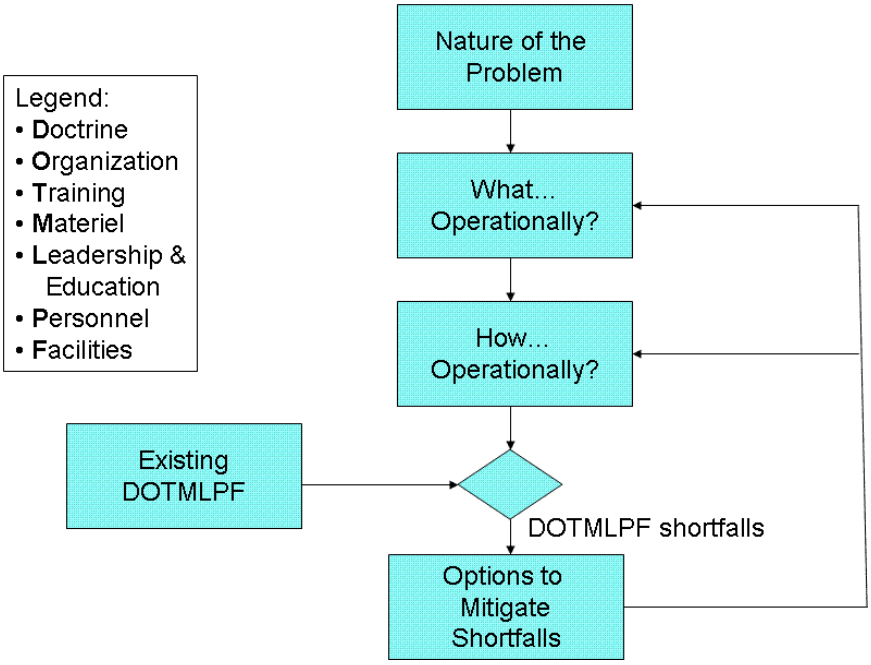

Figure 9. Strawman Framework for Analyzing Influence Operations

This process should be refined and applied to a broader variety of strategic, operation, and tactical influence operations. In particular, it can be used to explore the utility of employing new options in cyberspace to improve future influence operations (e.g., the "New Media", such as the Internet and social networks).

2.2.4. Cyberpower "Rules of Thumb" and Principles

One of the so-called "laws of cyberpower" was formulated by Bob Metcalfe [18]. He postulated that the value of a telecommunications network is proportional to the square of the number of users of the system (n^2). However, there is no empirical data to support this "law". In a recent article [19], it is observed that the value[7] is closer to nlog(n).

From an analytical perspective, the former Office of Force Transformation has supported a number of studies to relate the impact of net-centricity on enhancements in cyberpower (primarily in the military domain). These studies have demonstrated that net-centricity can have a substantial affect on mission effectiveness for selected mission areas. For example, the use of Link 16 by airborne interceptors in M-on-N combat can enhance air-to-air loss exchange ratios by approximately 2.5 [20]. However, the complexity of

[7] To illustrate the differences in these results, assume that one has a network of 100 users. According to "Metcalfe's Law", the "value" of the network is on the order of 10,000. However, the revised "Law" suggests that the value is on the order of 100x2=200.

modern conflict is such that it is difficult to assess the affect of net-centricity on complex missions (e.g., air-land operations; stability and reconstruction operations). This suggests that additional experiments will be needed to assess the quantitative value of net-centricity for complex missions, in which better control is exercised over potentially confounding variables.

2.3. Theoretical Aspects of Cyberstrategy

This white paper has identified an extensive list of entities that are being empowered by changes in cyberspace. This list includes individuals, hacktivists[8], non-governmental organizations (e.g., Red Cross), terrorists, trans-national criminals, corporations, nation-states, and international governmental organizations (e.g., the United Nations).

For the purposes of this white paper, attention has been focused on a sub-set of these entities. These include terrorists, trans-national criminals, and a subset of nation states (e.g., Estonia, China, Russia). From a USG national security perspective, two key issues stand out. First, is it feasible to achieve "tailored cyber deterrence"? Second, what steps should be taken to deal with cyber espionage?

2.3.1. Terrorist Use of Cyberspace

Terrorists are being empowered substantially by changes in cyberspace. With the loss of physical sanctuary in key areas (e.g., Afghanistan), they have been turning to the sanctuary of cyberspace to perform a variety of key, inter-related functions. These functions include, *inter alia,* recruiting of malleable candidates, raising resources to support their operations, planning their operations (employing such open-source tools as Google Earth), commanding and controlling their operations, conducting influence operations (e.g., disseminating their perspectives of operations in Iraq to sympathetic and uncommitted audiences), and educating and training supporters on a variety of subjects (e.g., interpretations of the Koran; building and deploying Improvised Explosive Devices (IEDs)).

Terrorists have found cyberspace to be an attractive milieu for several reasons. First, the cost of entry is low. One can acquire the latest cyber technology for hundreds-to-thousands of dollars and exploit key open-source software. In addition, terrorists can take full advantage of the extraordinary sums that have been invested by the commercial sector in cyber infrastructure (including communications and navigation systems). Second, cyberpace provides rapid, world-wide reach. Thus, they are able to transcend the limited geographic reach of their prior physical sanctuary and perform the key functions cited above. Third, it has been posited that the next-generation terrorists are being radicalized by on-line interactions[21]. Finally, there is concern that terrorists are developing linkages with trans-national criminals to support their objectives. The trans-national criminals are able to provide terrorists with cyber knowledge while profiting from the relationship.

[8] Wikipedia definition: Hacktivism (a portmanteau of hack and activism) is often understood as the writing of code, or otherwise manipulating bits, to promote political ideology…

Table 2. Options to Counter Terrorist Use of Cyberspace

Recommendations	Proposed Actions
Craft a compelling, multi-media counter-narrative for world-wide delivery	• Challenge extremist doctrine • Offer a compelling narrative • Use graphic visuals • Deliver the message through authentic sources • Amplify, augment grass-root non-extremist voices
Foster intra- and cross-cultural dialogue at all levels	• Address perceptions, realities of American Muslims alienation, marginalization • Enhance civic engagement • Increase people-to-people exchanges • Deal appropriately with the media
Address need for behavioral science research	• Deepen understanding of the radicalization process • Apply social networking theory
Deny or disrupt extremist use of the Internet	• Employ legal means • Undermine trust that binds adversary networks • Exploit convergence of human intelligence and cyberspace
Address capability gaps in USG	• Address cultural and linguistic deficiencies • Reclaim the high ground • Develop a strategic communication plan • Expand community policing programs

Recently, a number of reports have been issued that suggest strategies for the USG to pursue to counter the terrorists' use of cyberspace. As an illustration, the Special Report on Internet-Facilitated Radicalization [22] formulated five recommendations to address the cyber threat posed by terrorists[9]. The many actions associated with those recommendations are summarized in Table 2. From the perspective of this white paper on cyberspace theory, some of the more interesting actions involve developing a strategic communication plan based on a compelling narrative, implementing an innovative program on behavior science research, and addressing USG shortfalls in knowledge of culture and language.

[9] This report recommended that five steps be taken:
• Craft a compelling counter-narrative for worldwide delivery, in multimedia, at and by the grassroots level.
• Foster intra- and cross-cultural dialogue and understanding to strengthen the ties that bind together communities at the local, national, and international levels.
• Recognize and address the need for additional behavioral science research into the process of radicalization both online and offline.
• Deny or disrupt extremist access to, and extremist efforts through, the Internet via legal and technical means, and covert action, where appropriate.
• Remedy and resource capability gaps in government.

2.3.2. Criminal Use of Cyberspace

At a recent workshop on cyber issues at CTNSP, several of the participants focused on the challenges posed by cyber crime.Several of the speakers and panelists emphasized that the threat is real (and expanding). The speakers stated that "We are losing the global cyber war at an accelerated rate." In addition, they stated that "Cybercrime is effective because you can try to commit crimes an infinite number of times, but you need to succeed only a few times." Overall, it was stated that there are three elements of the threat: crime; industrial espionage; and traditional espionage. It was further noted that criminal attack vectors are comparable to those of state attacks.

The speakers also made the following observations. It was recommended that we focus on the "top 25 Common Weaknesses Enumeration (CWEs)". Furthermore, many of the panelists observed that current laws to deal with these issues provide limited value. In addition, it was noted that Web developers and code writers have **no** idea how to write secure code.

This raised the following question: When will the tide turn? It was suggested that we will make useful headway when we implement the following steps. First, it is critical to create safer software. One recommendation was to make business partnerships contractual (e.g., require the company to fix future flaws and security problems in the software). Second, it was observed that we need to stop existing attacks (e.g., implement more effective actions by the US Department of Justice and computer security specialists). However, in order to do so, we need to find the needed talent. As an example, it was observed that China's People Liberation Army periodically runs national talent searches for the best hackers.

2.3.3. Nation State Use of Cyberspace

From a nation-state perspective, different combinations of levers of power are employed to generate desired effects. From a theoretical perspective, these nations formulate their strategy though a mix of P/DIME activities. The effects of these activities are manifested in the areas of PMESII. Tools are being created to explore how alternative P/DIME activities can give rise to differing PMESII effects (see discussion below).

2.3.3.1. United States Use of Cyberspace

Using the P/DIME-PMESII paradigm, one can begin to characterize how cyber changes have empowered the US. In the political dimension, changes in cyberspace have encouraged democratic participation by the population. With respect to the Internet, it has provided a forum for the individual to articulate his views (e.g., proliferation of blogs, contributions to wikis). In addition, political candidates are finding the Internet to be a useful vehicle for raising resources from grass root supporters. Furthermore, Internet sites such as YouTube have enhanced the accountability of candidates.

In the military dimension, the concept of NCO has enhanced effectiveness in selected operational domains (e.g., air-to-air combat). Efforts are still required to quantify the military benefits that are achievable for more complex military operations (e.g., air-land maneuver).

Economically, the commercial sector has seen dramatic improvements in industrial productivity (e.g., Boeing's use of computer aided design tools to support the development of the 777 aircraft and the more recent development of the 787). These cyber-based advancements are giving rise to considerable improvements in responsiveness (e.g., time to market) and cost reductions (e.g., outsourcing "back-room operations" to other nations).

Socially, the development of cyberspace has increased social interactions in several ways. Tens of millions of users participate in social networking sites (e.g., MySpace, FaceBook). In addition, millions of users, world-wide, participate in virtual reality environments (e.g., Second Life). In fact, it has been rumored that terrorist organizations are using virtual reality environments to explore proto-typical operations.

In the information dimension, the Internet has increased dissemination of information, world-wide. Given the US' strong position in entertainment (movies, games) and advertising, it is argued that it provides a strong forum for promoting "soft (or smart) power" [23].

Finally in the infrastructure dimension, many critical infrastructures have been using the Internet to facilitate more efficient and effective operations. However, this constitutes a "double edged sword" because of the potential vulnerability of Supervisory Control and Data Acquisition (SCADA) systems [24].

Overall, it must be stressed that empowerment is more than the sum of the individual PMESII factors.

2.3.3.2. Near-Peer Use of Cyberspace

Various studies of nation-state empowerment provide insights on the projected uses and cyber-strategies of China and Russia. The relevant white papers discuss the recent writings from key conceptual thinkers in those nations and compares and contrasts these strategies. Those nations use a different vocabulary in discussing cyberspace and cyberpower. For example, Chinese writings on the subject focus on stratagems, objective and subjective reality, and the dialectic[10].

Two key aspects of the Chinese view of the Revolution in Military Affairs are particularly germane: "War with the objective of expanding territory has basically withdrawn from the stage of history, and even war with the objective of fighting for natural resources is now giving way to war with the objective of controlling the flow of financial capital."

Furthermore: "If we go our own path to develop military theory, weapons, and equipment, we will develop something never seen before in places that no one has ever thought of before; others will be unable to anticipate or resist our 'self-accommodating systems'."

As an illustration of "self-accommodating systems" against the superior foe, three ways are cited for making a cat eat a hot pepper: "stuff it down his throat, put it in cheese and make him swallow it, or grind it up and spread it on his back. The latter method makes the cat lick itself and receive the satisfaction of cleaning up. The cat is oblivious to the end goal. This is strategy."

[10] "Reasoning that juxtaposes opposed or contradictory ideas and seeks to resolve conflict".

2.3.4. Cyber Deterrence

There are three key challenges that must be addressed to deal with cyber deterrence [25]. These include the challenges of attribution, the lack of a cyber-deterrence track record, and the occurrence of unexpected higher-order effects.

The primary challenge is the perceived difficulty of attributing such attacks to a specific attacker (e.g., state, non-state actor). Note, for example, if competitors believe we cannot determine who is attacking us in cyberspace, they may convince themselves that such attacks involve little risk and considerable gain. However, there is a key trade-off that must be weighed: if we demonstrate our ability to detect and attribute cyberspace attacks we may provide intelligence about our capabilities. Thus, we may be posing a greater cyberspace threat to the nation in the future.

The second key challenge is the lack of a known historical track record of US detection, attribution, and response. This poses a series of key issues. They include the credibility of deterrent actions, emboldening potential attackers, and defining publicly what the US considers a cyberspace "attack" and the potential kinds of responses to such attacks.

The third challenge is the potential for producing higher order effects that might result in unintended consequences and possibly undesired consequences. There are three key issues associated with that challenge. First, it is a function of the nature of the attacker's goals and objectives. Second, if the competitor is concerned about unintended consequences, it could enhance the effects of our deterrence activities if it wishes to control escalation or fears "blowback" from its cyberspace operations. Finally, if the competitor's goal is to create chaos, deterrence could be undermined by the potential for unintended consequences.

In addition, there is interest in "tailoring deterrence" [26] to address the variety of adversaries that exist in cyberspace (e.g., non-state actors; state actors). However, there is a debate within the analytic community as to whether tailored deterrence is a viable concept for the full spectrum of adversaries of the US [27]. That issue represents an important element of the research agenda for the community. However, it is hypothesized that the full set of P/DIME options should be considered in developing a course of action to respond to a cyber attack. For example, the US might respond to a cyber attack through a variety of levers of power including diplomacy (e.g., a demarche) or economic actions (e.g., restricting the flow of technology).

2.3.5. Cyberstrategy "Rules of Thumb" and Principles

In weighing the cyberstrategy insights, three key insights emerged. First, the "low end" users (e.g., individuals, hacktivists, terrorists, trans-national criminals) have enhanced their power considerably through recent cyberspace trends. A tailored deterrence strategy will be needed to keep these entities in check.

Second, potential near-peer adversaries are aggressively exploring options to exploit attributes of cyberspace. In the near term, this is being manifested through acts of espionage that have resulted in the exfiltration of massive amounts of sensitive governmental and industrial data [28]. In the longer term, the US must be prepared to deal

with unique "cyber strategems" that reflect the unique cultural and military history of key nations (e.g., China, Russia).

To deal with the emerging cyber threat, the US must conduct experiments and exercises that feature a creative and aggressive cyber opposing force. It would be naïve and dangerous to assume that future adversaries will not seek to negate the benefits that the US hopes to achieve through net centric warfare.

2.4. Theoretical Aspects of Institutional Factors

This section of the white paper focuses on two critical institutional factors: governance of cyberspace and the legal dimensions of the problem. The section concludes by identifying key institutional issues and principles.

2.4.1. Governance

Table 3 characterizes key governance functions in cyberspace and the organizations that participate in these functions. It can be seen that the mechanisms for governance of the Internet are *exceedingly* complex. Organizational activities often overlap or fit end-to-end, requiring the expenditure of considerable resources in multiple forums to achieve objectives. Consequently, there is a core set of participants (generally in the private sector) that are involved in several of these key organizations.

Table 3. Governance of Cyberspace

Function	ICANN	ISOC*	ITU	OECD	CoE	EU	ISO	IEC	IEEE	W3C	UN
Domain names	●										
International domain names	●		●								
Core Internet functions		●									
Telecommunications standards			●								
World-wide web standards										●	
Product standards			●				●	●	●		
Development			●	●		●					●
Cyber Security**	●	●	●	●	●	●	●	●			

* Internet Society and related organizations (e.g., IETF, IESG, IAB)
** As well as National Governments

In an effort to evaluate the performance of Internet governance, we have introduced the following criteria: open, democratic, transparent, dynamic, adaptable, accountable, efficient, and effective. When assessed against these criteria, one can conclude that recent Internet governance has performed remarkably well.

However, as we look to future, the USG will be challenged to alter its position on Internet governance. Preliminary views on this subject are being articulated at the ongoing Internet Governance Forums (IGF). In fact, a recent white paper on the subject [29] made the following observations:

"Internet Governance is an isolating and abstract term that suggests a nexus with an official government entity. The term also implies a role for the US Congress in Internet decision-making. It is a misnomer because there is no true governance of the Internet; only a series of agreements between a distributed and loosely connected group of organizations and influencers. A more fitting term may be 'Internet Influence,' or for long-term strategy purposes, 'Internet Evolution'."

2.4.2. Cyber Law

One of the most challenging legal issues confronting the cyber community is as follows: "Is a cyberattack an act of war?" Legalistically, the answer is often presented as one of three possible outcomes: it is not a use of force under UN Article 2(4); it is arguably a use of force or not; it is a use of force under UN Article 2(4).

There are several frameworks that are being considered by the legal community to address this issue. Michael Schmitt has formulated a framework that defines and addresses seven key factors: severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility [30]. Once one has assessed each of those factors, one should employ multi-attribute utility theory to weight each of these factors and come to a determination. An associated challenge is to formulate responses to that attack that are consistent with the legal tenet of proportional response.

Overall, the area of cyber law is in its infancy. Although there have been preliminary rulings on sharing of music (e.g., Napster), there are major issues on the questions of sovereignty, intellectual capital, and civil liberties. These issues will be major areas for research for the foreseeable future.

2.4.3. Institutional Principles

Based on the insights developed during the course of this study, four major strawman principles have emerged in the arena of Institutional Factors.

First, given the complexity of the governance mechanisms, one should seek influence over cyberspace vice governance.

Second, the legal community has barely addressed the key issues that must be resolved in the cyber arena. For example, considerable research is needed to assess the following key questions:

- What is an act of (cyber)war?
- What is the appropriate response to an act of (cyber)war?

- What is the appropriate way to treat intellectual property in the digital age?
- How can nations resolve differences in sovereign laws associated with cyber factors?

Third, there is a need for a framework and enhanced dialogue between champions of civil liberties and proponents of enhanced cyber security to establish an adequate balance. Finally, guidance and procedures are required to address the issue of sharing of cyber information between the USG and industry. This approach should be based on the concept of risk management.

3. Connections

At the beginning of this white paper, it was noted that one of the reasons for a theory was the need to **connect** diverse elements of a body of knowledge. In general, the community is focusing on the issue of connecting the knowledge within a stratum of the pyramid. Even though this is challenging, it generally involves communicating among individuals with a common background and lexicon.

It is far more difficult to have individuals connect **across** the different strata of the pyramid. This requires individuals from different disciplines to work effectively together. In order to do so, it requires a holistic perspective on the Measures of Merit (MoMs) for cyber issues.

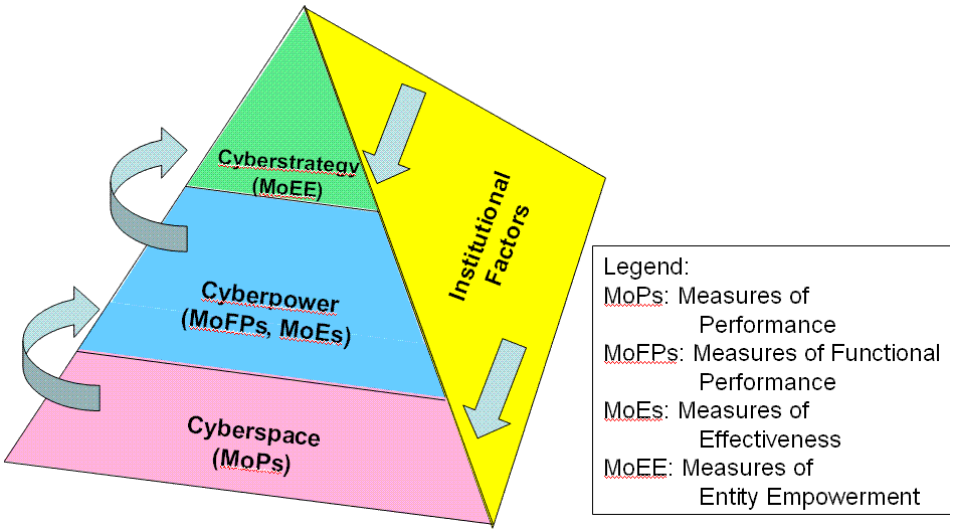

Figure 10. Measures of Merit

Figure 10 suggests a potential decomposition of the MoMs associated with the cyber problem. It identifies four linked sets of measures: Measures of Performance (MoPs),

Measures of Functional Performance (MoFPs), Measures of Effectiveness (MoEs), and Measures of Entity Empowerment (MoEEs). Since this field of endeavor is still in its infancy, the material is meant to be illustrative and not exhaustive.

MoPs are needed to characterize the key computer science and electrical engineering dimensions of the problem. A key measure is the amount of bandwidth that is available to representative users of cyberspace. As the bandwidth increases to the megahertz/sec range, the user is able to access advanced features such as imagery and video products. A second key measure is connectivity. For circumstances in which the cyber-infrastructure is fixed, a useful measure is the percent of people in a country that have access to the Internet. However, in many military operations, the cyber-infrastructure and the users are mobile. Under those circumstances, a more useful measure is the performance of Mobile, Ad hoc NETwork (MANET) users (e.g., their ability to stay connected). Third, one can introduce measures of the "noise" that characterizes the cyber-infrastructure. For example, the extent to which the quality of the Internet is degraded can be characterized by the unwanted e-mail that it carries ("spam"), which can subsume a substantial subset of the network's capacity. As an example, it has been estimated that in recent months up to 90% of the traffic on the Internet is spam [31]. In addition, the integrity of the information is further compromised by "phishing" exploits in which criminal elements seek to employ the Internet to perpetrate economic scams. Finally, MoPs can be introduced to characterize resistance to adversary actions, including denial of service attacks, propagation of viruses or worms, and illicitly intruding into a system.

Table 4. Selected Measures of Merit

Measures	Representative Measures
Performance	• System performance (e.g., latency, bandwidth, reliability) • Resistance to adversary attack (e.g., ability to withstand a DDoS attack)
Functional Performance	• Time to create, validate, disseminate messages • Number of meetings held with surrogate groups • Increase/decrease of anti-Coalition graffiti • Who is "waving", where
Effectiveness (against targeted groups)	• Media: Number of positive/negative stories published/aired • Clerics: Tone of mosque sermons • Military: Loss Exchange Ratios
Entity Empowerment	• Improvements in economic reforms (e.g., reconstruction projects completed effectively) • Political reforms (e.g., participation in elections, reconciliation) • Social reforms (e.g., status of critical infrastructures) • Security (e.g., number, severity of insurgent, terrorist attacks)

It is useful to introduce MoFPs that characterize how successfully selected entities are able to perform key functions, taking advantage of cyberspace. In the case of the US military, the concept of net-centricity is to employ advances in cyberspace to perform essential functions. These include the ability to enhance the performance of increasing levels of

information fusion. Similarly, a basic tenet of net-centricity is to propagate commander's intent so that the participants in the operation can synchronize and self-synchronize their actions.

MoEs are needed to characterize how effective entities can be in their key missions, taking advantage of cyberspace. In the context of Major Combat Operations, MoEs are needed to characterize the ability to exploit cyberspace in multiple dimensions. At one extreme, enhancements in cyberspace have the potential to reduce the time to conduct a campaign and the casualties associated with the campaign. At the other extreme, enhancements in cyberspace may substantially enhance Blue loss exchange ratios and the amount of ground gained and controlled.

From the perspective of cyberstrategy, there is interest is characterizing the extent to which enhancements in cyberspace can empower key entities. In the case of nation states, potential MoEEs might include selected PMESII variables. As an example, it might address the ability to leverage cyberspace to influence a population, shape a nation at strategic crossroads, and deter, persuade, and coerce an adversary.

Table 4 depicts candidate MoMs that may be employed in future cyber analyses.

4. Anticipation

From the perspective of the decision maker, the key challenge is to anticipate what will occur next in the cyber domain and to formulate coherent policy to cope with those issues. To begin to address that challenge, this section deals with four aspects of anticipation. First, it identifies key trends that are expected to characterize cyberspace. Second, it identifies the research activities that should be conducted to address those trends. Third, it briefly identifies the major policy issues that decision makers will need to address. Finally, it discusses the assessment needs that must be addressed to support the formulation and analysis of policy options.

4.1. Cyber Trends

It is extremely difficult to provide quantitative estimates as to how rapidly key trends in cyberspace will be manifested. Thus, the following should be regarded as a partial, qualitative list of some of the most significant potential changes.

First, there is an increased move to adoption of IP-based systems. As a consequence, one can anticipate a convergence of telephone, radio, television, and the Internet. As one example, there is a dramatic use of Voice over IP (VoIP) (with attendant security issues) in the area of telephony. Second, we are seeing the emergence of sensor networks that feature an extremely large number of heterogeneous sensors. As one manifestation, we are seeing the netting of extremely large number of video cameras in urban areas, raising issues in the civil liberties community. Third, we are seeing an inexorable trend towards proliferation of broadband and wireless. An example of this trend was the plan to have city-wide deployment of Worldwide Interoperability for Microwave Access (WiMax). However, this trend suggests the difficulty in predicting when a trend becomes a reality. NEXTEL had

made this objective the key to their strategy; however, they have recently observed that the technology has not matured sufficiently to implement it in the near-term [32]. Fourth, we are observing enhanced search capabilities, both for local systems and the entire Internet. One of the keys to this trend has been industrial competition to develop improved search engines (in part, to enhance advertising revenue). Fifth, we are seeing extraordinary efforts to enhance human/machine connectivity. As one example, we are seeing direct nerve and brain connections to computers or prostheses, arising from efforts to treat soldiers injured by IEDs in Iraq [33]. Sixth, we are seeing dramatic increases in user participation in information content. This trend is manifested through the proliferation of video blogs, contributions to wikis, participation in social networks (e.g., MySpace, FaceBook), and involvement in virtual reality environments (e.g., Second Life). Finally, some experts have postulated that we are entering the third phase of the Internet (i.e., phase 1: communicating; phase 2: content; phase 3: collaboration). This third phase is characterized by "cloud computing" where "information is stored and processed on computers somewhere else" [34]. One of the major issues associated with this paradigm is our ability to provide adequate security for the "cloud".

4.2. Opportunities for Cyber Research

As an application of the emerging theory of cyber, Table 5 identifies the major areas where cyber research should be pursued.

Table 5. Areas Where Additional Theoretical Research Is Required

Area	Research Areas
Cyberspace	• Perform technology projections to identify key breakthroughs • Develop techniques to protect essential data from exfiltration, corruption • Formulate an objective network architecture that is more secure, and identify options to transition to it
Cyberpower	• Extend analyses to other levers of power (e.g., diplomatic, economic) • Perform risk assessments to address cyber-dependence • Quantify the Blue-Red information duel
Cyberstrategy	• Conduct research on "tailored deterrence" • Explore options to address cyber espionage
Institutional Factors	• Perform research on cyber influence; legal frameworks; balance between security and civil liberties
Cyber Assessment	• Develop analytical methods, tools, data, and intellectual capital to assess cyber issues

4.2.1. Cyberspace Research

In the area of cyberspace, improved technology projections are needed to identify key breakthroughs that may substantially affect MoPs for cyberspace. Second, it is inevitable

that malevolent actors (e.g., insiders, adaptive adversaries) will gain access to the USG and defense industrial base cyberspace. This suggests that research is needed to protect the essential data in cyberspace from exfiltration or corruption.

Finally, additional research is needed to formulate an objective architecture for cyberspace that is inherently more secure than the existing architecture. Consistent with that effort, there is a need to address the challenging issue of transitioning from the existing to the objective architecture.

4.2.2. Cyberpower Research

Due to resource constraints, this evolving assessment of cyber theory has not adequately addressed all the levers of power (e.g., political, diplomatic, economic). As an initial step, assessments should be completed for these other levers of power. Second, existing assessments of the military lever of power have focused almost exclusively on the potential benefits that can accrue by creatively employing cyberspace. It is equally important to perform risk assessments to understand the potential downside of relying extensively on cyberspace. This includes conducting experiments and developing the methodology, tools, data, and intellectual capital required to perform military risk assessments. Similarly, it is important to conduct research into the potential benefits and risks associated with leveraging cyberspace developments for non-US military capability (e.g., NATO allies that are pursuing Network Enabled Capabilities (NEC)). Finally, in the area of information, additional research is needed to quantify the information duels that are likely to occur with potential adversaries.

4.2.3. Cyberstrategy Research

To deal with the challenges posed by the full array of entities empowered by enhancements in cyberspace, it is vital that the information-enabled societies conduct research on "tailored deterrence". This concept suggests that key alliances, such as NATO, must develop a holistic philosophy that understands each of the potential adversaries (e.g., its goals, culture, risk calculus), develops and plans for capabilities to deter these adversaries, and develops a strategy to communicate these concepts to the potential adversaries.

4.2.4. Institutional Factors Research

Theoretical research is needed to address key gaps in institutional knowledge in the areas of governance, legal issues, sharing of information, Internet regulation, and civil liberties.

First, in the area of governance, the USG must reassess the role of the Internet Corporation for Assigned Names and Numbers (ICANN) in the governance of the Internet. It is clear that, in the future, the USG must be more adroit in the area of "cyber influence" vice governance. This will require a thorough re-examination of all the institutional bodies that affect cyber governance and the development of a USG strategy to interact with them.

Second, "cyber legal" issues are in their infancy. The current situation is non-homogeneous with inconsistent laws in various sovereign nations (e.g., German hate-crime laws; limited signatories to the Council of Europe Convention on Cybercrime [35]. In particular, there is a need to clarify the issue of espionage in cyberspace (e.g., What is it?

What rights of response are left to the victims?). In addition, there is a need to adopt a consistent model that can be applied to determine whether a cyber attack is an act of war.

Third, there is continued controversy about the sharing of information between the USG and the private sector. Research is needed to determine what information should be shared, under what circumstances.

Fourth, it has been observed that regulatory agencies, such as the Federal Communications Commission, have the authority to regulate Internet Service Providers (ISPs) to redress selected cyber security issues. However, to date, regulatory agencies have been reluctant to address these issues.

Fifth, the recent debate about the Foreign Intelligence Surveillance Act (FISA) court has mobilized the civil liberties community to raise the specter of "Big Brother". As a consequence of the actions of civil liberties organizations, key USG programs have been terminated or modified (e.g., DARPA's Total Information Awareness (TIA), DHS's Multi-state Anti-Terrorism Information Exchange (MATRIX)). Research is needed to clarify the appropriate balance among actions to deal with adversaries while still protecting civil liberties.

4.2.5. Cyber Assessment Research

As discussed below, our ability to perform cyber assessments is extremely uneven. As a consequence, research efforts are required to develop analytical methods, tools, data, services, and intellectual capital to address key cyber issues in the areas of cyberpower, cyberstrategy, and infrastructure issues.

Table 6. Selected Policy Recommendations

Area	Issue/Recommendations
Cyberspace	• **Security:** USG should adopt a "differentiated security" approach • **Human capital, R&D:** Enhance cyber education & training; establish cyber labs; increase resources
Cyberpower	• **Net Centric Operations risks:** Employ an OPFOR that is highly cyberwar-capable • **CNA:** Reduce classification, enhance integration • **Influence Operations:** Adopt a holistic, multi-disciplinary, Interagency approach • **SSTR:** Adopt I-Power approach
Cyberstrategy	• **Organization:** Create a new organization to formulate/oversee policy on cyber issues • **Deterrence:** Formulate, implement "tailored deterrence" • **Espionage:** Conduct policy/legal review
Institutional Issues	• **Governance:** USG should develop, implement Internet *influence*

4.3. Cyber Policy Issues

Several major policy issues have been singled out that require further attention. For the purposes of this preliminary cyber theory, these issues have served to focus the boundaries of this study, although we have also addressed a number of lower priority policy issues. Consequently, emphasis has been placed on assembling the intellectual capital required to illuminate those issues.

In Table 6, these issues have been aggregated into the categories of cyberspace, cyberpower, cyberstrategy, and institutional factors. Most of these issues are extremely broad and contentious; consequently, additional analyses will be required to address them adequately.

4.4. Cyber Assessment

One of the major challenges confronting the analysis community is to develop the methods, tools, and data needed to support cyber policy decision makers. Figure 11 suggests the relative maturity of key tools in the areas of cyberspace, cyberpower, cyberstrategy, and institutional factors.

In the areas of cyberspace, there are several tools that the community is employing to address computer science and communications issues. Perhaps the best know is the OPNET simulation [36] that is widely employed to address network architectural issues. From an analytic perspective, techniques such as percolation theory [37] enable one to evaluate the robustness of a network. Looking to the future, the National Research Laboratory (NRL) has developed a GIG Testbed to explore the myriad issues associated with linking new systems and networks.

In the area of cyberpower, the community has had some success in employing live, virtual, and constructive simulations. For example, in assessments of air-to-air combat, insights have been derived from the live AIMVAL-ACEVAL experiments, virtual experiments in the former McDonnell Air Combat Simulator (MACS), and constructive experiments using tools such as TAC BRAWLER. However, the community still requires better tools to assess the impact of advances in cyberspace on broader military and informational effectiveness (e.g., land combat in complex terrain).

In the area of cyberstrategy, a number of promising initiatives are underway. In response to recent tasking by STRATCOM, a new methodology and associated tools are emerging (i.e., Deterrence Analysis & Planning Support Environment (DAPSE) [38]. However, these results have not yet been applied to major cyberstrategy issues. In addition, promising tools are emerging from academia (e.g., Senturion; GMU's Pythia) and DARPA (e.g., Conflict Modeling, Planning & Outcomes Experimentation (COMPOEX)). However, these are still in early stages of development and application.

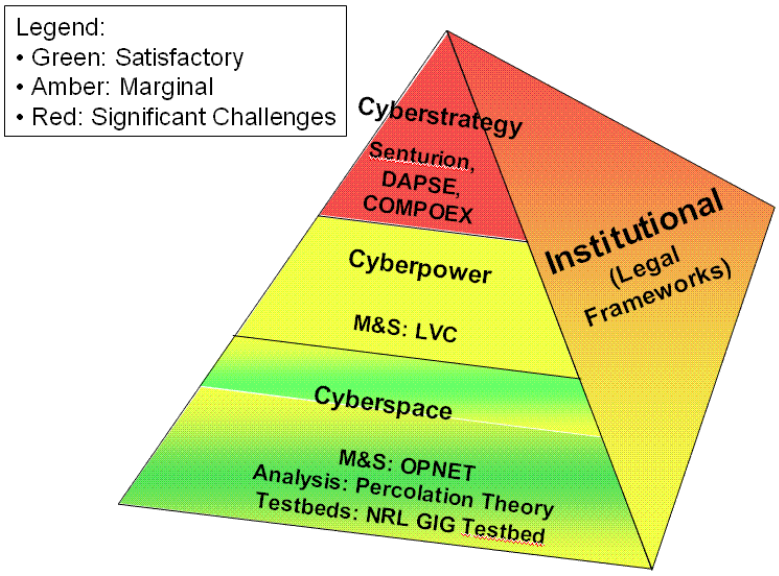

Figure 11. Subjective Assessment of MS&A for Cyber Policy Analyses

Finally, as noted above, there are only primitive tools available to address issues of governance, legal issues, and civil liberties. Some tools are being developed to explore the cascading effects among critical infrastructures (e.g., National Infrastructure Simulation and Analysis Center (NISAC) system dynamics models [39]); however, they have not yet undergone rigorous validation.

5. Summary

Consistent with the macro-framework that has been adopted to characterize the cyber problem, this section summarizes the key insights in the areas of cyberspace, cyberpower, cyberstrategy, and institutional factors. The section concludes by identifying the next steps that should be taken to refine the theory of cyberpower.

5.1. Key Insights

5.1.1. Cyberspace

Cyberspace is an environment that is experiencing exponential growth in key MoPs. There is an extraordinary diffusion of knowledge among all the stakeholders of cyberspace, including malevolent users. As a consequence of this diffusion of knowledge, cyberspace is being degraded by "noise" (e.g., proliferation of spam) and a broad variety of cyber attacks. The most troubling of these attacks includes Distributed Denial of Service, exfiltration of data, and the potential for corruption of data. In each instance, recent experience has

demonstrated that these attacks are relatively easy to implement (e.g., technically, financially) and extremely difficult to attribute.

These vulnerabilities arise from the basic architecture that has evolved from the original ARPAnet. A new cyberspace architecture may be required to halt the perceived erosion of security. However, there will be substantial difficulties in transitioning from the current architecture to one that is more robust against adversary action.

5.1.2. Cyberpower

As cyberspace evolves, it has the potential to enhance each of the levers of national power. This white paper has focused on two of these levers: military and information.

In the area of military power, it was observed that studies are underway to characterize the extent to which enhancements in cyberspace can enhance key MoEs. These studies tend to be unambiguous in the area of air-to-air combat where experiments suggest that enhanced digital communications can enhance loss-exchange ratios by a factor of approximately 2.5. Although studies of other military operations have also been undertaken, the results are generally confounded by other factors (e.g., mobility, protection).

To complement these experiments, an assessment of theories of environmental warfare was undertaken that critically reassessed the theories of land, sea, air, and space theory. Based on that assessment, it was concluded that a theory of cyberpower should focus on four key factors: technological advances, speed and scope of operations, control of key features, and national mobilization.

From the perspective of "information", this white paper has addressed influence operations from a strategic and tactical perspective. Based on prior experiences and an adaptation of earlier analytical frameworks, an approach was developed for linking operational objectives and processes to DOTMLPF requirements. These assessments suggest that developments in cyberspace can substantially affect future efforts to enhance influence operations (e.g., implement precision guided *messages*).

5.1.3. Cyberstrategy

The evolving theory of cyber has identified a range of entities that will be empowered by enhancements in cyberspace. These include: terrorist groups, who are employing cyberspace to, inter alia, recruit, raise money, propagandize, educate and train, plan operations, command and control operations; hacktivists, who are employing cyberspace to conduct "cyber riots" (e.g., Estonia) and implement exploits in cyberspace; transnational criminals, who pursue a variety of techniques (e.g., phishing, denial of service attacks) to raise substantial funds (reputed to be more than the money derived from drug trafficking); and nation states, the most advanced of whom are employing cyberspace to enhance all dimensions of PMESII activities.

However, changes in cyberspace have given rise to unintended consequences. Many of the entities at the "low end" of the entity spectrum (e.g., terrorists, hacktivists, transnational criminals) are making life more dangerous for information-enabled societies. In particular, these entities tend to be much more adaptable than nation states, causing the latter to

respond, belatedly, to the initiatives of the former. In addition, research about selected near-peers (e.g., China, Russia) suggests that they have new perspectives on cyberstrategy that will present information-enabled societies with new challenges in cyberspace.

5.1.4. Institutional Factors

From an institutional perspective, issues are emerging that will affect all aspect of cyber theory. This white paper has highlighted the challenges that exist in cyber governance, legal issues, exchange of cyber information between governments and industry, and the balance between national security and civil liberties.

From a theoretical perspective, one of the major challenges emerges from the difficulty in characterizing and responding to an attack in cyberspace. As demonstrated by recent events, it is extremely difficult to attribute an attack to an adversary that chooses to act anonymously. In light of that ambiguity, it is difficult to formulate a coherent response to such an attack. For example, it is still unclear how an alliance, such as NATO, might respond in the future to a cyber attack against one or more of its members.

5.2. Next Steps

This effort constitutes an evolving theory of cyberpower. To refine this product, it is recommended that the following steps should be pursued.

5.2.1. Define

There is still confusion about the definitions for the key terms in a theory of cyberpower. However, the community should find it relatively straightforward to go from the current base to agreement on key terms (e.g., "cyberspace"). However, additional work is still required to establish the linkage between cyber terms and the terms associated with information operations.

5.2.2. Categorize

The "cyber pyramid" has proven to be a useful taxonomy in "binning" key concepts. However, there is still a need to develop specific cyber frameworks and models to explore key policy issues that confront senior decision makers.

5.2.3. Explain

It is anticipated that this evolving theory of cyberpower will be incomplete. Additional efforts are needed to address key issues that are beyond the scope of this white paper. In the area of cyberpower, there is a need to assess how potential changes in cyberspace will affect political, diplomatic, and economic functionality and effectiveness. In the area of cyberstrategy, there is a need to assess the extent to which key entities are empowered by advances in cyberspace and cyberpower. These include individuals, NGOs, transnational corporations, selected nation states, alliances (e.g., NATO), and international organizations (e.g., UN). Finally, in the area of institutional factors, there is a pressing need to assess the

effect of changes in cyberspace on the balance between civil liberties and national security. In assessing these issues it would be useful to employ a risk management approach.

5.2.4. Connect

Currently, we have relatively little understanding about the appropriate Measures of Merit to employ in cyber assessments nor the relationships among those measures. For example, we do not have a clear understanding about how changes in cyberspace (e.g., MoPs such as bandwidth or resistance to enemy countermeasures) impacts the US's levers of power (i.e., P/DIME) or empowerment (i.e., PMESII). At a minimum, it is important to develop preliminary relationships so that a decision maker can understand the implications of how potential changes in cyberspace or institutional factors will affect cyberpower and cyberstrategy.

5.2.5. Anticipate

As noted in this white paper, cyberspace is in the midst of explosive, non-linear change. It is vital that more detailed technology assessments be undertaken to anticipate and understand potential break-throughs in cyberspace (e.g., the analogue of discovering giant magnetoresistance or fundamental changes in the architecture of the Internet). Furthermore, efforts should be made in the development and application of models, simulations, and analyses to assess the impact of these changes on cyberpower and cyberstrategy. These developments in methodologies, tools, and data should provide decision makers with the analytic support needed to explore the long-range affect of alternative cyber options.

References

[1] Dr. Harold R. Winton, Air War College, Maxwell AFB, "An Imperfect Jewel", presented at Institute of National Strategic Studies (INSS) workshop on theory of warfare, NDU, Washington, DC, September 2006.

[2] Jim Holt, "Unstrung", The New Yorker, October 2, 2006.

[3] William Gibson, "Neuromancer", Ace Science Fiction, 1984.

[4] Deputy Secretary of Defense Memorandum, "The Definition of Cyberspace", May 12, 2008.

[5] "The National Military Strategy of the United States of America – A Strategy for Today, A Vision for Tomorrow," Joint Chiefs of Staff, 2004.

[6] Joint Publication 3-0. "Joint Operations", Joint Staff, 17 September (incorporating change 1 13 February 2008).

[7] G.E.P. Box, "Robustness in the Strategy of Scientific Model Building, in "Robustness in Statistics", R. L. Launer and G. N. Wilkinson, editors, 1979, Academic Press: New York.

[8] John Markoff, "Military Supercomputer Sets Record", New York Times, June 9, 2008).

[9] Jeremy M. Kaplan, "A New Conceptual Framework for Net-Centric, Enterprise Wide, System-of-Systems Engineering," CTNSP/NDU, Number 29, July 2006.

[10] Sally Adee, "37 Years of Moore's Law", IEEE Spectrum, May 2008.

[11] H.J. Mackinder,"The Geographical Pivot of History", 1904.

[12] Alfred T. Mahan, "The Influence of Sea Power Upon History (1660 – 1783)", Little, Brown and Company, Boston, 1890.

[13] Giulio Douhet, "The Command of the Air", translated by Dino Ferrari, Coward-McCann, 1942.

[14] Colin S. Gray and Geoffrey Sloan, "Geopolitics, Geography, and Strategy", Routledge, 30 November 1999.
[15] David S. Alberts and Richard E. Hayes, "Power to the Edge", Command and Control Research Program, June 2003.
[16] David T. Signori and Stuart H. Starr, "The Mission Oriented Approach to NATO C2 Planning", Signal Magazine, PP 119 – 127, September 1987.
[17] Colonel Ralph Baker, "The Decisive Weapon: A Brigade Combat Team Commander's Perspective on Information Operations", Military Review, May-June 2006.
[18] George Gilder, "Metcalfe's Law and Legacy", Forbes ASAP, 13 September 1993.
[19] Bob Briscoe, Andrew Odlyzko, Benjamin Tilly, "Metcalfe's Law is Wrong", IEEE Spectrum, July 2006.
[20] Daniel Gonzales, et al, "Network-Centric Operations Case Study: Air-to-Air Combat With and Without Link 16", RAND, National Defense Research Institute, 2005.
[21] Marc Sageman, "The Homegrown Young Radicals of Next-Gen Jihad", Washington Post, page B-1, June 8, 2008.
[22] Homeland Security Policy Institute, "NETworked Radicalization: A Counter-Strategy", GWU, Washington, DC, May 2007.
[23] Joseph S. Nye, Jr., "Understanding International Conflicts: An Introduction to Theory and History", New York: Pearson-Longman, 2005.
[24] Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies", Wall Street Journal, April 8, 2009, page 1.
[25] Kevin Chilton and Greg Weaver, "Waging Deterrence in the Twenty-First Century", Strategic Studies Quarterly, Spring 2009.
[26] N. Elaine Bunn, "Can Deterrence Be Tailored?", Strategic Forum, Institute of National Strategic Studies, NDU, No. 225, January 2007.
[27] AFEI Conference on Cyber Deterrence, Tysons Corner, VA,Nov 1-2, 2007.
[28] John Markoff, "Vast Spy System Loots Computers in 103 Countries," New York Times, March 29, 2009.
[29] OASD(NII)/DOD CIO Globalization Task Force, "Development of an Internet Influence/Evolution Strategy for the Department of Defense",October 19, 2007.
[30] M. N. Schmitt, *Bellum Americanum:* "The US view of Twenty-first Century war and its possible implications for the law of Armed Conflict", Mich. J. Int. Law 19, 4(1998), pp. 1051-1090.
[31] John Soat, "IT Confidential: Is There Anything That Can Be Done About E-mail?", Information Week, February 17, 2007.
[32] Audi Lagorce, "Clearwire, Sprint Nextel Scrap WiMax Network Agreement", Market Watch, November 9, 2007.
[33] Michael J. Riezenman, "Melding Mind and Machine", the Institute, IEEE, June 2008.
[34] Geoffrey A. Fowler and Ben Worthen, "The Internet Industry is on a Cloud – Whatever That May Mean", Wall Street Journal, March 26, 2009, page 1.
[35] Convention on Cybercrime, Budapest, Hungary, November 23, 2001 (//conventions.coe.int/Treaty/EN/Treaties/Htm/185.htm).
[36] Emad Aboelela, "Network Simulation Experiments Manual", Morgan Kaufmann, publisher; 3rd edition, June 2003.
[37] Ira Kohlberg, "Percolation Theory of Coupled Infrastructures", 2007 Homeland Security Symposium, "Cascading Infrastructure Failures: Avoidance and Response", National Academies of Sciences, Washington, DC, May 2007.
[38] Strategic Multi-Layer Analysis Team (Nancy Chesser, Editor), "Deterrence in the 21st Century: An Effects-Based Approach in An Interconnected World, Volume I", sponsored by USSTRATCOM Global Innovation and Strategy Center, 1 October 2007.
[39] COL William Wimbish and MAJ Jeffrey Sterling, "A National Infrastructure Simulation and Analysis Center (NISAC): Strategic Leader Education and Formulation of Critical Infrastructure Policies", Centre for Strategic Leadership, US Army War College, August 2003.

Glossary

Abbreviation	Definition
C2	Command and control
COMPOEX	Conflict Modeling, Planning & Outcomes Experimentation
CNA	Computer Network Attack
CNO	Computer Network Operations
CTNSP	Center for Technology and National Security Policy
DAPSE	Deterrence Analysis & Planning Support Environment
DARPA	Defense Advanced Research Projects Agency
DIME	Diplomatic, Information, Military, Economic
DoD	Department of Defense
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership & Education, Personnel, Facilities
GIG	Global Information Grid
HSCB	Human, Social, Cultural Behavior
IAB	Internet Architecture Board
IED	Improvised Explosive Device
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
INSS	Institute for National Strategic Studies
IO	Information Operations
IP	Internet Protocol
IRTF	Internet Research Task Force
ISOC	Internet Society
JMEM	Joint Munitions Effectiveness Manual
JTRS	Joint Tactical Radios System
JWICS	Joint Worldwide Intelligence Communications System
MACS	McDonnell Air Combat Simulator
MANET	Mobile Ad Hoc Network
MoE	Measure of Effectiveness
MoEE	Measure of Entity Empowerment
MoFP	Measure of Functional Performance
MoM	Measure of Merit
MoP	Measure of Performance
NATO	North Atlantic Treaty Organization
NCO	Net Centric Operations
NCW	Net Centric Warfare
NDU	National Defense University
NEC	Net Enabled Capability
NMS-CO	National Military Strategy for Cyber Operations
NRL	Naval Research Laboratory
OLPC	One Laptop Per Child

OODA	Observe-Orient- Decide-Act
OS	Operating System
OSD	Office of the Secretary of Defense
P/DIME	Political/ Diplomatic, Information, Military, Economic
PMESII	Political, Military, Economic, Social, Information, Infrastructure
QDR	Quadrennial Defense Review
R&D	Research & Development
SME	Subject Matter Expert
SOA	Service Oriented Architecture
SSG	Strategic Studies Group
SSTR	Stability, Security, Transition, Reconstruction
STRATCOM	Strategic Command
TIA	Total Information Awareness
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USG	United States Government
VOIP	Voice over Internet Protocol
WIMAX	Worldwide Interoperability for Microwave Access