**Naval War College**
Newport, R.I.

# TECHNOLOGY AND OPERATIONAL INTELLIGENCE
## COPING WITH UNITENTIONAL CONSEQUENCES

by

Lorenzo S. Hiponia
LCDR, U.S. Navy

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____



07 November 1997

Paper directed by
G.W. Jackson, Captain, U.S. Navy
Chairman, Joint Military Operations Department





Wayne F. Sweitzer
CDR U.S. Navy

06 FEB 97
Date

Security Classification This Page

REPORT DOCUMENTATION PAGE

| | |
|---|---|
| 1. Report Security Classification: UNCLASSIFIED | |
| 2. Security Classification Authority: N/A | |
| 3. Declassification/Downgrading Schedule: N/A | |
| 4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED. | |
| 5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT | |
| 6. Office Symbol: C | 7. Address: NAVAL WAR COLLEGE<br>686 CUSHING ROAD<br>NEWPORT, RI 02841-1207 |
| 8. Title (Include Security Classification): TECHNOLOGY AND OPERATIONAL INTELLIGENCE: COPING WITH UNINTENTIONAL CONSEQUENCES (U) | |
| 9. Personal Authors: LORENZO S. HIPONIA, LCDR, USN | |
| 10. Type of Report: FINAL | 11. Date of Report: ~~07 NOV~~ Feb 97 |
| 12. Page Count: 24 | |
| 13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy. | |
| 14. Ten key words that relate to your paper: OPERATIONAL INELLIGENCE, TECHNOLOGY, INFORMATION OVERLOAD, SYSTEMS VULNERABILITY, UNINTENTIONAL CONSEQUENCES, INTELLIGENCE CYCLE | |

Technology has substantially affected operational intelligence and the intelligence support environment. The significant amount of intelligence available to the operational commander is directly attributable to technological advancements in computers, communications, and collection systems. More importantly, enabling technologies improve functions within the intelligence cycle, considerably increasing the quality and timeliness of intelligence. Technology has reshaped the intelligence support architecture and is the driving factor in defining the future intelligence environment. However, numerous complications and vulnerabilities result from an operational intelligence environment excessively dependent on computers, communications, and collection systems. Effective employment of technology requires recognition of unintentional consequences that distract and impede the operational commander's decision process. This paper examines operational intelligence and the intelligence cycle. The effect of technology is discussed, focusing specifically on unintended consequences. Three adverse consequences are identified: information overload, increased system vulnerabilities, and less emphasis on analysis. Each of these effects are examined and recommendations for contending with these undesirable consequences are provided.

| 16. Distribution / Availability of Abstract: | Unclassified | Same As Rpt | DTIC Users |
|---|---|---|---|
| | X | | |
| 17. Abstract Security Classification: UNCLASSIFIED | | | |
| 18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT | | | |
| 19. Telephone: 841-[redacted] 6461 | | 20. Office Symbol: C | |

Security Classification of This Page Unclassified

# ABSTRACT

Technology has substantially affected operational intelligence and the intelligence support environment. The significant amount of intelligence available to the operational commander is directly attributable to technological advancements in computers, communications, and collection systems. More importantly, enabling technologies improve functions within the intelligence cycle, considerably increasing the quality and timeliness of intelligence. Technology has reshaped the intelligence support architecture and is the driving factor in defining the future intelligence environment. However, numerous complications and vulnerabilities result from an operational intelligence environment excessively dependent on computers, communications, and collection systems. Effective employment of technology requires recognition of unintentional consequences that distract and impede the operational commander's decision process. This paper examines operational intelligence and the intelligence cycle. The effect of technology is discussed, focusing specifically on unintended consequences. Three adverse consequences are identified: information overload, increased system vulnerabilities, and less emphasis on analysis. Each of these effects are examined and recommendations for contending with these undesirable consequences are provided.

# TABLE OF CONTENTS

# LIST OF FIGURES

# I. INTRODUCTION

It is difficult to deny the significance of technology and its impact on operational intelligence. The exponential increase of intelligence data available to the operational commander is directly attributable to recent technological advancements in computers, communications, and collection systems. More importantly, enabling technologies improve functions within the intelligence cycle, significantly increasing the quality and timeliness of intelligence. Technology has considerably reshaped the intelligence support architecture and is the driving factor in defining the future intelligence environment. However, numerous complications and vulnerabilities result from an operational intelligence environment excessively dependent on computers, communications, and collection systems. Effective employment of technology requires recognition of unintentional consequences that distract and impede the operational commander's decision process. What are these unintentional consequences of technology and can they be successfully overcome? These questions are the central focus of this paper. First, operational intelligence is discussed in terms of purpose, scope, and emphasis. Next, the effect of technology on the intelligence cycle and the intelligence support environment is examined. Finally, three unintentional consequences of technology are identified and recommendations for contending with these undesirable effects are provided.

# II. BACKGROUND

## A. OPERATIONAL INTELLIGENCE

### 1. Definition

*Joint Pub 3-0* describes three general levels of war used to clarify links between strategic objectives and tactical actions.[1] Likewise, there are three corresponding levels of intelligence: strategic, operational, and tactical. Operational intelligence is defined in *Joint Pub 2-0* as "...intelligence required for planning and conducting campaigns and major operations to accomplish strategic objectives within theaters or areas of operations."[2] Operational intelligence blends current intelligence reporting with short- to mid-term predictive analysis and supports the Joint Force Commander's (JFC) decision process throughout the entire operation or campaign.[3] Effective operational intelligence support requires knowledge and practice of both strategic and tactical intelligence. Just as operational art links strategic goals with the tactical means of achieving those goals, operational intelligence combines the vision of strategic intelligence with tactical execution to support the operational commander.[4]

### 2. Scope and Emphasis

Operational intelligence focuses on the collection and identification of the enemy's critical factors, both tangible and intangible. It seeks to identify the enemy's strategic and operational centers of gravity (COG), which may or may not be directly related to his combat

---

[1] The Joint Chiefs of Staff, *Joint Pub 3-0: Doctrine for Joint Operations*, (Washington DC: 01 FEB 1995), II-1.

[2] The Joint Chiefs of Staff, *Joint Pub 2-0: Joint Doctrine for Intelligence Operations Support to Operations*, (Washington DC: 05 MAY 1995), vi.

[3] Wayne F. Sweitzer, "Battlespace Information, Command and Control (C2), Operational Intelligence, and Systems Integration.," An Unpublished Paper, U.S. Naval War College, Newport, RI: November 1996, 10.

[4] Michael L. Warsocki, "Intelligence within Operational Art." *Military Review*, March-April 1995, 49.

power.[5] Proper analysis of the enemy's COG requires an aggregate understanding of enemy critical factors at all levels. Operational intelligence evaluates tangible measures of the enemy such as orders of battle, air defense capabilities, and the command, control, communications ($C^3$) structure. More significantly, operational intelligence analyzes intangible aspects of an enemy such as leadership, morale, discipline, and training. An appreciation of the political and economic factors affecting the COG is also essential. For example, an enemy's will to fight, the degree of public support, and the extent of alliance cohesion are just a few examples of political factors influencing the COG. Additionally, operational intelligence seeks insight into the personalities and command style idiosyncrasies of enemy operational commanders.[6] In contrast to tactical intelligence, the realm of operational intelligence encompasses the entire physical space defined by a given theater of operations. This space includes all air, land, sea surface, and subsurface regions within a given theater.[7] Operational intelligence focuses on all aspects of the physical environment such as topography, oceanography, weather, and climate. The nature and scope of operational intelligence requires continuous theater-wide collection during peacetime and in war. It is usually too late to collect and evaluate data just prior a major operation or campaign.[8] Operational intelligence simultaneously supports the current operation and anticipates future contingencies within the theater of operations.

---

[5] Ibid., 48.

[6] Milan N. Vego, "Operational Functions," An Unpublished Paper, U.S. Naval War College, Newport, RI: August 1996, 19.

[7] Ibid.

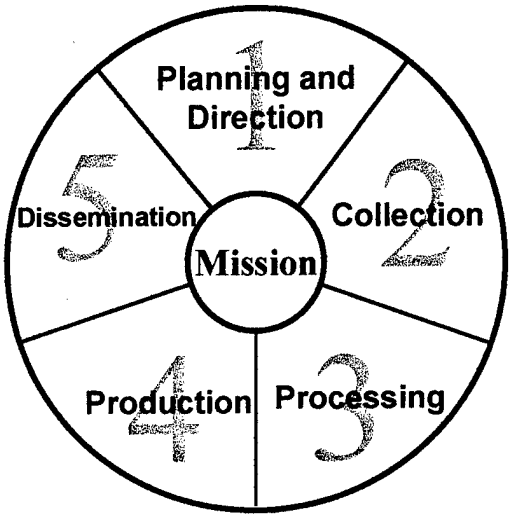
[8] Ibid.

## B. THE EFFECT OF TECHNOLOGY

### 1. The Intelligence Cycle

Operational intelligence employs all levels of collection ranging from national systems (such as satellites) to tactical reconnaissance assets (such as unmanned aerial vehicles). Transforming raw information collected from various sensors into a finished intelligence product is part of a larger process known as the intelligence cycle.

**Figure 1**
The Intelligence Cycle[9]




The intelligence cycle, depicted in Figure 1, consists of planning and direction, collection, processing, production, and dissemination. The operational commander determines intelligence requirements and data is collected based on assigned collection priorities. Once data is collected, the information is processed by converting the data into a suitable format for analysis. During production, the processed information is evaluated and

[9] *Joint Pub 2-0,* II-3.

integrated with data collected from other sources. The final product, finished intelligence, is disseminated to the operational commander through a variety of media.[10]

### 2. Changes to Intelligence Support

Although technology plays a vital role in each phase of the intelligence cycle, the greatest impact has been on collection and dissemination. Current technology improves collection capabilities, providing a greater depth of knowledge about the enemy than previously possible. For example, sensor technology expands the amount of data collected from the visible, non-visible, and electromagnetic spectrum; RADAR, infrared, and multi-spectral imagery routinely complement optical imagery. Today's manned reconnaissance aircraft are robust, multi-capable collection platforms. They collect any combination of electronic intelligence (ELINT), communications intelligence (COMINT), acoustic intelligence (ACINT), imagery intelligence (IMINT), and measurement and signature intelligence (MASINT). The advanced sensor technology and video capabilities of unmanned aerial vehicles (UAV) facilitate a new level of real-time situational awareness for the operational commander.

The most significant change to the operational intelligence support environment is the degree of access and independence given to the end user. The present intelligence architecture is a secure network of powerful multi-media information systems linking national level intelligence agencies with operational and tactical users. The architecture provides the end user an efficient means to access data, conduct liaison, and obtain intelligence *on demand* from any participating source within the network. Similar to the

[10] Ibid., II-3-II-7.

Internet, today's intelligence architecture resembles a classified Worldwide Web populated with intelligence "homepages" and databases. The primary advantages of an on-line, information sharing environment is the user's ability to query intelligence nodes according to operational requirements. Thus, the intelligence consumer is no longer restricted to a limited amount of intelligence "pushed" by production sites. Instead, the end user now "pulls" tailored intelligence from an extensive network of national, theater, and tactical intelligence sources.

Joint intelligence centers (JIC) form the backbone of the intelligence support structure within a defined theater of operations. They are repositories for all-source intelligence collected by strategic, operational, and tactical sources. In addition, JICs are the central focal point for all intelligence support requirements within a given theater of operations. They serve as the central clearing house for finished intelligence products and maintain accessible all-source intelligence databases. JIC databases are complemented by national level agency databases such as the National Security Agency (NSA), the Defense Intelligence Agency (DIA), the Central Intelligence Agency (CIA), and the National Imagery and Mapping Agency (NIMA). In addition, tactical level intelligence units such as carrier battle groups and reconnaissance squadrons maintain databases accessible at the operational level.

In summary, technology improves collection capabilities, increasing the amount and diversity of intelligence data available. Technology also provides expeditious dissemination of time-sensitive intelligence to users at all levels. Advancements in communications, computers, and mass storage capabilities provide the basis of an advanced information

infrastructure known as the joint intelligence architecture. This infrastructure is a dynamic, flexible structure comprised of intelligence centers, automated data processing equipment, and communications.[11]

## III. UNINTENTIONAL CONSEQUENCES OF TECHNOLOGY

While the preceding discussion described technological improvements to the intelligence cycle, there are profound consequences of that same technology. The ability to provide more complete, accurate, and timely information generates three significant problems associated with operational intelligence: information overload, increased system vulnerabilities, and less emphasis on analysis.

### A. INFORMATION OVERLOAD

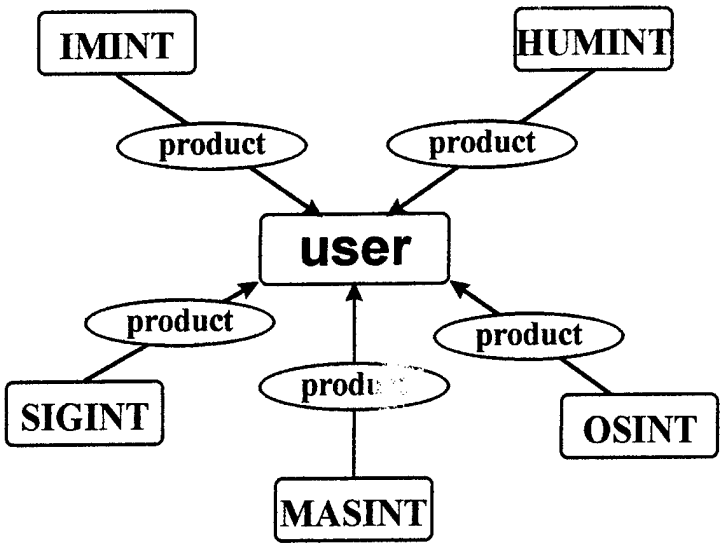
Historically, the intelligence environment has been a collection of numerous systems, each designed to solve a specific problem within a certain intelligence discipline. For example, an imagery workstation is used to analyze and manipulate various forms of IMINT while a separate ELINT workstation is used to analyze RADAR parameters and conduct hull-to-emitter-correlation (HULTEC). These systems were designed and built as isolated systems, each performing assigned tasks independent of each other. Figure 2 illustrates the "stovepipe" nature of these systems and depicts the user as the end point for the different systems.[12] The user can be interpreted as an intelligence analyst or an operator (user of intelligence). In either case, the user is responsible for fusing and integrating the various sources of data into one coherent intelligence picture.

---

[11] Ibid., GL-9.

[12] Rome Laboratories, Intelligence and Reconnaissance Directorate, "Intelligence Systems Technology Master Plan (ISTMP)," 21 August 1996, <http://www_ir.rl.af.mil/IRD/IRDS/ISTMP/istmp_home.html> (06 January 97).

**Figure 2.**
Current Intelligence Environment[13]




Information overload occurs when the sheer volume of data provided by the independent systems represented in Figure 2 overwhelms the user and critical intelligence is no longer distinct from extraneous data. Non-essential information masks vital intelligence and critical factors are overlooked. Failure to distinguish critical factors invariably leads to misidentifying the center of gravity. Another source of information overload is presentation scheme. Intelligence systems employ sophisticated forms of information presentation to cope with the tremendous amount of data that is displayed to the analyst. However, the more complex the presentation scheme, the more likely vital intelligence will be obscured by superfluous information.[14] Likewise, poor quality or incomplete data will go unnoticed and be interpreted as valid intelligence. The operational consequences are menacing. For

[13] "Intelligence Systems Technology Master Plan (ISTMP),", <http://www_ir.rl.af.mil/IR[illegible]RDS/ISTMP/intel-env.html> (06 January 97).

[14] David S. Albert, "The Unintended Consequences of Information Age Technologies," April 1996, <http://www.ndu.edu/ndu/inss/books/uc/concerns.html> (03 January 97).

example, if the enemy's point of main attack is masked by inconsequential data, own forces will be employed incorrectly and the enemy gains the initiative.

Another source of information overload stems from the expectation of near perfect intelligence. Since collection and dissemination capabilities have exponentially increased, there is a tendency to expect the arrival of new intelligence to clarify an ambiguous situation. The misguided notion of delaying a decision until more intelligence is received precipitates overload.[15]

Previously, dissemination of intelligence paralleled established command structures resulting in a highly constrained vertical flow of information. Because of the richly connected joint intelligence architecture, a significant amount of information now arrives from sources outside the organization's command structure. The result is a mixture of vertical and horizontal flows of information.[16] During a campaign or major operation, analysts receive inputs from multiple sources in an uncoordinated fashion. Asynchronous arrival of information confuses and distracts decision makers. Studies reveal the weight an individual places on information is related to the order the information is received.[17] This is a precarious aspect of information overload since asynchronous arrival of information can lead the operational commander to a false perception of the battlespace.

## B. SYSTEM VULNERABILITIES

The overarching nature of technology provides potential adversaries the capability to attack assets at any stage of the intelligence cycle. Furthermore, the Department of Defense's (DoD) increasing reliance on "commercial off the shelf" (COTS) hardware and

---

[15] Wendy L. Lichtenstien, "Managing Operational Intelligence Overload: Guidelines for Avoiding Decision Paralysis," Unpublished Research Paper, U.S. Naval War College, Newport, RI: 18 June 93, 9.

[16] Albert, <http://www.ndu.edu/ndu/inss/books/uc/impacts.html> (03 JAN 97).

software increases vulnerability by providing sophisticated adversaries familiarity with COTS elements incorporated into military systems.[18] All military equipment is subject to compromise either through capture or espionage. The increased portability of intelligence systems make them particularly vulnerable to capture or compromise when deployed afloat or in the field.

As the joint intelligence architecture continues to expand, system vulnerabilities increase due to the greater number of valid users accessing to the system. The larger number of users results in a greater probability of an "insider" threat. The recent espionage cases against Earl Pitts (FBI) and Aldrich Ames (CIA) illustrate the reality and severity of the "insider" threat. As the information infrastructure continues to expands, the number of nodes and entry points increase, providing more opportunities to penetrate the system from the outside. If a compromise does occur, the potential for damage is worse because the perpetrator has access to more information than in the past. As the size and complexity of the information infrastructure increases, the mere task of recognizing a penetration becomes difficult to discern.[19] Another system vulnerability is the omnipresent computer virus threat to intelligence databases and entire computer networks. As described previously, the joint intelligence architecture constitutes a robust information network connecting intelligence producers with intelligence consumers. This abundantly connected information infrastructure is particularly susceptible to damage because a single virus can spread practically at the speed of light.[20].

---

[17] Ibid., <http://www.ndu.edu/ndu/inss/books/uc/concerns.html> (03 JAN 97).
[18] Ibid.
[19] Ibid.
[20] Ibid.

In a recent study to evaluate the vulnerability of the Department of Defense (DoD) information systems to computer hackers, the Defense Information Systems Agency (DISA) conducted mock attacks on 8,000 unclassified DoD computers. It successfully broke into 88%. More disturbing, only five percent detected the break-in attempt and only five percent of those reported the incident.[21] In 1995, Julio Arita, a 21-year-old college student from Buenos Aires, was caught by federal agents accessing sensitive government files. Using stolen accounts and passwords, he gained access (via the Internet) to computers at the Naval Command Control and Ocean Surveillance Center, the Navy Research Laboratory, NASA's Jet Propulsion Laboratory and Ames Research Center, and the Los Alamos National Laboratory. Although Arita did not gain access to classified material, sensitive government research files dealing with satellite engineering, radiation, aircraft design, and RADAR technology were compromised. [22]

These few examples illustrate the vulnerability of information-based systems to attack and exploitation. A full discussion of information warfare is beyond the scope of this paper. However, the same principles of attacking information and exploiting system vulnerabilities are easily applied to the operational intelligence environment.

## C. LESS EMPHASIS ON ANALYSIS

Technology is steadily supplanting the "man-in-the-loop" in favor of highly automated systems. Emmett Paige, the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (C3I) comments, "We must strive for information superiority over any opponent through more rapid gathering, assimilation and transmission of

---

[21] Glen Buchan, "Information War and the Air Force: Wave of the Future? Current Fad?" March 1996, <http://www.rand.org/publications/IP/IP149> (03 January 97).

data as close as possible to the source, *with minimal human intervention*" [emphasis added].[23] Removing human interaction for the sake of efficiency results in an unintentional consequence: less dependency on the analytical skills of intelligence professionals. Previously, incomplete intelligence nurtured an environment where analytical savvy was the key to gaining situational awareness of the battlespace. Because of advancements in technology, the sheer volume of raw data available to the operational commander now provides some measure of situational awareness *independent of analysis*. Today's highly capable systems process data and display all the information required to support the Joint Force Commander's decision process. With such a preponderance of information already available to the commander, it is difficult to provide additional insight from human analysis.[24] Another factor to consider is the time required to analyze data. Because analysis is time consuming, an information bottleneck occurs, slowing information that some argue should go directly from "sensor-to-shooter."[25] To overcome this information bottleneck, new technology focuses on automated processing in favor of human analysis.

The search for a solution to information overload purposely minimizes human intervention. The future intelligence environment looks towards more capable systems with higher levels of inter-operability and information sharing to bypass human inefficiencies and delays.[26] Rome Laboratory, an U.S. Air Force research and development facility, is exploring future C3I technologies required to improve intelligence and reconnaissance capabilities.

---

[22] Bob Drummond, "U.S. Uses First Court-Ordered Wiretap on Computer Network," 26 March 1996, <http://www.azcentral.com/depts/compute/news/apr01/hacker.shtml>, (25 January 97).

[23] Emmett Paige Jr., "Striving for Information Superiority," Prepared remarks given to the 311th Theater Signal Command Activation Dinner, Fort Meade, MD. 22 June 1996, <http://www.dtic.mil/defenselink/pubs/di96/di1172.html>, (03 February 1997).

[24] Sweitzer, 14.

[25] Ibid.

Rome's conception of a "transitional" intelligence environment is depicted in Figure 3. In this intelligence environment, the user is no longer required to fuse different types of intelligence; all sources of intelligence will be integrated and fused prior to the production of finished intelligence. Vast improvements in communications bandwidth capability, mass storage technology, multi-source fusion applications, near-real time decision aids, and information representation must be realized before establishing this intelligence environment.[27]

**Figure 3.**
Transition Intelligence Environment[28]


More ambitious yet is Rome Laboratory's conception of the future intelligence environment illustrated in Figure 4. In this environment, all information and support applications operate in a seamless multi-media intelligence environment. The analyst does not need to know which application is being used or how access is gained to specific intelligence; it is not germane.[29] Users are only concerned with the task at hand and not the intelligence resources required to fulfill the task. Thus, communications capability,

---

[26] "Intelligence Systems Technology Master Plan (ISTMP)," <http://www_ir.rl.af.mil/IRD/IRDS/ISTMP/istmp_int_env_trans.html>, (06 January 1997).

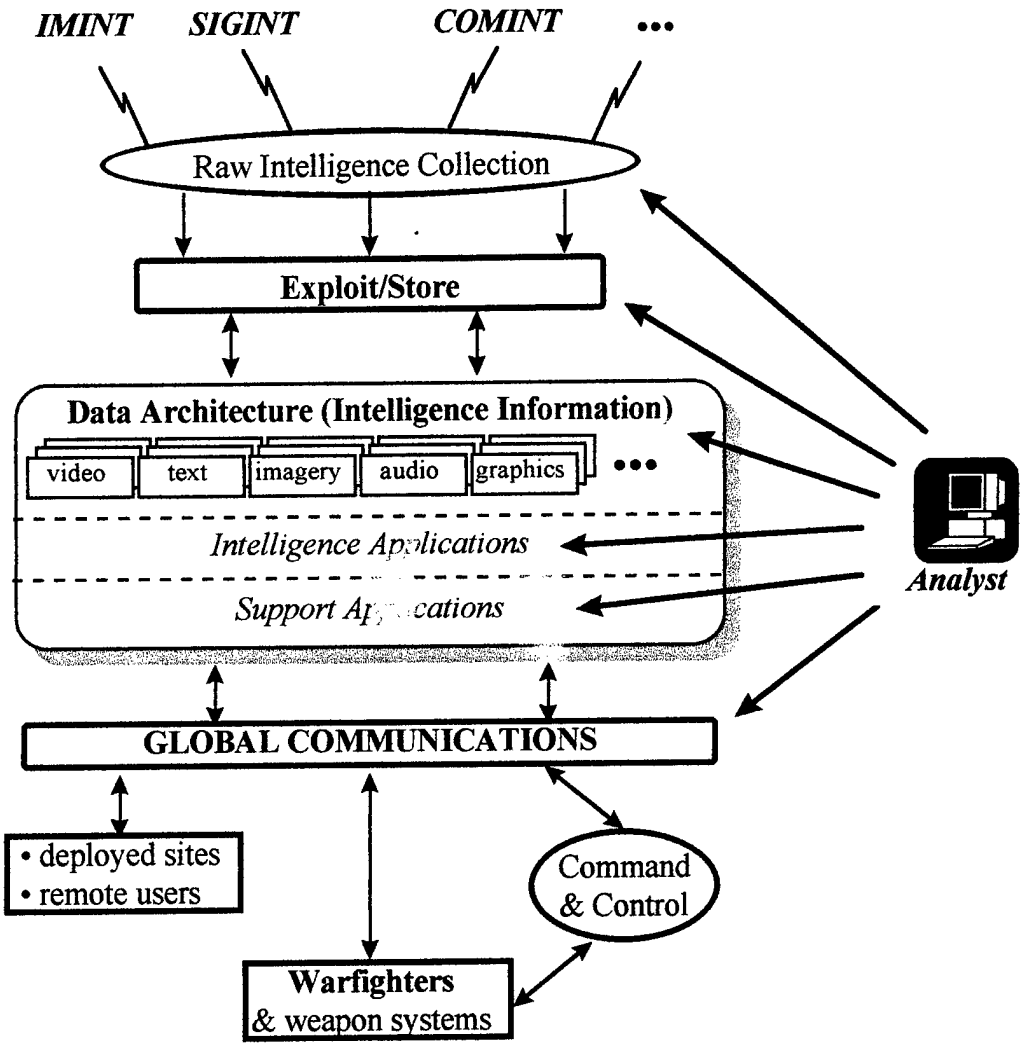
[27] Ibid.

[28] Ibid., <http://www_ir.rl.af.mil/IRD/IRDS/ISTMP/istmp_int_env_trans.html>, (06 January 1997).

[29] Ibid., <http://www_ir.rl.af.mil/IRD/IRDS/ISTMP/istmp_concerns.html>, (06 January 1997).

collection and exploitation assets, and the means for storing and disseminating intelligence will be transparent to the user.[30]

**Figure 4.**
Future Intelligence Environment[31]




The technology required to achieved the future intelligence environment is years away. However, the approach is basic: eliminate the "man-in-the-loop" in favor of automated processing. Research into artificial intelligence, audio and speech processing, and machine

[30] Ibid.
[31] Ibid., <http://www_ir.rl.af.mil/IRD/IRDS/ISTMP/istmp_int_env_fut.html>, (06 Janaury 1997).

vision are just some key technologies being developed to produce a more efficient intelligence cycle.[32] Efficiency dictates a required transition from human interaction to automated computer processing. The unintended consequence is less reliance on analysis provided by intelligence professionals.

# IV. RECOMMENDATIONS

Overcoming the unintentional consequences of technology entails careful examination of processes, procedures, training, and doctrine. Regardless of the technological improvements in collection and dissemination, operational intelligence remains a vital component of operational *art*.[33] Human intuition, biases, and perceptions are relevant due the predictive and intangible nature of operational intelligence. Human analysis remains important despite deliberate efforts to reduce human interaction. Knowing when and where to emphasize the human factor is the key to overcoming the unintended effects of technology.

## A. INFORMATION OVERLOAD AND THE HUMAN FACTOR

The most significant factor for reducing information overload is intelligence guidance from the operational commander. To avoid situations where too much information overwhelms the user, decisions must be made regarding what information is really needed, what information is nice to have, what information is distracting, and what information is irrelevant.[34] The operational commander must clearly articulate intelligence concerns and priorities required to support the campaign or operation. The intelligence officer (J2) then interprets the operational commander's guidance and tasks intelligence resources

[32] Ibid.
[33] Sweitzer, 11.

accordingly using Priority Intelligence Requirements (PIR), Essential Elements of Information (EEI), and Requests for Information (RFI). The operational commander must ensure the J2 thoroughly understands the mission and objectives because misinterpretation leads to unnecessary collection, futile analytical efforts, and irrelevant intelligence that inhibits the operational commander's decision cycle.[35]

Another way to reduce information overload is to synchronize intelligence with operations. The commander and the J2 must ensure all intelligence activities and assets are applied in time, space, and purpose to optimally support the Joint Force Commander's operational plan.[36] This synchronization process ensures totality of effort directed against the adversary's center of gravity.[37] Effective synchronization produces intelligence relevant to the operation and reduces the chance of introducing extraneous intelligence.

Refining intelligence requirements to support the mission and objectives of an operation is only the first step in overcoming the immediate effects of information overload. Better education, training, and doctrine are long term solutions to cope with the problem of information management. Specific emphasis should be placed on information processing under stress, operating in ambiguous information environments, and operating in information-rich scenarios.[38] Joint Professional Military Education (JPME) curriculums should familiarize students with information technology advantages, vulnerabilities, limitations, and applications to military affairs. JPME institutions should develop methods

---

[34] Ibid.
[35] Lichtenstien, 10-11.
[36] *Joint Pub 2-0*, IV-3.
[37] Ibid.
[38] Albert, <http://www.ndu.edu/ndu/inss/books/uc/concerns.html> (03 January 1997).

of teaching that enables students to become computer literate and familiar with electronic information retrieval.

Doctrine is vital because it ensures behavior consistent across the entire organization.[39] David Albert comments, "Changes in doctrine are essential if the benefits of new information systems are to be realized and inconsistencies between capacity and doctrine avoided."[40] For example, the operational commander can be influenced by the expectation of *near perfect* information. *Near perfect* information is less likely in operational intelligence due to the assumptions and inferences made in the process of analyzing the enemy's intangible factors. Furthermore, there is danger in delaying a decision in anticipation of better intelligence that clarifies an ambiguous situation. Doctrine should reinforce the concept of sufficient and necessary information versus desirable information.[41] Practice is the key to perfecting and maintaining skills required to function in an information-rich environment. Operational exercises, on the job training, and continued professional military education can lead to an effective approach to coping with information overload.

## B. COPING WITH SYSTEM VULNERABILITIES

All military equipment is susceptible to loss or compromise. To minimize potential damage, defensive measures must be incorporated into portable intelligence systems. These measures include unique cryptographic "keys" to identify authorized users, tracking devices for essential hardware items, authentication procedures, and security codes.[42] Increased emphasis on security screening is required to neutralize the "insider" threat. Also, software engineers and technicians developing COTS components should be subject to background

---

[39] Ibid.

[40] Ibid., <http://www.ndu.edu/ndu/inss/books/uc/recom.html> (03 January 1997).

checks if contracted for sensitive intelligence COTS components. Because of the rapid development in technology, intelligence systems undergo continuous development; replacement by more capable intelligence systems is inevitable. Acquisition procedures must consider security requirements and minimize potential exposure to exploitation vulnerabilities. [43] Some systems may be too sensitive to rely on COTS design or procurement regardless of cost benefit.

Increased system vulnerability is the inherent consequence of increased reliance on technology. The challenges of preventing an adversary's exploitation of information-based vulnerabilities are enormous. The previous discussion is only an introduction to defensive measures being explored. Extensive research on information vulnerability and information security is conducted at the National Institute of Standards and Technology and the National Computer Security Center (part of NSA). Both have the responsibility (given by the Computer Security Act of 1987) for protecting the National Information Infrastructure.[44]

## V. CONCLUSIONS

There are no easy solutions to the consequences of technology previously discussed. Research conducted at Rome Laboratory seeks to reduce information overload by shifting the burden of analysis from man to machine. This approach involves a trade off between "raw" or unprocessed data and information which contains a mixture of "fact" and inference derived from fusion algorithms and decision aids.[45] However, the most important aspect of technology employment is knowing that situational awareness does not reside on a computer

---

[41] Ibid.

[42] Ibid., <http://www.ndu.edu/ndu/inss/books/uc/concerns.html> (03 January 1997).

[43] Ibid.

[44] Buchan, <http://www.rand.org/publications/IP/IP149> (03 January 97).

screen, information network, or collection platform; rather, situational awareness exists in the minds of the opposing operational commanders.[46] Systems and technology are merely "tools" of the intelligence trade. The most technologically advanced system is useless unless the "craftsman" properly employs the "tools."[47]

Technology has overcome fundamental intelligence problems of the past by developing better collection platforms and dissemination means. In the process of providing more useful and reliable intelligence, technology has generated unintentional consequences: information overload, system vulnerabilities, and less emphasis on analysis. Doctrine, training, and education are several methods of dealing with these unwanted effects. Despite technological advancements and innovations, human intuition, biases, and perceptions will always be relevant due to the intangible factors within operational intelligence. Michael Handel best describes the relationship between human interaction, intelligence, and technology: "In the final analysis, intelligence problems are human—problems of perception, subjectivity, and wishful thinking—and thus are not likely to disappear no matter how much the technological means of intelligence improve."[48]

---

[45] Albert, <http://www.ndu.edu/ndu/inss/books/uc/concerns.html> (03 January 1997).
[46] Sweitzer, 3.
[47] Ibid.
[48] Michael Handel, quoted in Lichtenstien, 22.

## SELECTED BIBLIOGRAPHY


Albert, David S. "The Unintended Consequences of Information Age Technologies." April 1996. <http://www.ndu.edu/ndu/inss/books/uc/concerns.html> (03 January 1997).

Buchan, Glen. "Information War and the Air Force: Wave of the Future? Current Fad?" March 1996. <http://www.rand.org/publications/IP/IP149> (03 January 1997).

Bob Drummond. "U.S. Uses First Court-Ordered Wiretap on Computer Network." March 26, 1996. <http://www.azcentral.com/depts/compute/news/apr01/hacker.shtml>, (25 January 97).

Joint Chiefs of Staff. *Joint Pub 2-0: Joint Doctrine for Intelligence Operations Support to Operations.* (Washington DC: 05 May 1995).

_____. *Joint Pub 3-0: Doctrine for Joint Operations.* (Washington DC: 01 February 1995).

Lichtenstien, Wendy L. "Managing Operational Intelligence Overload: Guidelines for Avoiding Decision Paralysis." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 18 June 93.

Paige, Emmett. "Striving for Information Superiority." Prepared remarks given to the 311th Theater Signal Command Activation Dinner, Fort Meade, MD. 22 June 1996. <http://www.dtic.mil/defenselink/pubs/di96/di1172.html> (03 February 1997)

Rome Laboratories, Intelligence and Reconnaissance Directorate. "Intelligence Systems Technology Master Plan (ISTMP)." August 21 1996. <http://www_ir.rl.af.mil/IRD/IRDS/ISTMP/istmp_home.html> (06 JAN 97).

Sweitzer, Wayne F. "Battlespace Information, Command and Control (C2), Operational Intelligence, and Systems Integration.," An Unpublished Paper, U.S. Naval War College, Newport, RI: November 1996.

Vego,Milan N. "Operational Functions," An Unpublished Paper, U.S. Naval War College, Newport, RI: August 96.

Warsocki, Michael L. "Intelligence within Operational Art." *Military Review*, March-April 1995, 44-49.