

EXPRESS LANES AND POTHOLES OF THE INFORMATION SUPERHIGHWAY: THE INTERNET AND THE OPERATIONAL PLANNER

**A MONOGRAPH
BY
Major Michael G. Koba
Field Artillery**



**School of Advanced Military Studies
United States Army Command and General Staff
College
Fort Leavenworth, Kansas**

SECOND TERM AY 96-97

Approved for Public Release Distribution is Unlimited

19971107 016

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

NSN 7540-01-280-5500

ABSTRACT

EXPRESS LANES AND POTHOLES OF THE INFORMATION SUPERHIGHWAY:
THE INTERNET AND THE OPERATIONAL PLANNER by MAJ Michael G. Koba.
USA, 53 pages.

This study investigates the Internet as a potential tool as well as a threat to the operational planner. The Internet is changing how information is stored, processed, transmitted and utilized. The Internet is affecting the way people and nations interact and conduct business. As a global network, the Internet transcends national borders and allows an expanded collective awareness of events, issues and concerns.

This monograph reviews the history and functions of the Internet, and reviews some of the many varied sources available to the operational planner through the Internet. The ease of access the Internet offers into the global information environment has a direct impact on the ability to suppress, censor, limit or otherwise control information. Some governmental reactions to and policies for the Internet are reviewed. The employment of the Internet by advocacy groups, social movements and transnational actors is also covered for a perspective on how the Internet is being employed.

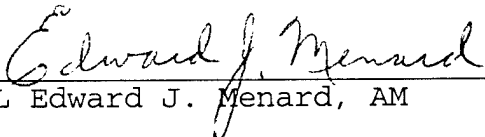
The study concludes that the Internet holds unique potential for the operational planner. The Internet may also pose dangers that operational planners need to be informed about. Operational planners should become familiar with the functions and capabilities of the Internet.

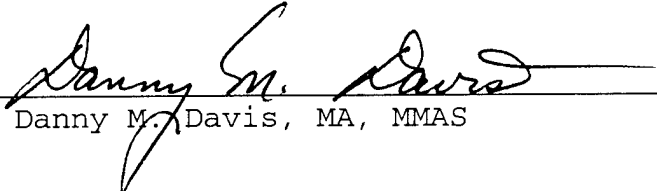
SCHOOL OF ADVANCED MILITARY STUDIES
MONOGRAPH APPROVAL

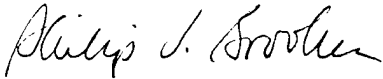
Major Michael G. Koba

Title of Monograph: *Express Lanes and Potholes of the
Information Superhighway: The Internet
and the Operational Planner*

Approved by:


COL Edward J. Menard, AM Monograph Director


COL Danny M. Davis, MA, MMAS Director, School of
Advanced Military
Studies


Philip J. Brookes, Ph.D. Director, Graduate
Degree Program

Accepted this 22d Day of May 1997

ABSTRACT

EXPRESS LANES AND POTHOLES OF THE INFORMATION SUPERHIGHWAY:
THE INTERNET AND THE OPERATIONAL PLANNER by MAJ Michael G. Koba,
USA, 53 pages.

This study investigates the Internet as a potential tool as well as a threat to the operational planner. The Internet is changing how information is stored, processed, transmitted and utilized. The Internet is affecting the way people and nations interact and conduct business. As a global network, the Internet transcends national borders and allows an expanded collective awareness of events, issues and concerns.

This monograph reviews the history and functions of the Internet, and reviews some of the many varied sources available to the operational planner through the Internet. The ease of access the Internet offers into the global information environment has a direct impact on the ability to suppress, censor, limit or otherwise control information. Some governmental reactions to and policies for the Internet are reviewed. The employment of the Internet by advocacy groups, social movements and transnational actors is also covered for a perspective on how the Internet is being employed.

The study concludes that the Internet holds unique potential for the operational planner. The Internet may also pose dangers that operational planners need to be informed about. Operational planners should become familiar with the functions and capabilities of the Internet.

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Major Michael G. Koba

Title of Monograph: Express Lanes and Potholes of the Information Superhighway: The Internet and the Operational Planner.

Approved by:

COL Edward J. Menard, AM Monograph Director

COL Danny M. Davis, MA, MMAS Director, School of Advanced
Military Studies

Philip J. Brookes, Ph.D. Director, Graduate
Degree Program

Accepted this _____ day of _____ 1997

TABLE OF CONTENTS

I. INTRODUCTION	1
II. THE INTERNET	3
- History of the Internet	4
- Functions of the Internet	7
- Sources for the Operational planner	12
- Governmental resources	15
- Department of Defense	17
III. GOVERNMENTAL REACTIONS AND POLICIES ON THE INTERNET	24
- United States	25
- Germany	26
- Singapore	27
- Indonesia	28
- China	29
- Gulf Co-operation Council	30
IV. USAGE OF THE INTERNET BY ADVOCACY GROUPS, SOCIAL MOVEMENTS AND TRANSNATIONAL ACTORS	32
- Serbia	32
- Mexico	35
- Peru	36
- Transnational actors	38
V. CONCLUSION	40
ENDNOTES	43
APPENDIX ONE: INTERNET CONNECTIVITY TABLE	46
BIBLIOGRAPHY	51

I. INTRODUCTION

The Joint Campaign should fully exploit the information differential, that is, the superior access to and ability to effectively employ information on the strategic, operational, and tactical situations which advanced U.S. technologies provide our forces.

Joint Pub 1

The Army, like the rest of the world, currently finds itself grappling with the issues of the coming Information Age. The Information Age is characterized by the rapid growth of information, information sources, and information dissemination capabilities supported by new technology. This is all having an impact on social, cultural, economic, and military patterns and operations. The information revolution is characterized by the decentralized, nonhierarchical flow of information.

Since 1990 the Army has seen its budget reduced approximately 40 percent and its manpower reduced by 450,000. Additionally, the Army has experienced a drastic increase in military operational tempo, with deployments increasing by 300 percent since 1990.¹ The fall of the Berlin Wall and the end of the Cold War fundamentally changed the way the United States Army approached its mission. The Army began its transition from a threat based force to a capability based force. This shift requires the Army to vigorously examine how it conducts operations today.

The combination of decreased resources and increased commitments clearly calls for the Army to be as flexible and innovative as possible. During this same period of

time, the Internet has developed into a truly worldwide communications means and information repository.

The ubiquitousness and speed of information transmission is having a serious impact on the conduct of military operations. Field Manual 100-6 *Information Operations* identifies information as a major influence on operations at the tactical, operational, and strategic levels.² In this environment of massive and rapid access to information, U.S. doctrine calls for the gaining of information dominance. Information dominance is the degree of information superiority that allows the possessor to use information systems and capabilities to achieve an operational advantage in a conflict, or to control the situation in operations other than war while denying those capabilities to the adversary.³

As one of the most visual and widely encountered manifestations of the Information Revolution, the Internet holds great potential as well as significant risk. The Internet is changing how information is stored, processed, transmitted, and utilized. The Internet is affecting the way people and nations interact and conduct business. As a global network, the Internet transcends national borders and allows an expanded collective awareness of events, issues and concerns.

The ease of access the Internet offers into the global information environment has a direct impact on the ability to suppress, censor, limit or otherwise control information. The Internet offers groups and individuals a powerful interactive communications tool that bypasses the controls placed on other mass media, yet retains its worldwide reach.

The purpose of this monograph is to assess the impact, if any, the Internet has on the operational planner. In Chapter II, I will first conduct a review of the Internet. This review will cover the establishment of the Internet, its development, functions and current state. This section will also review some of the different sources for the operational planner available on the Internet such as; search services, governmental resources, Department of Defense, professional journals, and news services. In Chapter III, the author will detail how different governments such as the United States, Germany, Singapore, Indonesia, and China are dealing with the Internet with an emphasis on policies and control measures. Chapter IV will explore how different advocacy groups, social movements and transnational actors are using the Internet to further their causes, generate income and create havoc. Chapter V will cover the author's conclusions.

II. THE INTERNET

The Internet is a global system of networked computers that allows users to operate, communicate, and exchange data files from one computer to any other on the network. Depending on the source, the Internet is accessible in over one hundred and fifty countries, with eleven thousand separate networks feeding into it containing up to 1.7 million host computers with estimates of up to 30 million users worldwide in 1996.⁴ It is estimated that 9 million adult Americans use the Internet daily.⁵ When you consider that many of the estimated 120-150 million personal computers in use

worldwide are capable of connecting to the Internet, the possibilities for growth and expansion are staggering. Whatever the numbers are, it is indisputable that the Internet is being used on a massive scale worldwide and continues to grow everyday. The Internet's dramatic growth is illustrated by the number of networks connected to it. In 1985, the Internet consisted of approximately one hundred networks. By 1989, the number of networks had risen to five hundred, by January of 1990 it had risen to 2,218, and by June of 1991 it was close to four thousand.⁶ There is almost no country in the world today that does not have access to the Internet. See Appendix One: Global Internet Connectivity Table for a complete list of countries and their status for Internet connectivity.

History of the Internet

The Internet originates from the Advanced Research Projects Agency (ARPA). J.C.R. Licklider first proposed the concept of networking, where everyone could quickly access data and programs at any site in the network in August 1962. As the first head of the computer research program at ARPA, he was able to convince others of the importance of this networking concept. In 1966, Lawrence G. Roberts went to ARPA to develop the computer network concept and published his plan for the "ARPANET" in 1967.

In 1968 after Roberts and ARPA funded contractors had refined the specifications for the ARPANET, ARPA released a request for the development of packet switches called Interface Message Processors (IMPs). The contract for the development of

IMPs was won by Bolt Beranek and Newman (BBN). In September 1969, BBN installed the first IMP at UCLA; this was followed by IMPs at Stanford, UC Santa Barbara and University of Utah. By the end of 1969, ARPA and BBN had four host computers connected to the ARPANET.⁷

The ARPANET was first demonstrated to the public at the International Computer Communication Conference in October 1972. It was also in 1972 that Ray Tomlinson of BBN wrote the first software for send and read electronic mail (email) as a means to ease coordination for people on the ARPANET.⁸ By 1983, ARPANET had grown to include a large number of defense research and development and operational organizations. It was at this time that it split into a MILNET supporting operational requirements and an ARPANET supporting research needs. Throughout the 1970's and early 1980's the utility of computer networking was beginning to take hold. During the 1970's and early 1980's most networks were designed for and restricted to closed communities of scholars and researchers.

In 1985, the US National Science Foundation (NSF) created the NSFNET to connect supercomputer sites around the US and research sites and schools that were around the supercomputers. As part of the NSF policy, schools were to make the Internet connection available to all qualified users on campus. From 1986 to 1995 the NSFNET backbone had grown from six nodes with 56 kbps (thousand characters per second) links to twenty-one nodes with multiple 45Mbps (million characters per second) links. It had expanded to over 50,000 networks on all seven continents and outer space, with approximately 29,000 networks in the US.

In 1991, the US Government passed legislation to rename NSFNET the National Research and Education Network (NREN) and to allow business to purchase part of the network for commercial purposes. This legislation has had a great impact on the commercialization of the Internet today.⁹

The world wide web (www or web) is one of the fastest growing areas of the Internet. The web brings hypertext and multimedia functionality to the Internet. Hypertext (links) allows the linking of material on the web in ways not previously possible on the Internet. Hypertext is usually displayed in a different color from the rest of the text and underlined. When clicked on, hypertext sends the viewer to a different set of information within that web page or even to a different web site entirely, for more detailed information on that subject. Hypertext is not limited to text only; the link may be to a multimedia site that includes audio or video material.

All sites on the Internet have a unique address, these addresses are known as uniform resource locators (URLs). URLs are an outgrowth of the Domain Name System (DNS), which is a method of administering names by giving different groups responsibility for subsets of names. Each level in the DNS is called a domain, and the subsections of the domain are separated by periods: for example *www.state.gov* the world wide web site for the State Department, part of the government domain or *www.army.mil* the world wide web site for the Army Homepage, part of the military domain. As you read these addresses from left to right through a name, the domains become larger. When the system was instituted, it possessed six “top-level” domains (see table 1). Because of the explosive growth of the Internet the decision was made

in February of 1997 to add several additional “top-level” domains to the DNS (see table 2). For sites outside of the United States a country extension is usually included in the URL. Most of the country extensions are easy to figure out, such as “us” for the United States, “fr” for France, and “mx” for Mexico. For a complete list of country extensions see Appendix One: Global Internet Connectivity Table.

Table 1 Original Top Level Domains

<u>DOMAIN</u>	<u>USAGE</u>
edu	Educational organizations
gov	Governmental organizations, non-military
mil	Military
org	Other organizations
com	Commercial organizations
net	Network resources

Table 2. Expanded Top Level Domains

<u>DOMAIN</u>	<u>USAGE</u>
firm	Firms and businesses
store	Business offering goods for purchase
web	www related entities
arts	Cultural/entertainment
rec	Recreation/entertainment
info	Information service providers
nom	Individual or personal nomenclature

Functions of the Internet

The Internet contains a number of functions that can be of use to the operational planner. These functions include File Transfer Protocol (FTP), Telnet a protocol

that allows remote logon to computers on the Internet. Electronic mail (email), Internet Relay Chat (IRC) real time chat rooms, Bulletin Board Systems (BBSs), and USENET newsgroups and lists.

FTP is a method for transferring files on the Internet and a type of Internet site. FTP allows a user to access a remote site, usually a server, to view all available files, and copy or download them to the user's computer. This function allows the rapid and easy transfer of information from computer to computer. It can be used to pass large databases, graphic files, or any other type of file. FTP sites are identified by the prefix *ftp* on the Internet. This is a very useful protocol for retrieving files from public archives from all around the Internet. Some useful FTP sites include the General Accounting Office(GAO) Reports Archive (*ftp cu.nih.gov*) that includes all the full text reports from the US GAO. SIMTEL20 (*ftp wsmr-simtel20.army.mil*), owned and operated by the US Army at White Sands Missile Range, contains a tremendous amount of public domain and shareware software for a variety of computers and operating systems.

Telnet is a function that allows a user to log on to remote computers to manipulate them and retrieve data. Additionally, it can be used to access a user's own account from a remote site. Telnet can be used to access many different types of public services available on the Internet, including library catalogs, both foreign and domestic, government libraries and publicly accessible databases.

Electronic mail (email) lets you send and receive messages electronically. Many consider email the core Internet application and it is certainly one of the most

commonly used functions of the Internet. Email allows you to communicate with people all over the world nearly simultaneously. But like all things, email has strengths as well as weaknesses and if email is to be used to its fullest potential these must be understood. One of the biggest advantages that email has is its speed of delivery. A user can send a message to any one in the world who has an email address and they will get the message in a matter of minutes to hours.

Users must be aware though, that there are two components of delivery time for any email message: the time it takes for the message to be delivered by the network to the user's computer and the time it takes the user to read it once it arrives. Another advantage to email is that it allows asynchronous communications. With email, the communications processes do not have to occur simultaneously. A user can compose messages, send and receive messages, and read them at his convenience. Email will hold messages in an inbox until the user is ready to read them. This function is important if one is communicating over long distances or with someone who has a different schedule or when you are just trying to manage your time more effectively.¹⁰

The conference aspect of email can also be very useful. Email allows a user to set up groups that he can communicate with very quickly, and any member of the group can communicate with the whole group or any part of the group at any time. This ability allows for the quick dissemination of information and the ability to query a large group quickly. Additionally, email allows a user the ability to capture all message traffic for accountability purposes. A factor that mitigates this capability

is that the sender's identity can be falsified. This points to email's biggest weakness, security.

The security of email is considered to be low. Since email takes a fairly predictable route through computers, it is susceptible to interception.¹¹

Additionally, system administrators or others who have attained root access to a system can gain access to all of a system's email traffic. Some email programs on the market today offer "Privacy enhanced mailers" that encrypt the message to overcome these security problems. For a secure email system to be effective, everyone the user communicates with must use the system. The bottom line is that email security at this time cannot be assured, so if security is required, a user will need to use some other form of communication.

Internet Relay Chat is another means of communication available on the Internet. IRC allows real-time multiple party conferencing between users. IRC offers a great way to communicate simultaneously to large groups of people in geographically dispersed locations. This system allows interpersonal communication worldwide on a massive scale. IRC is a good way to solicit immediate feedback, and has great potential for the conduct of on-line briefings.

Bulletin Board Systems (BBS) are computer-based announcement systems that can be connected with through the Internet or over a phoneline. BBS's are usually available 24 hours a day, and allow users to read, reply to, and originate messages, and also to exchange files including text, programs and graphics. BBS's generally adhere to a specific theme: there are approximately fifty thousand BBS's on various

topics available in the United States and the number continues to grow rapidly.¹²

Anyone with a personal computer, a phoneline, and the appropriate software can establish a BBS. Unlike IRC, BBS allow asynchronous communications, making them very useful to users on different schedules.

USENET is a network of newsgroups organized around a broad hierarchical structure. USENET comprises more than 9,000 different newsgroups, with upwards of 100 million characters being added everyday.¹³ Newsgroups are discussion groups focused around a particular topic. Some of the categories of USENET newsgroups available that are of interest to operational planners include *soc*, *talk* and *news*. Social issues and world cultures are the subject of the discussion in the *soc* category. The *soc* category is very useful in keeping up with the news from a particular country or region. The *talk* category focuses on political issues, and is a good way to get an awareness for grassroot feelings on current political issues. The *news* category concentrates on the Internet itself. It is in the news area that a user will find announcements on new newsgroups, and listings of frequently asked questions (FAQs). Most larger sites on the Internet have FAQ sites that cover the most frequently asked questions about those sites. FAQs are a good place to start if the user is unfamiliar with the area he is looking into as this will save the user a lot of time and aggravation. For listings of active USENET newsgroups go to *news.groups*, *news.lists*, or *news.announce.newgroups*. Newsgroups offer an extremely varied fare of material, ranging from excellent to mundane and from brilliant to obscene.

Sources for the Operational planner:

Search services

As the Internet continues to grow everyday, finding useful information quickly seems to get harder and harder. One of the best ways to overcome this glut of information, and obtain what is really wanted and needed is through the use of a search engine or Internet directory tool. Search engines and directory tools allow a user to find what he needs quickly. Search engines sort through large amounts of information quickly to help users locate just what they are looking for. Unfortunately, they also can provide large volumes of useless information.

The key to using any search engine is the input that the search is started with. The major search services do have some unique features, but there are some generic tips that are useful on any of the search sites. It is important to determine precisely what is wanted. Many people start their searches with single words, all this does is return long lists of sites which may be entirely useless. The more specific a search query is, the more useful the returned sites will be to the searcher. Do not be afraid to use natural language as part of the query, most search engines are designed to use the idiosyncrasies of natural language. Another area to watch is the spelling of the query. If unsure of the exact spelling of a word or phrase, try different combinations and let the search engine find which ones return the most responses. Another

variation on this is the use of synonyms in your query. Also consider use of capitalization in your queries, for best results proper nouns should be capitalized.

A technique to refine a search is through the use of the plus (+) or minus (-) keys. The use of the plus sign indicates that only sites that include that word following the plus sign will be returned with the search results. The use of the minus sign will ensure that that word following the minus sign will not appear in any of the sites returned for that search. If the object of the search is to locate a phrase or specific quote, the query should enclose the phrase or quote within “double quotation marks” the resulting return will include instances of that exact phrase or quote. Queries can contain combinations of the above limitors. AltaVista is a particularly good site to use when using advanced search like those mentioned above, due to its size and speed.

When getting started on a search a user needs to determine what type of query to employ. The decision to use a search engine such as AltaVista (www.altavista.digital.com), Lycos (www.lycos.com) or Infoseek (www.infoseek.com); or to use a web directory, such as Yahoo! (www.yahoo.com), Excite (www.excite.com) or Magellan (www.mckinley.com), depends on what the object of the search is. If the object is something specific, such as a particular page or the answer to a specific question, the searcher should start with a search engine that offers a comprehensive index of the web. If the object is to develop generic information about a topic, the searcher should use a web directory. The index searchers offer a wider view of the web, with tens of millions of pages included in

their indexes. While the directories are smaller, they offer more of a selective search. Most search services search the web as a default value. But most services also offer the capability to search areas beyond the web. These additional areas include Usenet newsgroups, email addresses, newswire feeds, and other varied sources depending on the search service being used. A particularly good site for expanded searches is Excite, it contains 50 million full text URLs and contains a pull down menu that allows the user to specify his search to the web, Excite reviews, Usenet, or Usenet classifieds.

The web directory Yahoo! is good for searching for categories and concepts as opposed to specific sites. Yahoo! has an extensive directory of topics including many military and political ones. Of particular interest to the operational planner are Yahoo!'s regional directories. These regional directories contain information on specific geographic areas, and includes links to sites within those areas.

Because search engines are currently a very competitive business, they are continuously adding new features. A good way to stay abreast of these new features is through a site on *The Net* (a magazine about the Internet www.thenet-usa.com) web site called search central. Search central contains links to all major search engines, the latest news about, and features from these search sites. When using search engines to locate information, it is recommended that a combination of searches using different services be used since even the best search engines only cover about 20% of what is available on the Internet.¹⁴

Governmental resources

Governmental sites contain an expansive amount of information for the operational planner. The Government Information Exchange (GIX) (www.info.gov) and FedWorld (www.fedworld.gov) are extensive sites that serve as overviews of the Federal government on-line. The GIX site connects the user to the Federal directory and Yellow pages; this site also has links to a number of Intergovernmental Collaboration sites. FedWorld is a comprehensive site that is accessible as a web page or through Telnet or FTP. For general information services FedWorld offers over 14,000 files via FTP, and access to 50 governmental agencies and 100 other government information systems through Telnet. It maintains searchable lists of web servers, ftp, gopher, and Telnet sites organized by National Technical Information Service subject categories.

FedWorld also hosts a number of very useful web sites including the National Technical Information Service (NTIS)(www.ntis.gov), Foreign Broadcast Information Service (FBIS) Glossaries(www.fedworld.gov/fbis) and World News Connection (wnc.fedworld.gov/). The NTIS contains scientific, technical, and business related titles, reports, databases, and software. The FBIS contains foreign language broadcast glossaries on specialized subjects from the FBIS. The World News Connection allows the user to locate time sensitive news from thousands of non-US media sources.

The Department of State (www.state.gov) maintains a particularly useful site for planners. Through State's site, it is possible to access U.S. Foreign policy for countries all around the world. This policy information can be accessed by region, country and issue. Recent articles available included the State Department's report to Congress on the enlargement of NATO, U.S. Policy on Bosnia and the status of the Middle East Peace Process. The State Department also maintains a Gopher site covering all of its previous press briefings. This site also provides foreign policy statements, reports, speeches and news. A list of treaties and other International agreements is available at (www.acda.gov.state).

The State Department's Overseas Security Advisory Council (travel.state.gov/osac.html) maintains a site that covers international security incidents, general crime, terrorist group profiles, and alert messages. These group profiles for terrorist groups are some of the best, and the most current open source information to found anywhere. The State Department also maintains a set of country background notes which include information on the geography, people, government, economy, defense, military issues and U.S. policy towards the country. Also included in these background notes are some very helpful historical and cultural highlights for the country.

The Government Printing Office(GPO) Access (www.access.gpo.gov/su_docs/aces/aces001.html) is a superb site to obtain Congressional reports, the Federal register, GAO reports, and anything else that the Government has printed. Though seemingly unwieldy, this site has an excellent set

of specialized search pages that greatly assist the user in locating exactly what they want.

The CIA is another Federal Government agency that maintains a presence on the Internet. Though rather shallow as a whole, the CIA site (www.odci.gov/cia) does offer an excellent set of publications(www.odci.gov/cia/publications/pubs.html).

Some publications that this site offers include: The World Fact Book 1996, CIA maps and publications, and Chiefs of State and Cabinet members of Foreign Governments.

The most useful CIA site is the World Fact Book

(www.odci.gov/cia/publications/nsolo/wfb-all.htm). The World Fact Book contains valuable information on countries worldwide. This is a great baseline source for up to date geographic, demographic, economic, political and military information about countries. A valuable source for the operational planner is the World Fact Book's entries on each country's transportation and communications infrastructure, as this information is not always readily available elsewhere.

Department of Defense

Department of Defense (DOD) sites are well represented on the Internet as is evidenced by the military being assigned one of the original top level domains (.mil).

The starting point for any DOD research is DefenseLink

(www.dtic.dia.mil/defenselink). DefenseLink has links to sites maintained by the Secretary of Defense, Joint Chiefs of Staff, the armed services and related defense organizations. One of the best links it provides is to all of the Unified Commands.

Though some of the Unified Commands links are only short PAO information pieces (Southcom, STRATCOM) others contain valuable information.

The best of the Unified Commands and the site that should be the role model for the others to emulate is United States European Command EUCOM (*199.56.154.3/*). The EUCOM site has all of the background data and fact sheets about the command but also allows access to many EUCOM publications including pamphlets, supplements, Directives, staff memorandums and policy letters. The DefenseLink site also offers current news, publications and a search capability. One of the best features of the EUCOM site is their Africa Homepage. The EUCOM Africa Homepage is an excellent source for information on all aspects of Africa and contains numerous links to alternate sources of information. This site serves as an excellent example of what is possible with the Internet. Another worthwhile Unified Command resource is the United States Atlantic Command ACOM (*www.acom.mil*) site.

DefenseLink includes links to BosniaLink (*www.dtic.mil bosnia index.html*), a site dedicated to covering all aspects of the U.S. involvement in Bosnia, and GulfLink (*www.dtic.mil gulfinfo*), a site covering Gulf War illness issues.

The primary site for the Army is The Army Homepage (*www.army.mil*). This is a good site for basic information and current news about the Army. This site is searchable using three types of criteria (date, organization, and key term). The value to this site lies in the number of links that it maintains; as of 21 April 1997 it

contained 726 active links to other Army related sites and is growing by approximately one additional site a day.

A very useful site is the Corps and Division Doctrine(CDD) Directorate (www.cgsc.army.mil/cgsc/cdd/cdd.htm), CDD is responsible for developing, writing and updating Army doctrine at the corps and division level and is responsible for over 50 Army doctrinal publications. This site maintains a library of all approved and draft manuals, white papers and doctrine notes that CDD is the lead agency for. From this site it is also possible to check on the status of any of CDD's publications.

The best source for Army related publications is the Army Training Digital Library (ATDL) (www.atsc-army.org/atdls.html) maintained by the Army Training Support Center. This site has on-line access to over 400 Field Manuals, 270 Mission Training Plans, 260 Graphical Training Aids, 40 Training Circulars, and a link to over 40 Joint Publications.

Other Army related sites for the operational planner include the Center for Army Lessons Learned CALL (call.army.mil:1100/call.html) and The Foreign Military Studies Office FMSO (leav-www.army.mil/fmsol/). CALL maintains operational and training lessons learned, tactics, techniques, procedures and research materials for most contingency operations since Vietnam including Domestic Support operations and Operations Other Than War (OOTW). The CALL site does require registration to obtain a password to access their filerooms where their information is stored. The extra effort required to access this site is well worth it, due to the depth and breadth of information available. CALL also has extensive lessons learned and trends from

all of the Combat Training Centers and the Battle Command Training Program. The Air Force also has an excellent lessons learned site which is maintained by Air Combat Command (ACC) at (*redwood.do.langley.af.mil*). This site has restricted access, the list of lessons learned by topic and exercise are available through the Internet, but to reach the complete text of the lessons learned requires access through the Secure Internet Protocol Router Network (SIPERNET).

FMSO gives the user access to regional military and security issues obtained through open-source media and direct contact with foreign military and security personnel. FMSO maintains a large list of publications, book reviews and research links. Both the CALL and FMSO site have good search engines that allow excellent access to their databases.

A link from the EUCOM page will take you to the Marshall Center (*www.marshalladsn.int marshall.html*). This is EUCOM's George C. Marshall Center for Security Studies, and like the EUCOM site it is an excellent resource. This site offers on-line access to many of its publications, documents and conference reports dealing with European security issues. Another very useful feature at this site is a listing of staff and faculty of their Research and Conference Center, and the College of Strategic Studies and Defense Economics that is linked to email for ease in contacting these personnel.

At the Joint level, the Joint Electronic Library (JEL) (*www.dtic.mil doctrine jel index.html*) is now available on-line. This is a superb site for up to date access to Joint publications. Included at the JEL site is a DOD

dictionary, capstone service publications (FM 100-5, AFM 1-1, FMFM 1, NDP 1 etc), and research papers dealing with topical joint matters of interest. The other services also maintain numerous Internet sites that may be of interest to the operational planner. A good place to start for the other services are MarineLink (www.usmc.mil), AirforceLink (www.af.mil) and Navy: Welcome aboard (www.navy.mil).

The assortment of Universities and Colleges that are run by the different services can also be of help to the operational planner. The National Defense University (NDU) (www.ndu.edu) provides a well structured site that contains links to its affiliated schools and organizations. Also available is the NDU phone book, listings of publications, library information, and an Internet resources guide. The Armed Forces Staff College (www.afsc.edu) has an excellent faculty directory that includes areas of expertise and contact information. The Armed Forces Staff College directory is searchable and includes address, phone, fax and email contact information. Another invaluable source available at the AFSC site is AFSC PUB 1 (www.afsc.edu/pub1.htm), *The Joint Staff Officer's Guide 1997*. Users can FTP the entire publication, or view portions of it online using Adobe Acrobat reader.

The National War College(198.80.36.91/ndu/nwc/nwchp.html), US Army War College (carlisle-www.army.mil), US Naval War College (users.ids.net/nwc/), Air War College (www.au.af.mil/au/awc/), all have a presence on-line. These sites are similar mostly in what they offer: mission, history, course descriptions, staff directories, etc. Most of this information is rather generic and does not offer much to

the operational planner, though there are some notable exceptions such as the US Army War College Strategic Studies Institute (www.army.mil/usassi/). This site has available a set of electronic catalogs that are indexed by functional area, regional topic areas, and special reports and essays. The functional areas include Operations Other Than War (OOTW), Civil Military Relations, and Revolution in Military Affairs (RMA). The regional topic areas include Western and Eastern Europe, Asia and Pacific, Middle East, Africa, and Latin America.

Another source of topical information for the operational planner is the growing number of professional journals available on-line. Military topics are well covered in journals such as: *Parameters*, *Military Review*, *Airpower Journal*, *Air Chronicles*, *Military Intelligence Professional Bulletin*, and *Special Warfare Magazine*. A large number of excellent publications covering International Security and Foreign Policy are available on-line. Some examples of these are: *Foreign Policy*, *National Review*, *World Politics*, *The Washington Monthly*, *Atlantic Monthly*, *Aussen Politik*, *Current History*, *Foreign Affairs*, *Fletcher Forum*, and *Defense Monitor*.¹⁵ Most of the magazines listed have the complete current edition available, and many have back issues available as well. Though many do not currently have an on-line search ability, this function is becoming more available. An excellent source for periodical publications is The Electronic Newstand (www.enews.com); this site has links to over 2,000 on-line magazines and includes a searchable database.

Private Organizations and think tanks can also be a valuable source for the operational planner. Examples of this include the Brookings Institute

(www.brook.edu), the Hoover Institute ([www-hoover.stanford.edu default.htm](http://www-hoover.stanford.edu/default.htm)), and the RAND Corporation (www.rand.org). The Brookings' site is excellent with a complete listing of its scholars, their areas of expertise, and contact information. The Brookings' site also has policy briefs, foreign policy studies, and the Brookings Press book catalog. The RAND site is also very good; it has listings of publications, hot topics, information on its centers and programs, the RAND research review, and a search capability that allows the search of RAND abstracts.

The area of news is another area where the Internet can provide an invaluable service to the operational planner. Some sources that could prove useful include Cable News Network Interactive (www.cnn.org), National Public Radio(www.npr.org), *The New York Times*(www.nytimes.com), *The Washington Post*(www.washingtonpost.com), News AP & UPI(www.fyionline.com) and Reuters(www.reuters.com). There is also a wide variety of regionally focused news sources on-line such as Inside China(www.insidechina.com), Russia Today(www.russiatoday), Central Europe(www.centraleurope.com), and Africa On-line(www.africaonline.com). The Internet makes the accessing of this information faster and more efficient than ever.

For more detailed information about countries, the Federal Research Division of Library of Congress has available Country Studies/Area Handbook Program ([lcweb2.loc.gov/frd cs country.html](http://lcweb2.loc.gov/frd/cs/country.html)); this collection is scheduled to include over 60 countries by June 1997. The Yahoo! search index also maintains an excellent

regional information database. This database can be accessed by region, country, and state.

III. Governmental Reactions and Policies on the Internet

Governments around the world are dealing with the Internet and its growth in a variety of ways. The competition between the spread of technology and desire to control information through censorship are causing governments a great deal of concern. Most governments are finding themselves caught between the desire for increased educational and economic advantages that the Internet offers and yet they want to retain control over the information available on the Internet. The way most governments are dealing with the Internet is through an increasing amount of restrictions on content and control of access to the Internet.

The Internet offers challenges to those who wish to censor it in that information on it has the ability to reach each and every user. Information on the Internet can be gathered and distributed at an extremely rapid pace, which means the amount of information available is increasing at an exponential pace. This explosion of information is thoroughly overwhelming attempts to monitor it, let alone censor it effectively.

Most Western nations are interested in limiting content on so called decency clauses, but these are essentially suppression of freedom of speech issues.¹⁶ Many

other nations have much more serious concerns about the Internet. These nations have mainly authoritarian governments which fear the freedom of information that the Internet allows. It is of interest that some of the only nations still without full Internet connections are the most authoritarian and repressive in the world, i.e., North Korea and Cuba (though the official Korean Central News Agency has opened an official web site on a server in Japan *www.kcna.co.jp* that provides English language news reports with the North Korean official view of things). Recently Cuba has closed a deal with Sprint to provide limited email access.

This monograph will now examine a number of countries' reactions to and policies for the Internet.

United States:

Even inside the U.S., one of the foremost advocates of free speech in the world, there has been a large amount of debate as to what should be allowed on the Internet. The concerns in the United States have centered mainly around pornography. These concerns resulted in the adoption of the Communications Decency Act (CDA), an amendment to the telecommunications reform bill signed in February 1996. The CDA criminalizes on-line communication that is "obscene, lewd, lascivious, filthy, or indecent, with intent to annoy, abuse, threaten, or harass another person" or "obscene or indecent" if the recipient of the communication is under eighteen years of age "regardless of whether the maker of such communication placed the call or initiated the communication." Human Rights Watch opposed the CDA on the

grounds that "indecent" speech is protected by both the U.S. Constitution and international law.¹⁷ The American Civil Liberties Union has filed a lawsuit with Human Rights Watch as a plaintiff challenging the CDA on constitutional grounds.

Germany:

Germany has been involved in a number of highly published censorship issues involving the Internet. A major incident occurred in December 1995 when the German government asked CompuServe to deny access to 200 newsgroups which the Government claimed were involved in pornography. After coming under considerable pressure, Compuserve reviewed their actions and by February 1996 it had allowed all but five of the newsgroups back on its servers.

The other significant action came in January 1996, when Deutsche Telekom (DT) the national telephone company, blocked its T-Online computer network from Internet sites being used to spread anti-Semitic information.¹⁸ Included in these sites was Web Communications, a U.S. computer service provider in Santa Cruz California, which carried a site by Ernst Zuendel. Zuendel is a German born neo-Nazi activist living in Toronto.

It is actions like these in the United States, Germany and others such as New Zealand, Australia and Canada that have cleared the way for more drastic measures in more authoritarian countries.

Singapore:

Singapore has fostered computer literacy, and developed a cutting edge infrastructure, all aimed at making the nation a highly competitive "intelligent island".¹⁹ Because of its efforts, Singapore is finding itself more than most caught between information control and freedom.

Singapore is unique in a way because the people of Singapore recognize and even desire governmental censorship, favoring caution and prevention over liberalism.²⁰ The Singapore government justifies the need for censorship in its multiracial/multireligious society because it believes that the unimpeded flow of ideas can have negative effects as opposed to leading to enlightenment. The Government points to a number of previous cases where media reports have lead to racial riots and the shedding of blood, such as the 1950 Maria Hertogh riots, the 1964 riots during Prophet Muhammad's birthday, and the 1969 riots spillover from Malaysia.²¹

Because the Singapore government sees "misinformation" as one its biggest threats, it has formed an administrative committee to provide information and rebut inaccurate information about Singapore on the Internet through "Singapore Infomap"(www.sg).²² Groups providing information for this service include the National Computer Board, the Economic Development Board, the Ministry of Information and the Arts, and Internet service providers.

The Government requires all Internet service providers to be licensed and to use filtering software. These measures are designed to limit sexually explicit material,

hate literature, and some political and religious materials.²³ The Government of Singapore has settled on a combination of traditional censorship and spin control to try to maintain control over the Internet. Another country that is trying the spin control angle is Indonesia.

Indonesia:

This country is relatively unique in its approach in that it has not actively sought to limit content available on the Internet. The Internet is more free than any other mass medium in Indonesia.²⁴ *Tempo*, a weekly news magazine which had been shut down by the Government in 1995, has opened a site on the web with the knowledge of the Government. The Indonesians are countering the Internet with web sites of their own; the Armed Forces and other ministries have set up sites to disseminate their positions. A danger of running an official site was demonstrated on the 10th and 15th of February when a group of Portuguese hackers (Portuguese Hackers Against Indonesia) modified the web site of the Indonesian Foreign Affairs Ministry (www.dfa-deplu.go.id). Among other things there was the title "Welcome to the Foreign Affairs Ministry of the Fascist Republic of Indonesia".²⁵ If Governments take this route of spin control, they must ensure the integrity (both physical and informational) of the sites they establish. They must ensure that their sites are of value and have meaning for their constituents.

China:

In China, the Minister for Posts and Telecommunications(MPT) Wu Jichuan says the government wants to build a technologically fully systematized state communications network. To do this, the MPT spent \$9.5 billion on ChinaNet (www.cnd.org) and other information services in 1995.²⁶ However, even with these desires in mind the government in China seeks to retain firm control of access to the Internet. The Chinese government controls access to the Internet by requiring users and Internet Services providers to register with authorities and it has outlawed the on-line transmission of pornography and state secrets.²⁷ Additionally, all international computer networks must run through channels set up by the MPT. It is estimated that China has about 100,000 Internet users.

The method of control that China has chosen is the control of access to the Internet. This is an effective method of control for many authoritarian regimes and developing countries due to the nature of their communications infrastructure. The manner in which China handles the integration of the 50 Internet service providers and the 200,000 - 500,000 Internet users in Hong Kong in July 1997 will be interesting to watch. The demographics of the current users in Hong Kong are as follows: 92% male and 61% hold a University degree or higher.²⁸ This group is not likely to give up their Internet access very easily.

Gulf Co-operation Council (GCC):

The members of the GCC; Saudi Arabia, Kuwait, Bahrain, Qatar, the United Arab Emirates, and Oman all regard themselves as under threat from the Internet.²⁹ Like other developing countries, they are caught in the double bind of desiring economical and educational benefits of Internet access and their desire to control the information available through the Internet. Though these Muslim nations see the ease of availability of “immoral” material as a threat, the biggest threat they face is the use of the Internet by groups making dissident political opinion available. Historically, these nations have all imposed various means of censorship on information from entering their countries. They have all censored mail and strictly controlled the import of other media, such as video cassettes and printed materials into their lands.³⁰ While stationed in Saudi Arabia during the Gulf War, the author’s copies of *U.S News and World Report* were often censored by the blacking out of or even removal of certain pictures and articles.

The countries of the GCC are reacting to the threat posed by the Internet through a combination of controlling access and competition. The primary method to deal with this threat is by strictly limiting access through approved Internet providers. In Saudi Arabia, for instance, only three institutions have official Internet access; the King Abdul Aziz City for Science and Technology, the King Fahd University of Petroleum and Minerals and the King Fahd Hospital.³¹ In other nations of the GCC, Internet access is only available through the national telecommunications company such as the Bahrain Telecommunications Company, Qatar Public

Telecommunications Corporation, and Etisalat (UAE national telecommunications company). This control by national telecommunications companies ensures they are able to censor, monitor or control what is available to users through their services.

It is important to note that there is no regulatory agency overall in charge of the Internet, it is meant to be self policing though there are some organizations such as Internet Society that promulgate technical standards. The very fact that there is no central controlling body for the Internet makes the control of content on the Internet nearly impossible. Attempts by system administrators to stop users from accessing objectionable sites or materials will simply result in the users finding other systems from which to access the material. The Internet, by its nature and design, is resistant to any blockage or stoppage of its links. The Internet will simply reroute any traffic through one of its other existing links. The Internet was designed to survive the loss of large sections through damage or destruction, yet still be able to function with its remaining nodes.

In the next section, this monograph will examine some cases where the Internet is increasingly being used to circumvent the controls on information that authoritarian governments use against their people.

IV. Usage of the Internet by Advocacy Groups, Social Movements and Transnational Actors

The Internet offers small groups of people and organizations a new way to coordinate their actions to influence, change, or fight governmental policy. The Internet makes it possible for diverse, dispersed actors to communicate, consult, coordinate and operate together across greater distances, on the basis of larger amounts of and better information than ever before.³² Because of the global nature of the Internet, the issues that this presents are international in that they transcend traditional national borders. In this section of the monograph, the author will examine some of the recent incidents in which the Internet has been utilized.

Serbia:

A good example of the power of the Internet is the events surrounding the Serbian municipal elections held in November 1996. The crisis began when the Opposition party, Together, claimed to have won a number of cities in the elections including the two largest cities in Serbia, Belgrade and Nis. President Milosevic in a move to retain control, quickly annulled the results of the elections. In an authoritarian regime like Serbia, an important aspect of maintaining domination over the people is the control of media and the resultant control of information that this entails. One of the biggest reasons that Slobodan Milosevic resisted acknowledging the results of the elections was that the positions voted on held the right to grant television and radio

licenses. The resulting freedom of information that this entailed was anathema to the Serbian regime.³³

Within hours of the annulment, messages calling for mass demonstrations to protest Milosevic's actions began appearing on Sezam Pro, an electronic bulletin board service in Serbia. This was not the first time that the people of Serbia had tried to protest against the government. There were street protests in March of 1991 in opposition to the imminent Balkan war, and in July 1992 to protest against the government after the start of UN sanctions. Both of these protest movements were quickly put down with riot troops and tanks, and drew little attention from the outside world. The students involved learned a valuable lesson in that the first action they took after the announcement of the annulment of the elections in November was to establish a Web site (<http://galeb.etf.bg.ac.yu/~protest96/>).³⁴

As the protests grew and the pressure mounted through the end of November and early December, Milosevic decided to take action by shutting down B92. B92 (207.10.94.56 [opennet b92inet.html/](http://opennet.b92inet.html/)), Belgrade's only independent radio station, had been broadcasting updates on the growing protests in the streets for the previous two weeks. Until this time, Radio Television Serbia and TV Belgrade had either been ignoring the protests completely or misrepresenting them as violent terrorist actions.³⁵

As soon as the government took B92 off the air, the student protesters rerouted the broadcasts to the Internet using RealAudio (a commercial service that allows the transmitting of audio over the Internet: <http://cgi.realaudio.com/welcome.html>). At this point, the broadcasts were picked up by the Voice of America and the British

Broadcasting Corporation and then retransmitted back into Serbia by short-wave. Fifty-one hours after B92 had been removed from the air, the Serbian government relented to internal and external pressures and allowed B92 to broadcast again.³⁶

People began referring to this as the Internet Revolution, because of the pivotal role that the Internet played in keeping the outside world informed on what was happening in Serbia.³⁷ At one point, the police ordered the students operating the computer server to shut down. The students had established mirror sites in Europe and North America, ensuring that they would be able to keep operating. The students would be able to send their information via modem to one of these sites, even if the Belgrade computer server had been shut down. In order to have prevented the information from being disseminated, the Serbian government would have had to shut down the entire telephone system in Serbia.³⁸

The students in Belgrade were able to keep in contact with other students throughout Serbia via the Internet for the duration of the protest. They were able to coordinate their efforts nationwide by the use of on-line discussions and email to ensure a unified front against the Milosevic government.³⁹ It is estimated that only about 10,000 people in Serbia used the Internet at the time of the protest. It was not the numbers that mattered in this case, but who the 10,000 were and how they used the Internet. The protesters were able to use the Internet as a bridge to the outside world and to obtain Western media attention for their cause. They even drew American Congressmen who spoke to the protesting crowds, encouraging them to

keep up their protests. Clearly, the Internet played a significant role in the success of the protest against the annulment of the elections in Serbia.

Mexico:

The use of the Internet by the Zapatista Army of National Liberation (EZLN) (YA BASTA! Unofficial EZLN Homepage www.ezln.org) has gained a large amount of attention in the media.⁴⁰ Arguably, the EZLN uprising in Chiapas would have remained much more obscure to the rest of the world had it not been for the Internet. The EZLN only fought with arms for 12 days before they called on the civil society of Mexico and the world to continue their battle for them by using the Internet.⁴¹ Since that time the military leader of the EZLN, Subcomandante Marcos, regularly posts communiqués to the Internet. Not only does the Internet allow the EZLN to get its version of what is happening heard, it gives the EZLN the ability to maintain contact with sympathetic groups throughout the world, and to organize responses to any moves by the government. The EZLN has even used the Internet to solicit medical attention for one of its important leaders, Comandante Ramona. The EZLN received numerous offers of help from around the world within hours of posting requests for urgent medical attention.⁴² Another good example of the impact that the Internet can have is seen in the case of the “Infamous Chase Report”.

The Chase Report refers to a memo written by Riordan Reott for Chase Manhattan Bank for Chase Emerging Markets clients. This report called for the Mexican Government to “eliminate” the Zapatistas to demonstrate its command over

the internal situation in Mexico.⁴³ This story and the report were leaked in Ken Silverstein and Alexander Cockburn's newsletter *Counterpunch*, but received little notice or publicity. It was not until it was uploaded onto the Internet through a large number of list servers and the USENET, that it gained widespread notice. The result was a large mobilization of people in protest against the U.S. and Mexican governments and Chase Manhattan. These protests led to Chase firing Roett and helped to force the Mexican government to halt its offensive in Chiapas in February 1995.⁴⁴

Peru:

In Peru, both the Tupac Amaru Revolutionary Movement (MRTA) (brun.ucsd.edu/~ats/mrta.htm) and Communist Party in Peru, sometimes referred to as Sendero Luminoso or Shining Path (www.csrp.org), have established a presence on the Internet. The MRTA and Shining Path have turned to the Internet as a powerful interactive communications tool that can bypass governmental censorship and the editorial control of other mass media outlets to get their message out.

Rebel supporters established a web page within one day of the MRTA seizing a large number of hostages at the Japanese ambassador's residence during a diplomatic reception in December 1996. Supporters posted photographs and communiqués from the rebels inside the residence with updates of the siege on the web page.⁴⁵ This web site allowed the MRTA to get their demands and story heard even after the Peruvian Government had blocked their cellular phone signals. The MRTA issued a call for

solidarity and asked supporters to send letters to the government of President Fujimori, with copies to human rights organizations and various media organizations throughout the world. They even included the addresses and fax numbers for the letters, and email addresses for numerous local and international media organizations.⁴⁶

The MRTA Solidarity Page allows access to all official communiqués issued by the MRTA as a result of the seizing of the Japanese Ambassador's residence. This page has background information on the organization, as well as interviews and statements by the MRTA leadership. Video clips of the MRTA commandos preparing for their action are also available on the site. Additionally, the Solidarity page maintains links to the German, Italian and Japanese World Wide Web pages of the MRTA.

The Committee to Support the Revolution in Peru (CSRP) site has many of the same types of items that the MRTA site contains, background information on the Communist Party of Peru, news about the revolution, and access to Party documents etc. A difference between the sites is the ability to purchase an assortment of materials from the CSRP site. Items for sale include numerous books, pamphlets, videos, music cassettes, T-shirts and buttons. Through the sale of material, the CSRP site expands on the traditional use of the Internet as an information source to a means of procuring active support. YA BASTA!, the EZLN site, has taken this a step further with an entire section on "What you can do to help". This section of the EZLN page lists seven ways to actively show your support to their cause:

1. Send letters of protest to Mexican Officials.

2. Send letters of support to the Zapatistas.
3. Send humanitarian aid to Chipas.
4. Raise money for EZLN.
5. Join a Peace Encampment.
6. Organize/attend a protest rally.
7. Educate your friends.

The EZLN provides these suggestions, including all the details required to follow through with any of the above actions.

Transnational Actors:

The United States has historically enjoyed a large measure of safety due to its relative geographic isolation. The advent of the global information infrastructure and the Internet has done much to erase the safety margin that the U.S. has enjoyed. The Internet makes it possible for individuals armed only with computers to gain access to a nation's borders.

Examples of the danger poised by this threat are becoming more common everyday. For three weeks in 1994 a 16 year-old British hacker and an associate made over 150 intrusions through the Air Force's top command and control research and development facility, the Rome Laboratory. From the Air Force computers the hackers were able to invade the computers of several defense contractors and the South Korean Atomic Research Institute. This is not an isolated incident, the Defense Information Systems Agency (DISA) estimates that the Department of Defense is attacked about 250,000 times per year. These attackers have stolen, modified, and destroyed data and software, disabled protection systems to allow

future unauthorized access, and shut down entire systems and networks to preclude authorized use. These attacks cost the Department of Defense hundreds of millions of dollars annually and DISA estimates that only about 1 in 150 attacks is detected and reported.⁴⁷

The Department of Defense is not the only target of attack by hackers. In 1994 Citibank was shocked to discover that a group of computer hackers in St. Petersburg, Russia had made \$10 million in illegal transfers from its branch offices around the world. Citibank was able to recover all but \$400,000, but in the process lost its top 20 customers to rival banks who claim better computer security.⁴⁸ *Fortune* estimates that the financial losses from computer crime reach as high as \$10 billion a year, with almost all attacks going undetected, and the attacks that are detected most often are not reported to law-enforcement agencies.⁴⁹ Bill Marlow, a banking security consultant, puts these crimes into perspective; the average bank robbery nets about \$1,900 and gets prosecuted 82% of the time, the average computer robbery nets \$250,000 and gets prosecuted less than 2% of the time.⁵⁰

These case studies begin to show the potential that the Internet offers to individuals and organizations who are willing and able to exploit it. The impact that the Internet is having on incidents like those detailed above is not yet fully understood. It is clear, however, that the Internet is playing a significant role in these events.

V. CONCLUSION

In this time of increasing demands and diminishing resources, the operational planner needs to be as flexible and innovative as possible. The Internet as a worldwide communications means and information repository holds unique potential for the operational planner. The Internet is playing an increasing role throughout the world in a wide array of social, economic, cultural, political, and military activities. The communication functions of the Internet allow people with unique expertise, information, motivations, and experiences to share and exchange ideas in ways not previously possible.

The Internet is a truly mass media. While very few individuals or groups can publish books or newspapers, make films, or produce a radio or television program, any person with a personal computer and a modem can communicate with a huge international audience. The Internet is an extremely powerful tool for gathering and disseminating information: anything placed on the Internet has the potential to reach millions of people worldwide instantaneously.

This monograph details some of the tremendous capabilities that the Internet offers an operational planner. The ability to communicate with other users in over one hundred and fifty countries, to transfer files and data quickly and inexpensively, to remotely access files, programs, and computers, all to an unprecedented extent, clearly impact on the operational planner.

Though much of what is currently available on the Internet may be available elsewhere in printed form, or on the radio; the ease of access that the Internet offers is unparalleled. The Internet, unlike any other mass media, allows the display of many types of information; i.e., text, images, graphics, sound, video, as well as interactive communications capabilities. Ever increasing amounts of information and services are available through the Internet. With a computer, modem, and phoneline an operational planner has worldwide around the clock access to the most extensive information source in the world. The Internet allows the operational planner to rapidly gather information in a width, depth, and context not previously possible.

The "Information Superhighway" is not without its potholes. As was detailed in Chapter IV, there is a downside potential to the Internet. The use of the Internet by subversive organizations and transnational actors can pose a danger that operational planners need to be aware of. Another potential danger is identified in a report by Reuters Business Information on the cost of the Information Revolution. The Reuters report states that an excess of information is strangling business and causing personnel to suffer mental anguish and physical illness. Specific findings of Reuters include; 43% of managers think that important decisions are delayed and the ability to make decisions affected as a result of having too much information, and 48% think that the Internet will be a prime cause of information overload over the next two years.⁵¹ Users of the Internet need to be aware of these concerns but they should not let them overshadow the fantastic potential the Internet offers them.

This monograph does not propose that the Internet replace anything that the operational planner is now using or doing to gather information. The Internet offers unique and complementary capabilities that must be understood and exploited. The Internet is one more tool for an operational planner to use to ensure that the Army wins quickly, decisively and with a minimum of casualties.

ENDNOTES

- ¹ General Dennis J. Reimer, "Soldiers are our Credentials", *Military Review*, September - October 1995, 5.
- ² US Army, Field Manual 100-6 *Information Operations*, (Washington DC: Department of the Army, 1996), v.
- ³ Ibid., Glossary-7.
- ⁴ *The World Almanac and Book of Facts*, ed., 1997, 207.
- ⁵ Internet Index; accessed 23 March 1997, available at <http://www.openmarket.com/intindex>, Internet.
- ⁶ "History of the Internet" on The Internet Society homepage; accessed 10 February 1997 available at <http://www.isoc.org>, Internet.
- ⁷ Ibid.
- ⁸ Ibid.
- ⁹ *World Almanac*, 207.
- ¹⁰ Ed Krol, *The Whole Internet: User's Guide & Catalog*, 2d ed., (Sebastopol CA: O'Reilly & Associates, 1994), 102.
- ¹¹ Ibid., 103.
- ¹² Charles Swett, "Strategic Assessment: The Internet"; accessed 10 February 1997 available at <http://www.fas.org/cp/swett.html>, Internet.
- ¹³ Karen Sorensen, "Silencing The Net: The Threat to Freedom of Expression On-line", *Human Rights Watch*, May 1996 Vol. 8, No. 2, 6.
- ¹⁴ Indexing Coverage Analysis of the Internet, accessed 24 April 1997, available at <http://www.mellee.com/mica/index.html>, Internet.
- ¹⁵ *Parameters* (carlisle-www.army.mil/usawc/parameters), *Military Review* (www-cgsc.army.mil/cgsc/milrev/milrev.htm), *Airpower Journal* (www.cdsar.af.mil/apje.html), *Air Chronicles* (www.cdsar.af.mil/air-chronicles.html), *Military Intelligence Professional Bulliten* (huachuca-usaic.army.mil/SCHOOL.DOTD.MIPB.mirand), *Special Warfare Magazine* (www.usasoc.soc.mil/swcs/dotd/sw-mag/sw-mag.htm), *Foreign Policy* (www.eneews.com/magazines/foreign_policy), *National Review* (www.eneews.com/magazines/national_review), *World Politics* (www.wps.princeton.edu/world_politics), *The Washington Monthly* (www.eneews.com/magazines/wash_month), *Atlantic Monthly* (www2.theatlantic.com/atlantic), *Aussen Politik* (www.isn.ethz.ch/au.pol), *Current History* (www.eneews.com/magazines/chistory), *Foreign Affairs* (www.foreignaffairs.org), *Fletcher Forum* (www.tufts.edu/fletcher_forum.html), and *Defense Monitor* (www.cdi.org/dm).
- ¹⁶ Sorensen, "Silencing The Net", 6.
- ¹⁷ Ibid., 8.

¹⁸ Ibid.

¹⁹ William McGurn, "Wired Singapore: Island state finds the Net a two-edged sword", *Far Eastern Economic Review*, July 27, 1995, 72.

²⁰ Dr. Peng Hwa Ang and Ms. Berlinda Nadarajan, "Netwatch Singapore Censorship and The Internet: A Singapore Perspective". On-line Index on Censorship.

²¹ Ibid.

²² Ibid.

²³ Sorensen, "Silencing The Net", 12.

²⁴ Ibid., 13.

²⁵ For a complete list of differences between the original page and the hacked page see <http://toxyn.pt.eu.org/timor/ndex.html>.

²⁶ "Invasion from Cyberspace", *Asiaweek*, Hong Kong, September 8, 1995.

²⁷ Michael Krantz, "China Wired", *Time*, April 22, 1996, 73.

²⁸ Hong Kong Internet User Survey 1996, accessed 20 April 1997, available at <http://acnielsen.com/countries/hongkong/netbro.htm>, Internet. This survey estimated that in mid 1996 there were 100,000 Internet accounts in Hong Kong, with approximately three users per account. Additionally the survey estimated that the forecast for users would double by the end of 1996. If the survey is correct there should be approximately 600,000 Internet users in Hong Kong by the end of 1996. I have used more conservative numbers of between 200,000 - 500,000.

²⁹ Dr. Andrew Rathmell, "Netwar in the Gulf", *Jane's Intelligence Review*, January 1997, 29.

³⁰ Ibid.

³¹ Ibid., 31.

³² Jason Wehling, "Netwars and Activists Power on the Internet", *Index on Censorship*, March 1995. This concept is from John Arquilla and David Ronfeldt, "Cyberwar is Coming", which first appeared in *Comparative Strategy*, Vol 12 pp 141-165.

³³ David S Bernahum, "The Internet Revolution", *Wired*, April 1997, 168.

³⁴ Ibid., 170.

³⁵ CNN Presents 22 Feb 1997.

³⁶ Ibid.

³⁷ Bennahum, "The Internet Revolution", p. 168.

³⁸ Ibid.

³⁹ Ibid., 170.

⁴⁰ For an excellent of account of Zapatistas actions in the use of the Internet see Harry Cleaver, "Zapatistas in Cyberspace", available on-line at <http://www.eco.utexas.edu/faculty/Cleaver/zapsincyber.html>, Internet.

⁴¹ Darrin Wood, "Net Wars", *Index on Censorship*, March 1995.

⁴² Ibid.

⁴³ Harry Cleaver, "Chiaps 95", accessed on 25 March 1997, available at <http://www.eco.utexas.edu/faculty/Cleaver/chipas95.html>, Internet.

⁴⁴ Ibid.

⁴⁵ MRTA Solidarity Page; accessed on 25 January 1997, available at <http://burn.ucsd.edu/~ats/mrta.htm>, Internet.

⁴⁶ "A Call For Solidarity With The MRTA", MRTA Solidarity Page; accessed on 25 January 1997, available at <http://burn.ucsd.edu/~ats/mrtasoli.htm>, Internet.

⁴⁷ Information Security: Computer Attacks at Department of Defense Pose Increasing Risks, GAO/AIMD-96-84 May 22, 1996.

⁴⁸ Richard Behar, "Who's reading your e-mail?" *Fortune*, February 3, 1997, 64.

⁴⁹ Ibid., 59.

⁵⁰ David Gow and Richard Norton-Taylor, "USA: Banks have good reason to fear thieves who hack their secret files", *Guardian* United Kingdom 7/12/96, 28.

⁵¹ Reuters Business Information, "Dying for Information? An investigation into the effects of information overload in the UK and Worldwide." accessed on April 17, 1997, available at <http://www.fireworks.org/firefly/clients/reuters/press/141096.html>. Internet.

APPENDIX ONE: INTERNET CONNECTIVITY TABLE

NUMBER OF ENTITIES WITH INTERNATIONAL NETWORK CONNECTIVITY = 186
 NUMBER OF ENTITIES WITHOUT INTERNATIONAL NETWORK CONNECTIVITY = 51

IP INTERNET

Col. 2 (Entities with international IP Internet links.)

I: = operational, accessible from the entire open IP Internet, 134 entities

UUCP

Col. 3 (Entities with domestic UUCP sites which are connected to the Global Multiprotocol Open Internet.)

u: minimal, one to five domestic UUCP sites, 64 entities

U: widespread, more than five domestic UUCP sites, 82 entities

FIDONET

Col. 4 (Entities with domestic FIDONET sites which are connected to the Global Multiprotocol Open Internet)

f: minimal, one to five domestic FIDONET sites, 43 entities

F: widespread, more than five domestic FIDONET sites, 65 entities

An entity is a geographical area that has an ISO two letter country code (ISO 3166).

These country codes are included in the Table below for each entity (Cols 7-8).

Note that the ISO codes do not always agree with the top level DNS (Domain Name) code(s) used by hosts in a particular entity. For example, Internet hosts in a number of countries have DNS names ending in .net or .com. In the United Kingdom, .uk is used while the official ISO code is .gb. There are still hosts in the former Soviet Union that use .su in their DNS names.

Restricted access or dial-up IP links exist in a number of countries. These are not included in the table as Internet connections. There are also a number of private Fidonet nodes that are used for specific projects or by designated groups. These are also not included.

---	AF	Afghanistan (Islamic Republic of)
I--	AL	Albania (Republic of)
I--	DZ	Algeria (People's Democratic Republic of)
---	AS	American Samoa
I--	AD	Andorra (Principality of)
--f	AO	Angola (People's Republic of)
-u-	AI	Anguilla
I--	AQ	Antarctica
Iu-	AG	Antigua and Barbuda
IUF	AR	Argentina (Argentine Republic)
IU-	AM	Armenia
I-f	AW	Aruba
IUF	AU	Australia
IUF	AT	Austria (Republic of)
IU-	AZ	Azerbaijan
-u-	BS	Bahamas (Commonwealth of the)
I--	BH	Bahrain (State of)
-U-	BD	Bangladesh (People's Republic of)
Iu-	BB	Barbados
IUF	BY	Belarus
IUF	BE	Belgium (Kingdom of)
IU-	BZ	Belize
I-f	BJ	Benin (People's Republic of)
IUF	BM	Bermuda
---	BT	Bhutan (Kingdom of)

IUF	BO	Bolivia (Republic of)
-u-	BA	Bosnia-Herzegovina
-uf	BW	Botswana (Republic of)
---	BV	Bouvet Island
IUF	BR	Brazil (Federative Republic of)
---	IO	British Indian Ocean Territory
I--	BN	Brunei Darussalam
IUF	BG	Bulgaria (Republic of)
-U-	BF	Burkina Faso (formerly Upper Volta)
---	BI	Burundi (Republic of)
-u-	KH	Cambodia
-Uf	CM	Cameroon (Republic of)
IUF	CA	Canada
---	CV	Cape Verde (Republic of)
I--	KY	Cayman Islands
I--	CF	Central African Republic
--f	TD	Chad (Republic of)
IUF	CL	Chile (Republic of)
IuF	CN	China (People's Republic of)
---	CX	Christmas Island (Indian Ocean)
---	CC	Cocos (Keeling) Islands
Iu-	CO	Colombia (Republic of)
---	KM	Comoros (Islamic Federal Republic of the)
---	CG	Congo (Republic of the)
-u-	CK	Cook Islands
Iuf	CR	Costa Rica (Republic of)
-Uf	CI	Cote d'Ivoire (Republic of)
IuF	HR	Croatia
-U-	CU	Cuba (Republic of)
I-f	CY	Cyprus (Republic of)
IUF	CZ	Czech Republic
IUF	DK	Denmark (Kingdom of)
I-f	DJ	Djibouti (Republic of)
---	DM	Dominica (Commonwealth of)
IUF	DO	Dominican Republic
---	TP	East Timor
Iu-	EC	Ecuador (Republic of)
IU-	EG	Egypt (Arab Republic of)
Iu-	SV	El Salvador (Republic of)
---	GQ	Equatorial Guinea (Republic of)
-uf	ER	Eritrea
IUF	EE	Estonia (Republic of)
--f	ET	Ethiopia (People's Democratic Republic of)
---	FK	Falkland Islands (Malvinas)
Iu-	FO	Faroe Islands
Iu-	FJ	Fiji (Republic of)
IUF	FI	Finland (Republic of)
IUF	FR	France (French Republic)
-u-	GF	French Guiana
-u-	PF	French Polynesia
---	TF	French Southern Territories
---	GA	Gabon (Gabonese Republic)
--f	GM	Gambia (Republic of the)
IUF	GE	Georgia (Republic of)

IUF	DE	Germany (Federal Republic of)
IUF	GH	Ghana (Republic of)
I--	GI	Gibraltar
IUF	GR	Greece (Hellenic Republic)
I--	GL	Greenland
-u-	GD	Grenada
-uf	GP	Guadeloupe (French Department of)
I-F	GU	Guam
Iuf	GT	Guatemala (Republic of)
-u-	GN	Guinea (Republic of)
---	GW	Guinea-Bissau (Republic of)
-u-	GY	Guyana (Republic of)
-u-	HT	Haiti (Republic of)
---	HM	Heard and McDonald Islands
Iu-	HN	Honduras (Republic of)
I-F	HK	Hong Kong
IUF	HU	Hungary (Republic of)
IUF	IS	Iceland (Republic of)
IUF	IN	India (Republic of)
IUF	ID	Indonesia (Republic of)
I--	IR	Iran (Islamic Republic of)
---	IQ	Iraq (Republic of)
IUF	IE	Ireland
IUF	IL	Israel (State of)
IUF	IT	Italy (Italian Republic)
Iu-	JM	Jamaica
IUF	JP	Japan
I-f	JO	Jordan (Hashemite Kingdom of)
IUF	KZ	Kazakhstan
IUF	KE	Kenya (Republic of)
-u-	KI	Kiribati (Republic of)
---	KP	Korea (Democratic People's Republic of)
IUF	KR	Korea (Republic of)
I--	KW	Kuwait (State of)
IU-	KG	Kyrgyz Republic
-uf	LA	Lao People's Democratic Republic
IUF	LV	Latvia (Republic of)
IU-	LB	Lebanon (Lebanese Republic)
-u-	LS	Lesotho (Kingdom of)
---	LR	Liberia (Republic of)
---	LY	Libyan Arab Jamahiriya
I-f	LI	Liechtenstein (Principality of)
IUF	LT	Lithuania
IUF	LU	Luxembourg (Grand Duchy of)
I-F	MO	Macau (Ao-me'n)
Iu-	MK	Macedonia (Former Yugoslav Republic of)
IU-	MG	Madagascar (Democratic Republic of)
--f	MW	Malawi (Republic of)
IUF	MY	Malaysia
---	MV	Maldives (Republic of)
-Uf	ML	Mali (Republic of)
Iuf	MT	Malta (Republic of)
-u-	MH	Marshall Islands (Republic of the)
---	MQ	Martinique (French Department of)

---	MR	Mauritania (Islamic Republic of)
IuF	MU	Mauritius
---	YT	Mayotte
IuF	MX	Mexico (United Mexican States)
---	FM	Micronesia (Federated States of)
IuF	MD	Moldova (Republic of)
I--	MC	Monaco (Principality of)
I--	MN	Mongolia
---	MS	Montserrat
IuF	MA	Morocco (Kingdom of)
IuF	MZ	Mozambique (People's Republic of)
---	MM	Myanmar (Union of)
IU-	NA	Namibia (Republic of)
-u-	NR	Nauru (Republic of)
Iu-	NP	Nepal (Kingdom of)
IUF	NL	Netherlands (Kingdom of the)
-u-	AN	Netherlands Antilles
-U-	NC	New Caledonia
IUF	NZ	New Zealand
Iu-	NI	Nicaragua (Republic of)
-U-	NE	Niger (Republic of the)
-Uf	NG	Nigeria (Federal Republic of)
-u-	NU	Niue
---	NF	Norfolk Island
---	MP	Northern Mariana Islands (Commonwealth of the)
IUF	NO	Norway (Kingdom of)
---	OM	Oman (Sultanate of)
IU-	PK	Pakistan (Islamic Republic of)
---	PW	Palau (Republic of)
IuF	PA	Panama (Republic of)
-u-	PY	Paraguay (Republic of)
IuF	PE	Peru (Republic of)
IuF	PH	Philippines (Republic of the)
---	PN	Pitcairn
IUF	PL	Poland (Republic of)
IUF	PT	Portugal (Portuguese Republic)
IUF	PR	Puerto Rico
---	QA	Qatar (State of)
Iu-	RE	Re'union (French Department of)
IuF	RO	Romania
IUF	RU	Russian Federation
---	RW	Rwanda (Rwandese Republic)
---	SH	Saint Helena
---	KN	Saint Kitts and Nevis
Iu-	LC	Saint Lucia
---	PM	Saint Pierre and Miquelon (French Department of)
-u-	VC	Saint Vincent and the Grenadines
-u-	WS	Samoa (Independent State of)
I--	SM	San Marino (Republic of)
---	ST	Sao Tome and Principe (Democratic Republic of)
I--	SA	Saudi Arabia (Kingdom of)
IUF	SN	Senegal (Republic of)
-u-	SC	Seychelles (Republic of)
--f	SL	Sierra Leone (Republic of)

IuF	SG	Singapore (Republic of)
IUF	SK	Slovakia
IUF	SI	Slovenia
-u-	SB	Solomon Islands
---	SO	Somalia (Somali Democratic Republic)
IUF	ZA	South Africa (Republic of)
IUF	ES	Spain (Kingdom of)
IU-	LK	Sri Lanka (Democratic Socialist Republic of)
--f	SD	Sudan (Democratic Republic of the)
Iu-	SR	Suriname (Republic of)
I--	SJ	Svalbard and Jan Mayen Islands
-u-	SZ	Swaziland (Kingdom of)
IUF	SE	Sweden (Kingdom of)
IUF	CH	Switzerland (Swiss Confederation)
---	SY	Syria (Syrian Arab Republic)
IuF	TW	Taiwan, Province of China
-uf	TJ	Tajikistan
--f	TZ	Tanzania (United Republic of)
IUF	TH	Thailand (Kingdom of)
-u-	TG	Togo (Togolese Republic)
---	TK	Tokelau
-u-	TO	Tonga (Kingdom of)
IU-	TT	Trinidad and Tobago (Republic of)
IuF	TN	Tunisia
I-F	TR	Turkey (Republic of)
-uf	TM	Turkmenistan
---	TC	Turks and Caicos Islands
-u-	TV	Tuvalu
I-f	UG	Uganda (Republic of)
IUF	UA	Ukraine
I-f	AE	United Arab Emirates
IUF	GB	United Kingdom (United Kingdom of Great Britain and Northern Ireland)
IUF	US	United States (United States of America)
---	UM	United States Minor Outlying Islands
IUF	UY	Uruguay (Eastern Republic of)
IUF	UZ	Uzbekistan
-u-	VU	Vanuatu (Republic of, formerly New Hebrides)
I--	VA	Vatican City State (Holy See)
IuF	VE	Venezuela (Republic of)
-U-	VN	Vietnam (Socialist Republic of)
---	VG	Virgin Islands (British)
I-f	VI	Virgin Islands (U.S.)
---	WF	Wallis and Futuna Islands
---	EH	Western Sahara
---	YE	Yemen (Republic of)
-uf	YU	Yugoslavia (Socialist Federal Republic of)
---	ZR	Zaire (Republic of)
I-f	ZM	Zambia (Republic of)
Iuf	ZW	Zimbabwe (Republic of)

Copyright 1996 Lawrence H. Landweber and the Internet Society. Unlimited permission to copy or use is hereby granted subject to inclusion of this copyright notice.

BIBLIOGRAPHY

Books

- Bellamy, Chris. *The Future of Land Warfare*. New York: St. Martin's Press, 1987
- Bellamy, Chris. *The Evolution of Modern Land Warfare*. New York: Routledge, 1990.
- Beniger, James R. *The Control Revolution, Technological and Economic Origins of the Information Society*. Cambridge: Harvard University Press, 1986.
- Campen, Alan D., Douglas H. Dearth, and R. Lthomas Gooden, eds. *Cyberwar: Security, Strategy, and Conflict in the Information Age*. Fairfax, VA: AFCEA International Press, 1996
- De Landa, Manuel. *War in the Age of the Intelligent Machine*. New York: Zone Books, 1991.
- Dupuy, Trevor N. *The Evolution of Weapons and Warfare*. Fairfax: Hero Books, 1994.
- Haffner, Kate and John Markoff. *Cyberpunk, Outlaws and Hackers on the Computer Frontier*. New York: Simon and Schuster, 1991.
- Kelly, Kevin. *Out of Control, The New Biology of Machines, Social Systems and the Economic World*. Reading, MA: Addison-Wesley Publishing Company, 1994.
- Krol, Ed. *The Whole Internet: User's Guide & Catalog*. 2d ed. Sebastopol, CA: O'Reilly & Associates, 1994.
- Pfaltzgraff, Robert L. and Robert L. Schultz, eds. *War in the Information Age*. Washington, DC: Brassey's (US), Inc., 1996.
- Schwartau, Winn. *Information Warfare, Chaos on the Electronic Superhighway*. New York: Thunder's Mouth Press, 1994.
- Toffler, Alvin and Heidi Toffler. *Creating New Civilizations, The Politics of the Third Wave*. Atlanta: Turner Publishing, Inc., 1995.
- Toffler, Alvin. *Powershift, Knowledge, Wealth and Violence at the Edge of the 21st Century*. New York: Bantam Books, 1990.
- Van Creveld, Martin. *The Transformation of War*. New York: The Free Press, 1991.

Dissertations, Theses, and Reports

- Anderson, Robert, Tora Bikson, Salley Ann Law and Bridger Mitchell. Universal Access to E-Mail: Feasibility and Societal Implications. Center for Information Revolution Analysis, RAND, 1995.
- Ang, Peng Hwa and Nadarajan, Berlinda. Netwatch Singapore Censorship and The Internet: A Singapore Perspective. Index on Censorship, Summer 1995.
- Arquilla, John and David Ronfeldt. Cyberwar is Coming. Santa Monica, CA: Arroyo Center, RAND, 1996. RAND/RP-223.
- Behar, Richard. Who's Reading Your E-mail? Fortune February 3, 1997.
- Bernahum, David. The Internet Revolution. Wired, April, 1997.
- Gow, David and Norton-Taylor. USA: Banks have Good Reason to Fear Thieves Who Hack Their Secert Files. Guardian United Kingdom. June, 12, 1996.
- Hundley, Richard and Eugene Gritton. Future Technology-Driven Revolutions in Military Operations. National Defense Research Institute, RAND, 1994.
- Kievit, James and Steven Metz. The Internet Strategist: An Assessment of On-line Resources. Parameters, Summer 1996.
- Krantz, Michael. China Wired. Time. April 22, 1996.
- McGurn, William. Wired Singapore: Island state finds the Net a two-edged sword. Far Eastern Economic Review, July 1995.
- Rathmell, Andrew. Netwar in the Gulf. Jane's Intelligence Review, January 1997.
- Reimer, Dennis. Soliders are our Credentials. Military Review, September - October 1995.
- Ronfeldt, David. Cyberocracy, Cyberspace and Cyberology: Political Effects of the Information Revolution. Santa Monica: RAND, 1991. DTIC ADB168540.
- Reuters Bussiness Information. Dying for Information? An investigation into the effects of information overload in the UK and Worldwide.
<http://www.fireworks.org/firefly/clinets/reuters/press/141096.html>

Sorensen, Karen. Silencing The Net: The Threat to freedom of Expression On-line. Human Rights Watch, May 1996.

Wehling, Jason. Netwars and Activists Power on the Internet. Index on Censorship, Summer 1995.

Wood, Darrin. Net Wars. Index on Censorship, March 1995.

Government Documents

General Accounting Office. Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. GAO/AIMD-96-84 May 22, 1996.

U.S. Army. FM 100-6, *Information Operations*. Washington, DC: GPO, 1996.

_____. TRADOC Pamphlet 525-5, *Force XXI Operations*. Washington, DC: Department of the Army, August 1994.