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.

STRATEGY RESEARCH PROJECT

THE NATIONAL SECURITY STRATEGY AND INFORMATION WARFARE

BY

COLONEL STEPHEN KLINEFELTER
United States Army

USAWC CLASS OF 1997
U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

The National Security Strategy and Information Warfare

by
COL Stephen Klinefelter
United States Army

COL Art Lyke, USA(Ret.)
Project Advisor

United States Army War College
Carlisle, Barracks, Pennsylvania 17013

ABSTRACT

AUTHOR: Stephen Klinefelter, (COL), USA

TITLE: Information Warfare And The National Security Strategy

FORMAT: Strategic Research Project

DATE: 7 April 1997 PAGES: 34 CLASSIFICATION: Unclassified

This paper examines how the National Security Strategy (NSS) and its new sub-component, the National Security Science and Technology Strategy (NSS&TS) address Information Warfare. The Executive Branch has put the Department of Defense (DoD) on the front lines of the national effort to define and build a National Information Infrastructure (NII). The Defense Information Infrastructure (DII) is described in its relationship to the NII. Two Information systems of the DoD are then examined. They are: Electronic Commerce/Electronic Data Interchange (EC/EDI) and the Defense Message System (DMS). They are described non-technically to press home three points. First, Information is a national strategic asset and that using it and protecting it should be national priorities. Second, the world and the United States are becoming extremely interconnected and interdependent during this Information Age. This represents a new dimension of warfare and national security across all levels of conflict and all locations of the battlespace. The NSS and the NSS&TS should explicitly recognize Information Warfare, probably under a different diplomatically acceptable name. Third, the Administration recognizes these trends and has accounted for them in the NSS even if not explicitly recognized.

TABLE OF CONTENTS

The National Military Strategy (NMS) concept embodied in "Win the Information War" should be an explicit National Security Strategy (NSS) objective.[1] "Information Dominance" should be accorded national visibility and it should be woven throughout our NSS as a strategic concept in support of every objective.[2] Further, Information should be explicitly viewed as a strategic asset.

This paper examines how the National Security Strategy (NSS) and its new sub-component, the National Security Science and Technology Strategy (NSS&TS) address Information Warfare. The Executive Branch has put the Department of Defense (DoD) on the front lines of the national effort to define and build a National Information Infrastructure (NII). The relationship of the Defense Information Infrastructure (DII) to the NII is described. Then two Information systems of the DoD are examined in that context. They are: Electronic Commerce/Electronic Data Interchange (EC/EDI), the Defense Information System Network (DISN) and the Defense Message System (DMS). They are described non-technically to press home three points. First, Information is a national strategic asset and that using it and protecting it should be national priorities. Second, the world and the United States are becoming extremely interconnected and interdependent during this Information Age. This represents a new dimension of warfare and national security across all levels of conflict and all locations of the battlespace. Therefore, the NSS and the NSS&TS should explicitly recognize Information Warfare, probably under a different diplomatically acceptable name. Finally, the Administration recognizes these trends and has accounted for them in NSS even if not explicitly recognized or in the full context of what Information is.

Information -- Warfare -- Dominance

Information with a capital "I" characterizes the following hierarchy that LTC Thomas Ward and Dennis Miner developed at the U. S. Army War College:[3]

WISDOM
SYNTHESIS ---------- COMMUNICATION
KNOWLEDGE
ANALYSIS ---------- COMMUNICATION
INFORMATION
COLLECTION ---------- COMMUNICATION
DATA

The center column represents layers or types of information. The left and right columns represent the information processes that transform information and make it useful. Note that communication is in between every layer and thus it is a key target to strike if you want to disrupt the process. Also, this author contends that the hierarchy is a two-way process and that data and communications represent the Global, National, or Defense Information Infrastructures.

Information warfare is more understandable considering this hierarchy. The side who exercises this hierarchy the best gains Information dominance, or wins the Information war. All aspects of the hierarchy must be protected but not necessarily isolated from the other side's processes. What one side controls will certainly be sought out (or attacked) by others to enhance their side's position or to weaken ours. This is more true today because of the following trends:

- The New World Order
- Computers Everywhere
- The Global Network
- Megabyte Money in a Financial Economy[4]

Information dominance is more than the side with the best intelligence, situational awareness or new command and control tools. Those are important government or military

security issues, but there are other types of Information that could be more important, affect more lives and directly challenge national interests. Here are three examples:

- The New York brokerage and trading houses alone pass $1.9 trillion over their computer networks every day. That's almost $800 trillion per year, which does not include Tokyo, London, Frankfurt, Hong Kong and other exchanges. The Federal Reserve System transfers $1 trillion every day over the Fed Wire.[5]

- France coordinates at the national level with the French commercial private sector to set national intelligence (Information) collection priorities in the economic, industrial, science and technology areas. This would be difficult to pull off in our country.[6]

- In another example, the Russians used to report to the Department of Commerce Technical Information Center to carry out shopping carts full of technical documents bought for $3.00 each under the Freedom of Information Act. While all unclassified, many of these technical reports originated from the Defense Technical Information Center and their compilation produced a windfall of data on industrial, defense and academic research budgets, priorities and capabilities.[7]

These examples help make the point that Information Dominance should be more than a military strategic concept and that Information should be considered a national strategic asset.

This puts the United States in a dilemma. One the one hand, it must be an open and accessible society as a modern moral democratic world class leader that wants to engage and enlarge its "connections" to the world. On the other hand, this very openness and position of strength can threaten the United States' security interests. This is particularly true at this time in the dawn of the Information Age. Where does current National Strategy stand at the beginning of the Information Age?

The National Security Strategy -- Engagement and Enlargement

President Clinton recognizes the threat of Information warfare and takes a non-isolationist stance early in the preface of the NSS by saying:

> "...the threat to our open and free society from the organized forces of terrorism, international crime and drug trafficking is greater as the technological revolution, which holds such promise, also empowers these destructive forces with novel means to challenge our security. These threats to our security have no respect for boundaries and it is clear that American security in the 21st Century will be determined by the success of our response to forces that operate within as well as beyond our borders."[8]

This had to be a brief statement by necessity, but we can assume that the Information revolution includes the technological revolution. He also recognizes that the revolution holds much promise. However, this is the only positive reference to technology in the entire preface. Rather, it highlights the threat by evil forces who will also take advantage of the Information revolution. It does not talk about developing the fruits of the Information revolution into a national strategic asset that would put Information warfare on a higher plain. Nonetheless, it is a remarkable statement because it carries the weight of his signature in the preface. However brief, he is the first president to recognize this technology and information revolution in an NSS.

The introduction expands the brevity of the preface with several ideas and issues. Information and technology are specifically tied together.

> "...the emergence of the information and technology age presents new challenges to U.S. strategy even as it offers extraordinary opportunities to build a better future. This technology revolution brings our world closer together as information, money and ideas move around the globe at record speed; but it also makes possible for the violence of terrorism, organized crime and drug trafficking to challenge the security of our borders and that of our citizens in new ways."
>
> "It is a world where clear distinctions between threats to our nation's security from beyond our borders and the challenges to our security from within our borders are being blurred; where the separation between international problems and domestic ones is evaporating; and where the line between domestic and foreign policy is eroding. ... We must therefore assess these forces for what they are, with our response based on the nature of their threat, not just where they occur."[9]

Money, information and ideas are linked to Information in the broader sense. Information is starting to take on the nature of a strategic asset indirectly. "The Global Network" and "The New World Order" and "Computers Everywhere" are clearly recognized here. The key point is that boundaries in this environment are difficult to define and that response to threats may have to follow different rules than ever used before.

There are several examples of people, organizations and countries taking advantage of this lack of understanding and blurring of borders. Remember the French and the Russians discussed earlier. Then there are all those young people who regularly make the news by breaking into important Information systems. That does not count the professional threats that the government would rarely publicly acknowledge. Other examples are the problems with the stealing of copyrighted information (by India and China), pornographics (from Europe) and propaganda (from everywhere) in a society that wants to be open but doesn't fully understand how to protect itself. Information can spread very fast and be easily manipulated in this new age.

The NSS objective, Enhancing our Security, covers several aspects of Information warfare. The threat of intrusions to our military and commercial Information systems is specifically recognized as a significant risk to national security. He goes on to state simply that it is being addressed.[10] Additionally, a significant portion of the NSS is devoted to "Strong Intelligence Capabilities."[11] Early warning, timely intelligence and the latest technologies are stressed. Then there is the following section that is critical of the intelligence community.

> "Intelligence producers must develop closer relationships with users of intelligence to make products more responsive to current consumer needs. This includes identifying emerging threats to modern information systems and supporting the development of protection strategies."[12]

It implies that the intelligence community has not been cooperating with the Defense Information Systems Agency and the National Security Agency who are charged with developing protection strategies within the DoD.

However, there is no doubt about the importance that the President places on leveraging the Information age by going back to the introduction where he announces the NSS&TS. It is the country's first comprehensive Presidential statement of national security science and technology priorities. The President states in the NSS that this new strategy component examined the role of science and technology in global stability and national security.

The National Security Science and Technology Strategy

This new national security strategy has four objectives.[13]

- Maintaining Military Advantage Through Science and Technology Investment
- Controlling Arms and Stemming the Proliferation of Weapons of Mass Destruction
- Meeting the Challenge of Global Threats
- Strengthening Economic Security

They flow directly from the NSS of Engagement and Enlargement and the President's commitment to leadership in global affairs. The first, third and fourth objectives specifically cite Information within each section as a way and means to the end. The second only does so indirectly in the sense of early warning systems and good intelligence.[14]

The National Science and Technology Council (NSTC) which the President chairs guided the preparation of the NSS&TS. The NSTC is a cabinet-level council charged with coordinating science, space, and technology policies throughout the Federal Government. An important objective of the NSTC is to establish clear national goals for federal science and technology

investments. The NSTC includes the Vice President, the Assistant to the President for Science and Technology, the Cabinet Secretaries and agency heads with responsibility for significant science and technology programs, and other key White House officials.[15]

There is less recognition in the President's opening statement and executive summary about open and free society, the technological revolution, or threats to our security. As they are, these items from the NSS only relate indirectly to the Information Revolution. The impression from the Presidential opening statement is that Information (with a capital "I") is only an enabler for more effective military power and a narrow range of other things. Information should have a much broader context than that. However, he will pick up on these themes later in the NSS&TS.

The body of the NSS&TS is organized around its four objectives. Lets examine in detail those objectives which the President ties to Information.

Maintaining Military Advantage Through Science and Technology Investment

Under the NSS&TS objective of "Maintaining Military Advantage through Science and Technology Investment," Information Warfare is more directly addressed in the broader context of Information. The following attributes are discussed:

- "Beyond the battlefield, the management of enormous amounts of data..."
- "...no enemy can disrupt the information systems on which we depend."
- "...preserve the information advantage over the adversary in all conflicts."
- "...need the means to positively distinguish friend from foe..."
- "Advances in information technologies contribute to a growing array of strategic capabilities..."[16]

These are seeds to grow into what is required for the NSS or the NSS&TS. Unfortunately, they are limited in scope by being tied only to the National Military Strategy. They might be rewritten to look something like this if they were elevated to a higher or broader status:

- We are tightly bound to the Global Information Infrastructure. We must leverage technology to manage data globally...
- We must maintain a robust secure National Information Infrastructure that cannot be disrupted or weakened by attack from within or from outside interests. Such strength will provide stability to the Global Information Infrastructure and advance our interests.
- Information in the broadest sense is a national strategic asset. It has economic, scientific and military value. Our super power status depends on our technological advantages and in protecting and using Information.

Later in the section, maintaining military strength, the intelligence community is again warned in the following manner:

> "In the coming years, as a result of the global technology explosion, the Intelligence Community faces both threats and opportunities--threats resulting from the worldwide proliferation of information processing and communications technologies, and opportunities resulting from the rapid advances in these and other technologies in the commercial marketplace. Now more than ever, well-planned S&T investments will position the Intelligence Community to provide timely, comprehensive, and detailed intelligence support to the U.S. warfighter."[17]

These comments could apply to any community if the reference to the Intelligence Community is deleted. As in the previous examples, this simple language should be elevated to the President's own words at the beginning of the strategy.

At the end of this section are the three reasons at the core of why the DoD is on the front lines of the national effort to define and build an (NII). They are:

- Defense Acquisition Reform, [18]
- Dual-Use Technologies
- and the Technology Reinvestment Project.

The defense policies and strategies in these sections have had an almost immediate impact. They were not designed to specifically address Information, but that is one area where they have had greatest impact. A technology friendly President, Vice President and Secretary of Defense (SECDEF) have enhanced their effect.[19]

One effect is that DoD has become more of a partner and leader in the national and even global forums for the development of standards when its interests are at stake. It was once left to the purview of the Departments of State and Commerce. The DoD would develop their own military specifications when commercial standards did not suit them.[20]

DoD took a slightly different approach with the Defense Message System. It adopted and helped support an already existing and promising international standard. The U.S. will be the first country to implement it on a large scale. It is an interesting case because it directly competes with a primitive defacto U.S. standard for email. Nonetheless, the message is the same; DoD should stop spending billions on unique standards and systems that cannot grow, change or keep up with modernizing commercial standards.[21]

As an outgrowth of this standardization drive, DoD is aggressively tying to eliminate already existing "stovepipe" systems with unique specifications. These legacy systems cost are expensive to maintain because no one else has such an information system. There are hundreds of these legacy systems within DoD. DoD is trying to let them expire gracefully and to replace them with systems that conform to open standards drawn from the best of the marketplace. This is particularly true of the Defense Message System. In addition, new big ticket systems now require review by the Joint Requirements Oversight Council (JROC) to ensure that modern standardization is achieved and that service unique systems are rare.

Dual-use technology policy reflects the recognition that our nation can no longer afford to maintain two distinct industrial bases. The goal is to move towards a cutting-edge national technology and industrial base that will serve military as well as commercial needs. Conversely,

the innovation and accomplishments that originate in defense programs and laboratories will move rapidly to the commercial sector. DMS is an example of dual-use technology.[22]

The Technology Reinvestment Project is closely related to dual-use technology initiatives but it is a specifically funded program administered by the Defense Advanced Research Projects Agency. It's oriented more on lowering the cost of modern technology by finding civilian uses for military technology, thus expanding the market. It is likewise about expanding the market of emerging technology in the civilian market place to defense and again bringing down the price.[23] The Global Positioning System (GPS) and night vision devices are excellent examples of this as is Defense Message System.[24]

The last aspect of Maintaining Military Strength with national science and technology strategy is the Advanced Concept Technology Demonstration (ACTD) program. ACTDs are acquisition programs designed to foster direct contact between operational forces, the commanders of unified commands (CINCs) and the technologists and to remove barriers between them. Representatives of the forces, including the Joint Staff, the JROC, and the CINCs, play a direct role in the management of ACTDs. ACTDs have four objectives:

- to understand the military utility of new technology before committing to acquisition,
- to develop corresponding concepts of operation and doctrine to make best use of new capabilities,
- to provide residual operational capability to operational forces, i.e. they can keep it and play with it,
- and finally, to facilitate a more inform acquisition decision.

ACTDs also seek new ways to integrate existing technologies to make platforms more effective in battle. ACTDs typically last two to four years, and the concepts are then given to one of the military services or a defense agency for formal acquisition.[25] Internet II, unmanned air

vehicles and the Bosnia Command and Control Augmentation Initiative are less formal examples of the ACTD concept, but they demonstrate how fast the latest technology can be applied to real world problems.[26]

Meeting the Challenge of Global Threats

The three strategy pillars that deal with the challenge of global threats are:

- Preventative diplomacy
- Promoting sustainable development
- Responding to global threats[27]

Information plays a critical role to all three of these and they are explicitly recognized under the first two in the NSS&TS.

Preventive Diplomacy emphasizes support for democracy, sustainable development, traditional diplomacy, and military strength to prevent conflicts from escalating into violence and to contain conflicts that do occur. Early warning systems and commitment to use warning information are noted as wise investments in national security.[28] Yet the entire strategy of engagement and enlargement from a position of strength with moral leadership is preventive diplomacy. Greater interaction with global Information, sharing knowledge and building strong infrastructure reduce tension and conflict.

The military already plays a role in preventive diplomacy by being ready, strong and willing to conduct a wide range of military operations. However, it is noteworthy that the Joint Staff is considering formation of a Joint Information Operations Staff as a new joint staff element on par with the J3 and separate from the J6. Offensive information operations are currently

performed under the purview of the J3. Prevention of conflict is one of their objectives besides defeating the enemy through effective information operations.

The NSS&TS states that the promotion and dissemination of knowledge are key to the promotion of sustainable development. The President sees a global community of scholars, united by a shared understanding of scientific methodology and responsibility, and linked by modern telecommunications networks as a positive force for promoting stability, democracy, and economic development. Hence, the Clinton Administration has made the development of a national and global information infrastructure national priorities. It is here that the President first explicitly identifies the importance of the Information Infrastructures in the physical sense and their relationship to the model for Information with a capital 'I'.[29]

> "The GII fosters a dialog between nations and ethnic groups and enables applications such as collaborative scientific research, distance learning, telemedicine, and electronic commerce. Electronic networking is transforming communications and the conduct of reset around the world. While this transformation is fastest in the industrialized world, it is taking place in the developing world as well.... The goal of the Administration's GII initiative is to foster the communication and cooperation that will be needed to spur the transformation of a thousand discrete networks in the developed and developing worlds into a connected, interoperable global information infrastructure."[30]

Except for distance learning, the leadership role of DoD in the other three will be examined as one of the "means" by which the President is achieving his national strategy.

This authors' experience is that many in DoD do not understand this larger role that DoD is playing in the national strategy. DoD has become a means to achieve national strategy in what some would consider a very non-military way. Many think that "Information Dominance" came about only as modern "way" for the National Military Strategy. However, the roots of "Winning the Information War" from the NMS go deeper than that and relate to more than just the military

objectives of the NSS. This is aptly demonstrated under the last objective of the NSS&TS and again later in the example of EC/EDI.

Strengthening Economic Security.

The Administration is pursuing a strategy with the following elements or policy priorities to equip American companies and workers to compete and win in the international economy:[31]

- Creating a climate that fosters private-sector innovation and commercialization.
- Supporting industry-led technology development partnerships.
- Facilitating the rapid deployment of civilian technologies.
- Building a 21st-century infrastructure.
- Maintaining strong support for basic science.
- Supporting education in science and technology.
- Leveraging dual-use technologies for commercial markets.
- Promoting international economic development and trade thought international collaboration.

It should be apparent that all of these are elements of Information strategy and policy. This last section spends a surprising amount of time on the fourth element, building a 21st-century infrastructure, and the importance of the GII and NII to the economic well being of the country. Therefore, the technologies that are building this infrastructure have strategic value. The Administration desires that all this will lead to universal, accessible and affordable applications to enhance U.S. economic and national security in the 21st-century.[32]

The NII includes the Internet, the public switched networks, cable, wireless, and satellite communications. It includes public and private networks. As these networks become more interconnected, individuals, organizations, and governments will use the NII to engage in multimedia communications, buy and sell goods electronically, share information holdings, and receive government services and benefits.[33] It's happening all around us already. Taxes can be

filed electronically. Money can be transferred electronically. Research is conducted over the Internet. Services can be bought over the Internet. There are many other examples.

Yet there are plenty of nay-sayers and technical challenges. A mistake is made with the argument that the country lacks an Information policy or an Information strategy because particular technical or policy challenges have not been solved perfectly yet. The most often cited reason for nay-saying is security. However, the NSS&TS explicitly recognizes those challenges by saying that...

> "...Information security is critical to the development and operation of a viable NII. One of the goals of *The National Information Infrastructure: Agenda for Action* is to insure information security and network reliability. Without confidence that information will go where and when it is supposed to go--and nowhere else--the NII will not be used to support health, education, commerce, public services, and advanced communications to the fullest extent. In the NII, elements of effective public security include assuring confidentiality--the assurance that information will be held in confidence with access limited to appropriate persons; integrity--the confidence that information will not be accidentally or maliciously altered or destroyed; reliability--the confidence that systems will perform consistently and at an acceptable level of quality; and availability--the assurance that information and communications services will be ready for use when expected. These are important building blocks of the NII strategy."[34]

The Administration has chosen to press on in the belief that these things will sort themselves out through better technology. A vision and a strategy are still necessary. In addition, the pressures of the global economy are tremendous and the United States wants to maintain it's leadership role and healthy economy.

Telecommunications is good example. It is currently a $33 billion market outside the United States. It is projected to double to $64 billion by 1998. The highest demand will be in the developing countries. The development of the GII will facilitate the sharing of information and creating a global Information market place. A GII could serve United States industry by opening

overseas markets, eliminating barriers caused by incompatible standards, and examining international and domestic regulations.[35]

The Defense Information Infrastructures (DII)

The DII is the totality of all DoD data, information, information systems, and telecommunications systems resources required for the support of DoD missions and functions. As currently defined, the DII is the DoD shared or interconnected system of computers and communications resources and includes data, applications, security, people, training and other support structures that satisfy DoD's local and worldwide Information needs. The DII connects mission support, command and control, intelligence computers and users through voice, data, imagery, video and multimedia services. It provides information processing and value added services to DoD subscribers which includes mobile or deployed extensions all over the world.[36] It's the largest and most extensive array of information services of its kind in the world belonging to one authority.[37]

The NII, a federal enterprise in concert with industry and state and local governments, will evolve into a national high-speed information processing and transfer network. The evolution of the NII includes national telecommunications policy to encourage growth of the information technology industry. The NII is proposed to bring universal, big-pipe, interactive, digital communications and services to every school, hospital, home, and work place. (Big pipe means large amounts of information that can travel fast.) The capabilities of each will eventually overlap. The DII could provide information services to selected non-DoD customers. For example, NII services could be extended globally through DII capabilities. Also, strategic cooperation between

organizations planning DII and NII will foster development of dual-use technologies, technology transfer, and defense technology conversion. This will reduce costs to the government of providing information services while increasing the ability to complete internationally in information technology.[38]

Because DoD has the largest information systems network of any kind belonging to one authority, the Administration has tasked it to jump start several programs. Examples are: long distance learning, telemedicine, real time collaborative planning, electronic commerce, Internet II and DMS.

The Defense Message System

The Defense Message System is the DoD's attempt to fix its archaic message transfer system, the Automatic Digital Network (AUTODIN), and a myriad of email systems that cannot talk to each other. It depends on some very new technologies and it is using some very different methods of acquisition. DMS is a bold move forward that carries some risk.

The Automatic Digital Network (AUTODIN) is the current official message transferring system within DoD and several other government agencies such as the State Department. Funding for it stops at the end of 1999. It is a fairly robust multi-level secure precedence-based system built on outdated technology and custom software that requires rigid adherence to formatting to make it work. Users find AUTODIN difficult to use because of its security requirements. Its infrastructure is heavily dependent on relatively large facilities with many people to run it. Addressing and directories are centrally coordinated and distributed. It is a text handling system only! General purpose electronic mail or email has mostly surpassed it for

administrative or general use. Email's characteristics are almost the exact opposite of AUTODIN.

In 1992, there were about 50 active email systems within the Pentagon and they mostly could not talk to each other.[39] DMS is an attempt to rid the DoD of "stovepipe" systems or unique systems and to unify all of DoD under one standard. An international set of standards was chosen, X.400 and X.500. These standards are far more capable that the informal defacto standard called SMTP. For example, all manners of attachments are allowed such as documents, graphics, video, sound, software, etc. You can locate a person's address while on-line anywhere in the world by name or organization or country or locations. Along with the international standards, DMS will come with multiple levels of security, writer to reader security and digital signatures. DMS is the first large scale implementation of the international standard in the world and NATO governments are watching the program with great interest.

The development and acquisition of DMS are unique. DMS is a major acquisition under the watch of the Joint Requirements Oversight Council (JROC). DISA is the program office. The Air Force is the lead military department for implementation. Lockeed/Martin is the prime contractor. These entities are responsible for the parts of the system that will make it work but that users will not see. Microsoft, Lotus and EXL are developing the user software that every user will see. The user software will look much like and work with their current office productivity software. They are doing this at no cost to the government and under no commitment to the acquisition contract. They could drop out at any time with no legal repercussions to themselves. Loral has no other vendor to go to if they do drop out of the partnership. However, the financial rewards will be great if it does catch on and spread outside

the DoD to the rest of government. These companies will be selling the software module embedded in the standard office productivity suite of each user and owner of a PC.

DMS was chosen as an example the acquisition reforms and administration policies discussed earlier. It represents the acquisition of the latest technology with some risks. It incorporates international commercial standards and eliminates stovepipe systems. It represents a unique partnership with industry and the search for dual-use technology and technology reinvestment opportunities. It will enlarge our contacts with our allies and engage them if it catches on successfully.

Electronic Commerce/Electronic Data Interchange[40]

EC/EDI is an example of an information systems initiative that decisively serves our National and Military interests and objectives. EC/EDI will electronically interconnect all the Federal Government and commercial sector as never before for processing small procurements. Fast inter-agency cooperation was accomplished because the impetus began at the national policy level. However, EC/EDI is not typically thought of as a subset of our NSS. This is as much a part of information warfare as building a better high tech command and control system.

EC/EDI started early during President Clinton's administration when he charged Vice President Gore to lead the National Performance Review. The review was about making government administration more efficient and stream lined and about reducing government. It was also about pursuing the long range goal of a paperless government by leveraging commercially available Information Age technology faster that the government was already doing. Individual agencies were pursuing their agendas in this area with mixed success and varying

standards. At about the same time, the government announced commercially consistent Federal and DoD standards for processing small procurement actions, $2,500 to $100,000, by electronic means.[41] This might have gone mostly unnoticed had it not been for the National Performance Review and the intense push afterwards to demonstrate success.

In 1994, DoD was charged to stand up the first demonstration of EC/EDI using the Small Procurement Transaction Set. DoD was also charged to set up the program for the entire Federal Government. There were two primary reasons for this action. First, the DoD had the most robust and extensive worldwide data network of any government agency, and second, the DoD had one of the largest small procurement budgets.

Here is how the system works. There are 26 electronic entry points called Value Added Networks (VANs) throughout the U.S. Any company can interface with these VANs electronically by dial-in modem or the INTERNET. Companies connect to the VANs to react to government requests for proposals, to provide bids and to accept contracts. All companies or trading partners must be registered in the Government Central Contractor Register. Foreign companies can also participate but they are limited access to one or two VANs.. The VANs are commercial entities and not government owned. The government deals only with the VANs and the VANs deal only with the trading partners. Transactions are received at the VANs from trading partners where they are processed for format and time-date stamped. DoD's 16 consolidated computing centers or megacenters then automatically pick up the transactions electronically through the existing government data network to which the VANs are also connected. Finally, all of DoD's posts, camps and stations interact normally with the megacenters where most of their general processing needs are met.[42]

The strategic importance of this kind of initiative should be obvious. The potential for growth is immediate. EC/EDI is processing 90 to 92 % of all the small procurement actions in DoD and some other government agencies. The system processes about 55,000 transactions on a normal day and up to 130,000 transactions per day near the end of the fiscal year. The State Department is about to become part of the system with all of its embassies. Work is on going to connect the rest of the Federal Government and to include other kinds of transactions such as finance, medical and larger procurements.

Again, this example was picked because it is not typically thought of as Information warfare or part of our national security strategy. Yet, it cuts across the entire Federal Government and the commercial sector. EC/EDI also addresses other published national strategic goals such as streamlining government and revamping the DoD procurement process. The point is that this system succeeded in the difficult inter-agency environment because of visibility in national strategic strategy. It is also a demonstration of technology reinvestment.

Conclusions

This National Security Strategy is the first to address the Information Age. The current NSS ties Information warfare to our national security and recognizes the global borderless nature of it. It also properly recognizes that there are Information Warfare opportunities that the United States must exploit. However, the NSS presents the Information warfare threat weakly. The threat is only characterized as intrusions through the networks to the NII. The NSS also fails to demonstrate a complete understanding of Information in a broad sense as a national strategic asset.

The National Security Science and Technology Strategy is a new strategy that was produced at about the same time as the NSS. Information is recognized as a national strategic asset in this strategy. The President sees Information as critical to the well being of the nation and to maintaining leadership in global affairs. Information further strengthens the Administration's strategy of Engagement and Enlargement.

There is no attempt in either strategy to coin an equivalent term for Information warfare or Information operations. The rest of the world would probably perceive any attempt to do so as threatening. However, the strategy components to deal with it are all there, particularly in the NSS&TS. An argument cannot be made that the country lacks an Information policy or an Information strategy because particular technical or policy challenges have not been solved perfectly yet. The President has recognized those challenges and apparently decided that technology will solve them. These challenges do not negate the need for a vision and a strategy.

ENDNOTES

[1] Office of the Chairman of the Joints Chiefs of Staff, National Military Strategy of the United States of America (Washington: U.S. Department of Defense, 1995), 15.

[2] "Information" is a capitalized word throughout this paper to high light its broader meaning which is explained later.

[3] Thomas E.Ward, LTC, USA, "Information Warfare: Is it Feasible? Desirable?" United States Army War College Strategic Research Project (Carlisle, PA, 1996). Although, the author borrowed this idea from this source, LTC Ward also cites parts of it to another source. He then modified it to it's present form.

[4] Winn Schwartau, Information Warfare: Chaos on the electronic Super-Highway (New York: Thunder Mouth Press, 1994), 64.

[5] Ibid.

[6] Office of the Chairman of the Joints Chiefs of Staff, National Military Strategy of the United States of America. The strategy objectives, "Win the Information War" and "Information Dominance," come from this document, the NMS. The words themselves are diplomatically difficult at the international level, but the concept is exactly what's needed in the NSS in some form.

[7] Paul M. Klinefelter, the author's father, worked for the Defense Technical Information Center (DTIC) for 40 years from 1951 to 1991 as a program director. DTIC originally existed in two parallel operations . One was run by the Navy out of the Library of Congress and the other was run by the Air Force out of Wright Paterson AFB. GEN Marshall, as Sec of Defense, brought all non-intelligence technical information services under the Deputy Director for Defense Research Development, Testing and Engineering. DTIC was never designed to be an intelligence center but it was an intelligence target and used by out own intelligence services.

[8] Office of the President of the United States, A National Security Strategy of Engagement and Enlargement (Washington: The White House, February 1996), i.

[9] Ibid., 1-2.

[10] Ibid., 13.

[11] Ibid., 23-25.

[12] Ibid., 25.

[13] Office of the President of the United States, National Security Science and Technology Strategy (Washington: The Committee for National Security of the National Science and Technology Council, undated), cover pages.

[14] Ibid. There is a slight disconnect with the NSS in that the NSS&TS quotes the President's three primary NSS objectives differently than the from the NSS itself. This could be because work on both was primarily done during the last three quarters of 1995 and that they came out at about the same time. If you read both

carefully, it even looks like the NSS&TS was ready before the NSS. However, in spirit and vision they seem fairly well in synch.

[15] Ibid. It is interesting to note that the President never mentions through out the document any sound bites form the many public vision statements concerning the "bridge to the future", the "information super highway" and a "paperless government." It could be that these are not viewed as national security issues. The author feels that they are connected.

[16] Ibid., 9. These are directly based on the National Military Strategy.

[17] Ibid., 15.

[18] Ibid., 19. In October 1993, President Clinton signed into law the Federal Acquisition Streamlining act of 1994, legislation that reformed Federal procurement. The act provides for three key statutory changes. (1) Made it easier for Federal Agencies to buy commercial components, products, and services. (2) Streamlined contracting procedures for small purchases. (3) Authorized DoD to undertake pilot test programs. Then in June 1994, the Secretary of Defense announced a reversal of the Pentagon's long-standing policy toward military specifications--"milspecs," the 31,000 specifications and standards that prescribe how military items are to be made and tested, down to the most minute detail. Secretary Perry instructed the services to use commercial (or performance-based) specifications and standards in lieu of milspecs "unless no practical alternative exists." Together these statutory and administrative reforms enable the Pentagon to take full advantage of the inventiveness and efficiency of today's dynamic commercial market.

[19] That's the author's assessment that the President, Vice President and SECDEF were technology friendly. The author bases his assessment of the SECDEF on his work at DISA in support of the SECDEF's personal communications requirements while he was traveling compared to other SECDEFs and DoD notables. In addition, he personally became involved in the go ahead to implement the Bosnia Command and Control Augmentation Initiative that required taking risk and committing $100M on a very short notice unfunded requirement. As for the Executive Branch, the President is well known for his "Bridge to the Future" vision and Vice President Gore has been cited as the impetus to build Internet II.

[20] The development of the ADA programming language is an good example, albeit not a very successful one yet. DoD led the entire effort to invent a standard computer programming language and got the academic community and commercial sector to help develop it. DoD was spending billions to support outdated software written in many different languages. ADA was an attempt to create a language that contained all the attributes of the best languages for the time and do what any language could do. That appealed to the academic community. The international community took an interest because the United States set the standard for all things in computing at the time. The commercial community took an interest because the cost of writing and maintaining software was starting to exponentially outstrip hardware. DoD had billions of dollars of lines of code that needed to be converted or maintained. However, it never gained acceptance outside of defense contractors and valuable lessons were learned.

[21] X.400 and X.500 are the new international electronic mail transfer and directory services conventions many organizations are trying to make overtake the Simple Mail Transfer Protocol (SMTP). SMTP is the email convention in widespread use today over the Internet. SMTP is simple which may partly explain its early widespread acceptance. There are other conventions in use. It is ironic that SMTP helped make email so accepted, because users now want more sophisticated services, particularly DoD.

ENDNOTES

[22] Office of the President of the United States, National Security Science and Technology Strategy, 20.

[23] Ibid., 22.

[24] Night vision goggles used to cost $5000-$7000 a pair in '80s. They were for many years sensitive items that only the military could get. They are now under $1000. Hunters, wildlife photographers and police buy them regularly. The other example, GPS, has become imbedded in commercial, international and military information systems. GPS is basically a global system of satellites maintained by the Air Force to provides timing signals that can help determine location in the air as well as on the ground. Cryptographic devices are required to access it's most accurate signals, but it has found very widespread application and acceptance in non-military applications. The commercial devices that can read the signals and interpret location can be easily connected to computers and information systems, and hence, their tremendous power is achieved beyond a person in the field pinpointing his location. The new car computers with maps depend on GPS. Transportation companies track ships, trucks, vans and shipments using it. As a result, a basic GPS device can be had by the average person for several hundred dollars. But perhaps, its most important feature is the least visible to the public. GPS is now a method of choice to provide correct time to telecommunications systems and many other things with atomic clocks. Many digital communications systems all over the world derive their synchronization from GPS. That makes GPS a global strategic target and not just a military one.

[25] Office of the President of the United States, National Security Science and Technology Strategy, 21.

[26] BC2A was a $100M project was pulled together after a Defense Science Board white paper in the summer of 1995. It was approved 5 months later by the SECDEF for implementation in 3 months. It was a joint DISA and DARPA led project that brought digital communications pipes to a navy command ship 8 times larger than previously possible. It introduced a heavy commitment to international satellite assets that performed flawlessly. Direct satellite broadcasts using commercial set-top-box technology were tired in an operation environment for the first time. Real-time unmanned aerial surveillance video was broadcast to an entire theater as well as back to the United States for the first time. The project facilitated the testing of telemedicine in an operation environment for the first time. There were other examples. The decision to execute this kind of project lined up perfectly with the NSS and NSS&TS. Thus, it was made quickly. The author was the lead project officer from DISA for the initiative. The other principle project officers were Col. Ed Mahen from DARPA and Gladys Reichlin from the DISA/DARPA Joint Program Office.

[27] Office of the President of the United States, National Security Science and Technology Strategy, 45.

[28] Ibid., 45.

[29] Ibid., 51.

[30] Ibid., 52.

[31] Ibid., 60.

[32] Ibid., 64

[33] Ibid.

[34] Ibid.

[35] Ibid., 69.

[36] DISA/JIEO, "DISN Architecture," Baseline Coordination Draft, 8 December 1993.

[37] This is based on the author's experience in the DISA Global Control Center at Hqs DISA in Washington, D.C.

[38] DISA, "Strategic Plan," Coordination Draft, FOUO, undated from 1994.

[39] The author was the chief of the DMS transition office in D3, Operations Directorate, at DISA. Its mission was twofold: (1) to develop and coordinate the shutdown plan for AUTODIN and (2) to transition DMS from Program to Operations.

[40] George Bettis, Lt. Col., USAF, Defense Information Systems Agency Program Manager for Electronic Commerce/Electronic Data Interchange, telephone interview by author, 13 October 1996. As a former member of DISA, The author is very familiar with EC/EDI and he worked some of its issues. However, Lt. Col. Bettis helped him with most of the background information on the subject. The program's implications and the program's association to the National Security Strategy and information policy are the author's work and do not represent the views of DISA or the EC/EDI Program Office.

[41] These standards are consistent with the American National Standards Institute (ANSI) X.12 standard.

[42] This sensitive but unclassified network is called NIPRNET, Non-classified Internet Router Protocol Network. It is separate from the INTERNET but connected to it at spots.

BIBLIOGRAPHY

Acquisition Working Group of the Interagency Management Council. "Post-Federal Telecommunications System-2000 (FTS-2000) Program Strategy." December 1994.

Bettis, George, Lt. Col., USAF, Defense Information Systems Agency Program Manager for Electronic Commerce/Electronic Data Interchange. Telephone interview by author, 13 October 1996.

Dibbell, Julian. "Keys to the Kingdom." Time Magazine, 11 November 1996.

DISA/JIEO. "DISN Architecture." Baseline Coordination Draft. 8 December 1993.

DISA/JIEO. "DISN Architecture, Addendum No. 1: DISN Deployed/Mobile Extension." Final Report. 3 February 1995.

DISA. "Strategic Plan." Coordination Draft. Undated from 1994.

The Joint Staff and National Defense University. Information Warfare: Legal, Regulatory, Policy and Organizational Consideration for Assurance. 2nd Edition, 4 July 1996.

Levy, Steven. "Trying to Find the Key." Newsweek, 14 October 1996.

Mahen, Edward, Col., USAF, Defense Advanced Research Projects Agency Program Manager for the Bosnia Command and Control Augmentation Initiative. Telephone interview by author, 14 October 1996.

Office of the Chairman of the Joints Chiefs of Staff. National Military Strategy of the United States of America. Washington: U.S. Department of Defense, 1995.

Office of the President of the United States. A National Security Strategy of Engagement and Enlargement. Washington: The White House, February 1996.

_____. National Security Science and Technology Strategy. Washington: The Committee for National Security of the National Science and Technology Council, undated. (It was probably printed in late 1995. However, it references and is based on the 1996 National Security Strategy.)

Stein, George. J., "Information Warfare." Air Power Journal, Spring, 1995.

Schwartau, Winn. Information Warfare: Chaos on the electronic Super-Highway. New York: Thunder Mouth Press, 1994.

BIBLIOGRAPHY

Szafranski, Richard, Col., USAF. "A Theory of Information Warfare: Preparing for 2020." Air Power Journal, Spring, 1995.

Whisenhunt, Robert H., LTC, USA. "Information Warfare and the Lack of a U.S. National Policy." United States Army War College Strategic Research Project, Carlisle, PA, 1996.

Ward, Thomas E., LTC, USA. "Information Warfare: Is it Feasible? Desirable?" United States Army War College Strategic Research Project, Carlisle, PA, 1996.