STRATEGY
RESEARCH
PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

STRATEGIC LEADERSHIP'S ROLE IN INFORMATION WARFARE

BY

COMMANDER KEVIN R. WALTER
United States Navy

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

USAWC CLASS OF 1998

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

STRATEGIC LEADERSHIP'S ROLE IN INFORMATION WARFARE

by

Commander Kevin R. Walter

Colonel Dan Henk
Project Advisor

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Kevin R. Walter

TITLE: STRATEGIC LEADERSHIP'S ROLE IN INFORMATION WARFARE
FORMAT: Strategy Research Project

DATE: 19 May April 1998 PAGES: 43 CLASSIFICATION: Unclassified

This study examines the appropriate role of strategic leadership in the development of a National Information Strategy and supporting policies. It examines current policy and evaluates its reliance on information technology as a means to implement the policy. It offers a history of the Internet, a look at its accelerated growth, and its relevance to national interest. It concludes by arguing for a coherent, effective National Information Strategy and supporting policies to carry the country into a new millennium.

TABLE OF CONTENTS

STRATEGIC LEADERSHIP'S ROLE IN NATIONAL INFORMATION STRATEGY AND SUPPORTING POLICY

INTRODUCTION

Information is a strategic asset. According to Branscomb, "In virtually all societies, control of and access to information became an instrument of power, so much so that information came to be bought, sold and bartered by those who recognized its value".[1]

The quantum increase in available data in the aftermath of the "Information Revolution" makes it increasingly important to recognize the distinction between "information" and "data". This is analogous in industry to the difference between a raw material and the manufactured product. This research paper will examine ramifications of the increasing amount of data on the World Wide Web and the challenge of getting useful, accurate, and reliable information from these data. Recognizing the distinction between data and information will be increasingly important for strategic leaders.

The inter-relationship of national security strategies with respect to advances in technology and the recognition of national information vulnerabilities to information warfare threats is also examined. A coherent national information strategy and supporting policies are essential as the nation copes with the challenges and opportunities of the "Information Age".

NATIONAL DIRECTION

The President, in his 1998 State of the Union address, reaffirmed the fact that we are now in the "Information Age": an age when it is nearly possible to reach every book ever written. He acknowledged the need for a new way of governing in the Information Age, an age of learning in which an "information superhighway" crosses not only party lines but national borders. According to the President, if we want America to lead, we've got to set a good example, one which others will follow.[2] The significance of the fact that the nation has entered the Information Age is also reflected in several important strategic planning documents published by the national government. These documents are highlighted below.

NATIONAL SECURITY STRATEGY

The Clinton administration's grand strategy, *The National Security Strategy for A New Century* (1998), calls attention to the fact that the flow of information can and does transit borders, and the distinctions between foreign and domestic policies continue to merge and blur.[3] National security is becoming more dependent on information infrastructure and is highly interdependent and increasingly vulnerable to tampering and exploitation. [4] According to the strategy, the nation must implement policies, technologies and concepts to engage these new and futuristic threats and opportunities. A vision for the Information Age and the policies to support the vision are of paramount importance to the nation's future.

NATIONAL MILITARY STRATEGY

Rapidly evolving information technology has profound military implications. *The 1997 National Military Strategy - Shape, Respond, Prepare Now--A Military Strategy for a New Era*, identifies "information superiority" and "technological innovation" as two important elements of this strategy.[5] The document defines Information Superiority (IS) as the capability to collect, process, and disseminate an uninterrupted flow of precise and reliable information, while denying the enemy's ability to do the same.[6] At its best, IS would enable a military leader to direct widely dispersed personnel while maintaining a thorough knowledge of the entire battlefield.

Any nation seeking to maintain IS would be obliged to leverage emerging technologies to continually improve the capabilities of its forces. The notion of using the increasing abilities of technology to enhance national defense is not solely a U.S. aspiration. Russian Defense Minister Sergeyev has posed the question:

> " Why will I need countless hordes and fleets of tanks if a potential war is going to be a war of technologies." [7]

QUADRENNIAL DEFENSE REVIEW

The *Report of the Quadrennial Defense Review* (QDR)(1997) identifies new threats and dangers that are harder to define and more difficult to track than in the past. This document suggests that it will be increasingly difficult to separate fact from fiction and antiquated assumptions from current realities.[8] According to the document, the new programs that are undertaken by the Department of Defense will exploit the potential of information technologies and other advancing technological opportunities to transform the way the nation provides the military arm of national security.[9] The QDR highlighted the danger to our nation and implications of "asymmetric threats". Such threats range from nuclear, biological, chemical weapons to attacks via *information warfare* and terrorism.[10]

A former Chairman of the Joint Chiefs of Staff has emphasized the importance of information superiority: "we will need to integrate existing and new information systems while exploiting commercial technology. We must also have effective defensive and offensive information capabilities."[11]

STRATEGIC ART

Strategic Art may be defined as the skillful formulation, coordination, and resources (objectives), ways (courses of action), and application of ends (means), to promote and defend the national interest. Mastering this art requires vision to see over and beyond bureaucratic barriers.[12] Successful strategic leaders of the future will cultivate new skills (technologies), one of the most important of which is the ability to select and extract vital information from the great mass of useless surplus data. " Innovativeness, conceptual thinking, a willingness to accept risk, the ability to exploit rapid and persistent change, openness to continuing education, and general mental flexibility will separate masters of strategic art from apprentices".[13]

In a time when our reliance on technology is well documented, it is critical that national policies keep pace with the changing capabilities offered by technology. Leveraging technology by itself cannot and will not fill the requirement for a vision for the future. This vision must address clear national interest and not be driven or motivated solely by a desire for corporate profits. The responsibility for formulating a coherent national information strategy and supporting policy cannot be abrogated to corporate America, which answers to the "bottom line" and not the welfare of the nation.

INFORMATION WARFARE

> "...Attaining one hundred victories in one hundred battles is not the pinnacle of excellence. Subjugating the enemy's army without fighting is the true pinnacle of excellence."
>
> Sun Tzu, The Art of War

Thomas Rona, an early proponent of information warfare (and originator of the term) offered the following definition of the discipline: The strategic, operation and tactical level competitions across the spectrum of peace, crisis, crisis escalation, conflict, war, war termination, and reconstitution/restoration, waged between competitors, adversaries or enemies using information means to achieve their objectives. [14]

Martin Libicki suggests some adjustments to Rona's definition and identifies seven distinct forms of information warfare:

- Command and control - strikes against enemy command structure.
- Intelligence - protects and denies information.
- Electronic - radio or cryptographic information dissemination.
- Psychological - use of information against individual minds.
- Hacker - unauthorized intrusion into computer systems.
- Economic - blocking economic data
- Cyberwar - futuristic information-based warfare[15]

A recent Army doctrinal publication introduced the concept of Opposing Force Informational Warfare (OPFOR-IW): "information" operations by a hypothetical enemy faced by the United States in the future. This hypothetical opponent can be expected to conduct, "Specifically planned and integrated actions to achieve an information advantage, at critical points and times. The attacker gains an advantage by affecting adversary information and information systems and defending his own information and information systems"[16]

The Army's OPFOR IW doctrinal concept integrates all elements of power---Political, Economic, Military, and Information---to implement an "informational" strategy. It also introduces a concept called "perception management", which is broader than psychological operations (PSYOP) in that its audience is not limited to foreign audiences. The Army's hypothetical enemy uses truth, false information, and misinformation. It also "spins" information to fit its needs.

"Any person or organization with access to commercially available technology and an information strategy can conduct IW. Commandante Marcos of the Zapatista rebels in Mexico [1997] and the Chinese students in Tianamen Square [1989], for example, harnessed technology, had an information strategy, and marshaled international support for their causes."[17]

Some authors using the term "information warfare" restrict it to the military or cyber domains dominated by computers. This narrow definition, however, overlooks other important forms of communications or processing information, and unnecessarily constrains relevant broad policy questions. The many questions regarding IW's impact during peacetime, during a transition to crisis and ultimately during hostilities are all important to national security.[18] Broad policy issues in need of attention by policy makers include the following:

- Except in rare instances, isolation of military, national, public, and private information systems is not possible. Military communications are carried on national infrastructure systems. Public and private sectors are heavily interdependent and this linkage will continue to grow.[19]

- Interposing military forces between threats or adversaries and their targets no longer can protect the U.S. heartland. Traditional military forces can be bypassed at the speed of light by Information Age attacks on the general population or key infrastructure systems.[20]
- In questions of information security, there is no consensus on the appropriate boundary between the Department of Defense roles and missions, and those of law enforcement and intelligence organizations, and on those of the commercial sectors.[21]

Elements of Information Warfare

"Psychological" and "hacker" warfare are two elements of Information Warfare which could have profound impact on the daily lives of American citizens in an Information Age society. The impact of technology on these two element of IW can be captured in the following quote from Mark Slouka's *War of the Worlds*: "Technology is never neutral: it orders our behavior, redefines our values and impacts our lives in ways we can't always predict"[22] To optimize information technology, must move beyond traditional, linear battlefield conceptualizations that hold us to an unrealistic, almost dysfunctional thinking mode. Instead, we must develop an open-ended method that enables us to visualize warfare in nonlinear terms - as a series of occurrences rather than as a single, sequential event. This concept requires a strategic vision to recognize the collective impact of these apparently independent events.[23]

Psychological Warfare

Libicki identifies four categories of psychological warfare:

- operations against the national will
- operations against opposing commanders
- operations against troops
- cultural conflict

While all of these areas are important, this paper is more concerned about psychological warfare (PSYWAR), which targets the national will. PSYWAR can take the form of commercial news events such as media broadcasts in 1993 of Somalis dragging the corpses of U.S. soldiers through the streets of Mogadishu.[24] The technologies available in this area are growing, and now include Direct Broadcast Satellites (DBS) and the Internet, which afford a nation's leadership or ordinary citizens the opportunity to communicate directly to the people in other nations. National boundaries are porous to information penetrations. Staged events can be camouflaged to appear as "breaking news" and will be used more in the future to blur the distinction between reality and virtual reality.[25]

The use of deception using technology is also recognized in current Russian literature. A recent Russian military article described offensive information warfare as designed to use the Internet channels for the purpose of organizing PSYOP.[26] The article notes that the human element is often mistakenly neglected in the rush to develop new technologies. This is significant, since the capabilities to alter the information processing systems of the human body could hold the key to the success of future information warfare campaigns.[27]

HACKER WARFARE

Hacker warfare can be defined in its simplest terms as the unauthorized access into someone else's computer space, often referred to as "cyber space". Even though cyberspace is not marked by physical boundaries such as a door, unauthorized entry is just as intrusive. "Information is power: It is the hacker creed." [28]

In 1996 the government accounting office (GAO) reported that as many as 250,000 attempts may have been made to penetrate military computer networks, with sixty-five percent being successful. The GAO report suggested that the potential for catastrophic damage is great." [29] Computer hacker break-ins are estimated to be a $10 billion-a-year problem and there are almost 2,000 Web sites offering tips and techniques to hackers.[30] " The bad actors who use these tools range from the recreational hacker who thrives on the thrill and challenge of breaking into somebody else's computer, to the national security threat posed by information warriors intent on achieving strategic advantage." [31]

Louis Gerstner, CEO of IBM supports a program in which government and industry work together to set standards for security practices, such as hacker-resistant encryption codes. "We should be encouraging the widespread adoption of encryption technology right now, led by U.S. - based manufacturers," Gerstner said.[32] These types of break-ins are a world wide problem in the private sector. The United Kingdom's National Computer Center reported a 60 percent increase in computer based theft in the U. K. during 1995.

Even if the information on your Web server is of little value, you should worry about a deliberate denial of service by hackers, Web page tampering and hijacked connections. Last year, 360 Web pages were changed, several of which resulted in embarrassing press reports. Some of the most notable include:

- On the CIA's home page in September 1996, the agency name was changed to Central Stupidity Agency and links were redirected to Playboy magazine's home page.
- In August 1996, the Department of Justice home page was altered to contain sexually explicit images and obscenities.
- For much of October 1997, the State Department limited access of American embassies to the computer network and sent couriers around the world to circulate sensitive information on paper. This action was taken after the GAO reported that two unauthorized users had been discovered at two embassies. The U.S. Government and contractors were obliged to devote considerable effort to flaws in the system, which links computers in Washington with 250 U.S. embassies and consulates.[33]
- A computer hacker tampered with the Air Force home page over a weekend in November 1997, forcing the Pentagon to

shut down most of its public access web sites, including the Army, Navy, Air Force and the Gulf War illness home pages. The hacker inserted the headline, "Welcome to the Truth".

- In 1997, a disaffected AT&T administrator employed a software program called "packet sniffers" on the company's internal local area network (LAN). The "sniffers" expose customer passwords and allow unauthorized access to customer information.[34]
- In 1997, a 16-year-old from Brockville, Ontario, swiped 1,300 user ID's and passwords from local Internet Service Provider (ISP) called RipNet and passed them out to four of his high school buddies.[35]
- In 1997, the new release, AOL4FREE.com was circulated with a "Trojan horse" clandestine program that erases user files.[36]
- An airport was disabled in 1997 when a teenaged hacker disabled communications to the air traffic control tower in Worcester Massachusetts. This unfortunate teen has become the first juvenile charged in federal court with illegal computer hacking.[37]

Commenting on still another hacker intrusion into Pentagon computers in February 1998, Deputy Secretary of Defense John Hamre said, " it was the most organized and systematic attack the Pentagon has seen to date". [38] Two juveniles are believed responsible for these recent attacks, however, they appear to have been the pawns for a more accomplished hacker who calls himself the "Analyzer". He is an Israeli citizen who befriended the two youths over the Internet. He essentially coached the youths from his home in Israel.

The statement by Mr. Hamre in conjunction with the knowledge of who was behind these attacks confirms the facts that hacker activity could be a cheap, easy and potentially lethal weapon if employed with destructive intent. Israeli Prime Minister Netanyahu, when asked about the teen-agers' infiltration of the Pentagon computers responded, "...damn good...and very dangerous" [39] The pause in his response indicates a high level awareness and recognition of the potential threat posed by skilled computer hackers in the "Information Age". In this case, the hackers were caught, however, the kind of information warfare attacks that should cause most concern are the ones that are not detected.[40]

According to a warning on the Defense Technical Information homepage, breaking into government computers violates the Computer Fraud and Abuse Act of 1986, and can result in administrative, disciplinary or criminal proceeding. This warning obviously has not discouraged hacker activity. Nor are most government networks particularly well protected by their operators. According to Pam Hess, editor of the Defense Information and Electronic Report, non-classified but secure military networks are commonly maintained and upgraded by low ranking personnel who, until recently, have rarely been held accountable for security breaches. This should be a cause for serious concern, because once root access is obtained, a hacker can deface or delete entire Web sites, or install destructive and near-invisible programs.[41] From a malicious hacker's point of view, artificial boundaries such as organizational ownership or national boundaries are meaningless.[42] The number of intrusions by hackers continues to increase, a trend likely to continue unless actions are undertaken to improve network security and develop a coherent National Information Strategy and supporting policies.

During a 1997 U. S. Government exercise, a special U.S. national security team secretly tested the vulnerability of the nation's computer systems using software found on the Internet. It succeeded beyond its planners' wildest dreams in illustrating the vulnerability of the nation's computer systems.[43] Among other "successes", government hackers gained control to a U.S. electric power grid system which could have been sabotaged to plunge much of the nation into darkness.[44] As a direct result of the exercise the Department of Defense plans to spend nearly $1 billion a year for the next several years to improve its classified and unclassified computer security.[45]

Contributing to the growing threat to the U.S. National Information Infrastructure (NII) security, are the following:

- Investigations by the victims of computer intrusions tend to be reactive and event driven. Given the recent escalation of sophisticated infrastructure attacks, the investigations alone will do little to halt the problem.
- The introduction of new technology at such a fast rate precludes effective threat assessment.
- The potential threat is not fully acknowledged by U.S. society. Everyone in the Information Age is a potential victim of breaches in computer security.
- Fear of publicity which could damage customer confidence, shared by both government and commercial organizations. It

tends to limit accurate reporting and therefore degrades formulation of effective countermeasures.[46]

INTERNET

The Internet generally is the medium used by individuals and by public and private organizations to gain access to computers. Ironically, its origin lies with the U.S. government, traceable to U.S. humiliation resulting from early Soviet success in the space race. Fear of a Soviet advantage resulted in increased Congressional funding for the Department of Defense's Advanced Research Projects Agency (ARPA). In 1963, ARPA devoted $5-$8 million to computer research for the development of information processing. This research led to the development of ARPAnet, the connection of several computers into a network. This network enabled various remote locations to obtain expensive and hard-to-access computer time, better utilizing the scarce computer resources. Under the leadership of Senator Edward Kennedy, legislation in the late 1960s ensured that ARPA (which was receiving Defense Department dollars) was truly working on defense projects. This facilitated a name change to Defense Advanced Research Projects Agency (DARPA). The obvious advantage of ARPAnet has carried through to what we commonly refer to today as the INTERNET.[47]

The World Wide Web or "WEB" was born in 1989, and Tim Berners-Lee is acknowledged as the father of the "WEB".[48] Berners-Lee has maintained a proprietary interest in his creation, and a concern for its refinement. In an interview with Kim Nash of COMPUTERWORLD in 1995, Berners-Lee identified critical improvements he hoped to see prior to the turn of the century. These desired improvements all could be used to form the foundation of a strategic vision for the future of the Web and include:

- Solid standards. These would include accepted protocols for embedding hypertext links inside electronic mail messages and the replication of databases behind Web applications. Such improvements would increase access to information without the delay of opening additional software.
- Invisible browsers. Rather than launch a separate application for looking at the Web, users would have browser-like functions in their PC software. According to Berners-Lee, "I say the browser should disappear"[49] This would enable the free flow of information between applications and the Web, giving users direct "seamless" access to the Web.

- User verification. The Web at present lacks a reliable means to verify and authenticate who created and sent a given document. According to Berners-Lee, "Encryption and other security methods must be built into Web utilities"[50]
- Intelligent agents. These are a means of helping users better understand the Web. "Agents" are chunks of code that can be programmed to perform routine tasks such as retrieving stock quotes or sports scores.

At the Seventh International World Wide Web Consortium (W3C) conference held in April 1998, Lee identified privacy as a top priority. When speaking on the subject of Web censorship through legislation, he argued that technology could make legislative control unnecessary: "...sometimes it's necessary to roll out technology so that we can make, on top of the Web, a society which we're proud of and which represents our values". [51] This vision would employ individual PC software to limit access but not change the existing wide access of Web users. Such changes exhibit a small example of strategic leadership in an attempt to provide a vision for the Web of the future.

In the early 1990s, the automobile age metaphor of the "Information Superhighway" was introduced. This was the point at which the U.S. government was being petitioned to fund some portion of this information infrastructure. Some state legislatures, many public interest groups and most small companies saw government sponsorship as a means of ensuring that the telecom giants would not dominate an entirely privatized network system. Presumably, the public sector could assure that no telecommunications monopolist would dominate the industry like the "railroad barons" of the 19th century.[52]

One model acceptable to the small actors was the interstate highway system, a public works project constructed in the name of national defense and General Motors, and powerfully overseen in the Senate by the father of Al Gore. (Ironically, the latter subsequently became the most vocal proponent of the "Information" Superhighway.)[53]

In April 1997, plans for INTERNET 2, the next generation Internet, were announced by Vice President Gore. These included $50 million of funding for the Defense Advance Research Projects Agency (DARPA). Its proponents hoped that this new Internet will be 100 to 1,000 times faster than the current network. Internet 2 will "...help guarantee U.S. leadership in a critical industry and build the infrastructure of the 21st century economy", Gore told a news conference.[54]

" I am fascinated by the World Wide Web [and] am much sobered by the fact that no one predicted its occurrence," said Bellcore luminary Robert Lucky in 1996. "It seems to me almost a case study in chaos theory. There was a time at Bell labs when the 'future' was 10 years out, now it's two weeks. One billion people will be on the Internet in 2000.[55]

Information technology, including business on the Internet, is growing twice as fast as the overall economy according to the Commerce Department. "Information technology is truly driving the U.S. economy -- more than previous estimates had revealed," said Rhett Dawson, president of the Information Technology Industry Council.[56]

According to an "Internet industry" analyst, the United States holds a one to three year lead over its closest competitors in the development and use of Internet technologies. People outside the U.S. accounted for 23 percent of all web users in 1995, and this is expected to reach 50 percent by the end of the decade. Asia currently accounts for 20 to 30 percent of all Internet software sales. About 25 percent of all new ".com" domain name registrations come from outside the U.S. [57] The growth of the Internet outside the conventional national borders of the U.S. provides a virtually unlimited cyberspace access to the country. Of course, the resulting vulnerabilities are by no means limited to the U.S. Canada is the most wired country in the world and Finland has twice as many Internet connected computers per 1,000 residents as the United States.

The potential impact of this growing "open border" environment should be examined from a strategic perspective. The vulnerabilities to U.S. infrastructure and security should be of sufficient concern to motivate development of a coherent National Information Strategy and supporting policies.

The rate of growth that the Internet is experiencing is significant and also very relevant to national security. "The Internet has the potential to become the United States' most active trading vehicle within a decade, creating millions of high-paying jobs".[58]

To ensure that the U.S. maintains its advantage in this technology with a sound vision and good public policies, its operation and impact must be thoroughly understood. A national information policy with respect to this very powerful international tool is critical to maintaining the current leadership position in the market, along with a leadership role in the design and formulation of international policy.

Information Policy could establish the ground rules for living in "cyberspace", protect the privacy of citizens and safeguard them from sophisticated fraud, and define the expected ethics in dealing with other peoples and countries when we meet them there.[66] This policy formulation would provide the strategic vision of where individual and corporate users should go, and the degree to which users can expect the protection of national and international law.

ISP (INTERNET SERVICE PROVIDER)

Internet service providers are the commercial enterprises which provide the Internet connection and host customer Web sites for most Internet users. One of the country's largest ISPs is America On-line (AOL). Most of the large ISPs claim that they are "security conscious". Such assertions are mainly lip service.[67] During an audit of a very large company that specializes in Internet services, two hackers were hired to investigate a network break-in. They found that the network lacked adequate protection. There were holes in the operating system's software, which allowed unauthorized users unlimited access to data. Users were able to enter unencrypted, establish connections, and gain control of machines for which the network administrator did not give them access.[68] This is more indicative of the security of the system than the pronouncements of its managers.

supporting policies. However, this concern is not widely shared by civilian policy makers.

A Commerce report issued in April 1998 recommended that government stay out the growing industry of electronic commerce, infering that government involvement would burden the industry with extensive regulation, taxation or censorship. According to the report, government instead should develop legal frameworks for business on the Internet. Rules should result from "private collective action, not government regulation".[61] The report found that:

- Traffic on the Internet doubles every 100 days.
- In 1994, a mere 3 million people were connected to the Internet. By the end of 1997, more than 100 million were using it.
- The Internet is growing faster than all other technologies that have preceded it. Radio existed for 38 years before it had 50 million listeners, and television took 13 years to reach that mark. The Internet crossed that line in just four years.
- Internet commerce among business will likely surpass $300 billion by 2002.
- Using credit cards, 10 million people in the United States and Canada had purchased something on the World Wide Web by the end of 1997, an increase from 4.7 million people six months earlier.
- Without information technology, inflation in 1997 would have been 3.1 percent, more than a full percentage point higher than the 2 percent it was.[62]

CIA Director George Tenet told CEOs at a recent computer security conference that " The government's never made a product that anybody thought was any damn good, it's your responsibility to create that kind of infrastructure.... U.S. industry has to get off its butt and get this done."[63] This is yet another example of a senior government official failing to recognize the strategic importance of a coherent national information strategy.

With the use of the Internet and countless web sites, information is exploding. " It's been estimated that there are more words published on the net in a week than in the United States in a year.[64] The value of this information is in question however. Nothing guarantees it is in fact true and factual. Anyone can say anything on the Internet in the current absence of controls for accountability or responsibility. Among other things, this leads to a proliferation of conspiracy theories, promulgation of philosophies of hate groups, and frauds of various kinds. All users must understand that it is incumbent upon them to validate the data found on the Internet and be party to the transformation of this data into information. Despite legitimate concerns to preserve 1st amendment rights, the potential for abuse is very great.

In the business world, information regarding clients and customers is increasingly integrated and accessed through the "inherently insecure Internet and the underlying telecommunications infrastructure".[65] A useful National Information Policy could establish the ground rules for living in "cyberspace", protect the privacy of citizens and safeguard them from sophisticated fraud, and define the expected ethics in dealing with other peoples and countries when we meet them there.[66] This policy formulation would provide the strategic vision of where individual and corporate users should go, and the degree to which users can expect the protection of national and international law.

ISP (INTERNET SERVICE PROVIDER)

Internet service providers are the commercial enterprises which provide the Internet connection and host customer Web sites for most Internet users. One of the country's largest ISPs is America On-line (AOL). Most of the large ISPs claim that they are "security conscious". Such assertions are mainly lip service.[67] During an audit of a very large company that specializes in Internet services, two hackers were hired to investigate a network break-in. They found that the network lacked adequate protection. There were holes in the operating system's software, which allowed unauthorized users unlimited access to data. Users were able to enter unencrypted, establish connections, and gain control of machines for which the network administrator did not give them access.[68] This is more indicative of the security of the system than the pronouncements of its managers.

When business is making the decision of whether to host it's own Web site or contract the service from an ISP, more than cost should be analyzed. The cost to "outsource" this function is $42,000, while the in-house solution cost $221,000, according to estimates by Forrester Research, in Cambridge, Mass.[69] The financial difference would make this decision easy if it were simply an economic decision. The decision to outsource, however, must include a risk assessment, which includes in its analysis the ability to provide security for the page, adaptation to change and control of the Web server. It is the page security, the ability to protect the integrity of the data, which must receive increased emphasis. If the storage and display of data is going to be provided by an ISP, then integrity and reliability of this data must be assured by the ISP. This is still another area which could benefit from a sound national information strategy.

INFRASTRUCTURE

When computer networks are examined with respect to their impact on infrastructure, some ominous implications emerge.

National "infrastructures" include such systems as telecommunications, the National Information Infrastructure (NII), transportation, emergency services, oil and gas, power generation and distribution, health care and financial services. These are critical to orderly functioning of a technologically sophisticated society.[70] National infrastructures are highly interdependent. Because of the size, complexity, physical and organizational distribution and rate of change, it is impractical to ever fully diagram or map the information component of an infrastructure. However, individually or collectively, these systems are vulnerable to information attack. Because they are so complex, they are very difficult to protect against such threats.[71]

POLICY ISSUES

A workshop on Information Warfare and Deterrence held at National Defense University in 1996 identified the following policy issues that warrant further exploration:

- What is (what constitutes) an information attack?
- When is an information attack an "act of war"?
- How is an information attack verified?
- How is an attacker identified and confirmed?
- Does system penetration equate to an attack?
- Can one define an IW version of "hostile intent"?

- Are there potential triggers in defining IW acts of war?
- How should the United States respond to IW attack?
- Who should respond for the United States? [72]

Deterring Information Warfare Attack

The U.S. can deter information attacks using those means and policies currently employed to deter other types of attack. As a sovereign state, the United States is entirely within its rights to respond to threats with all appropriate means, including law enforcement and military power.[73]

But the responsibility cannot rest with the government alone. Accountability and responsibility for information and information integrity is a responsibility that spans the entire computer network. "Individuals need to understand what ethical behavior means in this electronic and communication age and the consequences of unethical or illegal actions".[74] A national information policy is need to provide the strategic leadership and develop a vision for the future of cyberspace.

RECENT POLICY CHANGES

In March 1998, top defense officials announced the creation of an offensive information warfare (infowar) operation within top echelons of the Department of Defense which gives information warfare - both offensive and defensive - increased visibility and clout.[75] The proposed plan calls for a new Deputy Assistant

Secretary for Information Operations within the office of the Assistant Secretary of Defense for Command, Control, and Intelligence. It would set up two new directorates under the Deputy Assistant Secretary, one for information assurance/defensive information warfare and one for offensive operations.[76] "Defensive" capabilities under the new directorate are funded in FY99 to the tune of $3.6 billion. Jacques Gansler, DoD Undersecretary for Acquisition and Technology, expressed the new perspective when he told a joint Senate/House hearing that the United States can no longer be satisfied with reactive information assurance solutions."[77]

Barry Collins, senior research fellow at the Stanford-based Institute for Security and Intelligence, provided additional insight into evolving DOD concern for information warfare. He said tapping a single person to be responsible for information operations and offensive information warfare will tie together and formalize many disparate projects in the military and intelligence organizations.[78] "It shows the maturing nature of information operations as an offensive tool, which is new. It's going to be taken seriously. It says both the attention and dollars will be there."[79]

CONCLUSION

The key challenge for the nation's strategic leaders is to recognize the trends in technology and cyberspace. They now must create a vision which guides the country through the challenges posed by these trends. A logical result would be implementation of a coherent National Information Strategy and supporting policies, which can maintain the U.S. advantage in this area. The Administration should create a position to lead the country in the area of "Information Management", preferably at the cabinet level, responsible for the development of a National Information Strategy and supporting Policies.

Word Count: 5,881

[69] Paula Jacobs, "Outsourcing your Web site." Infoworld , 20 January 1997, 57.

[70] Ibid.,7.

[71] Ibid.,8.

[72] Hayes and Wheatley, 4-5.

[73] Ibid., 4-5.

[74] "Principles of an Information Security Framework ," 10 February 1998; available from <hhtp://gopher.harvard.edu/security-committee/handbook/chapterII.html> Internet; accessed on 10 February 1998. 2-5.

[75] Bob, Brewin and Heather, Harreld, "DOD Ads Attack Capability to Infowar." Federal Computer Week, March 1998.

[76] Ibid. , 1-2.

[77] Ibid.

[78] Ibid.

[79] Ibid.

[15] Martin C. Libicki. What is Information Warfare? (Center for Advanced Concepts and Technologies Institute for National Strategic Studies, National Defense University, August 1995), x.

[16] Ervin.

[17] Ibid., 5.

[18] Richard E. Hayes and Gary Wheatley, Information Warfare and Deterrence. (NDU Strategic Forum, Number 87, October 1996), 1.

[19] Ibid.

[20] Ibid.

[21] Ibid.

[22] Mark Slouka, War of the Worlds. (Basic Books, Harper Collins Publishers. 1995), 8.

[23] Antulio J. Echevarria II. Optimizing Chaos of the Nonlinear Battlefield.(Military Review Oct1997).

[24] Libicki, 36.

[25] Ibid.

[26] Timothy L. Thomas. The Mind Has No Firewall. (Parameters Spring 1998), 86.

[27] Ibid., 84.

[28] Deborah Radcliff, Is you ISP SECURE? (Infoworld, March 2, 1998), 97.

[29] Channel 4000 News, (http://www.wco.com/news/stories/news-980227-112124.html 3/3/98)

[30] Ann, Kellan. CEOs hear the unpleasant truth about computer security. (CNN.com, 6April 1998).

[31] Ibid.

[32] Ibid.

[33] Report: Hackers may have infiltrated State Department (hhttp://www.cnn.com/tech/9803/23/state.dept.computers.ap/ 3/23/98).

[34] Radcliff, 97.

[35] Ibid.

[36] Ibid.

[37] "Teen Hacker faces federal charges," available from <http://cnn.com/tech/computing/9803/18/>; Internet; accessed 18 March 1997.

[38] "Suspects in Pentagon Hacking," 27 February 1998; available from<hhttp:/www.wcco.com/news/stories/news-980227-112124.html>; accessed 6 March1998.

[39] Ibid.

[40] Bob, Brewin and Heather, Harreld. "DOD Adds Attack Capability to Infowar" Federal Computer Week, 2 March 1998.

[41] James Glave, "DOD-Crackdown Team Used Common Bug." available from <hhttp://www.wired.com/news/technology/story/10737.html> Internet; accessed 6 March 1998.

[42] Ibid., 9.

[43] "Security team finds Pentagon computers unsecure", available from <http://cnn.com.TECH/computing/9804/16/cyberwar.ap> Internet, accessed 16 April 1998.

[44] Ibid.

[45] Ibid.

[46] Ibid.,10.

[47] Adam C. Engst, The Internet Starter Kit (Hayden Books Indianapolis, IN). 37-46.

[48] Kim S. Nash."Father of Web asks for far-reaching standards," Computerworld, Dec. 1995, 12.

[49] Ibid.

[50] Ibid.

[51] Associated Press, "Web founder admits concern about Internet privacy", <http://cnn,com/TECH/computing/9804/15/,aust-internet.ap/index.html> ;Internet; accessed 15 March 1998.

[52] Ross, Andrew. "Dividing Our Time: The Other Side of the Net." NPQ ,winter 1997. 14-16.

[53] Ibid.

[54] "Gore pledges $50 million for next generation Internet," 14 April 1998; available from<(hhtp://cnn.com/TECH/computing/9804/14/internet2/indes.html> ; Internet; accesses 14 April 1998.

[55] Gary H. Anthes, "Predicting the future.", Computerworld , 3 June 1996, 70.

[56] "Government study finds blazing growth on Web," 15 April 1998; available from <http://cnn.com/TECH/9804/15/internet.commerce.ap>. Internet. Accessed on 15 April 1998.

[57] Angela Hickman. "It's a Wired World." PC Magizine,18 November,1997. 29.

[58] "The Clinton Administration's Framework for Global Electronic Commerce," Bisiness America, January 1998.

[59] Ibid.

[60] Ibid., 10.

[61] "Government study finds blazing growth on Web" 16 April 1998; available from <http://cnn.com/tech/computing/9804/15/internet.commerce.ap/; Internet; accessed 16 April 1998.

[62] Ibid.

[63] Ann Kellan., 3.

[64] Ibid., 42.

[65] <httpz://kea@aracnet.com > Internet. Accessed 12 January 1998. 3.

[66] Winn Schwartau, Information Warfare: Chaos on the Information Superhighway (Thunder's Mouth Press: New York,1994), 319.

[67] Deborah Radcliff, "Is you ISP SECURE?" Infoworld, 2 March 1998, 97.

[68] Ibid., 97.

[69] Paula Jacobs, "Outsourcing your Web site." Infoworld , 20 January 1997, 57.

[70] Ibid.,7.

[71] Ibid.,8.

[72] Hayes and Wheatley, 4-5.

[73] Ibid., 4-5.

[74] "Principles of an Information Security Framework ," 10 February 1998; available from <hhttp://gopher.harvard.edu/security-committee/handbook/chapterII.html> Internet; accessed on 10 February 1998. 2-5.

[75] Bob, Brewin and Heather, Harreld, "DOD Ads Attack Capability to Infowar." Federal Computer Week, March 1998.

[76] Ibid. , 1-2.

[77] Ibid.

[78] Ibid.

[79] Ibid.

BIBLIOGRAPHY

Anthes, Gary H. "Predicting the future." Computerworld, 3 June 1996, 70.

Alexander, Steve. "Training mind-set." Computer world Internet Careers, December 1997.

Associated Press. "Web founder admits concern about Internet privacy," 15 April 1998; available from<http://cnn.com/TECH/computing/9804/15/aust_internet.ap/index.html>. Internet. Accessed 15 April 1998.

Associated Press. "Government study finds blazing growth on Web," 15 April 1998; available from <http://cnn.com/TECH/computing/9804/15/internet.commerce.ap.>Internet. Accessed 15 April 1998.

Associated Press. "Security team finds Pentagon computers unsecured," 16 April 1998; available from <http://cnn.com/TECH/computing/9804/16/cyberwar.ap.>Internet. Accessed 16 April 1998.

Associated Press. "Millions of Web pages overwhelm search engines," 2 April 1998;<http://cnn.com/Tech/computing/9804/2/.>Internet. Accessed 2 April 1998.

Balderston, Jim. "Search-Engine vendors eye Intranets." Infoworld, July 1996, 41.

Basch, Reva. "Surfing and Searching." Fortune. January 1997, 151-154.

Brewin, Bob and Harreld, Heather. "DOD Adds Attack Capability to Infowar." Federal Computer Week, 2 March 1998.

Cohen, Warren. " Online malls move closer to home." U.S. News&World Report,
1 December 1997, 86.

Cohen, William S. "Report of the Quadrennial Defense Review." May 1997.

Chittum, Marc J. "Electronic Authentication Technologies." Business America, January 1998, 10.

Clinton, William J. A National Security Strategy for A New Century, The White House, May 1997.

DeSantis, Hugh. Beyond Progress, an interpretive Odyssey to the future. University of Chicago Press, Chicago, ILL, 1996.

Edwards, Karen. "Yahoo!'s Net of Partners." BRANDWEEK, February 10, 1997.36-37.

Engst, Adam C. Internet Starter Kit for Macintosh. Hayden Books, Indianapolis, IN, 1995, 38.

Goldberg, Ivan. "Institute for the Advanced Study of Information Warfare (IASIW)." 10 July 1996; available from <http://iasiw.com> Internet. Accessed 22 January 1998.

"Government study finds blazing growth on Web," 16 April 1998; available from<http//cnn.com/tech/computing/9804/15/internet.commerce.ap/>; Internet; accessed 16 April 1998.

Hayes, R. C. and G. Wheatley. " Information Warfare and Deterrence." Strategic Forum. NR87, October 1996.

Hickman, Angela. "It's a Wired World." PC Magazine. 18 November 1997, 29.

Hill, Eleen. " Intellectual Property Protection and Electronic Commerce." Business America. January 1998, 11.

"Information Warfare: A Two-Edged Sword." available from<http://www.rand.org/publications/rrr/rrr/fall95.cyber/info-war.html. Internet accessed 26 January 1998.

Jacobs, Paula. "Outsourcing your Web site." Infoworld. 20 January 1997, 57.

Kellan, Ann. "CEOs hear the unpleasant truth about computer security." 6 April 1998; available from<http://CNN.com/TECH/computing/9804/6/. Internet accessed 6 April 1998.

Kinsley, M. "In Defense of Matt Drudge." Time, 2 February 1998. 41.

Krantz, Michael. "Censor's Sensibility" Time, 11 August 1997, 48.

Libicki, M. C. "Information Dominance." Strategic Forum , NR132, November 1997.

Libicki, M. C. What is Information Warfare? Washington DC: National Defense University Press, 1995.

Marsh, Robert T. Critical Foundations - Protecting America's Infrastructure. The Report of the President's Commission on Critical Infrastructure Protection, Washington D.C., 13 October 1997.

Miles, Robert H. Leading Corporate Transformation. Jossey-Bass Publishers, San Francisco, CA. 1997.

Nash, Kim S. "Father of Web asks for far reaching standards." Computer World.
18 December 1995.

Notess, Greg R. "On The Nets." Database. June/July 1996, 86-88.

Odeen, Philip A. " Transforming Defense, National Security in the 21st Century." Report of the National Defense Panel December 1997.

O'Harrow, Robert Jr. " Are Data Firms Getting Too Personal?" Washington Post 3 March 1998; available from<http://washingtonpost.com/wp-srv/frompost/march98/privacy8.html>. Internet. Accessed 10 March 1998.

Petersen, J. L. The Road to 2015 Profiles of the Future. Waite Group Press, Corte Madera, CA. 1994.

Quitter, Joshua. " Invasion of Privacy." Time, 25 August 1997, 29-35

Quitter, Joshua. "Why AOL is still the Pits." Time, 22 September 1997, 60-62.

Radcliff, Deborah. "Is Your ISP Secure?" INFO WORLD. 2 March 1998, 97-100.

Richter, Betsy. "Digging up Research in the Data Mines." Workforce. March 1997, 80.

Ross, Andrew. "Dividing Our Time: The Other Side of the Net." NPQ . Winter 1997, 16.

Saxby, Stephen. The Age of Information. New York University Press, New York. 1990.

Staver, E. J. and Hilliard, R.S. "Information Warfare: OPFOR Doctrine - An Integrated Approach." September 1996; available from<http://call.army.mil/call/nftf/sepoct97/infowar.html>; Internet. Accessed 26 January1998.

Schwartua, Winn. Information Warfare : Chaos on the Information Superhighway . Thunder's Mouth Press, New York, 1994.

Schwartzstein, Stuart J.D. The Information Revolution and National Security, Dimensions and Directions. Washington , D.C.: The Center for Strategic and International Studies, 1996.

Shalikashvili, John M. Joint Vision 2010. Chairman of the Joint Chiefs of Staff, Washington , D.C. 1996.

Shalikashvili, John M. Information Warfare A Strategy for Peace...The Decisive Edge in War. Chairman of the Joint Chiefs of Staff, Washington, D.C. 1996.

Shalikashvili, John M. National Military Strategy. 29 September 1997; available from <http://www.dtic.mil/jcs/nms> Internet. Accessed 10 January 1997.

Slouka, Mark. War of the Worlds. BasicBooks a division of Harper Collins Publishing, 1995.

Stein, G.J. "Information Warfare." Available from <http://www.cdsar.af.mil/api/stern.html> Internet accessed 26 January 1998.

"The Clinton Administration's Framework for Global Electronic Commerce." Business America, January 1998, 5.

"The Federal Bureau of Investigation National Compute Crime Squad," 23 March 1998; available from<http://www.fbi.gov.programs/nccs/compcrim.html>Internet. accessed on 23 March 1998

Thomas, Timothy L. "The Mind has no Firewall." Parameters 1(Spring 1998): 84-92.

"Threat Assessment for Information Networks and Infrastructure," available from <http://www.aracnet.com/~kea/papers/threat_white_paper.shtml> Internet. accessed 26 Jan 1998.

U.S. Department of the Army. Leading and Managing In The Strategic Arena A Reference Text 1996-1997. U.S. Army War College, Carlisle Barracks. 19 July 1996.

U.S. Congress. House Committee Computer Security, Science Committee Technology Subcommittee, Rayburn House Office Building Washington, D.C. 2/11/97. videocassette ID 78781, tape 97-02-11-10-1

Widnall Shiela E. and Folgeman Ronald R. "Cornerstones of Information Warfare"

Wellbery, Barbara S. and Wolf, Claudia C. "Privacy in the Information Age." Business America, January 1998, 12 - 13.

Zorn, Peggy J. "Solving Searching Mysteries and False Drops." Online , May/June 1996, 28.