

PEERING INTO THE FUTURE:
PEER-TO-PEER TECHNOLOGY AS A MODEL FOR DISTRIBUTED JOINT
BATTLESPACE INTELLIGENCE DISSEMINATION AND OPERATIONAL
TASKING

BY
MARK D. BONTRAGER

A THESIS PRESENTED TO THE FACULTY OF
THE SCHOOL OF ADVANCED AIRPOWER STUDIES
FOR COMPLETION OF GRADUATE REQUIREMENTS

SCHOOL OF ADVANCED AIRPOWER STUDIES
AIR UNIVERSITY

MAXWELL AIR FORCE BASE, ALABAMA

JUNE 2001

Report Documentation Page		
Report Date 01JUN2001	Report Type N/A	Dates Covered (from... to) -
Title and Subtitle Peering into the Future: Peer-to-Peer Technology as a Model for Distributed Joint Battlespace Intelligence dissemination and Operational Tasking	Contract Number	
	Grant Number	
	Program Element Number	
Author(s) Bontrager, Mark D.	Project Number	
	Task Number	
	Work Unit Number	
Performing Organization Name(s) and Address(es) School of Advanced Airpower Studies Air University Maxwell AFB, AL	Performing Organization Report Number	
Sponsoring/Monitoring Agency Name(s) and Address(es)	Sponsor/Monitor's Acronym(s)	
	Sponsor/Monitor's Report Number(s)	
Distribution/Availability Statement Approved for public release, distribution unlimited		
Supplementary Notes The original document contains color images.		
Abstract		
Subject Terms		
Report Classification unclassified	Classification of this page unclassified	
Classification of Abstract unclassified	Limitation of Abstract UU	
Number of Pages 95		

Disclaimer

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University.

About the Author

Major Mark D. Bontrager was born in Kokomo, Indiana on 21 July 1964. He attended Plantation High School, Plantation, Florida where he graduated in 1982. He attended the University of Florida in Gainesville, Florida and graduated in 1987 with a Bachelor of Science degree in Computer Engineering and a reserve commission in the Air Force through the Reserve Officer Training Corps. Major Bontrager attended Undergraduate Space Training at Lowry Air Force Base, Colorado in 1987. He was then assigned as a Deputy Crew Commander in the United States Space Command's Missile Warning Center, Cheyenne Mountain Air Force Base, Colorado. In 1990 he moved to the 1013th Combat Crew Training Squadron, Peterson Air Force Base, Colorado as an Missile Warning Center Training Instructor. In 1991 he served as an instructor with the General Officer Space Operations Orientation Course and the Staff Officer Space Operations Orientation Course. He completed his Master's degree in Engineering, Space Operations Option, at the University of Colorado in 1992. Major Bontrager was reassigned to the 1st Space Launch Squadron at Cape Canaveral Air Station, Florida in January 1994. He served as Chief, Electrical Booster Processing, Launch Vehicle Flight Commander, Operations Support Flight Commander and Bravo Flight Commander. He was the launch controller for NASA's Near Earth Asteroid Rendezvous satellite launch in February 1996. Immediately following the launch, he was selected to serve as the Executive Officer to the Group Commander for the 45th Operations Group and in April

1996, he was selected as the Executive Officer to the Wing Commander for the 45th Space Wing. Major Bontrager was reassigned to the Commanders Action Group at Headquarters Air Force Space Command, Peterson Air Force Base, Colorado in May 1997. In 1999, he attended the Naval Command and Staff College Newport Naval Station, Rhode Island and graduated with distinction in June 2000. After graduating from the School of Advanced Airpower Studies in June 2001, Major Bontrager was assigned to the Strategic Plans and Policy Directorate of the Joint Staff. Major Bontrager wears the senior space badge. Major Bontrager is married to the former Julie Wilmeth of Colorado Springs, Colorado. They have two sons, Joshua and Daniel.

Acknowledgments

Many people assisted me during the research and writing of this thesis. I especially want to thank General Richard Myers, Vice Chairman, JCS for his support and sponsorship of this thesis. I also wish to express my gratitude to Mr. Keith Hall, Director NRO, LTG James King, Director NIMA, Lt Gen Bruce Carlson, Director J-8, Joint Staff, and Lt Gen Lance Lord, Assistant Vice Chief of Staff, HQ USAF, for their very valuable time and comments in the early stages of my research.

Many individuals spent significant time reading and reviewing draft versions of this thesis. Their inputs were invaluable and I am deeply indebted to them for their selfless efforts to help me get across the main messages of this work. I am especially appreciative to: Dr. Bob Anderson, RAND; Mr. Jeff Fliesher, NIMA; LTC Mike Dorohovich, OSD/C3I; Major Jonathan Clough, AFRL; and CDR Bill Cunningham, HQ USN.

A special note goes to others who provided research materials and insight into the central concepts behind this thesis. Special thanks to: Maj David Cohen, NIMA; Mr. John Black, Groove Networks; Mr. Bob Knuth, JFCOM/J9; LCDR Mike Siracuse, JFCOM/J9; Mr. C.C. Hill, JFCOM/J9; Lt Col John Murphy, OSD/C3I; Mr. Mark Norton, OSD/C3I; Mr. Jerry Dussault, AFRL; Mr. Ed Mornston, NIMA; Lt Col Susan Durham, NRO; and Ms. Christine Pearson, NRO.

I also am indebted to those who helped me find others within the Defense Department that are thinking and wrestling with similar concepts to enable information support for the warfighters. I am especially grateful to: Col Doug Nowak, OSD/C3I; Ms. Susan Roby, OSD/C3I; Mr. John Landon, OSD/C3I; and Mr. Mark Norton, OSD/C3I.

I would have never attempted to tackle this subject without the "nudging" of LTC Earl Wardell and Maj Andre Shappell from the office of the Vice Chairman, JCS who gave me the opportunity to "excel" with this project. I don't know how I could repay them—but I'll be working on it.

Finally, my two boys Joshua and Daniel also deserve special note for their selfless understanding when Daddy was always disappearing to the office to "study." I am forever indebted to my lovely wife, Julie who supports me daily with encouragement and strength—my gratitude goes beyond words.

Abstract

This thesis focuses on the capabilities of an emerging technology known as Peer-To-Peer (P2P) technology and its potential to improve intelligence support to operational and tactical warfighters. First popularized by a popular music-sharing program called Napster in May 1999, P2P technology enabled the sharing of millions of music files over the Internet between anyone who wanted to share. Some advocates believe that P2P technology will fuel the next Internet revolution. A radical departure from previous hierarchical networking technologies, P2P promises to empower users at the edges of a network by giving them the ability to connect to each other directly without going through a central server. This thesis evaluates this new technology and its potential to link operational and tactical users at the edges of military networks directly to sensors and analysts that provide intelligence information.

This study seeks to answer the question, "How would peer-to-peer technology improve the current intelligence tasking, processing, exploitation and dissemination (TPED) process to benefit operational and tactical users?" To answer this question, the study surveys the various deployments of P2P technology that are currently in use in the commercial marketplace, explores some conceptual foundations of P2P technology and discusses the promises and perils that the technology brings. Following this conceptual overview of the technology, the study defines the TPED process and explores its current strengths and weaknesses. Finally, this study explores the intersections between each

step of the intelligence process and proposes options for P2P technology to improve each step by evaluating applicability, effectiveness, and ease of implementation.

The study concludes that P2P technology offers operational and tactical users at the edges of a network unprecedented power. It offers them direct access to sensors, other users, information, and ultimately knowledge of the battlespace to enable decision superiority. P2P technology can improve the tasking, processing, exploitation, and dissemination process to benefit operational and tactical users and brings tremendous opportunity for greater situational awareness and decision superiority. The most significant benefits could be radically improved warfighter access and a more responsive intelligence system. The most significant technical obstacles will be security and bandwidth. Finally, the study concludes by discussing the cultural, organizational and doctrinal changes that will be necessary to bring such benefits to the warfighters.

Contents

	<i>Page</i>
DISCLAIMER	ii
ABOUT THE AUTHOR	iii
ACKNOWLEDGMENTS	v
ABSTRACT.....	vii
LIST OF ILLUSTRATIONS.....	x
LIST OF TABLES	xi
INTRODUCTION	1
THE PROMISES AND PERILS OF P2P TECHNOLOGY	11
INTELLIGENCE INFORMATION FLOW.....	42
P2P MEETS TPED.....	56
CONCLUSION.....	76
BIBLIOGRAPHY.....	81

Illustrations

	<i>Page</i>
Figure 1: Client-Server Framework	4
Figure 2: Peer-To-Peer Framework	4
Figure 3: Broker Model	18
Figure 4: No-Broker Model	19
Figure 5: Cycle-Sharing Model	22
Figure 6: Example Gnutella Network Including Reflectors	37
Figure 7: TPED Description	45
Figure 8: TPED -Database Transactions.....	49

List of Tables

	<i>Page</i>
Table 1. Applicability of P2P Models to TPED	59
Table 2. Effectiveness of P2P Models	64
Table 3. Ease of P2P Implementation.....	72

Chapter 1

INTRODUCTION

A soldier . . . in peacetime is like a sailor navigating by dead reckoning. You have left the terra firma of the last war and are extrapolating from the experiences of that war. The greater the distance from the last war, the greater become the chances of error in this extrapolation.

Sir Michael Howard
Military Science in an Age of Peace

The Fog of Peace

When the next war starts, no one will be fully prepared. As Sir Michael Howard said, "Usually everybody starts even and everybody starts wrong . . . the advantage goes to the side which can most quickly adjust itself to the new and unfamiliar environment and learn from its mistakes."¹ This ability to adapt and adjust to new and unfamiliar environments is one of the premier tasks of any military in peacetime. Today, the US military spends millions of dollars to innovate and improve the tools available to the information age warrior. These improvements aim to bring about decision superiority—to equip warriors and leaders with the right information, at the right time to make the right decisions.² Ideally, decision superiority will give US forces the ability to adapt more quickly in wartime and make it more difficult for an adversary to counter U.S. military dominance.

However, in today's "age of peace" no one knows for sure what capability tomorrow's adversary will possess. As this peacetime uncertainty dominates all strategic decisions, one of

¹ Sir Michael Howard, "Military Science in an Age of Peace," *Royal United Services Institute for Defence Studies*, March 1974, 6.

² Department of Defense, *Joint Vision 2020*, (Washington D.C.: Chairman of the Joint Chiefs of Staff, 2000), 8.

the most significant decisions will be to determine which innovations to pursue to enable future military success. Pre-World War II Germany pursued a combined arms approach known as Blitzkrieg. The Wehrmacht's spectacular success at the beginning of World War II is well known. In the late 1980s, the United States pursued advanced stealth aircraft and precision guided munitions that significantly contributed to victory in Desert Storm. Such innovations gave clear advantages over the enemy.

However, the uncertainty of today's strategic environment leads one to question the dangers in pursuing innovations that could lead the US military down the wrong road. Such "bad" innovations could leave the US at a disadvantage in future conflict. Steven Rosen argues in his book *Winning the Next War*, that he has been unable to find clear-cut cases of such "bad" innovation. He writes, "The United States military has made many mistakes . . . but they all appear to have been the result of failures to innovate, rather than inappropriate innovations."³ This indicates that innovation may always be good because it forces people and organizational cultures to become adaptable to meet an uncertain future.

The information age offers many innovative technologies. Which ones should the US military pursue? Which emerging technologies will provide the biggest advantage and adaptability in future conflict?

Peer-To-Peer Technology

This thesis focuses on the capabilities of an emerging technology known as Peer-To-Peer (P2P) technology. Since the spring of 2000, P2P technology has taken the Internet computing world by storm. First popularized by a popular music-sharing software called Napster founded in May 1999, the number of P2P companies went from zero to fifty in less than 12 months.⁴ P2P technology made headlines when, in August 2000, the Intel Corporation announced that it was taking the lead and establishing an industry-wide working group to advance infrastructure

³ Stephen P. Rosen, *Winning the Next War*, (Ithaca, New York: Cornell University Press, 1991), 53.

⁴ "Peer-To-Peer Computing," *Peer-To-Peer Working Group*, Adobe Acrobat Document, 10; on-line, Internet, 8 February 2001, available from http://www.peer-to-peerwg.org/specs_docs/collateral/P2P_IDF_Rev1.11-web.pdf.

standards for peer-to-peer computing.⁵ This Peer-To-Peer Working Group (P2PWG) aims to tackle standards, security, reliability and other issues. Other high-tech giants such as Hewlett-Packard and IBM quickly joined the working group.

Hailed as the next Internet revolution, P2P advocates point to the early 1990s when a program called Mosaic allowed people to "browse" the Internet. This browser led to an explosion in web servers from less than 50 in 1992 to over 10,000 in 1994. Similarly, P2P technology proponents predict that with standard P2P protocols, another revolution in capability is just around the corner.

Since P2P's 1999-2000 debut and early hype, many P2P companies have felt the sting of reality as the "dot-com" investment bubble popped in Spring 2000 and its effects spread throughout the industry over the year. Moreover, Napster, the most recognizable name in the P2P industry lost its legal battle with the Recording Industry Association of America (RIAA). The RIAA challenged Napster's right to facilitate distribution of copyrighted material and court orders have forced Napster to filter songs to prevent the sharing of unauthorized tunes. However, in spite of such a high-profile setback to the industry, P2P technology continues to be viable and "an inevitable evolution for computing."⁶

P2P computing is defined as the sharing of computer resources and services by direct exchange.⁷ At first glance, that does not sound very revolutionary. However, in reality it turns the networked world upside down. Currently, most networks are designed with large and powerful servers as "hubs" for information and control. These servers are powerful computers that do the "heavy-lifting" by providing storage, printing capabilities, or network control. In a classic architecture, servers exist to support "clients" that are out at the "edges" of a network. Clients may be personal computers (PC), workstations, printers, or sensors that use the server as central hub for resources, such as files, devices (like printers), and even processing power.⁸ (See Figure 1).

⁵ "Welcome," *Peer-To-Peer Working Group*, n.p.; on-line, Internet, 8 February 2001, available from <http://www.peer-to-peerwg.org/index2.html>.

⁶ J. Sweeney et al., *The Five Peer-to-Peer Models: Toward the New Web*, Gartner Group Research Note COM-12-4447 (Stamford, Conn: Gartner Group, February 2001), 3; on-line, Internet, 21 May 2001, available from <http://www3.gartner.com/Init>.

⁷ Ibid.

⁸ "Client/Server Architecture," *zdwebopedia*, n.p.; on-line, Internet, 8 February 2001, available from http://www.zdwebopedia/TERM/c/clinet_server_architecture.html.

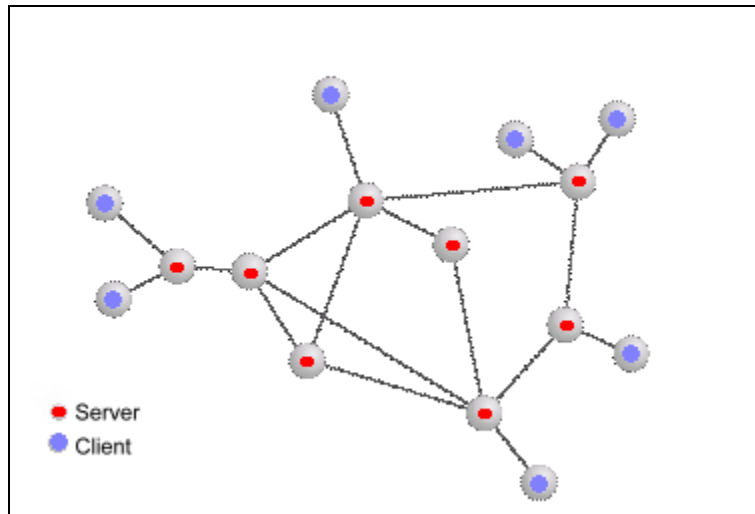


Figure 1: Client-Server Framework

With P2P, clients on a network can simply bypass the server and exchange information over the network directly. This adds value to the edges of a network where the information is being collected and used. (See Figure 2).

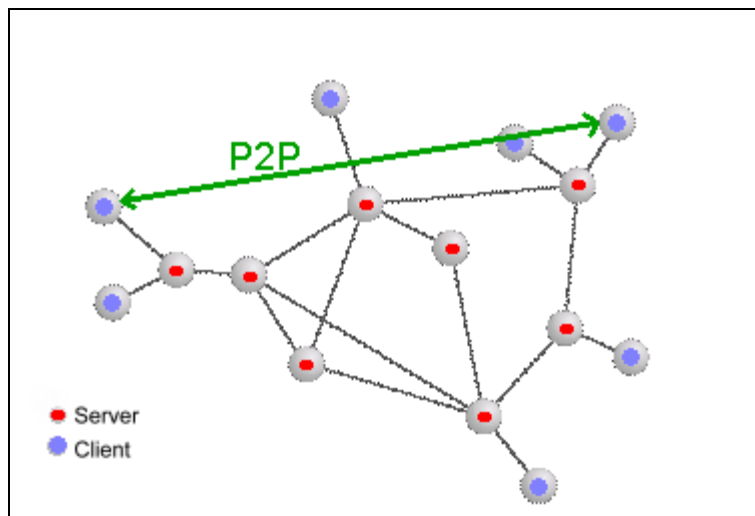


Figure 2: Peer-To-Peer Framework

The Military Connection

What does this have to do with the military? Consider what is located at the edges of a military network—warfighters and sensors. Imagine the possibilities if warfighters could link

directly to sensors of their choice. Imagine the possibilities of linking sensors to other sensors to build an accurate battlespace picture not only in some command center thousands of miles from the front, but also in the hands of the front-line warfighters. The proliferation of communications and computers in the battlespace continues unabated. P2P technology could leverage these systems to make everything a peer—linking battlespace sensors, analysts, shooters, and decision-makers.

In many cases, the flow of information from sensor to shooter is hampered by a traditional hierarchical data flow. For example, during Desert Storm, when a SCUD missile was launched, a satellite in space detected the missile's launch plume. That information was then relayed to a ground station in the Eastern Hemisphere. From there it was relayed to Colorado Springs where it was analyzed and reformatted. After that it was forwarded by voice, to the CENTCOM command center in Saudi Arabia. Finally, it was forwarded to the Patriot Missile Defense units who most needed to know about an incoming SCUD launch. In commenting on this process, General Richard Myers, the Vice Chairman of the Joint Chiefs of Staff, in a speech to the National Reconnaissance Office commented, "This took several minutes, far too long when an SRBM flight profile itself took only several minutes. Wouldn't it have been far better for our Air Defense soldiers—themselves among the best and brightest in the Army—to get the information directly from the satellite, with the authority to respond immediately?"⁹ P2P technology could enable that transfer of information from sensor to shooter.

P2P technology offers more than just linking sensors to shooters. It presages a new way of thinking about how to take advantage of the information and intelligence that reside at the edges of a network. For example, most organizations have well defined processes and procedures. These hierarchical, centralized, and repeatable processes evolved to enable the organization consistently to meet its objectives. However, when an "unusual" or unanticipated crisis arises, the organization must adapt. Ad-hoc, spontaneous, and agile teams form to address the new situation. Such dynamic and adaptable solutions draw greatly on the intelligent people and their information at the edges of a network. P2P technology enables edge-based organizational adaptability by providing tools for teams to form quickly and efficiently.

⁹ General Richard Myers, Vice Chairman of the Joint Chiefs of Staff, US Air Force, address to National Reconnaissance Office Senior Leaders' Strategic Management Conference, Williamsburg, Virg., 2 November 2000.

A basic understanding of P2P technology, as evolving in the commercial world, can serve as a launching point for further understanding of the information age possibilities that P2P technology brings.

Peer-To-Peer Models

The P2PWG defined three models of P2P computing that conceptually capture the different uses of P2P technology today. These models are Broker Mediated File Sharing, Peer-To-Peer File Sharing, and Cycle Sharing.¹⁰ This thesis will use the terms Broker, No-Broker, and Cycle Sharing. Each model offers certain strengths and weaknesses that are explored in Chapter 2.

With the Broker model, users register files with a broker for sharing. When looking for files a user simply asks the broker where to find files to copy. Napster epitomizes this type of P2P program. It is based on a simple premise: to allow members of a "community" to share computer files on the Web. Napster's service accepts requests for certain music files, searches listings of other community members and links the requestor with the source.¹¹ The broker model is a central "index" or "database" that keeps track of what users have what files. However, once requestor and source are linked, the central index is no longer necessary.

With the No-Broker model, users register files with network neighbors. In a network, a neighbor is any node that has direct contact with another node. When looking for files a requestor asks its neighbors if they know where to find a specific file. If that neighbor does not know or does not have it, it relays the request to its neighbors. Eventually, a source is found or the request runs out of neighbors. If a source is found, the address of the source is passed back to the requestor who is then linked with the source. Programs like Gnutella and Freenet provide this No-Broker capability and emerged soon after Napster's legal challenges began. These no-broker programs also share files over the Internet. Many of these programs were developed as "open source" programs and can be modified and improved by computer programmers worldwide. Thus, the P2P software landscape is continually changing.

¹⁰ "Peer-To-Peer Computing," *Peer-To-Peer Working Group*, Adobe Acrobat Document, 13-15; on-line, Internet, 8 February 2001, available from http://www.peer-to-peerwg.org/specs_docs/collateral/P2P_IDF_Rev1.11-web.pdf.

The Cycle Sharing model takes advantage of unused computer processing power across a network. In this model, small chunks of data are sent to many users on a network. The users process the data on their computers and return it to the sender. The Search for Extraterrestrial Intelligence at Home ([SETI@Home](http://setiathome.berkeley.edu)) is one example of cycle sharing. With over 2 million users worldwide donating spare computing power, SETI may be the largest supercomputer in the world.¹² Companies such as Intel, Boeing, and Pratt & Whitney have also embraced the cycle-sharing model.

As the high-tech computing industry matures all of these P2P models into viable, profit-oriented businesses, the U.S. military will need to explore how it can leverage this and other technologies in support of national security.

Information and Decision Superiority

The Department of Defense (DoD) clearly recognizes the potential impact of information technology on military operations. *Joint Vision 2020*, the strategic vision for the U.S. military, acknowledges, "advances in information capabilities are proceeding so rapidly that there is a risk of outstripping our ability to capture ideas, formulate operational concepts, and develop the capacity to assess results."¹³ With this recognition, the goal for military operations is Information Superiority that leads to Decision Superiority over any adversary. In this context, Information Superiority is defined as "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (JP1-02)"¹⁴ Information Superiority then enables a joint force to take advantage of "superior information converted to superior knowledge to achieve 'decision superiority'—better decisions arrived at and implemented faster than an opponent."¹⁵ All of these concepts support the overarching goal of "Full Spectrum Dominance."

¹¹ Dennis Michael, "Win or lose, Napster has changed Internet," *CNN.com*, 2 October 2000, n.p.; on-line, Internet, 3 October 2000, available from <http://www.cnn.com/2000/SHOWBIZ/Music/10/02/napster/index.html>.

¹² "SETI@home: Massively Distributed Computing for SETI," *Computing in Science and Engineering*, n.p.; Internet, 8 February 2001, available from <http://www.computer.org/cise/articles/seti.htm>.

¹³ *Joint Vision 2020*, 8.

¹⁴ Ibid.

¹⁵ Ibid.

Identifying the centrality of the "network" to future military operations, the DoD's Information Superiority vision develops and explores the concept of Network-Centric Forces. Moreover, the vision identifies the importance of agility and adaptability to ensure a competitive advantage.¹⁶ The Naval War College curriculum teaches multiple lessons on the concept of Network Centric Warfare and has incorporated the concept into its student wargames. The Navy has developed a Network Centric Innovation Center to further the opportunities offered by a network-centric construct.¹⁷ These efforts, along with others in all services and at the Joint Staff serve to improve the process of turning data into knowledge that leads to better decisions.

This emphasis on the information domain has led to the development of an entire profession called Knowledge Management. The DoD has established numerous knowledge management offices including the creation of Chief Knowledge Management officers. This emphasis on knowledge, enabled by networked inputs, will ultimately lead to decision superiority.

While some of the information needed by operational and tactical warfighters comes from "organic" collection assets, the Intelligence Community provides large amounts of information from space-based assets and other collection platforms. Moreover, in many cases the Intelligence Community may be the only source of real-time information in areas where there is no US military presence. Concurrent with the explosion in information technology and its associated capabilities, the Intelligence Community has come under increased scrutiny. Attention has been explicitly focused on the intelligence collection and dissemination processes. Recent congressionally chartered reviews of the National Reconnaissance Office (NRO) and the National Imagery and Mapping Agency (NIMA) have questioned whether the process of tasking, processing, exploitation and dissemination (TPED) is grounded in modern information systems thinking.¹⁸ Illustrating the significance of information technology, the NIMA commission report devoted an entire section of their report to "NIMA and Its Information Architecture—A Clean Sheet." Furthermore, many books and articles have been written challenging the Intelligence

¹⁶ Information Superiority, Making the Joint Vision Happen (Washington D.C.: ASD/C3I), 2.

¹⁷ More information about this capability is available on the Internet at <http://www.ncic.navy.mil/collaboration.asp>.

¹⁸ Independent Commission on the National Imagery and Mapping Agency, *The Information Edge: Imagery Intelligence and Geospatial Information in an Evolving National Security*

Community for its "industrial age" thinking and the opportunities it may be missing offered by the information age with its new concepts of operation, organization and architecture.¹⁹ As the Intelligence Community implements the commissions' recommendations, many different information architectures will be evaluated. P2P technology may provide answers to some of the challenges that architecture developers will face.

More than just an issue for the Intelligence Community, US military forces are focused on improving a similar process called Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR). C4ISR is really a combination of two other acronyms, C4 and ISR. More than just a handy combination, this merging of terms captures the essence of the concept. C4 gives a purpose to ISR—to serve the commander by improving information flow. C4ISR brings together "stovepiped systems into an integrated system of systems" to serve decision-makers and warfighters.²⁰ Both TPED and C4ISR serve the goal of making information available and most usable to the ultimate customer (warfighter, operational commander, policy maker, etc.) and are often be used interchangeably. The most significant difference is that C4ISR is an all-encompassing term that is frequently used to address issues from doctrine to system architectures where TPED concentrates on the intelligence process of getting knowledge to the appropriate user.

P2P and TPED

The P2P revolution may provide a capability to improve the joint battlespace information domain and contribute significantly to decision superiority. This thesis explores the various P2P concepts in the commercial marketplace and addresses their potential applicability to DoD and each element of the TPED process. The research question that this thesis seeks to answer is: How would peer-to-peer technology improve the current intelligence tasking, processing, exploitation and dissemination process to benefit operational and tactical users?

Environment, xi; on-line, Internet, <http://www.NIMACommission.com>.

8 January 2001, available from at

¹⁹ Bruce D. Berkowitz and Allan E. Goodman, *Best Truth: Intelligence In The Information Age* (New Haven, Connecticut: Yale University Press, 2000), ix-xi.

²⁰ Aerospace Command & Control, Intelligence Surveillance, and Reconnaissance Center, "AC2ISRC Mission," n.p.; on-line, Internet, 2 May 2001, available from <http://www2.acc.af.mil/ac2isrc/Mission.asp>.

To answer this overarching question, chapter 2 will discuss the attributes and capabilities of P2P technology. Chapter 2 defines P2P technology and the details of how it is deployed over the Internet. This chapter fleshes out how each of the three models work and explores the conceptual foundations of a notional P2P infrastructure. Finally, it analyzes the different models to expose their strengths and weaknesses and provide a better appreciation for the promises and perils in deploying P2P technology.

Chapter 3 describes the flow of intelligence information to the warfighter. It examines and explores each element of the TPED process and describes how the intelligence community is adapting to meet the intelligence needs of operational and tactical users.

Armed with an understanding of P2P technology and the current TPED process, Chapter 4 analyzes each model of P2P and its applicability to each element of the TPED process. It then describes how effectively each model could improve TPED for the warfighters. Finally, it proposes various deployment options for P2P applications for each element of the TPED process. Finally, it is important to note that any change in technology may drive cultural responses and vice versa. Chapter 5 will describe some cultural, organizational, and doctrinal changes that will allow P2P technology to influence TPED. While this thesis will not explicitly address cultural issues that are present throughout any large organization, if P2P technology is adopted, it will certainly have cultural impacts throughout the DoD and the Intelligence Community. Ultimately, while technology may influence culture, it is only true culture change that will allow any true innovation to flourish.

Chapter 2

The promises and perils of P2P TECHNOLOGY

If a million people use a Web site simultaneously, doesn't that mean that we must have a heavy-duty remote server to keep them all happy? No; we could move the site onto a million desktops and use the Internet for coordination. Could Amazon.com be an itinerant horde instead of a fixed Central Command Post? Yes.

David Gelernter
The Second Coming—A Manifesto

What is P2P Technology?

The CNET on-line computer glossary defines P2P as "A network where there is no dedicated server. Every computer can share files and peripherals with all other computers on the network, given that all are granted access privileges."²¹ The Gateway on-line glossary defines P2P as "A communications network that allows all workstations and computers in the network to act as servers to all other users on the network."²² These definitions illustrate the general, intuitive understanding of peer-to-peer. However, the ZDWebopedia definition expands the definition somewhat by differentiating a P2P network from a client-server type network. "A type of network in which each workstation has equivalent capabilities and responsibilities. This differs from client-server architectures, in which some computers are dedicated to serving the

²¹ "Peer-To-Peer Network," *CNET Glossary*, n.p.; on-line, Internet, 24 February, 2001, available from <http://www.cnet.com/Resources/Info/Glossary/Terms/peer.html>.

²² "Peer-To-Peer Network," *Gateway.com Help Glossary*, n.p.; on-line, Internet, 24 February, 2001, available from http://www.gateway.com/help/glossary/glossary_p.shtml.

others."²³

Is P2P technology really something new? Is all of the media hype over its potential really valid? Actually, P2P technology has been around for a long time. Windows 95 and Windows 98 software has allowed personal computers (PCs) connected on a network to share files and printers since the mid-1990s. So, why all the hype? What has changed?

P2P technology has been enabled by significant changes in the capabilities of the average desktop and laptop PC. The average PC now has the same computing power and hard-drive storage that only a server could have just a few years ago. Furthermore, the advent of cable modems and digital subscriber lines (DSL) has allowed PCs to receive and transmit high volumes of information.²⁴ "What has changed is what the nodes of these P2P systems are-- Internet-connected PCs, which had been formerly relegated to nothing but clients—and where these nodes are—at the edges of the Internet."²⁵ Thus, the real impact of Napster and other P2P technologies is that they are "leveraging previously unused resources."²⁶ These resources on the Internet are hundreds of millions of people and their PCs, laptop computers, cell phones and other devices.

However, one of the major challenges of P2P technology lies in the transient nature of these resources. Up until 1994, the Internet connectivity model assumed that the nodes were always on and always connected.²⁷ Large servers run by universities and businesses were the main nodes, were always on, and operated as peers. However, with the invention of the web browser, in the early 1990s, and the subsequent explosion of web sites to serve consumers

²³ "Peer-To-Peer Architecture," *ZDWebopedia*, n.p.; on-line, Internet, 24 February, 2001, available from http://www.zdwebopedia.com/TERM/p/peer-to-peer_architecture.html.

²⁴ A modem is a device or program that enables a computer to transmit data over telephone lines. Computer information is stored digitally, whereas information transmitted over telephone lines is transmitted in the form of analog waves. A modem converts between these two forms. A cable modem is a modem designed to operate over cable TV lines. Because the coaxial cable used by cable TV provides much greater bandwidth than telephone lines, a cable modem can be used to achieve extremely fast access to the World Wide Web. DSL technologies use sophisticated modulation schemes to pack data onto copper wires. They are sometimes referred to as last-mile technologies because they are used only for connections from a telephone switching station to a home or office, not between switching stations.

²⁵ Clay Shirky, "What is P2P ... And What Isn't," O'Reilly Network, n.p.; on-line, Internet, 24 February, 2001, available from <http://www.openp2p.com/pub/a/p2p/2000/11/24/shirky1-whatisp2p.html>.

²⁶ *Ibid.*

around the world, more people used a modem to connect their PCs to the Internet through telephone lines. With the growth of consumers wanting to connect to the Internet, Internet Service Providers (ISPs) like America On-line and CompuServe rushed to meet the demand. ISPs offer a phone number that allows a user's PC to link with a large server that links to the Internet. Once connected, a PC is assigned a temporary Internet Protocol (IP) address. This address allows servers to send and receive information to and from each PC. These PCs go "on-line" for relatively short periods of time and would enter and leave the network cloud frequently and unpredictably.²⁸ Furthermore, ISPs typically assigned a different IP address when the PC came on-line. Thus, information housed on a PC could never be consistently addressed and it was virtually impossible to know with any level of certainty who was at a given IP address. As a result of these transient connections and limited computing power, PCs were relegated to lower-class status compared with the "heavy-lifting" servers.

P2P technology can change the limitation of transient connections by establishing a method to deal with the nature of people who are always coming and going at the edges of the network. They do this by indexing "pseudonyms" so that when a user connects, their IP address can be updated in real-time. For example, Aimster is a very popular P2P Internet chat and file sharing network. When the user first signs up for Aimster, they create a pseudonym or username that they use every time they sign-on to Aimster. This pseudonym identifies the user, not a specific PC with a specific IP address. When a user signs on to Aimster, Aimster checks its pseudonym database and links the user and his current IP address. Thus, Aimster overcomes the limitation of constantly changing IP addresses by creating a central index or database so that people can connect to each other through pseudonyms. This ability to overcome the transient connection limitation gives P2P the ability to "handle unpredictability, and nothing is more unpredictable than the humans who use the network."²⁹

Yet, the network exists to serve the humans and other devices at the edges of the network and the continuing challenge has been to make the network more people friendly. With the increase in computing power and connection speed, PCs now can operate as nodes like servers had in the past. On any network, value is added to the information through the nodes at the

²⁷ Ibid.

²⁸ Ibid.

edges of a network. This is where people or sensors add intelligence to the information to increase (or decrease) the information's value. However, until recently, the information at the edges was largely inaccessible. Instead of moving or copying this valuable information to a central, shared server, P2P moves the server to each of these devices.³⁰ Thus, a P2P network takes advantage of the "intelligence" at the edges of a network by allowing them to link together directly without the "controlling" influence of a central server.

The fact that just about any device can now connect to the Internet and serve as a node is a radical departure from the previous client-server mindset. The network, which was previously dominated by large resource-rich processors, is now populated by a variety of smaller devices ranging from laptops to personal digital assistants to cell phones to embedded controllers.³¹ Currently, industry is scrambling to develop tools and standards that will eventually build a P2P infrastructure. One of the primary purposes of the P2PWG, among other forums and working groups, is to facilitate the development and widespread adoption of an infrastructure that will enable peer-to-peer technology.³² Gene Kan, one of the original developers of the Gnutella communications protocol writes, "Tomorrow's applications will take this infrastructure for granted and leverage it to provide more powerful software and a better user experience in much the same way modern Internet infrastructure has."³³

²⁹ Clay Shirky, "Listening to Napster," in *Peer-To-Peer: Harnessing the Power of Disruptive Technologies*, ed. Andy Oram, (Sebastopol, CA: O'Reilly & Associates, Inc., 2001), 24.

³⁰ Gregory A. Bolcer et al., *Peer-to-Peer Architectures and the Magi Open-Source Infrastructure*, White Paper , (Irvine, CA: Endeavors Technology, 6 December 2000) 6; Internet, available at <http://www.endtech.com/news.html>.

³¹ Bolcer, 6.

³² Other efforts in addition to the P2PWG include the JXTA Project by Sun Microsystems and Groove. A JXTA infrastructure will address the network fundamentals of searching, sharing, and storing information with P2P technology. (Source: Terry Hostetler, "Project JXTA to be Unveiled," *P2P Tracker*, n.p.; on-line, Internet, 7 April 2001, available from <http://www.p2ptracker.com/news/announce/jxta040201.htm>.) See also Sun's JXTA Project web page at <http://www.sun.com/jxta/>. For more information on the Groove infrastructure see www.groove.net.

³³ Gene Kan, "Gnutella," in *Peer-To-Peer: Harnessing the Power of Disruptive Technologies*, ed. Andy Oram, (Sebastopol, CA: O'Reilly & Associates, Inc., 2001), 122.

Back to the Future: The History of the Internet³⁴

In many ways, the advent of P2P takes the Internet back to its roots as a true P2P system. In the early 1960s, the RAND Corporation began research into robust, distributed communication networks for military command and control. The Department of Defense's Advanced Research Project Agency (ARPA) built the first ARPANET by linking four universities in 1969. ARPANET treated each node as an equal and linked them together as peers rather than in a client-server relationship.³⁵

The original "killer app" was e-mail.³⁶ This application was very popular because it enabled researchers to collaborate on scientific endeavors. Twenty-three universities and government research centers were connected on ARPANET by 1971. Throughout the 1980s, parts of the original ARPANET were commercialized and the Internet expanded from 200 to 60,000 nodes. Furthermore, software developed that quickly became the common language of all Internet computers and allowed two-way communication between nodes. In the mid-1980s, the formation of the Internet Advisory Board and the Internet Engineering Task Force served a critical function by providing a forum for designers, operators, and researchers to collaborate and incorporate "best standards for protocols and procedures."³⁷ One primary example of a protocol promoted by the IETF is the Hyper-Text-Transfer-Protocol (http) that begins virtually every web address. The late 1980s witnessed the first major security attacks and the establishment of the Computer Emergency Response Team (CERT) to address security concerns across the Internet.

Throughout the 1980s, federal agencies shared the cost of a common infrastructure and managed "interconnection points." The National Science Foundation (NSF) encouraged its regional networks, primarily academic institutions, to pursue commercial customers to use their networks and lower funding for all. The NSF restricted use of their networks to "Research and Education Only" which encouraged the growth of private, long-haul that became the foundation

³⁴ The bulk of the information for this section is taken from "Life on the Internet Net Timeline," PBS.ORG, n.p.; on-line, Internet, 24 February, 2001, available from <http://www.pbs.org/internet/timeline/index.html>.

³⁵ Nelson Minar and Marc Hedlund, "A Network of Peers," in *Peer-To-Peer: Harnessing the Power of Disruptive Technologies*, ed. Andy Oram, (Sebastopol, CA: O'Reilly & Associates, Inc., 2001), 4.

³⁶ A *killer app* is an application that surpasses (i.e., kills) its competitors.

for the information superhighway. All of these decisions created a vast network of networks that led to the decommissioning of ARPANET in 1990.³⁸

The 1990s saw the most explosive growth of the Internet. In 1991, the National Science Foundation (NSF) raised the restrictions on commercial traffic across the NSFNET Internet backbone. In 1993, the first "web browser" became available which enabled the average computer users to browse the web. This led to an explosion of Internet use and traffic on the Internet expanded at a 341,634 percent annual growth rate. By 1996, there were over 10 million nodes with over 40 million people connected to the Internet. In 1998, the US Department of Commerce selected a non-profit corporation, the Internet Corporation of Assigned Names and Numbers (ICANN) to function as "the global consensus entity to coordinate the technical management of the Internet's domain name system, the allocation of IP address space, the assignment of protocol parameters, and the management of the root server system."³⁹

The original Internet was P2P—with servers acting as clients to other servers and vice versa. The relationship was symmetric and every host on the net could serve any other host.⁴⁰ The exponential user growth of the 1990s forced the Internet away from its P2P roots and led to the ubiquitous deployment of the client-server model. Furthermore, the limited capability of client computers made them more useful as a receiver of information rather than a processor and transmitter of information. As a result, the client-server model surfaced as a way to deal with both challenges. First, the model is simple and straightforward: "the client initiates a connection to a well-known server, downloads some data and disconnects . . . It just needs to know how to ask a question and listen for a response."⁴¹ Furthermore, if the server is safe from security problems, then the client can also be protected. Second, most of the information is transmitted "downstream" to the user and thus most of the communication "pipes" have more downstream than upstream throughput. This downstream paradigm may be challenged by the P2P revolution

³⁷ "The Internet Engineering Task Force," IETF Web Page, n.p.; on-line, Internet, 31 March 2001, available from <http://www.ietf.org/index.html> and <http://www.ietf.org/rfc/rfc2026.txt>.

³⁸ Barry M. Liener et al., "A Brief History of The Internet, Version 3.31" Internet Society Web Page, 4 Aug 2000, n.p.; on-line, Internet, 25 May 2001, available from <http://www.isoc.org/internet/history/brief.html#Transition>.

³⁹ "ICANN Fact Sheet," Internet Corporation for Assigned Names and Numbers, n.p.; on-line, Internet, 25 May 2001, available from <http://www.icann.org/general/fact-sheet.htm>.

⁴⁰ Minar and Hedlund, 5

⁴¹ Ibid., 9.

where client computers may need to send large quantities of information just like the "heavy-lifting" servers.

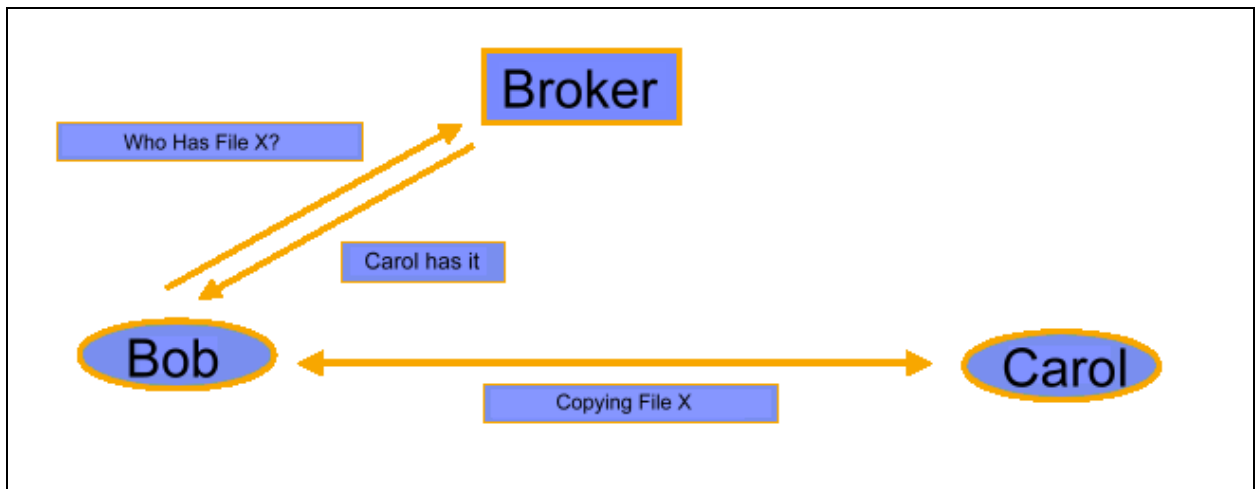
P2P Models

P2P technology can be divided into three major categories or models. These models are Broker, No-Broker, and Cycle-sharing. Depending on the application of the technology, these models may be combined to yield an optimal solution. Thus, the key components of each can be merged to best fit the situation in which it would be used.

Broker Model

The first P2P application to hit the Internet and receive widespread use was the music-sharing program called Napster. Written by a 19-year old college student, Napster instantly met a need and grew to over 40 million users in two years.⁴² The Napster concept is simple and perfectly illustrates the Broker model. When on-line and running the Napster program, users register their song files with a Napster server (www.napster.com). Napster then allows other users to query their server that serves as a central index of registered files. When a user is looking for a song, it queries the Napster central server to discover what other users, currently using Napster, have that specific song file. Armed with that information, the user is then free to link directly to the other Napster user and copy the song file directly from their hard drive. Napster is the Broker that provides visibility from the requestor to the source. (See Figure 3).

⁴² Shirky, "Listening to Napster," 27.



Source: Adapted by author from original by Bob Knighten, "Peer to Peer Computing," briefing to Peer-To-Peer Working Group, 24 August 2000, 13; on-line, Internet, 11 October, 2000, available from http://www.peer-to-peerwg.org/downloads/collateral/200008_IDF/PtP_IDF.pdf.

Figure 3: Broker Model

While not completely decentralized, Napster combines just enough centralization to get the job done. Once users become aware of each other, Napster shifts control of the file transfers to the users. Each user had access to gigabytes of songs and was virtually connected to thousands of other users. For example, while writing this paragraph, the author logged onto Napster and had instant access to over 7,000 users hosting over 1.5 million song files (6,588 Gigabytes).⁴³

There are three dominant strengths of the broker model. First, the central server index minimizes search traffic to find a specific file. With the central server, users only need to query one source rather than searching through all of the users on the network. Second, the broker provides some level of accountability by forcing users to register their files on the central server. Finally, the central server can function as the most up-to-date source for information and when new information becomes available, only one index must be updated.

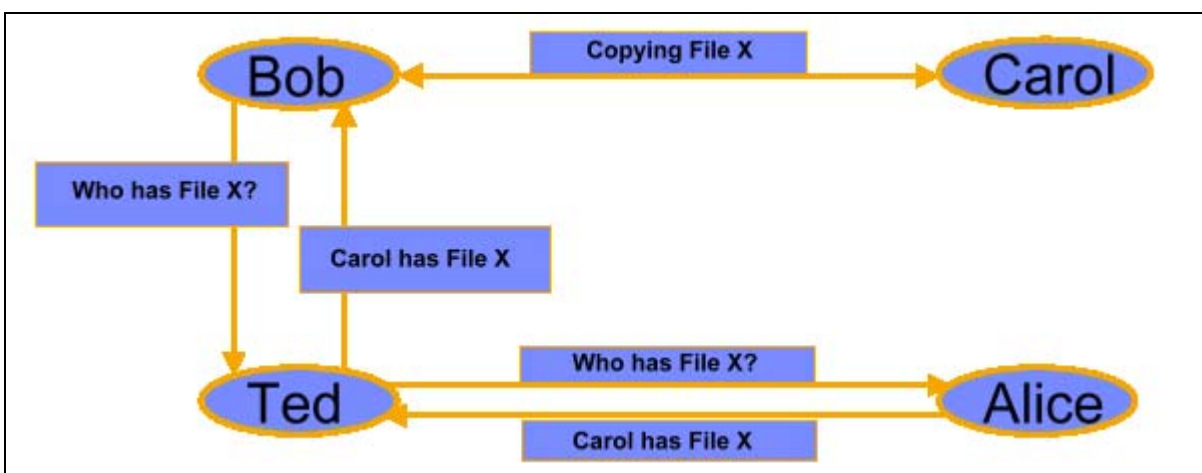
The primary weakness of the central server mirrors its primary strength—centralization. With a central server or servers to make the entire system work, it is certainly vulnerable to physical or information attacks. In the case of Napster, it is also vulnerable to legal attacks as

⁴³ The first draft of this paragraph was completed in January 2001. Because of RIAA's successful lawsuits against Napster in the Spring of 2001, the number of files shared on Napster

shown by the RIAA's successful lawsuits that forced Napster to filter out unauthorized songs from their "index." Another way to think of the central server is as a "single-point of failure." Thus, if it were disabled, the entire system could be rendered inoperable. However, this weakness in no way invalidates the power of the Broker model concept that decentralizes the file-sharing task.

No-Broker Model

The no-broker model overcame the most significant limitation of the broker model. In the no-broker model, there is no central server to provide the "index" to all of the other users. Here users register the files that they want to share with their network neighbors. If someone is looking for a file, they ask their neighbors if they have it, or if they know someone who does. That request is propagated throughout the network until the file is found. When found, the requestor is linked with the owner and the file transfer is enabled. (See Figure 4).



Source: Adapted by author from original by Bob Knighten, "Peer to Peer Computing," briefing to Peer-To-Peer Working Group, 24 August 2000, 14; on-line, Internet, 11 October, 2000, available from http://www.peer-to-peerwg.org/downloads/collateral/200008_IDF/PtP_IDF.pdf.

Figure 4: No-Broker Model

A prime example of a decentralized network is the Gnutella network. Developed in 14 days in early March 2000, the Gnutella protocol overcame the central server drawbacks of

have dropped significantly. In May 2001, the author had access to only 72,747 files (256 Gigabytes)—an over a 90 percent drop in songs available on one Napster server.

Napster.⁴⁴ "More than just a software program, Gnutella is really an internet built on top of the Internet."⁴⁵ As users connect to the Internet, they link-up with other Gnutella users and the network is then created. As each node connects, it brings some network capability which is instantly integrated into the fabric of the network at large.⁴⁶ Thus, the physical infrastructure of wires and routers doesn't change, but which wire and routers participate in the network changes by the second. This makes it a dynamic virtual infrastructure built upon a fixed physical structure.⁴⁷ The Gnutella network expands as more nodes connect to the network, and, likewise it does not exist if no users run Gnutella nodes.⁴⁸ In Gnutella, every machine in the network is connected to every other machine and no single node is responsible for distributing all of the content. So, if one machine goes down the network is unaffected, because all the other machines are connected to each other through multiple redundant connections.⁴⁹ Another way to think of Gnutella is like a bucket brigade. "Messages are relayed by a computerized bucked-brigade which forms the Gnutella network. Each bucket is a message and each brigadier is a host. The messages are handed from host to host willy-nilly, giving the network a unique interconnected and redundant topology."⁵⁰

For example, assume that a user is looking for a recipe for strawberry rhubarb pie. Once connected to the network, the user asks its immediate neighbors if they have the recipe. If so, a positive reply is sent to the requestor. Just in case other users might have a better recipe, the user's request is also forwarded to the other nodes in the network. Thus, a large portion of the network is canvassed and many replies are sent to the requesting user.⁵¹ With dozens of recipes to choose from, the user then chooses which recipe he wants and then downloads it from the other users.

There are three strengths of the no-broker model. First, the distributed nature of the

⁴⁴ Kan, 95.

⁴⁵ Ibid., 100.

⁴⁶ Ibid., 107.

⁴⁷ Ibid., 97.

⁴⁸ Ibid., 100.

⁴⁹ "What Is Gnutella," *Free Peers Inc.*, 2001, n.p.; on-line, Internet, 25 May 2001, available from <http://www.bearshare.com/gnutella.htm#whatis>.

⁵⁰ Kan, 104.

⁵¹ In Gnutella, there is a concept of a horizon. Rather than repeat a request across the network forever, each request is limited to seven hops. Typically, a seven-hops canvasses about 10,000 nodes. (Kan, 110).

network makes it very hard to stop. Without a centralized server (broker) that could be physically, informationally, or legally targeted, it is virtually impossible to shut down such a network. As Thomas Hale, CEO of Wired Planet, said, "The only way to stop Gnutella is to turn off the Internet."⁵² Second, the no-broker model is designed to operate with transient connections. This more-accurately reflects the way users connect and overcomes one of the significant limitations of the server side of the client-server model that operates best with always-on connections. Third, one of the unanticipated benefits of the no-broker model may be a more intelligent search capability. Traditional search technologies apply only one intelligence to the body of data they search.⁵³ With Gnutella, for example, each node interprets a user's request differently, which may result in a "richer" set of responses to a specific query. For example, if a user enters "MSFT" each node may return a different type of answer based on how it interprets the request. In this case, a financial node may return Microsoft's current stock price. A news node may return a list of news stories mentioning Microsoft. Or, a clip-art node might return a graphics file with the Microsoft logo. Thus, the no-broker model has significant strengths that make it a unique capability in the peer-to-peer domain.

The weaknesses of the no-broker model stem from its lack of a central server. The "willy-nilly" nature of its searching function makes it inefficient relative to the straightforward broker model. For a no-broker system, a standard search requires high traffic to query the connected nodes. As more nodes connect, more queries are routed throughout the network. This can lead to saturation and an overcrowded network. Second, given the transient nature of the network, sources of information (nodes or hosts) that were "there" the last time a user logged on, may not be available the next time. This drawback relates directly to the ad-hoc nature of the no-broker network. This ever-changing topology of the no-broker model can be major problem if only one node contains the information that a user desires.⁵⁴ Third, many of the commercially available no-broker applications build anonymity into their systems. While this may be a benefit to information providers who wish to remain anonymous, users generally evaluate the validity of information by knowing who is providing the information to them. Thus, in many cases, anonymous information transfer is a weakness rather than a strength. Overall, the no-broker

⁵² Kan, 99.

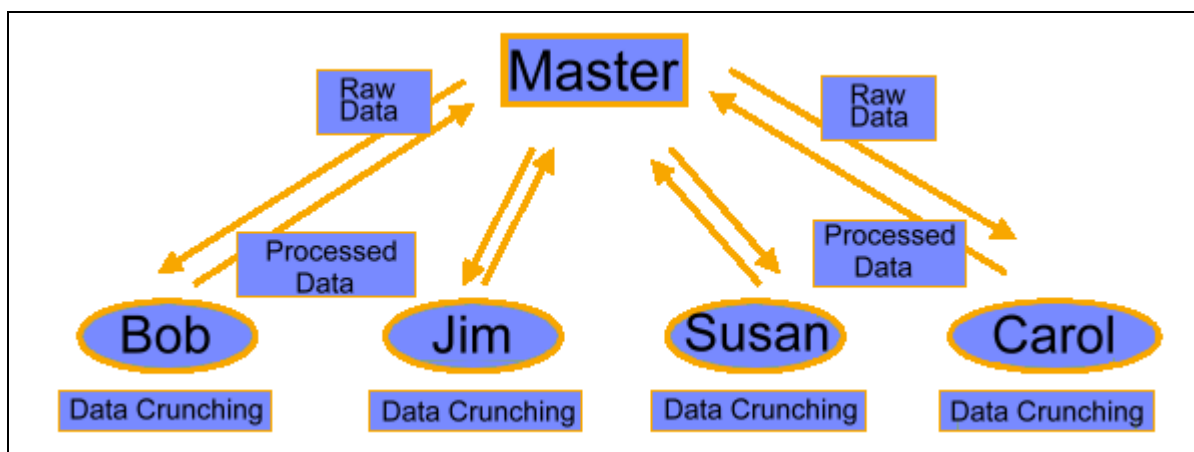
⁵³ Ibid., 103.

model offers some promising capabilities especially by providing a infrastructure for transient nodes to interact directly through a virtual dynamic network.

Cycle-Sharing Model

The cycle-sharing model offers another promising application of P2P technology by taking advantage of unused computing power connected to a network. Some estimate that only 5% of the average desktop's computing power is used. This is a huge, untapped processing resource that is just beginning to be exploited. Super-computing power is available by linking many computers together, over a local area network, or even the Internet. Many companies are taking advantage of this capability by taping the power of the PCs through their corporate LANs.

The cycle-sharing model lends itself to solving problems that can be broken down into smaller chunks that can be distributed to different computers and then recombined. Normally, a master server distributes raw data to each processor on the network. Each processor "crunches" the data and returns its results (or processed data) to the master server. (See Figure 5).



Source: Bob Knighten, "*Peer to Peer Computing*," briefing to Peer-To-Peer Working Group, 24 August 2000, 15; on-line, Internet, 11 October, 2000, available from http://www.peer-to-peerwg.org/downloads/collateral/200008_IDF/PtP_IDF.pdf.

Figure 5: Cycle-Sharing Model

⁵⁴ This would also be a problem in the Broker model if only one node contained the needed information and that node was not available when the user requested that needed information.

The most visible example of the cycle-sharing model is a cycle-sharing program called SETI@Home developed by a team at the University of California, Berkeley. SETI, the Search for Extra Terrestrial Intelligence, uses data from radio telescopes around the world to search for evidence of extraterrestrial life. SETI@Home provides a screen-saver and program that runs on a users computer and processes data that is collected from a 1000-foot aluminum dish radio telescope in Arecibo, Puerto Rico.⁵⁵ The raw data is shipped to the University of California, Berkeley and divided into "work units" that are distributed to users around the world who run the SETI@Home. These users donate their machines' idle processing time to search small chunks of radio telescope data for patterns that might signal intelligent life elsewhere in the cosmos.

How powerful is such a system? Scientific computations are measured in units of floating-point operations. A common measure of supercomputer speed is trillions of floating-point operations per second (TFLOPS). The fastest supercomputer currently available is the ASCI White built by IBM for the Department of Energy. It costs \$110 million, weighs 106 tons and has a peak performance of 12.3 TFLOPS. SETI@Home processes about 20 TFLOPS at less than 1% of the ASCI White cost.⁵⁶

When the first SETI@Home client software was released in May 1999, over 200,000 users downloaded and ran the client software.⁵⁷ By October 2000, SETI@Home had received over 200 million results which may be the largest computation ever performed. Today, SETI@Home has over 2 million users that donate processing time to the SETI project.

Computing power is not the only benefit, since the costs are much lower than buying supercomputers. Corporations like Intel, Boeing, and Pratt & Whitney, among others, take advantage of this cycle-sharing model. Intel figures it has saved \$500 million in hardware costs over ten years by using such a system to design its next generation computer chips. J.P. Morgan is using cycle-sharing to simulate trades in interest rate derivatives on 250 PCs in its London offices. Boeing links up hundreds of computers around the world to calculate acoustic and electromagnetic effects on the fuselages of fighter planes when they are in steep angles of

⁵⁵ David Anderson, SETI@Home, in *Peer-To-Peer: Harnessing the Power of Disruptive Technologies*, ed. Andy Oram, (Sebastopol, CA: O'Reilly & Associates, Inc., 2001), 68.

⁵⁶ Anderson, 74-75.

⁵⁷ Anderson, 74.

attack.⁵⁸ All of these companies clearly see the financial and operational benefit of using such vast untapped computing cycles at the edges of their networks. However, it is important to note that not all problems lend themselves to distributed computing. Many problems have complex interdependencies that cannot be broken down into pieces.

Hybrid Options

The broker, no-broker, and cycle-sharing models can be combined to create new hybrids that maximize strengths and minimize weaknesses. For example, when the Gnutella network was in its infancy, the only way to find a Gnutella node was by word of mouth. However, users soon became frustrated by the difficulties of getting onto the network. Thus, a program called GnuCache was developed that served as a broker to help users find the rest of the network. This program combined the benefits of the no-broker model with the broker model.

Hybrid systems may also provide a layered Broker capability. For example, the open source community has cloned Napster-like software known as OpenNap. The Napigator program gives users statistical information about servers that are running OpenNap and allows users to link with the server of their choice. The user can then choose which server to connect with to join an OpenNap file-sharing system. Another type of hybrid system that might be promising is a layered cycle-sharing model where the master server might distribute raw data to client systems. These client systems may, in turn, serve as master servers (brokers) to allow file sharing between other clients for cycle-sharing between peers on a local network. The concept of hybrid or layered P2P systems is in its infancy, yet, there may be many possible configurations that would enable future capability.

Dominant Characteristics of Robust P2P Infrastructure

Clearly, P2P technology offers significant potential to revolutionize how data, information, knowledge and wisdom are gathered, processed and transmitted to, from, and between the edges of the network. However, implementation of P2P technology requires an infrastructure to bring these edges together in a coherent and productive way. Such an infrastructure would provide the standards and protocols that would enable P2P interaction.

⁵⁸ Bruce Upbin, "Sharing Power," *Forbes*, 27 November 2000, n.p.; on-line, Internet, 3 March, 2001, available from http://www.forbes.com/forbes/2000/1127/6614278a_print.html.

What would such an infrastructure need to provide to allow the full range of P2P functionality? Endeavors Technology recently released a first-order attempt to outline conceptually those necessary characteristics. Their white paper explored eight dominant characteristics of a P2P Infrastructure.⁵⁹ While these characteristics are not necessarily unique to a P2P infrastructure, P2P technology enables many of these characteristics to be deployed in unique ways that may lend flexibility and robustness. This section defines and explores the dominant characteristics that enable a robust P2P infrastructure and these dominant characteristics serve as the basis for analysis in Chapter Four where they are evaluated for their ability to improve the current TPED process.

Placement

The first dominant characteristic that a P2P infrastructure must provide is the ability for peers to place information. The idea of placement includes the ability to add information, search for information, and transfer information without altering its "type." It must remove obstacles that impede the free and seamless transfer of content and services from one peer to another. This would allow content to naturally migrate to where it is most needed and accessed. Given the transient nature of many peers, information destined for them must be held somewhere until they reconnect to the network. Thus, the infrastructure must allow for the "transparent introduction of 'intermediaries,' peers whose role is to cache or migrate content and service from the origin to the point of use."⁶⁰

In the military context, the placement characteristic allows virtually every user and sensor to place information into the "infosphere."⁶¹ This infosphere may be a combination of various

⁵⁹ This white paper serves as the basis for all of the dominant characteristics in this section. This paper was one of the only sources for conceptual thought on the subject of P2P available in the early Spring of 2001. Gregory A. Bolcer et al., *Peer-to-Peer Architectures and the Magi Open-Source Infrastructure*, White Paper, (Irvine, CA: Endeavors Technology, 6 December 2000) 7-11; Internet, available at <http://www.endtech.com/news.html>.

⁶⁰ Cache (cash): a special high-speed storage mechanism. Many ISPs employ cache servers to keep the most frequently requested web pages handy for quick retrieval when requested by a client. On a personal computer, it can be either a reserved section of main memory or an independent high-speed storage device. (Source: Zdwebopedia, Internet, available at <http://www.zdwebopedia.com/TERM/c/cache.html>); Bolcer, 8.

⁶¹ P2P may be an enabling technology for the Joint Battlespace Infosphere. This concept, originally described in the 1998 Scientific Advisory Board (SAB) report *Information Management to Support the Warrior*, is defined as "a combat information management system

disparate systems linked together through a P2P technology. Once linked, the concept of intermediaries could serve as "fusers" to aggregate and fuse data from multiple sources to present a comprehensive knowledge-centric view of the battlespace. One of the most radical capabilities that P2P technology brings is the transformation of control. The users or edge-systems control what information is placed rather than a centrally controlled hierarchical entity.

Security

Security is one of the most difficult problems that P2P technology must address. Thus, security must be foundational to any P2P infrastructure. At a minimum, a robust infrastructure should provide authentication (confirming the identity of a user), authorization (permission to access a network resource), confidentiality (usually through encryption), and data integrity.

This function is most important in the military context. In most networks, security is only as good as the weakest link. However, with security classification restrictions, the military will require a relatively robust authentication process to confirm the identity of a network user. With authentication confirmed, the next biggest challenge will be to encrypt the information while it is transiting potentially unsecure or even hostile nodes. In this case, a robust P2P architecture should allow the ability to evaluate the different nodes in the network for their "trustworthiness" and have the ability to remove nodes from the network who prove to be untrustworthy. This reputation establishing function is similar to interpersonal relationship building and is discussed in the security section below.

Sharing

P2P technology enables the sharing of information at the edges of the network in ways never before contemplated in the client-server world. However, sharing should be at the discretion of the content or service owner. The creator/publisher of a specific piece of information should have the ability to control what users see and use that information whether they are specific individuals, groups, or devices on the network. This characteristic would be modified by the

that provides individual users with the specific information required for their functional responsibilities during crisis or conflict." (Source: United States Air Force Scientific Advisory Board, *Report on Building the Joint Battlespace Infosphere, Volume 1: Summary*, SAB-TR-99-02, 17 December 2000, iii; on-line, Internet, available from <http://www.sab.hq.af.mil/Archives/1999/JBI/JBIExecutiveSummary.pdf>.)

security characteristic below. Four distinct forms of sharing should be supported by a P2P infrastructure:

- Computation and data storage. This should be shared to maximize the aggregate computing power and data storage power of the network nodes.
- Content. The ability to share content is foundational to any P2P network and gives value to the P2P concept. However, a robust infrastructure will support the sharing of metadata that may serve as a surrogate for the data itself.⁶² For example, rather than share a large graphic file across the network, a description of the file (metadata) may be all that is necessary until a user needs the entire file.
- Relationships. Relationships serve as the conduits for the exchange of information. Thus, the ability to share the relationships that one user or device has developed with another user or device must be supported by a P2P infrastructure. This might be simply a list of links that could be passed from one user or device to another. One example of relationship sharing would be the ability to share "buddy lists" between users or devices.
- Activities. Collaboration is one of the most powerful applications that P2P technology brings to life. The ability for teams of people, who are not co-located, to engage in complex cooperative interactions can be easily enabled by a P2P infrastructure. Since P2P technology can uniquely meet the needs of transient users or devices, users must be able to work independently off-line and then be able to reconnect on-line and share information with the rest of a team. The infrastructure should support the on-line and off-line work in progress and provide a seamless way to interweave both.

The concept of sharing is foundational to P2P technology usefulness in the military context. The sharing of computation and data storage, given a secure environment, could have tremendous impact in the near term. Without purchasing expensive, state-of-the-art systems every few months to keep up with current technology, local cycle-sharing and storage-sharing capabilities could equal or even surpass the newer systems. For example, consider the need to

⁶² Metadata: Data about data. Metadata describes how and when and by whom a particular set of data was collected, and how the data is formatted. Metadata is essential for understanding

process sensor data. A cycle-sharing application could be deployed on a local area network by tying older processors together to process sensor data for use by local commanders or analysts.

Content sharing could enable imagery files or intelligence reports to be shared with others on the network. Relationship sharing could allow the links that one peer (soldier, tank, unmanned aerial vehicle (UAV), satellite, guided bomb unit (GBU). . .) has developed to be shared among other peers. Thus, if a tank is destroyed that is serving as a peer to multiple other peers, the network would be able to reconfigure and absorb the relationships that the tank had developed. This ability to share links minimizes the impact of a node that is either isolated or destroyed.

Activity sharing is potentially one of the most fruitful near-term applications of P2P technology for the military environment. Most military activities take place within a team environment where people come together to plan or execute a military operation. P2P activity sharing allows this collaboration. With the shared information resident on each user's device, ad-hoc teams can establish and disestablish quickly and securely without the need for a central server.⁶³

In the far-term, the sharing characteristic could allow a UAV to link with a tank and a soldier and a pair of binoculars and even the sensor on a Guided Bomb Unit (GBU). This information could be shared real-time between sensors, analysts, shooters, and command centers. Other examples of sharing could enable battle damage assessment to be accomplished in near real-time by linking sensors directly to analysts and operators. Command and control could be distributed to self-synchronizing forces that would ideally be aware of each other's actions and intent. Thus, the sharing characteristic offers significant potential to multiply the effectiveness of military operations.

Governance

If content or service can be owned by the creator/publisher, then a P2P infrastructure should provide the creator/publisher with the ability to control who may use what, when they may use it,

information stored in data warehouses. (Source: Zdwebopedia, Internet, available at <http://www.zdwebopedia.com/TERM/m/metadata.html>).

⁶³ One of the leading companies providing P2P collaboration tools is Groove Networks. Groove is currently providing first-generation P2P collaboration tools to the Joint Staff and other government agencies. More information can be found at Groove's web site: at <http://www.groovenetworks.com>.

and in what manner. This concept of governance may range from simple support for distributed authoring to complex and elaborate digital rights management languages.⁶⁴

For warfighters at the tactical level, classified intelligence information is often limited to the stovepipe of its original collection-centric domain. The governance characteristic may allow intelligence providers to control who gets what information and thus enable sharing of information among users that have appropriate authentication and authorization. This would be especially useful in a coalition environment where different coalition partners have access to different information sources.

Access

Access will be one of the most fundamental principles of any robust P2P architecture. Any device, regardless of its source or capability, should have access to the network. This means that a Personal Digital Assistant (PDA) may be a peer to a high-powered server that may be a peer to a pager. The concept of access "demands that peers acknowledge the underlying differences of platform and negotiate with one another at a more abstract level—that of protocol and service. Homogeneity is the rule rather than the exception in peer computing."⁶⁵ Although the devices that are peered may have very different capabilities (bandwidth, processing power, memory, persistence of network communication), access captures the concept of embracing the differences and accommodating them in a systematic and uniform fashion. This will require an infrastructure that allows peers of very different capability and language to interact. Finally, access might mean that "larger, resource-rich peers routinely accommodate smaller resource-constrained peers by reducing their service expectations, transcoding content, or acting as proxies for service requests that exceed the capabilities of their less capable brethren."⁶⁶

Control

Control gives the ability to control any peer from any other peer, given the appropriate permission and access. For example, a cell phone may be used to adjust a home climate control system or a PDA may be used to test a remote pumping station. The P2P infrastructure should enable these types of transactions to take place in a way that is transparent to either user/device.

⁶⁴ Bolcer, 9.

⁶⁵ Ibid.

In the military context, the ability to control another peer may allow a platoon commander to control a UAV flying over his area. It may allow a ground unit to take terminal control of an incoming GBU. Certainly, this type of control would have to be subject to proper authentication and authorization. It would also need to be addressed doctrinally to ensure the most efficient use of military resources. Investigating these complex issues would be an appropriate focus for an in-depth warfighting and experimentation program.

Specialization

Access and control allow both the users and peers to specialize. This capability allows the user to specify what information he wants and how he wants it presented (personalization). From the peer's perspective it is the power to offer peer-specific content and services that differ from other peers (specialization). Ideally, a P2P infrastructure would allow a user to personalize his "space" and then take it with him to wherever he accesses the network (cell, PDA, desktop, laptop . . .). Furthermore, specialization will allow the actual user interface to be a peer. Specialization provides the infrastructure to allow the user to enjoy the power of choice and select the 'interface peer' that provides just the form of interaction that is desired on the device selected by the user.⁶⁷

For example, the future warfighting environment may require each warfighter to use a PDA in the battlespace. Each user will have different needs depending upon their position and responsibility. Thus, the ability to personalize a peer to provide the most accurate and comprehensive information tailored to meet the needs of the warfighter will be a powerful tool.

Stewardship

Stewardship encourages peers to seek assistance from other peers in the network. For example, a cell phone may forward the most difficult tasks to a larger, more-capable peer. "Stewardship relieves peers of the burden of providing all services to all peers, thereby permitting large classes of peers to specialize and simplify."⁶⁸ Theoretically, stewardship would recognize bandwidth and processing power limitations of neighbors and thus self-regulate to prevent bottlenecks or over-tasked peers.

⁶⁶ Ibid., 10.

⁶⁷ Ibid., 11.

Summary

The eight dominant characteristics of a P2P infrastructure—placement, security, sharing, governance, access, control, and stewardship—capture the most valuable and important concepts that should be present in any P2P infrastructure. Moreover, they expand the ability to conceptually understand P2P technology and its potential applications.

Promises of P2P Technology

P2P technology is a powerful capability that could potentially unleash countless computing cycles and expose virtually infinite amounts of storage space. However, as with any new technology it could be misused or create vulnerabilities if not implemented properly and with caution. The promises of P2P technology center on the distributed nature of the technology. This section will explore some of the advantages that P2P will bring in the near future.

First, the major advantage of P2P technology lies in its distributed nature. If implemented with adequate security, P2P overcomes one of the most significant disadvantages of the current client-server framework—the central server. By distributing the nodes, and the information resident on them, there is no single point of attack or failure. This is exactly the same strength of the current Internet, however, P2P technology distributes the information even further to the countless PCs and edge devices connected to the Internet.

Second, the ability of a P2P network to handle transient connections creates an ever-changing network topology that has no critical or central mass. It would be like trying to destroy a cloud. If a node is targeted and destroyed, the network can continue to operate without a hitch since it is designed to operate with nodes engaging and disengaging all the time. Thus, the only way to destroy such a network would be to target every node.

This concept is similar to ad-hoc mobile wireless cellular network technology that is currently being developed for Special Operations Forces. These forces require networks that can be rapidly deployed and that do not rely on any pre-existing infrastructure. Furthermore, given the mobile nature of SOF forces, the ability to maintain a constant network topology is impossible. Thus, the network constantly reconfigures and routes information dynamically rather than through any one primary information node.⁶⁹

⁶⁸ Ibid.

⁶⁹James B. Michael, "Ad Hoc Wireless Communications For Special Operations Forces (SOF)," Naval Post Graduate School, n.p.; on-line, Internet, 8 March 2001, available from

Third, one of the most powerful promises of P2P technology lies in the area of relationship creation. With P2P, the edges of the network can link directly and exchange information. Today, in the military context, tactical units at the edges of the network link through the use of the radio. Without the radio, coordinated maneuver, fires, and other battlefield operations are impossible. However, radio communication is primarily limited to voice communications. P2P technology would allow the transfer of data and information in addition to voice to any other peer in the network. Moreover, it would provide the ability to relay relationships with other battlefield entities. This relationship-relay would enable rapid network reconfiguration and could provide a battlefield commander with a much richer information environment to enable decision superiority.

Fourth, P2P technology is naturally focused and responsive to users. Rather than information pushed to the user from a provider who *thinks* he knows what the user wants, the user defines the information that they want and need and how they want it presented to them. Furthermore, applications must be simple to use and clearly value-added or users will not take the time to use them. Thus, competition between interface providers will drive user interfaces that present the clearest, most accurate, most tailorable and most timely picture with the simplest interface. In the commercial world, this competition would occur in the marketplace with interface providers competing for business. In the military environment, if edge-devices like PDAs become commonplace, there will also be competition to provide the most effective and valuable interface.

Fifth, P2P technology provides a means to save significant resources by taking advantage of the latent, unused computing power resident on a network. Much of the current hierarchical information flow originated because of the limited processing capability at the edges of the network. The edges simply served to relay information back to the more powerful nodes that could perform the processing functions. With the processing power that cycle-sharing brings, much of the processing could be accomplished at the edges of the network. In many cases this

<http://www.cs.nps.navy.mil/people/faculty/bmichael/cs4554/SOFNetwork.pdf>. Another example of such a mobile communications program is the Situational Awareness System sponsored by the Defense Advanced Research Projects Agency (DARPA). This system uses high-capacity, low-power radios linked together by a self-configuring network to keep soldiers connected with each other. Source: Leopold, George, "Darpa mobile project preps 'soldier's radio,'" EETimes.com, 21 March 2001, n.p.; on-line, Internet, available from <http://www.eetimes.com/story/OEG20010321S0049>. See <http://www.darpa.mil/ato/programs/suosas.htm> for more information.

may be closer to the users and eliminate or minimize the need for "reachback." By processing some information at the edges, only the processed information would need to be transmitted back to a central location. This might help minimize the impact of P2P technology on bandwidth utilization.

Sixth, P2P technology provides the ability to scale to meet the demands of users. One of the limitations of the client-server model is the central server (or servers) that holds the information. If many users try request information from that central server simultaneously, the server may become overloaded and unable to respond to any requests. Or, it will try to service all of the requests at the same time resulting in decreased service and speed for each user. Furthermore, the bandwidth pipe that connects the user to the server may also become overloaded resulting in the same detrimental effects. P2P technology may help overcome this limitation by distributing the information between many nodes (rather than just one node). If a central repository of information were necessary, another alternative provided by P2P technology would allow a central server to replicate itself on other nodes under its immediate control. The ability to scale to meet increased demand could allow the distribution of storage capacity to non-server entities like PCs or laptops.

Overall, the ability of P2P technology offers many promises that will be explored throughout industry. However, military applications of P2P technology may mirror the industrial applications or extend beyond the profit/loss model. In other words, specialized P2P applications may be needed for military use that would require government investment to meet the needs of users in the field. Field experimentation with various P2P technologies should yield significant insight into the P2P applications most relevant to operational and tactical users. Moreover, throughout history, when a new technology has been made available, the fielded forces often find a new use for that technology that was never anticipated in the laboratory.

Perils of P2P Technology

The biggest challenges facing P2P technology are anarchy (lack of a central, controlling server), bandwidth limitations, and security. Each of these challenges impinges upon the other with both negative and positive effects.

Anarchy

P2P technology fundamentally removes hierarchical control over information and cycle-sharing. First, with the no-broker model and each node operating independently and potentially going straight to each other node, the benefits of a centralized Broker were removed. This Broker could direct traffic and cut-off those nodes that were unproductive or damaging. Without a Broker, anarchy could lead to very inefficient networks. For example, if many nodes request the same information, each request is relayed across the network until sources are found. A Broker could simply point all of the users to the data without the "overhead" required for relaying multiple requests. Second, while giving freedom to each node to participate or not, it may also negatively affect the whole. Like the real world, "peer-to-peer communities depend on the presence of a sufficient base of communal participation and cooperation in order to function successfully."⁷⁰ Thus, if other nodes choose not to participate, or a sufficient number of nodes are removed from the network, the network could disappear or become bogged down with only a few nodes supporting it.

Bandwidth

P2P technology depends on sufficient bandwidth.⁷¹ The availability of relatively high bandwidth (broadband) providers combined with the increase in processing power and storage capacity fueled the current P2P mania. As a result, current P2P applications need lots of bandwidth and without it, they often break down ungracefully. There are a number of reasons for this limitation.

First, P2P depends upon a connection between peers and is limited by the quality of that connection. For example, if a dial-up modem is a peer to a high-speed server, and the limited throughput capabilities of the modem are not identified, then the modem could be expected to perform like a high-speed server and would be quickly overwhelmed. In this scenario, the

⁷⁰ Theodore Hong, "Performance," in *Peer-To-Peer: Harnessing the Power of Disruptive Technologies*, ed. Andy Oram, (Sebastopol, CA: O'Reilly & Associates, Inc., 2001), 205.

⁷¹ Bandwidth: The amount of data that can be transmitted in a fixed amount of time. For digital devices, the bandwidth is usually expressed in bits per second (bps) or bytes per second. The bandwidth is particularly important for I/O devices. For example, a fast disk drive can be hampered by a bus with a low bandwidth. (Source: Zdwebopedia, available at <http://www.zdwebopedia.com/TERM/b/bandwidth.html>).

network is only as fast as its weakest link. This is what happened with the early Gnutella network. Gene Kan, one of the Gnutella developers writes, "Early Gnutella software would obstinately maintain connections to nodes in spite of huge disparities in carrying capacity. The effect was that modem nodes acted as black holes into which packets were sent but from which nothing ever emerged."⁷² One fix to this problem is to build intelligently a network topology that has the fastest nodes at the center of the network and the slowest nodes at the edges. This was done with Gnutella by forcing high-speed nodes to disconnect those nodes that are bandwidth disadvantaged. This process created a virtual network control function and an ad-hoc backbone where, over time, the high-speed nodes migrated to the center of the network and carried the bulk of the traffic.

Second, the no-broker models, without the benefit of a central index, depend upon frequent query searches throughout the network. Each peer must repeat the query until the information is found, or the query times out. This repetition process consumes much bandwidth and can lead to traffic overloads that can slow down the network and its ability to meet requests.

Solutions to the bandwidth challenge are forthcoming. P2P technology is relatively immature and most proponents of P2P technology propose that with time, many of the current limitations will be overcome. Here are some ways that P2P applications are working to reduce the bandwidth demands of the technology.

One of the most promising ways to respond to the bandwidth challenge is to build a rich metadata function that lets users evaluate with confidence metadata rather than the file itself. For example, rather than passing a large image file over the network to each user, a much smaller metadata file would be passed. Each user could determine, by evaluating the metadata, if the image file would meet their needs. If so, then the image file could be passed. This would decrease traffic significantly. The biggest challenge will be encouraging metadata discipline by those who would expose information to the network.

Another way to respond to the bandwidth challenge is to duplicate the most popular files throughout the network. In this case, a given file could be hosted by 10,000 individual computers, eliminating the need to use precious bandwidth to access the one location that has the file. This is what many ISPs do today. They capture the most frequently used web pages so that they can serve them quickly to their subscribers. Freenet, another P2P application, also does this

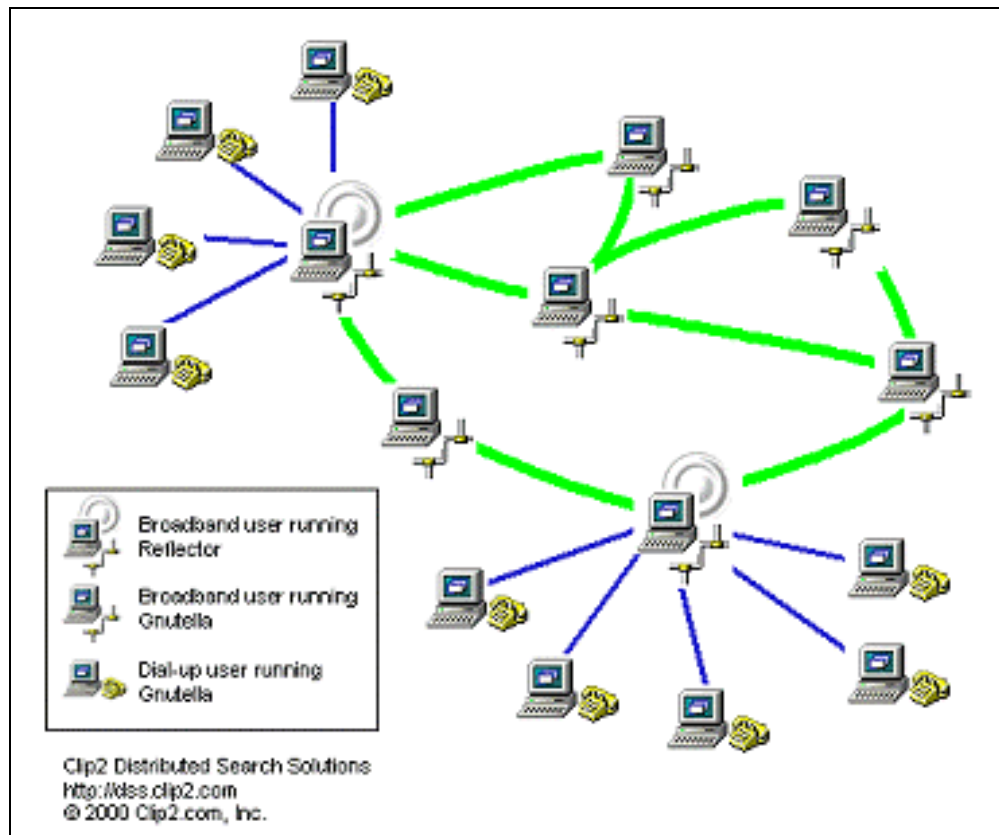
⁷² Kan, 108.

without the benefit of a central server. Freenet migrates the most-frequently requested information as close as possible to the people who routinely ask for it. Furthermore, its technology has enough information built in that requests can be routed almost directly to the place where the content is likely to be without having to search every connected computer.⁷³

Another solution to the limited bandwidth problem on the Gnutella network was the creation of "super peers" that remember results from other similar searches. Called "Reflectors™," these super-peers index file collections of nodes that connect to it and can subsequently serve as a proxy for these nodes and relieve them from much of the burden of traffic processing.⁷⁴ Thus, rather than repeat a common query throughout the network, and use bandwidth unnecessarily, initial responses can be relatively quick and thorough. (See Figure 6).

⁷³ John Borland, "Democracy's Traffic Jams," *CNET News.Com*, 26 October 2000, n.p.; on-line, Internet, available from <http://news.cnet.com/news/0-1005-201-3248711-2.html?tag=unkn>.

⁷⁴ Clip2, "Reflector Overview," *Clip2.com*, 4 January 2001, n.p.; on-line, Internet, available from <http://dss.clip2.com/reflector.html>.



Source: Clip2, "Reflector Overview," *Clip2.com*, 4 January 2001, n.p.; on-line, Internet, available from <http://dss.clip2.com/reflector.html>.

Figure 6: Example Gnutella Network Including Reflectors

Overall, bandwidth demand will be a continuing challenge for P2P technology. As bandwidth availability increases with the deployment of fiber-optic networks, demand will probably continue to increase even faster. However, within the military context, nodes on a military P2P network may be designed to be good stewards of the limited bandwidth that is available. Moreover, military forces could deploy with applications that already have the maps and key images loaded on the individual systems and thus would require only updates rather than complete information packages. In addition, limited short-range tactical bandwidth, that is currently used for voice, may be able to frequency-share to allow bandwidth for a P2P system. Furthermore, even in the short time since P2P technology became popular, various quick fixes have minimized the bandwidth limitation problem. It is reasonable to assume that as the

technology continues to mature, solutions to the bandwidth limitation problem will be more successful.

Security

Security is one of the biggest challenges facing P2P technology. With the client-server model, servers were the fortresses that held the data and, as a result, were the most valuable targets for attack. Most protection measures focused on protecting the servers from attack from outside the network. One of the most effective tools to prevent unauthorized access are firewalls. Firewalls "stand at the gateway between the internal network and the Internet outside. They filter packets, choosing which traffic to let through and which to deny."⁷⁵ They are very effective at protecting a network from attack by denying any entity outside of the network from initiating a connection to an entity inside the network. In other words, "a firewall is like a one-way gate: you can go out [to surf the web . . .], but you cannot come in."⁷⁶ However, they pose a serious obstacle to P2P models because P2P requires the ability to establish two-way sharing relationships with other nodes regardless of location.

On the web today, secure communications are encrypted between the server and the client using technologies such as Secure Sockets Layer (SSL).⁷⁷ Such encryption technologies are used for countless daily web transactions. Moreover, authentication processes are relatively mature to ensure that the server can be trusted.⁷⁸ For example, many companies maintain certificates with Verisign who serves as a reliable third-party and "vouches" for the reliability and trustworthiness of its certificate holders. Thus, the client-server model provides mature security functions to enable confident transactions.

The challenge for P2P technology is that virtually any device can be a server at some level. Since each peer is untrusted and it is difficult to easily confirm the identity of a transient node with any confidence, security becomes a much more difficult problem than in the client-

⁷⁵ Minar and Hedlund, 13.

⁷⁶ Ibid.

⁷⁷ Secure Sockets Layer: A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a private key to encrypt data that's transferred over the SSL connection. Source: "SSL," *ZDWebopedia*, n.p.; on-line, Internet, 24 February, 2001, available from <http://www.zdwebopedia.com/TERM/S/SSL.html>.

⁷⁸ Nelson Minar, "Security Issues of Peer-to-Peer Systems," Briefing, O'Reilly Peer-To-Peer Conference, San Francisco, Calif., 14 February 2001, 5.

server model. Moreover, the massive increase in nodes offered by P2P technology may make a network more vulnerable because there are more places to attack. Finally, with the "sharing" characteristic of a P2P infrastructure, viruses and other threats could be quickly and easily shared throughout the network. For example, in November 2000, McAfee Inc. sent out an anti-virus update file that crashed Windows PCs. If that corrupted anti-virus file been sent to a P2P network, the file could have proliferated exponentially faster.⁷⁹

At a minimum, P2P technologies must address the apparent vulnerabilities of a P2P network. The functions necessary to minimize security breaches are essentially the same as those necessary in any network environment. However, the implementation of security functions has some unique challenges in a P2P environment.

Security Functions

One of the most important functions of any networked system is its ability to authenticate the identity of the users. Authentication merely ensures that the individual is who he or she claims to be. Usually this is done with a username and password. However, with the transient nature of users and machines in P2P systems, a user may use multiple systems and multiple usernames to access a P2P network. Thus, the ability to authenticate becomes extremely difficult.

In response to this challenge, many P2P applications are working to develop a reliable reputation system. For example, eBay, the on-line auction site, allows buyers to comment on the quality of service that they received from sellers. Over time, sellers build either a good or bad reputation. This works well most of the time, however, if a seller begins to receive a bad reputation, they can just change their username and create a new on-line identity. The reputation and trust building concepts are still in their infancy.

Within the military context, the military will be distributing "Smart Cards" to all military and contractor personnel. These cards will also contain private keys for digital signatures and access authentication.⁸⁰ The ability to authenticate may also help determine priority for

⁷⁹ Dennis Fisher and Scott Berinato, "Making peer-to-peer secure," *Eweek*, 12 November 2000, n.p.; on-line, Internet, 15 March 2001, available from <http://www.zdnet.com/eweeek/stories/general/0,11011,2652477,00.html>.

⁸⁰ John Hamre, Deputy Secretary of Defense, memorandum to the Department of Defense, subject: Smart Card Adoption and Implementation, 10 November 1999. As of May 2001, the

information travelling through a P2P network. Certainly some information is very time critical and needs to be expedited across the network. With such strong authentication processes in place, P2P technology in the military context may offer some significant advantages over the industry context.

Another significant security function is authorization. Authorization determines which resources a user has permission to access based upon their authentication. This relates to the concept of governance that a P2P infrastructure should provide. With governance, the creator/publisher of the information can authorize certain users access to the information. A commercial company called Authentica has developed the ability to govern documents that are distributed by e-mail. For example, with Authentica a user can create a document, attach it to an e-mail, and determine when each recipients can read it and for how long. The recipient can only view the parts of the document that they are given specific permission to view. Furthermore, the ability to view the document can be revoked at the discretion of the sender.⁸¹ This capability illustrates the power that can be linked with specific authorizations in a P2P network.

Every user of a network needs to know that the information they are receiving has not been altered. This is known as data integrity. Furthermore, in many cases the information is confidential and must be protected from compromise. Common data integrity functions and encryption routines are used worldwide to provide a fairly high level of security. However, P2P technology may increase the vulnerability of the networked system. In an effort to quantify system vulnerability, the Army Research Labs states, "the likelihood exists that an individual vulnerability of one system in the architecture may in fact snowball and affect other systems that

Army has already started fielding Smart Cards in beta tests that will replace the standard military identification card. Such cards will enable the sending of digital signatures and encrypted e-mail. Source: George Seffers, "Army deploying smart cards," *Federal Computer Week*, 15 May 2001, n.p.; on-line, Internet, available from <http://fcw.com/fcw/articles/2001/0514/web-smart-05-15-01.asp>.

⁸¹ For more information see <http://www.authentica.com>. Many companies are now offering similar information control capabilities. Reliable Network Solutions also offers a similar capability. See http://www.rnets.com/product_overview.htm for more information. Another company working with government applications is the Texar Corporations s-Peer network security features. See <http://www.p2ptracker.com/news/releases/texar051501.htm> for more information.

are networked with that particular system."⁸² For example, consider the snowball effect of information that is collected by a UAV and then intercepted and manipulated by a hostile source. The manipulated information could then be spread throughout the network leading to erroneous targeting data. Thus, data integrity will be another critical function of any P2P infrastructure. The need to provide confidence in the integrity of the data residing on the network will be a paramount consideration.

Security functions will be necessary to provide authentication, authorization, data integrity and encryption. Without robust security functions, P2P technology is vulnerable to the same type of the informational attacks that currently plague the Internet at large.

Conclusion

Peer-to-Peer technology offers dramatic increases in computing power and storage space by empowering and linking the edges of a network. The broker, no-broker, and cycle-sharing models each offer unique capabilities and limitations. The advantages of a P2P network lie in its distributed nature and its ability to handle transient users and devices. Furthermore, linking the various models together may provide more capability than any one model on its own. However, P2P technology is not appropriate in all circumstances. The client-server model, which has served the Internet very well, is much simpler than P2P and it would not be wise to abandon the simple for the complex without a clear benefit.⁸³ Ultimately, a combination of P2P with the client-server model will provide the operational and tactical users with the flexibility and robust information architecture to enable decision superiority.

⁸² U.S. Army Research Laboratory, *Digitization and Survivability*, (Aberdeen Proving Grounds, MD: US Army Research Laboratory, 2000), 26.

⁸³ Andy Oram, ed., *Peer-To-Peer: Harnessing the Power of Disruptive Technologies*, (Sebastopol, CA: O'Reilly & Associates, Inc., 2001), 396.

Chapter 3

INTELLIGENCE INFORMATION FLOW

Future battlespace victory belongs to those who can turn data into information, information into knowledge, and knowledge into superior battlespace decisions. Having the information in our intelligence system doesn't do a thing for the joint warfighter if he can't act on it in time.

General Richard Myers
Address to National Reconnaissance
Office Senior Leaders Conference

Intelligence Information For The Warfighter

Decision superiority requires the right information at the right place at the right time. Today, the Intelligence Community (IC) provides much of the information that the warfighter needs to accomplish his mission. Encompassing a vast network of human assets, fleets of satellites, high altitude reconnaissance aircraft and sophisticated listening posts around the world, the IC focuses its energy to meet the needs of its consumers. With the increased complexity of today's world and the capabilities afforded by dramatic advances in information technology, these consumers demand more timely, accurate and actionable information than ever before.⁸⁴ As Bruce Berkowitz and Allan Goodman point out in their book, *Best Truth: Intelligence In The Information Age*:

⁸⁴ George Tenet, Director of Central Intelligence Annual Report for the United States Intelligence Community (Washington, D.C.: Central Intelligence Agency, March 2000) 1.

People have come to expect information on demand. They often prefer to be in direct contact with whatever sensor or human reporter is collecting information for them. If they cannot be in direct contact, they at least expect to know how their information is being gathered so that they can assess its credibility and accuracy for themselves, and so that they can make adjustments.⁸⁵

Another significant challenge that warfighters face today is the increased availability of information to future adversaries.⁸⁶ For example, commercially available, high-resolution imagery is now available over the Internet.⁸⁷ Thus, the US intelligence process must feed better information to the US warfighter faster in order to put us "inside the adversary's decision cycle."⁸⁸

To meet the ever-increasing demands from warfighters, the IC continues to pursue more advanced collection capabilities such as the Future Imagery Architecture (FIA).⁸⁹ While such a system will be a valuable addition to the nation's imagery collection capability, some studies indicate that additional effort should be focused on value-added systems and processes collectively known as "TPED"—the tasking, processing, exploitation and dissemination of intelligence information.⁹⁰ It is a responsive and dynamic TPED process that enables decision superiority and allows US warfighters to stay at least "one step ahead" of any future adversary.

⁸⁵ Bruce D. Berkowitz and Allan E. Goodman, *Best Truth: Intelligence In The Information Age*, (New Haven, CT: Yale University Press, 2000), 21.

⁸⁶ Craig Covault, "NIMA InfoTech Retools US Space Recon Ops," *Aviation Week & Space Technology*, 7 August 2000, 63.

⁸⁷ Vernon Loeb, "Spy Satellite Will Take Photos for Public Sale," *Washington Post*, Saturday, 25 September 1999, A03.

⁸⁸ Independent Commission on the National Imagery and Mapping Agency, *The Information Edge: Imagery Intelligence and Geospatial Information in an Evolving National Security Environment*, December 2000, 71; on-line, Internet, 16 March 2001, available from <http://www.nimacommission.com/>.

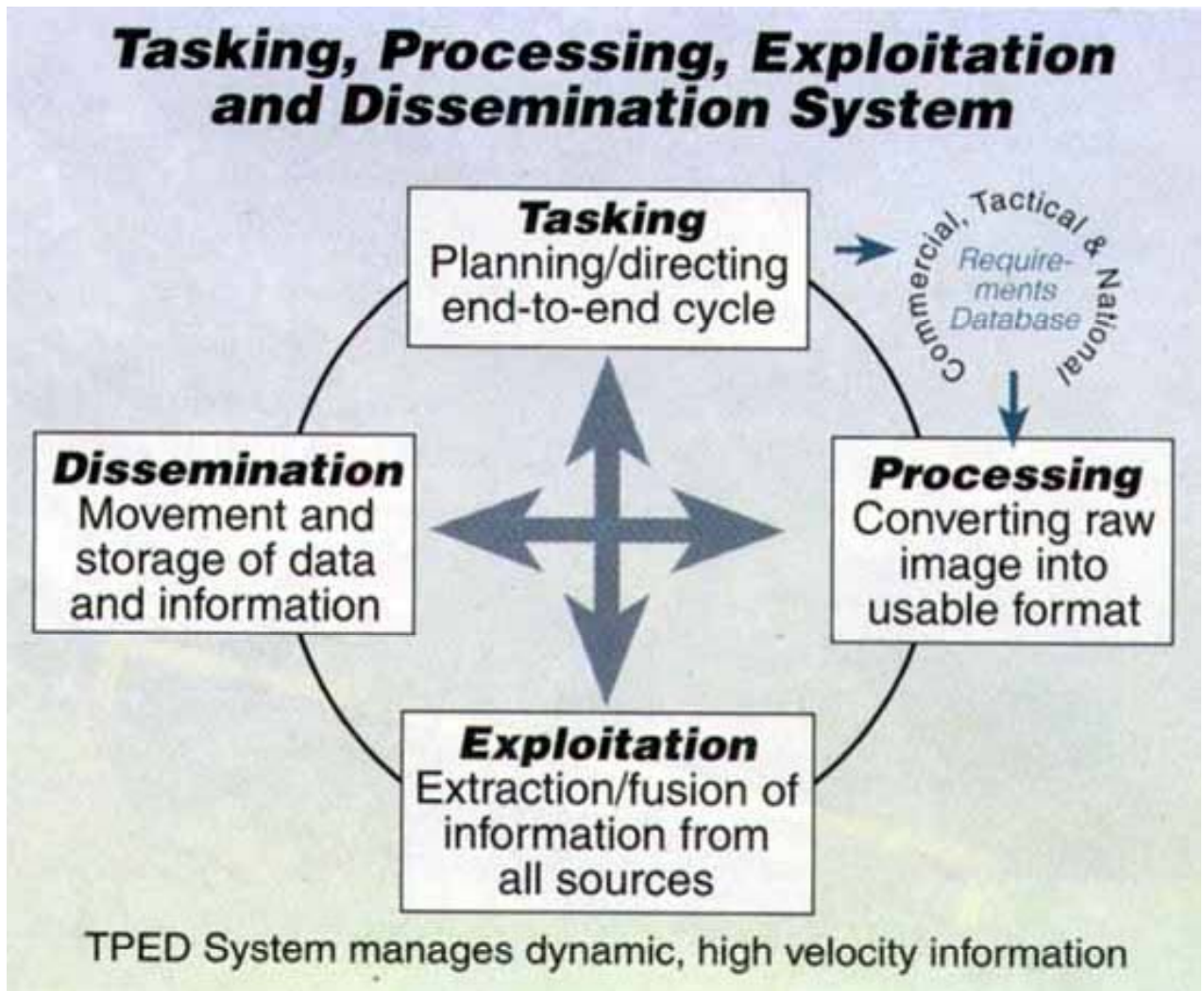
⁸⁹ More information on FIA can be found on the Internet at <http://www.fas.org/irp/program/core/fia.htm>.

⁹⁰ NIMA Commission Report, viii.

TPED Defined

TPED is an acronym that stands for Tasking, Processing, Exploitation, and Dissemination. It really captures the most important elements of the intelligence process and has evolved into a quick shorthand way to describe the "steps" that the intelligence community executes to provide knowledge to its consumers. For example, the TPED process for imagery would consist of "tasking" an imagery reconnaissance satellite, "processing" its raw collection, "exploiting" its processed collection take, and "disseminating" the resultant information products. (See Figure 7). As described, it seems like a relatively linear and serial process. It is not.⁹¹ However, TPED serves as a valuable way to categorize the tasks that add value to an intelligence collection system. Where other proposed constructs more accurately describe the value-adding process, they will be discussed in each section below.

⁹¹ Ibid., 72.



Source: Craig Covault, "NIMA InfoTech Retools US Space Recon Ops," *Aviation Week & Space Technology*, 7 August 2000, 62.

Figure 7: TPED Description

Tasking

Tasking is the value-adding process that ensures that the right information is collected at the right time. To put it simply, it is the process of collecting the right data. It may involve tasking a satellite to take a picture or maneuvering an Unmanned Aerial Vehicle (UAV) to a specific location and turning on its sensors to take a picture. Alternatively, tasking may simply require a database query to determine if the information desired has already been collected. In most cases, collection capacity (satellite, airborne reconnaissance platform, UAV) is a scarce resource and

understanding the limitations of the collection systems requires some significant technical expertise. Thus, there will always be a "corps of trained intermediaries" to allocate these scarce resources and provide the appropriate technical oversight of the collection systems.⁹²

An alternative term that may add more description to the concept of tasking is gathering. This term captures the idea of gathering information from multiple sources or an already existing database. It may also involve the concept of pulling apparently unrelated pieces of information together to produce a more accurate assessment.⁹³

Processing

Processing takes raw data that is produced from the collection assets and translates the data into information that can be understood by humans or automated systems. Processing is technically linked to the collection system and can be relatively well defined by the collection system specifications. For example, some collectors may have the ability to process the raw data "on-board" and provide an exploitable product. In other cases, the processing may be done at a "down-link" site or even transmitted to a central location for processing. If this ability to process raw data is automated, the "processing" part of TPED can be virtually transparent to the exploiter that needs to evaluate the information.⁹⁴

An alternative term that may be more descriptive is creation or fusion. This term captures the idea of a multi-sensor view rather than a single-sensor view. By combining multiple sensors raw data, a new view of the battlespace may improve the ability to exploit the information.⁹⁵

Exploitation

This element of the TPED process requires human or intelligent interaction with the data. It comprises all those value-adding activities that transform information into

⁹² Ibid., 72.

⁹³ Ibid., 72.

⁹⁴ Ibid., 73.

⁹⁵ Ibid., 72.

knowledge.⁹⁶ Exploitation often takes place within two domains and can be highly collaborative process. The first domain is the single-INT domain such as imagery, signals, or human intelligence exploitation.⁹⁷ For example, an analyst may exploit an image by adding information from other imagery sources. The second domain is in the multi-INT domain where analytical collaboration can take place across INTs.⁹⁸ This type of exploitation may take an image and add information from signals or human intelligence to provide a more comprehensive and accurate representation of the battlespace.

An alternative term that may capture the essence of exploitation is analysis. Analysis captures the varied disciplines and value of experience that would add value to the information.⁹⁹

Dissemination

Dissemination refers to the process of storing and communicating the knowledge to the consumers. It is the process of making the right information available to the right place at the right time. One of the most challenging aspects of the dissemination element is deciding "what information goes where."¹⁰⁰

An alternative term to dissemination could be sharing. Sharing information could be a many-to-many model where information is shared in a more open forum rather than dissemination's one-to-one model of data movement.¹⁰¹

⁹⁶ Ibid., 74.

⁹⁷ The term "INT" is used to refer to a certain type of intelligence information. SIGINT is signals intelligence, HUMINT is intelligence collected by humans, IMINT is imagery intelligence, and MASINT is intelligence of the measures and signatures of objects. (Source: Berkowitz and Goodman, 47).

⁹⁸ The concept of a two-domain collaborative environment came from an interview with Mr. Keith Hall, Director, National Reconnaissance Office, interviewed by author, 22 February 2001.

⁹⁹ NIMA Commission Report, 72.

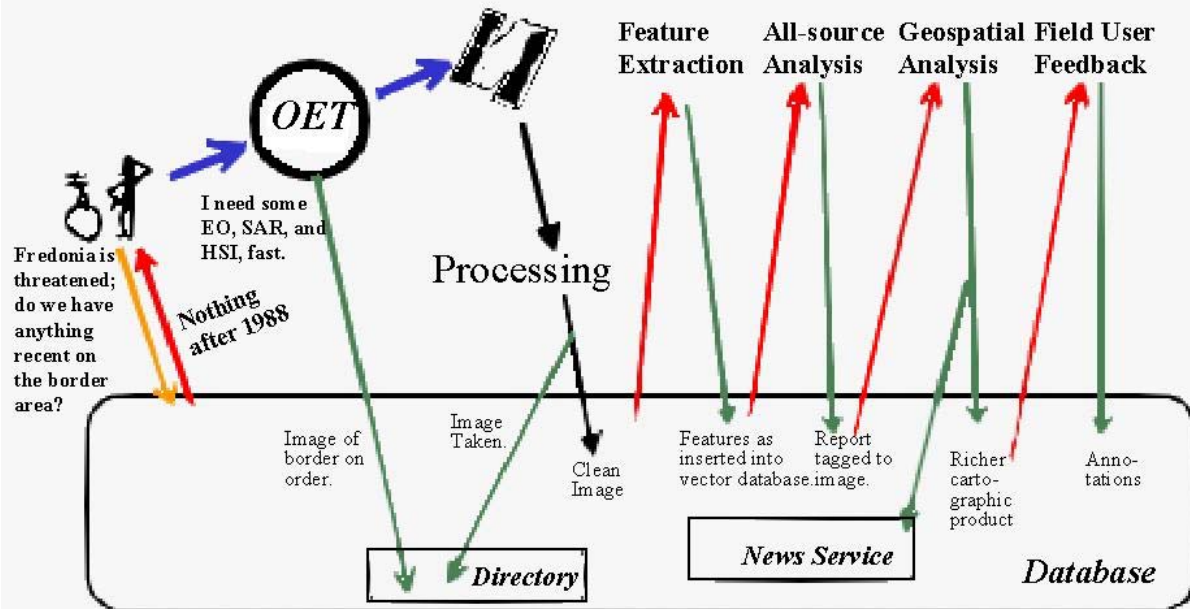
¹⁰⁰ Ibid., 74.

¹⁰¹ Ibid., 72.

Linear or Cyclical?

Some argue that TPED connotes a more linear, assembly-line view of intelligence production, while others argue that in reality it is really a cyclical process that requires constant interaction between the elements. The NIMA commission proposed a new way of looking at the TPED process—as a series of transactions against a database. (See Figure 8). Either way, the demands of today's users are driving a more transparent process that involves the users in all stages of the TPED process to insure that consumers and warfighters get the information they need.

A Notional TPED as a Series of Database Interactions



TPED Can be Perceived as a Process of Continual Database Enrichment

Source: Independent Commission on the National Imagery and Mapping Agency, *The Information Edge: Imagery Intelligence and Geospatial Information in an Evolving National Security Environment*, December 2000, 105; on-line, Internet, 16 March 2001, available from <http://www.nimacommission.com/>. OET = Acronym used in the tasking process. EO = Electro-Optical Imagery. SAR = Synthetic Aperture Radar Imagery. HIS = Hyper-Spectral Imagery.

Figure 8: TPED -Database Transactions

Strengths and Weaknesses of the Legacy TPED Process

At least three major strengths marked the legacy TPED process that evolved throughout the Cold War. A hierarchical analytical system, specialized INTs, and highly secure systems and procedures were fixtures of the intelligence process.¹⁰² Such systems and processes were most appropriate for the threats faced during those years: a Soviet-style threat, where technology change was incremental and geared to the political process, a large institutionalized military threat, and weeks or months of strategic warning of any possible attack.¹⁰³ However, what may have produced such a successful intelligence apparatus then, may not be adequate to meet the demands of today's warfighters in a rapidly changing multi-polar world.

The hierarchical analytical system of the Cold War ensured that coordinated products reflected the consensus of the department or intelligence community. When the current organizational bureaucracies were created in the late 1940s, "information was scarce, expensive, and considered authoritative when provided by organizations with accepted credentials."¹⁰⁴ As a result, the traditional TPED processes and systems evolved to incorporate standard operating procedures like a standard coordination process. During the Cold War, these processes would sometimes take 2-3 weeks to produce a product. However, today's warfighters demand much quicker information within hours rather than days or weeks.¹⁰⁵ While these processes may have been (and may still be) appropriate in some cases, they are frequently inflexible when unusual requests or high-

¹⁰² Berkowitz and Goodman, 114.

¹⁰³ Ibid., 121.

¹⁰⁴ Ibid., 22.

¹⁰⁵ Craig Covault, 64.

priority analysis is needed. Thus, when something unusual came along, ad-hoc teams or task forces were quickly formed to address the new challenge.¹⁰⁶ In these cases, the hierarchical system gave way to decentralized, fluid processes to meet the time demands of customers.

During the Cold War, specialized INTs allowed analysts and technical experts to focus on one discipline to produce unique and ingenious intelligence products. As a result, analysts became experts in one area and only through the coordination process were products exposed to information from other INT domains. This strength was also reflected in a collection-centric mindset that may have been beneficial during the Cold War, but may be more of a weakness today. The director of the National Imagery and Mapping Agency, Lieutenant General King commented on this shortfall. He said, "we were collecting the imagery we needed, but we were not processing it, exploiting it or disseminating it in a manner that would allow our customers [such as the military services, the White House and State Dept] to achieve information superiority."¹⁰⁷ This collection-focused mindset within the IC led to congressional scrutiny on TPED as shown by the Senate Select Committee on Intelligence's statement, "the Committee has long been concerned that intelligence collection continues to outstrip analysis, and is troubled that funding for the latter remains woefully inadequate."¹⁰⁸

¹⁰⁶ Berkowitz and Goodman, 73.

¹⁰⁷ Craig Covault, 63.

¹⁰⁸ Senate, *Authorizing Appropriations For Fiscal Year 2001 For The Intelligence Activities Of The United States Government And The Central Intelligence Agency Retirement And Disability System And For Other Purposes*, 106th Cong., 2nd sess., 2000, S.R. 106-279, n.p.; on-line, Internet, 14 April 2001, available from http://www.fas.org/irp/congress/2000_rpt/s106-279.html.

Moreover, there was little interaction between consumers and analysts.¹⁰⁹ As a result, products were often standardized for the analysts without considering the specific needs of the consumer.¹¹⁰ Today, with the speed and reliability demands of the average user, cross-INT collaboration is vital to produce a well-rounded product that reflects information from all of the INTs. Furthermore, the ability to fuse information from multiple INTs could yield clues to adversary behavior and strategy that might otherwise be invisible when analyzing a situation from a single INT.

Finally, highly secure and compartmented systems were developed to channel intelligence information to its processing and exploitation locations. This required highly efficient methods to encrypt information and ensure the protection of the source. Many of these requirements still exist today. However, the threats are much different and the growth of weapons and information technology offers adversaries never-before capabilities to challenge U.S. leadership and its military forces. As a result, systems and processes will need to overcome existing security barriers to prevent unnecessary information delay.¹¹¹ For example, during Operation JOINT ENDEAVOR, "a brigade commander who had requested overhead imagery of his area complained that 'the system'

¹⁰⁹ The influence of the "Information Revolution" is reflected in the vernacular change from "consumer" to "customer" in many intelligence reports and process descriptions. Customer reflects a more user-focused effort rather than a collection-focused effort.

¹¹⁰ Berkowitz and Goodman, 72.

¹¹¹ If the goals of information advocates come to pass, it may be possible to get information too quickly. Information validity could suffer if information is provided too quickly without appropriate checks and balances. For example, multiple reports could be generated from an initial source that was invalid. Without confirming evidence from another source, to corroborate the original source, inappropriate or even disastrous decisions could be made. (Source: Author's interview with Mr. Hall). One solution to this challenge would be to provide the consumers with pedigree or genealogy on the information. This would give the end-users some ability to assess validity.

took 3 weeks to provide photographs that eventually turned out to be 6 months old."¹¹²

While such examples may be extreme, one contributing factor to such delay is the existence of security barriers. A C4ISR task force of civilian, military and contractor personnel traveled the Balkans in 1995, 1996, and 1999 to review C4ISR operations and recommend improvements. Major General (Retired) Robert Rosenberg noted one of the most significant problems was security barriers when he said,

We must redefine the Cold War security classification paradigm which so badly slows down the OODA loop with so many separate security systems, resulting in islands of computers connected by miles of sneaker nets, fat fingers and air gaps—to allow the flow of information electronically across the many stovepiped network centric systems and shared with our coalition partners . . . Only the "ultra secrets" should be behind such barriers—and not shared.¹¹³

Security of information and sources will always be a challenge, yet, the needs of the customers will demand more streamlined processes to give them the information edge over an adversary.

TPED processes need to adapt to the promise of information technology and its ability to offer decentralized, market-based, fluid processes that can to evolve to meet the demands of today's consumers of intelligence information.¹¹⁴ Fortunately, multiple efforts are on-going to streamline the TPED process and provide better and faster knowledge to enable decision superiority.

¹¹² Larry Wentz, ed., *Lessons From Bosnia: The IFOR Experience*, April 1998, Ch 10, n.p.; on-line, Internet, 17 March 2001, available from <http://www.dodccrp.org/bosch10.htm>.

¹¹³ Major General Robert A. Rosenberg, Retired, "Improved Application of Information To The Battlefield, Revisited," (White Paper, 1999), 3.

¹¹⁴ Berkowitz and Goodman, 122.

Encouraging Trends

The Intelligence Community has emphasized improving support to today's consumers by pursuing multiple projects to improve TPED and overall consumer responsiveness. As a result of congressional scrutiny, the National Imagery and Mapping Agency (NIMA) initiated a TPED modernization plan to "provide the infrastructure to execute the full spectrum of operations, from national pursuits through to the tactical level."¹¹⁵ One of the most significant recommendations of the NIMA commission focused on the need for an Extraordinary Program Office to help transition NIMA to a "data-centric web centric design."¹¹⁶ The Defense Intelligence Agency is leading an effort known as the Joint Intelligence Virtual Architecture (JIVA) to enhance information sharing with state-of-the-art collaboration tools and to improve the quality of intelligence electronic distribution specifically tailored to the requirements of the user.¹¹⁷ Although current JIVA efforts are focused on the client-server model, P2P technology may offer other capable models. Another promising development is NIMA's customer-focused United States Imagery and Geospatial Information System (USIGS). USIGS puts the customer at the center of its information cycle to provide dominant battlespace awareness.¹¹⁸ NIMA is also pursuing a capability similar to the Geography Network that

¹¹⁵ Federation of American Scientists, "Tasking, Processing, Exploitation & Dissemination (TPED) TPED Analysis Process (TAP)," n.p.; online, Internet, available from <http://www.fas.org/irp/program/core/tped.htm>. Further information on Senate Authorization of funding for the TPED Modernization Program can be found at http://www.fas.org/irp/congress/2000_rpt/s106-279.html.

¹¹⁶ NIMA Commission Report, 91.

¹¹⁷ Frederick Thomas Martin, *Top Secret Intranet*, 15 November 1998, Ch. 10, n.p.; online, Internet, available from <http://www.topsecret.net/chapter10.htm>.

¹¹⁸ National Imagery and Mapping Agency, "USIGS Architecture Framework," (Bethesda, Maryland: National Imagery and Mapping Agency, 23 June 1998), 1-12.

will allow users to access disparate geographic databases through a web portal.¹¹⁹ By linking intelligence information to geospatial objects, NIMA is working to build an information architecture to serve as the virtual repository for intelligence information to support all users. These are just a few of the many on-going efforts to improve the TPED process to benefit operational and tactical users.

As information technology continues to provide more benefits to customers, the IC TPED processes and systems will evolve to meet their needs. P2P technology may offer some promising capabilities to extend these benefits even further—to the operational and tactical warfighters at the edges of a network.

¹¹⁹ For an example, see <http://www.geographynetwork.com>.

Chapter 4

P2P Meets TPED

You can't just give them a computer . . . they'll use it!

Lieutenant General Lance Lord¹²⁰

Improving TPED With P2P Technology

This chapter seeks to answer the question of how P2P technology would improve the TPED process to benefit operational and tactical users. Armed with knowledge of P2P technology (Chapter 2) and an understanding of the TPED process (Chapter 3), this chapter will explore the potential benefits and drawbacks of P2P technology if deployed within the TPED domain. Consider a primary purpose of P2P technology—connecting the intelligent edges of a network (humans/sensors). The TPED process facilitates such interaction. Customers request intelligence and knowledge and exploiters (intelligence analysts) gather information from sensors and seek to meet the customer's needs. To put it another way, customers need information/knowledge (tasking and dissemination) and intelligence analysts use sensors and processing systems to produce the most accurate and timely information for the customer (processing/exploitation).

This chapter will explore the ability of P2P technology to improve the TPED process by looking at the major intersections between TPED and the three P2P models

¹²⁰ Lt Gen Lord's intent with this statement was to challenge those who argue against empowering people with new technology because of fears about tracking/managing the systems rather than acknowledging the operational benefits that come from deploying such technology. Source: Interview with author, 17 April 2001.

(Broker, No-Broker, Cycle-Sharing). Answers to the following four questions should expose the most significant benefits and drawbacks of P2P applied to the TPED domain. First, how well does each model apply to each element of TPED? For example, does it make sense to deploy the Broker model to improve Tasking? If so, why, and how would it improve the tasking process? Second, how effectively will P2P technology meet the needs of tactical and operational users? Third, what are the most significant dominant characteristics of P2P when applied to the TPED domain? Fourth, how easily could P2P technology be deployed for each element of TPED? Ideally, the answers to these four questions will reveal the most important benefits and drawbacks of P2P technology applied to TPED. Before exploring the applicability and effectiveness of P2P applied to TPED, it is important to note that P2P technology will require many other technologies to be effective.

Not Too Fast

Other technologies will mature and help P2P offer significant and tangible improvements to TPED for operational and tactical users. One of the most significant developments, the digitization of intelligence information, must happen before P2P technology can offer widespread benefit. NIMA's TPED initiatives take the first steps down the road by taking an "e-business" approach to build Web enabled or Web served information.¹²¹ In the near term, other significant technologies must become available for the deployment of P2P applications. For example, P2P requires sufficient bandwidth and computing power at each of its nodes. Without these, the ability of P2P to enable value-added interaction becomes severely limited and potentially counter-productive. The Gartner Group, a technology and research company anticipates a "Supranet" that will combine wireless, wired telephony, data, satellite, television, and radio networks.¹²² Another vital near-term technology to enable P2P applications is an advanced P2P search

¹²¹ NIMA Commission Report, 34. See also, Craig Covault, "NIMA InfoTech Retools US Space Recon Ops," *Aviation Week & Space Technology*, 7 August 2000, 63.

¹²² S. Hayward et al., *Beyond The Internet: The 'Supranet'*, Gartner Group Research Note COM-11-4753 (Stamford, Conn: Gartner Group, February 2001), 1; on-line, Internet, 21 May 2001, available from <http://www3.gartner.com/Init>.

application to give insight into the billions of files shared on user's storage media. Aids for human reasoning, such as Project Genoa by DARPA, are demonstrating the power of knowledge discovery, structured argumentation, and the importance of collaboration in enabling decision superiority.¹²³ In the far term, other technologies will help improve the effectiveness of P2P applications. Edge devices (PCs, PDAs, cell phones) will become more capable with the advancement of chip design for wireless devices and potentially even light-based computers that run at quantum speeds.¹²⁴ Intelligent search agents that can search the information domain for specific pieces of information could make P2P even more effective at meeting the information needs of its customers.¹²⁵ Progress is already being made toward these types of technologies with concepts like the Semantic Web and the DARPA Agent Markup Language.¹²⁶ Finally, multiple technologies will evolve to improve the capabilities of each part of the TPED process and thus improve the effectiveness of P2P technology. For example, advances in target recognition software and change detection software may help move some of the exploitation efforts back into the processing element of the TPED process.¹²⁷ With the advantage of these technologies, P2P becomes more powerful and offers increased applicability and effectiveness to benefit operational and tactical users.

¹²³ Defense Advanced Research Projects Agency, "Project Genoa Executive Summary," n.p.; on-line, 28 May 2001, Internet, available from <http://www.darpa.mil/ato/programs/genoa.doc>.

¹²⁴ Brian Bergstein, "Intel to Describe New Chip," *ExciteFor@Home*, 16 May 2001, n.p.; on-line, 17 May 2001, Internet, available from <http://home-news.excite.com/printstory/news/ap/010516/19/intel-wireless-chip>. See also "New Light-Based Computer Runs At Quantum Speeds," *Science Daily*, 16 May 2001, n.p.; on-line, 16 May 2001, Internet, available from <http://www.sciencedaily.com/print/2001/010515075526.htm>.

¹²⁵ The Central Intelligence Agency's Office of Advanced Information Technology is addressing the challenge of mining data from the Internet. They are using various software tools to gather information from audio, imagery, geospatial and other sources. For more information see Vernon Loeb, "Making Sense Of The Deluge of Data," *Washington Post*, 26 March 2001, A23.

¹²⁶ Tim Berners-Lee, James Hendler And Ora Lassila, "The Semantic Web," *Scientific American*, May 2001, n.p.; on-line, Internet, 29 May 2001, available from <http://www.scientificamerican.com/2001/0501issue/0501bern timers-lee.html>. For information on DARPA Advanced Markup Language see www.daml.org/.

¹²⁷ NIMA Commission Report, 105.

Applicability Test — One Size Does Not Fit All

When considering each P2P model (Broker, No-Broker, Cycle-Sharing) and their applicability to each part of the TPED process, it becomes clear that each model offers different functionality. Table 1 summarizes the most significant findings to be explored in this section.

Table 1. Applicability of P2P Models to TPED

	Broker	No-Broker	Cycle-Sharing
Tasking	Yes	Yes	No
Processing	No	No	Yes
Exploitation	Yes	Yes	No
Dissemination	Yes	Yes	No

Tasking

Tasking is the process of collecting the right data. It can be accomplished by either tasking a sensor (satellite, reconnaissance aircraft, UAV, etc.) or by querying a database. For sensor tasking of strategic assets (satellites, some reconnaissance aircraft) by operational and tactical users, centralized control is still necessary due to the limited number and strategic importance of some of the sensors. However, in the far-term, satellite and airborne sensors may become responsive to operational and tactical users. In such cases, tasking by such users may be applicable.

The only models that appear to have applicability to improve the Tasking element are the Broker and No-Broker models. Cycle-sharing offers little potential for improving the tasking process.

Broker. The Broker model would provide little functionality for sensor tasking. However, when tasking a database, the Broker model could yield a very powerful solution to improve user access to information. One possible application would be a Napster-like capability (NIMAster), where a Broker holds metadata on current intelligence information (IMINT, SIGINT, All-source reports, etc.). In this case, the actual intelligence information (files) would not be held by the broker, but would be distributed between different databases and among the many other users of the P2P application. A requestor could query the Broker that would provide visibility into which other users held the data that the requestor desired. The requestor could then download

the information from any of the other users or even from multiple users simultaneously (dissemination). A Broker could continually update its links to point users to the most reliable and accurate information. Furthermore, if the request could not be filled immediately, the Broker could monitor the status of a user's request and provide that status back to the user. This concept would be similar to current package tracking with FedEx or UPS where the sender can track his package from pick-up to delivery.

No-Broker. For tasking sensors, until networks advance to the point where sensors are peered with other sensors and users, the No-Broker model offers little functionality to operational and tactical users. However, in the future, if such robust peering networks emerge, the No-Broker model becomes very applicable. Consider a No-Broker Sensor-Info-Net consisting of a network of peered sensors and databases that share information and data between each other with no central node. It would be responsive to requests of users and could self-synchronize to meet the requests of users. For example, when a user requests information from one node of the Sensor-Info-Net, that node, if unable to meet the request, would forward the request to other nodes until the request is satisfied. This may require tasking sensors to collect additional information. One drawback of such a system would be the difficulty of providing the user with insight into the availability of information and the status of the user's request. This stems from that fact that no one node has insight into the status of the request until it is answered. Another use of the No-Broker model could allow one sensor to task another sensor to automatically refine information to improve accuracy.

For database tasking, the concept of a horizon (where a request only "hops" so many nodes before it is dropped) limits the near-term applicability of the No-Broker model. In this case, if the information requested were located at only one node, the request may never reach that node and the request would go unfilled although the information requested might be available.

Processing

Processing takes raw data that is produced from collection assets and translates that data into information that can be understood by humans or automated systems. The most applicable P2P model for processing is the Cycle-Sharing model.

Cycle-Sharing. The Cycle-sharing model offers significant computing power to process raw data and produce exploitable information. By capturing the latent computing power at the edges of a network, a cycle-sharing model could be deployed in many different configurations. For example, the cycle-sharing model could be used to process tactical sensor data on a local tactical network. In the near-term for security purposes, it would be most beneficial to deploy such a network behind existing firewalls. As the technology matures, cycle-sharing applications could be deployed to process sensor data throughout a military network. One of the drawbacks of the cycle-sharing model is the requirement to have many processors and robust links available. If the number of processors available or the reliability of the links drop, the ability to process sensor information drops as well. Thus, a tactical or operational deployment would need to consider the number of available nodes.

Exploitation

Exploitation is the value-adding process that involves human or automated agents to take the information produced by processing and turn it into knowledge. Ultimately, this process makes the information most valuable to a user or requestor. More than any other element of the TPED process, exploitation would benefit most from the collaboration of analysts at the edges of a network. P2P technology offers powerful tools to link such exploiters directly in an information-rich environment to improve the final exploited product. Both the Broker and No-Broker models are applicable to the Exploitation process.

Broker. The Broker model could be deployed to provide a central repository or directory of links to exploiters throughout a domain. For example, consider a specific target type that requires the expertise of several analysts to provide a comprehensive multi-INT product. By querying the Broker, an analyst could "virtually locate" other analysts that are currently working on similar products. The P2P Broker enables collaboration. In many ways, this would be similar to the current JIVA collaboration efforts except it would not require the central server to hold the exploitable information. A P2P broker would simply provide links and the information would reside on the edge devices. Such

an application could be deployed at multiple levels from the tactical to the operational to the strategic.

No-Broker. The No-Broker model would allow the quick formation of ad-hoc collaboration groups without the need for a central server. However, the challenge would be how to find other collaboration partners. This would require another process to provide a directory of approved and trusted collaboration partners. Telephone, e-mail and other means would be relatively simple ways to provide such a directory.

Dissemination

Dissemination refers to the process of storing and communicating knowledge to the customers. It is the process of making the right information available to the right place at the right time. Dissemination provides a significant domain for the use of P2P technology. The meteoric rise of Napster and Gnutella were driven by the ability of these programs to disseminate information (music, graphics, videos, etc.) quickly and easily to users worldwide. Similarly, both the Broker and No-Broker models can assist in the dissemination process. However, it is important to note that a primary advantage of P2P for users is the ability to pull information from continually updated intelligence databases. However, once a link is established, P2P may offer a "push" capability where exploiters could "push" information to users.

Broker. A Broker application to disseminate information closely matches the Tasking-Broker application when tasking a database. Reference the above Tasking-Broker section for more information.

No-Broker. The tasking process for a database tasking would allow a user to use a No-Broker model to query his neighbor for information. This query would be replicated throughout the network until the information is found. The dissemination process would facilitate the transfer of that information to the requestor. If the No-Broker infrastructure allowed copies of the requested information to be "cached" on each node as it is passed back to the requestor, the most requested information would be "closer" to the

requestor, and thus, more readily available to other requestors.¹²⁸ The drawback of the No-Broker model is data integrity. If the information is passed through several nodes on its way back to the requestor, it could also be altered by those nodes. Thus, the security functions of a No-Broker infrastructure would need to be designed to prevent data corruption.

P2P Applicability to TPED

As discussed above the three different models of P2P offer different benefits for each element of TPED. Any deployment of a P2P model requires sufficient bandwidth, computing power and security at the edges of a network. With the existence of such robust capabilities, P2P offers significant functionality to each element of TPED process to improve TPED value to operational and tactical users.

Effectiveness Test—Meeting the Needs of Operational and Tactical Users

Given the applicability of P2P to TPED, how will P2P technology improve TPED for the average operational or tactical user? In other words, how will P2P help the user improve his knowledge of the battlespace? The effectiveness of the different P2P models differs from the perspective of the operational or tactical users. For example, while a Broker application may benefit an intelligence analyst, the single-point Broker may be considered a vulnerability for the Company Commander. This section seeks to explore the effectiveness of each of the models described in the applicability section above.

To measure the effectiveness of the different P2P models, each model is assessed for its ability to provide responsiveness, simplicity and tailorability. In this context, a P2P/TPED model is responsive if it improves the speed and accuracy of a user's intelligence information requests. A P2P/TPED model is simple if it provides a user with relatively intuitive request capability. In other words, it should be easy for the user to get

¹²⁸ This "caching" function is fundamental to the Freenet P2P system. Source: Adam Langley, "Freenet," in *Peer-To-Peer: Harnessing the Power of Disruptive Technologies*, ed. Andy Oram, (Sebastopol, CA: O'Reilly & Associates, Inc., 2001), 124.

the information he needs.¹²⁹ Finally, tailorability refers to the ability to customize the user interface to meet the needs of the user. Tailorability could refer to both the requesting action and the receiving/displaying action. As each model is evaluated for its effectiveness, the dominant characteristics of P2P as defined in chapter 2, lend explanatory power to each model. Table 2 summarizes the most significant findings to be explored in this section.

Table 2. Effectiveness of P2P Models

Effectiveness of P2P Models for Tactical and Operational Users	Broker	No-Broker	Cycle-Sharing
Tasking	A Database or <u>local sensor:</u> Responsive Simple Tailorable <u>A Distant Sensor:</u> Not Responsive Simple Tailorable	Limited Responsiveness Simple Tailorable	N/A
Processing	N/A	N/A	Responsive
Exploitation	Responsive Simple Tailorable	Not Responsive Simple Tailorable	N/A
Dissemination	Responsive Simple Tailorable	Not Responsive Simple Tailorable	N/A

¹²⁹ This concept of simplicity comes from observing the popularity of Napster. Napster is easy to use, that is one of the reasons why it has been so widely accepted and used. Source: Clay Shirky, "Listening to Napster," in *Peer-To-Peer: Harnessing the Power of Disruptive Technologies*, ed. Andy Oram, (Sebastopol, CA: O'Reilly & Associates, Inc., 2001), 26.

Tasking

Given that the Broker and No-Broker models are applicable to the tasking element of TPED, how effectively would such models improve the TPED process for operational and tactical users? Consider that tasking involves either tasking a sensor or database to provide data or information.

Broker-Responsiveness. How would the Broker model be responsive to the needs of the users? When tasking a database or local sensor, the sharing characteristic of P2P technology makes significant amounts of information available to all users of a Broker network. As each exploiter or sensor "exposes" their finished (or unfinished) product to the broker, the information is instantly available to any user on the network. Furthermore, as different users copy the product, it is replicated throughout the network and can be copied from any other user. This makes the information widely available and responsive to users. The governance characteristic of a P2P model allows the exploiter to control access to information. In this case, the broker might serve as a "gate-keeper" to monitor users and authorize access to various products. This capacity is similar to the client/server model where the server holds the information. However, the difference with a P2P model is that the broker does not hold the final products, but may only hold metadata with pointers to the final products. Finally, in the case of tasking a local sensor, the control characteristic would allow a user to control a specific asset to collect data/information. For example, a company commander may need to control a UAV flying over his area of responsibility. A P2P model would allow a broker to facilitate the transfer of control of that UAV from one commander to another. Thus, a Broker model could provide a valuable and responsive link between users and the information and knowledge that they seek.

Broker-Simplicity. How would the P2P Broker model provide a simple means to task sensors or databases? The specialization characteristic would allow the user to fine-tune his tasking interface to most-efficiently request information from databases or sensors. Once customized, the interface would be relatively simple and intuitive to the user.

Broker-Tailorability. The specialization characteristic would allow a user to customize or tailor the display of information in a way that best meets his needs. This ability to tailor provides different functionality for different users. Different users may have

different needs for the same information. For example, consider the number of artillery shells fired by a friendly artillery unit. A Battalion Commander may want to know that information to determine which of his units is currently under heavy attack. A logistics officer may want the same information to determine if more materiel should be brought forward in the next few days. A medical officer may use the same information to focus medical attention and supplies. Thus, the specialization characteristics allows the tailoring of information to best meet the needs of the user.

In the case of tasking a distant sensor that has historically been centrally controlled (satellites, airborne reconnaissance assets, etc.), the Broker model would do little to improve responsiveness. However, if such tasking were necessary, the specialization characteristic of P2P would allow for a relatively simple requesting process and a tailored user interface. Furthermore, once a request for tasking has been submitted, the broker model may allow for insight into the status of the user's request. It may also allow the request to be met by other sensors outside of the user's direct control.

No-Broker. For a database tasking, the no-broker model would offer limited responsiveness to users due to the concept of a horizon within the no-broker model. As a result of this horizon, caused by a limited number of hops for a request, the request may never arrive at a source that can provide the requested information. Simplicity and tailoring can both be provided by the specialization characteristic of P2P technology.

However, to overcome the horizon concept, a hybrid Broker/No-Broker model could be deployed. In this case, a no-broker model at the tactical level could be combined with a broker model at the operational or strategic levels. In this case, responsiveness would be greatly improved by providing more assurance of linking the user with the most reliable or productive source. For example, consider a tactical deployment of a company of soldiers linked together with a no-broker P2P system. If information on a specific threat is needed that is not available from organic sensors, any soldier could "task" an operational-level Broker. The Broker could return the information and forward it to any one soldier who would in-turn relay the information through the No-Broker P2P system to the rest of the company.

Processing

The P2P model most applicable to processing is the Cycle-Sharing model. In this case, given enough processing power and networked bandwidth at the user's disposal, a user may locally process data from both local sensors and distant sensors (those historically under centralized control). For local sensors, a Company Commander may be able to process information for his organic sensors more quickly with less demand on a specific processor. For distant sensors, a Company Commander, using his latent network processing power might process data from satellites or airborne reconnaissance platforms if they down link raw data directly. However, this capability could be dangerous if the user does not have an organic ability to exploit the information. Thus, the Cycle-Sharing model could improve responsiveness for users. Finally, simplicity and tailorability are not applicable because processing is usually transparent to the users. However, if a user wanted to process data from distant sensors, the specialization characteristic of P2P technology enables a simple and tailorable interface.

Exploitation

Given that the Broker and No-Broker models are applicable to the exploitation element of TPED, how effectively would such models improve the TPED process for operational and tactical users? The exploitation element, like tasking and dissemination, involves those users at the edges of a network that add value to the information. Intelligence analysts add value to information to produce knowledge. Tactical and operational users take advantage of this knowledge to make better decisions. P2P offers a means to link the exploiters and users directly to collaborate in the production of interim or final product. P2P also offers a means for exploiters to link directly with other exploiters. Because of this link, the information/knowledge provided by exploiters should more accurately meet the needs of users than if that link did not exist.

Broker. If the Broker serves as a "trusted agent" to provide a directory of trusted collaboration sources, responsiveness to user needs improves. In this domain, the sharing characteristic enables such interaction. The placement characteristic allows virtually any information provider to "expose" information to the broker. Other information providers and exploiters could use this information to improve their products. The access and

stewardship characteristics allow a user with limited processing power or bandwidth to link with an exploiter that may have very high-power tools available. Finally, the specialization characteristic allows simple and tailorable user interfaces.

No-Broker. In the No-Broker model, the nodes may be constantly changing. Without a central broker to provide visibility to link users with trusted exploiters, the responsiveness of this model is unlikely to meet the needs of the users in the near term. This model could also be open to significant deception efforts if no other system exists to confirm the reliability of exploiters and users.

However, the No-Broker model would be very useful if the users that would normally collaborate were already cognizant of each other and had other means of communication (e-mail, radio, or telephone). In this case, a No-Broker application could be easily deployed on each user's device without the need for a central Broker. For example, intelligence analysts who know each other, have established trustable reputations, and the need to collaborate on a product, could quickly and easily link together in a "shared space."¹³⁰ Once linked, the interaction and secure sharing of information could yield better, more comprehensive products. Finally, the specialization characteristic would allow simple and tailorable user interfaces.

Dissemination

Dissemination is the process of actually transferring the information to the user. Unlike tasking which is a search to see if the information is available, dissemination refers to the process of storing and moving the "bits" to the requestor. A Broker model for dissemination would ideally allow users to pull information from multiple sources simultaneously. If the information resides in multiple locations, the user could choose which node (or nodes) he wants to pull the information from. However, like tasking above, dissemination in a P2P context enables "pulling" by the operational and tactical users. Intelligent agents and advanced search mechanisms could automatically aid in the pulling of needed information. However, once a link is established between users and exploiters, information could also be pushed to users. In this case, the specialization characteristic of P2P technology allows a user to customize both the pushed and pulled

¹³⁰ For an example of shared spaces see Groove Networks at <http://www.groove.net>.

information for simple display and tailored uses. Other benefits and drawbacks of the Broker and No-Broker models discussed in the Tasking section above also apply to dissemination.

Some Characteristics More Dominant Than Others

Through exploring the applicability and effectiveness of P2P technology on the TPED process, certain dominant characteristics play a more significant role in enabling edge interaction.¹³¹ While all of the dominant characteristics are necessary, some become more dominant when evaluated in light of TPED. In other applications of P2P technology, like command and control, other dominant characteristics may become more significant. This section discusses each dominant characteristic and its applicability to improving the TPED process to benefit operational and tactical users. In the TPED context, the most significant characteristic is security and the least significant is stewardship.

Security

Security is the most necessary characteristic for TPED applications of P2P technology. By providing authentication, authorization, encryption, and data integrity, this characteristic enables all of the other characteristics to function reliably. Without security, the system would be open to deception, data spoofing, denial of service, and other attacks that would make its ability to meet user needs virtually impossible.

Sharing

The sharing characteristic provides the real benefit of P2P technology to any endeavor. By enabling edges to connect directly, sharing makes it easy to gather

information, collaborate, cycle-share and develop a more comprehensive knowledge of the battlespace. Sharing breaks down stovepipes and can speed-up the processing, exploitation and dissemination elements of TPED. Furthermore, sharing can provide insight into the tasking process for users.

Specialization

The specialization characteristic allows users to personalize or customize their interface with their devices and the information. By customizing the interaction between the edges, more effective communication can take place and thus, potentially greater understanding and knowledge of the battlespace. This characteristic consistently makes the interfaces simple and tailorable to meet the needs of users.

Governance

This characteristic modifies the characteristic of sharing. It allows an originator or publisher to control who has access to what information. This will be a necessary characteristic in the compartmented world of intelligence information that is designed to protect sources and means. However, effective governance and security functions, will enable more sharing to take place with appropriate users. The interplay (or conflict) between sharing and governance will dominate the P2P deployment environment and will ultimately shape P2P's usefulness to users. For example, consider the need to protect sources of classified information. In an effort to protect such sources, intelligence information is compartmentalized so that only certain people with appropriate clearances can access that information. Compartmentalization is one way to govern information. The sharing characteristic runs counter to governance. Thus, as P2P technology matures and provides more robust security functions that enable governance, sharing information may become more fluid.

¹³¹ See chapter 2 for detailed descriptions of each dominant characteristic.

Placement

This characteristic, where any device, or peer, can place information, would allow value-adding contributions to databases and collaborative forums. Moreover, without this function, the concept of sharing is stripped of its value.

Access

Access allows virtually any device or peer to access other peers and the information necessary to carry out its mission. This characteristic enables peers to specialize and share information from any authorized source. Moreover, it would allow peer to peer tasking if necessary to improve battlespace awareness.

Control

The ability to control peers from other peers would be most applicable at the tactical level where a user would need to control another peer for tasking purposes. For example, a Company Commander may want to control a UAV to collect information in his area of responsibility. This characteristic enables that interaction.

Stewardship

The ability for one peer to assist another peer and be cognizant of its limitations will enable the entire P2P effort. It is the grease that keeps the information flowing without bogging down because of inefficient routing or inappropriate tasking.

Dominant Characteristics Explored

It becomes evident from the above analysis that each of the dominant characteristics is necessary to provide effective P2P functionality to operational and tactical users. However, deploying a P2P capability within the TPED context reveals the importance of some characteristics over others.

Implementing P2P

How easily could P2P technology be deployed to improve each element of the TPED process? Which combinations of P2P technology and TPED are most "ripe" for

deployment? This section will address each element of the TPED process to explore ways to deploy P2P to maximize benefit and minimize security risks. In virtually every case, it appears most prudent to start with small P2P deployments and expand to larger deployments as the capabilities and concepts become more robust. Furthermore, except for the exploitation case, it appears that Broker models are easier to deploy and offer more effectiveness in the near term. However, as the characteristics of each model become more clearly understood through experimentation and wargaming, hybrid options may prove the most valuable. To evaluate and determine the potential of P2P technology in the real world, any initial deployment of P2P should take place within secure environments such as Intranets or Virtual Private Networks (VPN).¹³² Table 3 summarizes the more significant findings explored in this section.

Table 3. Ease of P2P Implementation

	Near-Term	Far-Term
Tasking	Broker	No Broker
Processing	Cycle-Sharing	
Exploitation	No Broker Broker	
Dissemination	Broker	No-Broker

Tasking

To deploy a Broker model application with access to existing databases and information sources appears doable in the near-term. The Broker could be a server or servers that provide pointers to information resident in many disparate databases

¹³² Intranet: A network based on [TCP/IP protocols](#) (an internet) belonging to an organization, usually a corporation, accessible only by the organization's members, employees, or others with [authorization](#). An intranet's Web sites look and act just like any other Web sites, but the [firewall](#) surrounding an intranet fends off unauthorized [access](#). Virtual Private Network: A [network](#) that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the [Internet](#) as the medium for transporting data. These systems use [encryption](#) and other [security](#) mechanisms to ensure that only [authorized](#) users can access the network and that the data cannot be intercepted. Source: "Intranet" and "VPN," *ZDWebopedia*, n.p.; on-line, Internet, 20 April 2001, available from <http://www.zdwebopedia.com/TERM/i/intranet.html> and <http://www.zdwebopedia.com/>

throughout an enterprise (either single or multi-INT). To deploy such a capability on existing intranets or VPNs and behind protective firewalls would minimize the security risks imposed by exposing a P2P application to the Internet. Another option is the deployment of a broker application with pointers only to unclassified, open-source information.¹³³ The no-broker model for tasking would be more difficult due to the horizon limitation and the security challenges of constantly changing nodes.

Due to the relatively immature infrastructures available for P2P applications, deploying a Broker or No-Broker model beyond the protective walls of intranets, VPNs and firewalls could pose significant security risks at this point. However, the P2P infrastructure may mature quickly and provide the requisite security functions soon enough to expand P2P applications beyond a local deployment. In other words, the capability to deploy reliable and robust P2P applications may quickly move from the far-term to the near-term.

Processing

A Cycle-Sharing P2P application to assist with some processing operations also appears doable. While some data may not lend itself to a distributed solution, exploring the opportunities may yield significant savings and potentially free up limited processing systems for the more important tasks. Initially, it would be prudent to deploy such an application within existing firewalls without exposure to outside networks.

Exploitation

No-Broker P2P applications for collaboration are already on the market today. These applications allow the creation of "shared spaces" for secure collaboration without

TERM/V/VPN.html.

¹³³ Some estimate that "more than 80% of the data used by the intelligence community now comes from open sources. Even during the Cold War, George Kennan reflected recently, the vast majority of information U.S. policymakers required could have been obtained by analysts using such open sources as the nation's libraries, archives, and the media." Source: Bruce D. Berkowitz and Allan E. Goodman, *Best Truth: Intelligence In The Information Age*, (New Haven, CT: Yale University Press, 2000), 78.

the need for a central broker or server overhead.¹³⁴ These applications provide their own infrastructure and reside on each user's device. Furthermore, they can be tailored to provide tools with the most functionality for the user. However, the users must have another means of contact and trust verification before linking through the P2P application. As with all other P2P deployments, it would be prudent initially to deploy such an application within existing firewalls without exposure to outside networks.

Broker P2P applications could be deployed to link exploiters and users. The links provided by the Broker would provide a sense of trust by holding pointers to only those nodes that are available or are trustworthy. However, it appears that the No-Broker model, already available in the commercial marketplace, is preferable in the near term, especially if other means of connecting users (telephone, e-mail, message, etc.) can be provided.

Dissemination

The Broker application for dissemination would be most easily deployed in the near term by building a Napster-like application that would hold pointers to already exploited products. These products would ideally be located at many different nodes to enable the user to "pull" information simultaneously from different databases.

A No-Broker application for dissemination would require multiple nodes to support the No-Broker search mechanisms. Furthermore, the constantly changing node population combined with the concept of a horizon could limit its effectiveness by not giving users a complete picture of the information truly available. However, if databases were replicated throughout the network, a No-Broker application would become more viable.

Conclusion

As the above analysis shows, P2P technology offers significant potential to improve TPED to benefit operational and tactical users. Each model offers different functionality with the Broker model offering the most near-term benefit. However, in the

¹³⁴ For one of the most mature No-Broker P2P collaboration applications, see <http://www.groove.net>.

case of exploitation, a No-Broker model could provide valuable near-term functionality. The most "ripe" areas for development include: 1) the Tasking/Dissemination Broker model with a Napster type application (NIMaster) to provide users with the means to "pull" post-exploitation information and 2) an Exploitation No-Broker model with commercially available applications to facilitate collaboration between analysts and users and 3) a Processing Cycle-Sharing model to take advantage of latent processing power already deployed in current networks.

Chapter 5

CONCLUSION

Often the hardest part of adopting technology is simply understanding the potential opportunities a new technology offers.

Bruce Berkowitz and Allan Goodman
Best Truth: Intelligence In The Information Age

Peering Into the Future

Peer-to-Peer (P2P) technology offers operational and tactical users at the edges of a network unprecedented power. It offers them direct access to sensors, other users, information, and, ultimately, knowledge of the battlespace to enable decision superiority. As the foregoing analysis illustrates, P2P technology can improve the tasking, processing, exploitation, and dissemination process to benefit operational and tactical users. It offers a tremendous opportunity to bring greater situational awareness and decision superiority to users. However, like any new technology, P2P brings with it promises and perils, strengths, and vulnerabilities. The difficulty lies in the balance between risk and reward. One extreme would be to pursue the promises and ignore the perils while the other extreme would be to focus only on the perils and miss the promises.

Is the reward worth the risk? This brings one back to the challenges confronting strategic decision makers today—peacetime uncertainty. In the case of P2P technology, the true risk and reward is unknown today. Ultimately the only way to completely answer that question is to experiment and try it—put P2P technology through its paces and see if it can live up to its promise and improve battlespace awareness.

However, technology is only one small part of the changes necessary to bring about decision superiority. As US Joint Forces Command's proposal for a Common Relevant

Operating Picture states, "the success of future data collection and processing, information dissemination, and knowledge presentation depends on having the *right* people, in the *right* place, at the *right* time to ensure the application of this technology. Technology, by itself, is not the master of our future."¹³⁵

Consider the case of Germany early in the 20th Century. Just prior to the outbreak of World War II, the German army (Wehrmacht) developed an operational concept known as Blitzkrieg. A culture of ruthless experimentation and self-critical examination honed Blitzkrieg into a devastating concept that was unleashed at the beginning of World War II. As a result, the Nazi's dominated the European continent in relatively short order. At the center of the Blitzkrieg concept were tanks—a technology first developed by the British in World War I. During the inter-war period, the Wehrmacht borrowed concepts developed by British military theorists like J. F. C. Fuller and B. H. Liddell-Hart who suggested that mechanization would transform warfare. They argued that tanks would evolve into fast, heavily armed vehicles that could punch through enemy lines to encircle enemy forces. The British failed to develop their own blitzkrieg concept for many reasons. Some argue that the most significant reason was the British inability to abandon old dogma that tied the tanks to the infantry. In other words, "Until military leaders could let go of the old ideas, they could not take advantage of the new technology."¹³⁶ Thus, it was not technology that limited effectiveness, but culture. Like mechanized tank warfare, P2P technology, if adopted will require cultural, organizational, doctrinal, and other changes to be effective.

Culture, Doctrine, and Organization

The Information Revolution continues to drive change in the business community as well as the government. This technical revolution is moderated by many factors such as strategy, culture, policy, organization, doctrine, fiscal constraints, and strategic environment. Some of the most significant factors are culture, doctrine and organization. Culture change has ramifications that are even more significant in the intelligence community whose core business is information—the best information available. Moreover, it takes more time for culture change than technological change. As Retired Vice Admiral Tuttle postulated in a recent presentation to

¹³⁵ US Joint Forces Command Concepts Division, "A White Paper for The Common Relevant Operating Picture," (Draft White Paper, version 1.1, Norfolk, Virg., 21 April 2000), 1-0.

the Joint Military Intelligence College,

When a new age is entered, technology leads by two decades the organizational, policy, strategy, doctrinal, operational procedures and cultural changes necessary to exploit the technologies. The limiting factor in progress is not our ability to imagine the future or invent it, but our willingness to embrace it.¹³⁷

The intelligence community finds itself at the center of an on-going revolution as information technology transforms how information is collected, analyzed and disseminated. Specifically, the best information must be delivered in a way that meets the needs of individual users.¹³⁸ As the community attempts to transition from a Cold War mindset where users needed information in 2-3 weeks within a standard, well-defined process, to an information age mindset where users need customized, tailored information in 2-3 minutes, cultural change must occur. This challenges many of the Cold War organizational structures and intelligence processes because "no centralized planning can adequately anticipate mission needs, let alone identify and assess all of the alternatives for meeting them."¹³⁹ P2P technology offers a decentralized solution that may help take advantage of opportunities on the horizon.

Another challenge facing the intelligence community is how far to lower the security bar. Today's compartmented intelligence world was designed for a Cold War Soviet threat. While it may still be applicable in many ways today, such restrictions may handcuff the sharing of information to the detriment of the operational and tactical users. "Secrecy and deniability may be necessary for some intelligence operations. Even so, the aim should be to limit the requirements for secrecy and deniability to the lowest level possible."¹⁴⁰ Adoption of P2P technology may allow more sharing and less compartmentalization.

Doctrinally, P2P technology offers a radically different way to organize forces. By empowering the users at the edges—those truly at the front lines—the ability to centrally control such forces becomes extremely difficult if not impossible. Similarly, Heinz Guderian, commander of Germany's Panzer Forces enabled the Blitzkrieg concept by empowering each

¹³⁶ Berkowitz and Goodman, 59.

¹³⁷ Jerry O. Tuttle, "Decision Superiority and Intelligence," *Defense Intelligence Journal*, September 2000, 70.

¹³⁸ Berkowitz and Goodman, xi.

¹³⁹ Ibid.

¹⁴⁰ Ibid., 28.

tank commander with a primitive P2P device—the radio. Thus, just as the radio enabled the Blitzkrieg concept, P2P technology could lead to new doctrinal concepts.

Other concepts for future conflict that have been envisioned by theorists and strategists become possible with P2P technology. One such concept, Swarming, would benefit greatly from P2P technology. Swarming is "a deliberately structured, coordinated, strategic way to strike from all directions, by means of a sustainable pulsing of force and/or fire, close-in as well as from stand-off positions." It requires many small, dispersed, *networked* maneuver units. (emphasis added)¹⁴¹ Moreover, many of these doctrinal concepts cannot be anticipated in the laboratory. Operational and tactical users at the edges of the network that may get the most benefit from P2P technology will develop unanticipated doctrinal concepts.

Doctrine certainly informs organization. In many cases, "greater centralized control is exactly the opposite of what is desired to maximize the benefits of information technology."¹⁴² To meet the needs of those warfighters at edges of the networks, "the information-age military needs the shared information gathering advantages of a networked organization with the decentralized decision making advantages of a flattened hierarchical organization."¹⁴³ Experiments recently conducted during the Task Force XXI Advanced Warfighting Experiment showed that the structure and organization of units needed to be dynamic. In the experiment,

Addressing was implemented in a manner that forced users to operate in fixed organizational structures; not taking into account the necessity to move units across the structure of a network architecture. The network architecture of the digitized force must take into account the reality that individual missions will require commanders to dynamically change the structure and organization of their subordinate units.¹⁴⁴

¹⁴¹ John Arquilla and David Ronfeldt, *Swarming and the Future of Conflict*, RAND Report DB-311-OSD (Santa Monica, Calif: RAND, 2000), vii; on-line, Internet, 22 April 2001, available from <http://www.rand.org/publications/DB/DB311/>.

¹⁴² Lt Col Gregory A. Roman, "The Command or Control Dilemma: When Technology and Organizational Orientation Collide," Research Report AU/AWC/RWP198/96-04 (Maxwell AFB, Ala.: Air War College, 1996), vi.

¹⁴³ Ibid.

¹⁴⁴ U.S. Army Research Laboratory, *Digitization and Survivability*, (Aberdeen Proving Grounds, MD: US Army Research Laboratory, 2000), 31.

Thus, a myriad of influences must eventually conspire to bring about decision superiority. As always, technology will not be the limiting factor. "The greatest inhibitors to decision superiority are cultural and the resistance to share information and intelligence."¹⁴⁵

P2P and the Future

As P2P technology in the commercial world becomes more commonplace and takes its position with the client-server model in the information domain, the US government should take steps today to understand and leverage the capabilities that P2P technology brings. It is important to note that P2P technology offers benefits to many more domains than just the intelligence TPED process. Command and control, logistics, information operations and other network-orientated fields could benefit from this technology.

Although the technology is still immature, and various corporations are competing to produce an infrastructure to support P2P applications, it is never too early to begin thinking about the potential of this new technology. Some initial steps would include: 1) Conduct an in-depth analysis and review of P2P possibilities for TPED from a classified perspective, 2) experiment with P2P concepts and applications at US Joint Forces Command, and 3) train software developers and information operations personnel on P2P applications and their possibilities. Another fruitful area of research would be to consider how to counter an adversary who deploys a P2P system.

In conclusion, P2P technology is really about enabling people. It does this by enabling information-rich interaction at the edges of a network and between the most intelligent parts of any network—the people. It is people that can uniquely adapt to changes in the military, economic, natural, or any other environment. P2P technology may be the grease that lubricates the adaptability engines of military, intelligence, and commercial enterprises and enables decision superiority for the US.

¹⁴⁵ Tuttle, 70.

Bibliography

- Aerospace Command & Control, Intelligence Surveillance, and Reconnaissance Center, "AC2ISRC Mission," n.p. On-line, Internet, 2 May 2001, Available from <http://www2.acc.af.mil/ac2isrc/Mission.asp>.
- Alberts, David S., John J. Gartska and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*. Washington D.C.: DoD C4ISR Cooperative Research Program, 1999.
- Arquilla, John and David Ronfeldt, eds. *In Athena's Camp: Preparing for Conflict In The Information Age*. Santa Monica, Calif.: RAND, 1997.
- _____. *Swarming and the Future of Conflict*. RAND Report DB-311-OSD. Santa Monica, Calif.: RAND, 2000. On-line. Internet. 22 April 2001. Available from <http://www.rand.org/publications/DB/DB311/>.
- Bateman, Robert L. *Digital War: A View from the Front Lines*. Novato, Calif: Presidio Press, 1999.
- Bergstein, Brian. "Intel to Describe New Chip." *ExciteFor@Home*. 16 May 2001. n.p. On-line. 17 May 2001. Internet. Available from <http://home-news.excite.com/printstory/news/ap/010516/19/intel-wireless-chip>.
- Berkowitz, Bruce D. and Allan E. Goodman. *Best Truth: Intelligence In The Information Age*. New Haven, Conn.: Yale University Press, 2000.
- Berners-Lee, Tim and James Hendler And Ora Lassila. "The Semantic Web." *Scientific American*. May 2001. n.p. On-line. Internet. 29 May 2001. Available from <http://www.scientificamerican.com/2001/0501issue/0501bern timers-lee.html>.
- Bolcer, Gregory A. et al. *Peer-to-Peer Architectures and the Magi Open-Source Infrastructure*. White Paper. Irvine, Calif: Endeavors Technology. 6 December 2000. 6. On-line. Internet. Available from <http://www.endtech.com/news.html>.
- Borland, John. "Democracy's Traffic Jams." *CNET News.Com*. 26 October 2000. n.p. On-line, Internet. Available from <http://news.cnet.com/news/0-1005-201-3248711-2.html>.
- Clip2, "Reflector Overview." *Clip2.com*. 4 January 2001. n.p. On-line. Internet. Available from <http://dss.clip2.com/reflector.html>.
- CNET. *CNET Glossary*, n.p. On-line, Internet. 24 February 2001. Available from <http://www.cnet.com/Resources/Info/Glossary/>.
- Covault, Craig. "NIMA InfoTech Retools US Space Recon Ops." *Aviation Week & Space Technology*. 7 August 2000. 62-65.
- Federation of American Scientists. "Tasking, Processing, Exploitation & Dissemination (TPED) TPED Analysis Process (TAP)." n.p.; On-line, Internet, Available from <http://www.fas.org/irp/program/core/tped.htm>.
- Fisher, Dennis and Scott Berinato. "Making peer-to-peer secure." *Eweek*. 12 November 2000. n.p. On-line. Internet. 15 March 2001. available from <http://www.zdnet.com/ewee k/stories/general/0.11011.2652477.00.html>.

Free Peers Inc. "What Is Gnutella?" 2001. n.p. On-line. Internet. 25 May 2001. Available from <http://www.bearshare.com/gnutella.htm#whatis>.

Gateway.com. *Gateway_com Glossary*, n.p. On-line, Internet. 24 February 2001. Available from <http://www.gateway.com/help/glossary>.

Hamre, John. Deputy Secretary of Defense. Memorandum. To Department of Defense. Subject: Smart Card Adoption and Implementation, 10 November 1999.

Hayward, S. et al. *Beyond The Internet: The 'Supranet'*. Gartner Group Research Note COM-11-4753. Stamford, Conn: Gartner Group, 2001, 3. On-line. Internet. 21 May 2001. Available from <http://www3.gartner.com/Init>.

Howard, Sir Michael. "Military Science in an Age of Peace." *Royal United Services Institute for Defence Studies*, March 1974, 6.

Independent Commission on the National Imagery and Mapping Agency. *The Information Edge: Imagery Intelligence and Geospatial Information in an Evolving National Security Environment*, xi. On-line, Internet, 8 January 2001. Available from <http://www.NIMACommission.com>.

Internet Engineering Task Force. "The Internet Engineering Task Force." n.p. On-line. Internet. 31 March 2001. Available from <http://www.ietf.org/index.html> and <http://www.ietf.org/rfc/rfc2026.txt>.

Internet Corporation for Assigned Names and Numbers. "ICANN Fact Sheet." n.p. On-line. Internet. 25 May 2001. Available from <http://www.icann.org/general/fact-sheet.htm>.

Kelly, Kevin. *New Rules for the New Economy: 10 Radical Strategies for a Connected World*. New York, New York: Penguin Books, 1998.

Knighten, Bob. "Peer to Peer Computing." Briefing. 24 August 2000. On-line. Internet. 11 October. 2000. Available from http://www.peer-to-peerwg.org/downloads/collateral/200008_IDF/PtP_IDF.pdf.

Leopold, George. "Darpa mobile project preps 'soldier's radio.'" *EETimes.com*. 21 March 2001. n.p. On-line. Internet. Available from <http://www.eetimes.com/story/OEG20010321S0049>.

Liener, Barry M. et al., "A Brief History of The Internet, Version 3.31" Internet Society Web Page. 4 Aug 2000. n.p. On-line. Internet. 25 May 2001. Available from <http://www.isoc.org/internet/history/brief.html#Transition>.

Loeb, Vernon. "Spy Satellite Will Take Photos for Public Sale." *Washington Post*. Saturday, 25 September 1999. A03.

_____. "Making Sense Of The Deluge of Data," *Washington Post*, 26 March 2001, A23.

Martin, Frederick Thomas. *Top Secret Intranet*. 15 November 1998. Ch 10. n.p. On-line, Internet, Available from <http://www.topsecret.net/chapter10.htm>.

Michael, James B. "Ad Hoc Wireless Communications For Special Operations Forces (SOF)." Naval Post Graduate School. n.p. On-line. Internet. 8 March 2001. Available from <http://www.cs.nps.navy.mil/people/faculty/bmichael/cs4554/SOFNetwork.pdf>.

Michael, Dennis. "Win or lose, Napster has changed Internet." *CNN.com*, 2 October 2000, n.p. On-line. Internet. 3 October 2000. Available from <http://www.cnn.com/2000/SHOWBIZ/Music/10/02/napster/index.html>.

Minar, Nelson. "Security Issues of Peer-to-Peer Systems." Briefing. O'Reilly Peer-To-Peer Conference, San Francisco, Calif. 14 February 2001.

Money, Arthur L. *Report on Network Centric Warfare: Sense of the Report*. Washington D.C.: ASD/C3I, 2001.

- Murray, Williamson and Allan R. Millet, eds. *Military Innovation in the Interwar Period*. New York: Cambridge University Press, 1996.
- Myers, General Richard, Vice Chairman of the Joint Chiefs of Staff, US Air Force. Address. National Reconnaissance Office Senior Leaders' Strategic Management Conference. Williamsburg, Virg., 2 November 2000.
- National Imagery and Mapping Agency. "USIGS Architecture Framework." Bethesda, Maryland: National Imagery and Mapping Agency, 23 June 1998.
- National Research Council. *Realizing The Potential of C4I: Fundamental Challenges*. Washington D.C.: National Academy Press, 1999.
- Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence). *Information Superiority, Making the Joint Vision Happen*. Washington D.C.: ASD/C3I, 2.
- Oram, Andy, ed. *Peer-To-Peer: Harnessing the Benefits of a Disruptive Technology*. Sebastopol, Calif.: O'Reilly & Associates, 2001.
- Peer-To-Peer Working Group. *Peer-To-Peer Computing*. Adobe Acrobat Document, 10. On-line. Internet. 8 February 2001. available from http://www.peer-to-peerwg.org/specs_docs/collateral/P2P_IDF_Rev1.11-web.pdf.
- Public Broadcasting Service, "Life on the Internet Net Timeline." *PBS.org*. n.p. On-line, Internet. 24 February 2001. Available from <http://www.pbs.org/internet/timeline/index.html>.
- Roman, Lt Col Gregory A. "The Command or Control Dilemma: When Technology and Organizational Orientation Collide." Research Report AU/AWC/RWP198/96-04 Maxwell AFB. Ala.: Air War College, 1996.
- Rosen, Steven P. *Winning the Next War: Innovation and The Modern Military*. Ithaca, New York: Cornell University Press, 1991.
- Rosenberg, Robert A. "Improved Application of Information To The Battlefield, Revisited." Unpublished White Paper. 1999.
- SETI@home: Massively Distributed Computing for SETI. *Computing in Science and Engineering*, n.p. Internet. 8 February 2001. Available from <http://www.computer.org/cise/articles/seti.htm>.
- Shirky, Clay. "What is P2P ... And What Isn't." *O'Reilly Network*. n.p.; On-line. Internet. 24 February, 2001. Available from <http://www.openp2p.com/pub/a/p2p/2000/11/24/shirky1-whatisp2p.html>.
- Stoll, Clifford. *High Tech Heretic: Why Computers Don't Belong in the Classroom and Other Reflections by a Computer Contrarian*. New York: Doubleday, 1999.
- Sweeney, J. et al. *The Five Peer-to-Peer Models: Toward the New Web*. Gartner Group Research Note COM-12-4447. Stamford, Conn: Gartner Group, 2001, 3. On-line. Internet. 21 May 2001. Available from <http://www3.gartner.com/Init>.
- Tenet, George. *Director of Central Intelligence Annual Report for the United States Intelligence Community*. Washington, D.C.: Central Intelligence Agency. March 2000.
- Tuttle, Jerry O. "Decision Superiority and Intelligence," *Defense Intelligence Journal*, September 2000, 67-71.
- Upbin, Bruce "Sharing Power." *Forbes*. 27 November 2000. n.p. On-line. Internet. 3 March. 2001. Available from http://www.forbes.com/forbes/2000/1127/6614278a_print.html.
- US Air Force Scientific Advisory Board. *Report on Building the Joint Battlespace Infosphere, Volume 1: Summary*. SAB-TR-99-02. 2000. On-line. Internet. Available from <http://www.sab.hq.af.mil/Archives/1999/JBI/JBIExecutiveSummary.pdf>.

- US Army Research Laboratory. *Digitization and Survivability*. Aberdeen Proving Grounds, Maryland: US Army Research Laboratory, 2000.
- US Department of Defense. *Joint Vision 2020*. Washington D.C.: Chairman of the Joint Chiefs of Staff, 2000.
- US Joint Forces Command Concepts Division. "A White Paper for The Common Relevant Operating Picture." Draft White Paper, version 1.1., Norfolk, Virg.: 21 April 2000.
- US Senate. *Authorizing Appropriations For Fiscal Year 2001 For The Intelligence Activities Of The United States Government And The Central Intelligence Agency Retirement And Disability System And For Other Purposes*. 106th Cong., 2nd sess., 2000, S.R. 106-279.
- Wentz, Larry, ed. *Lessons From Bosnia: The IFOR Experience*. April 1998. Ch 10. n.p. On-line. Internet. 17 March 2001. Available from <http://www.dodccrp.org/bosch10.htm>.
- ZdNet. Zdwebopedia, n.p. On-line, Internet. 8 February 2001. Available from <http://www.zdwebopedia>.