T.C

YEDİTEPE UNIVERSITY

GRADUATE INSTITUTE OF SOCIAL SCIENCES

AFTER GLOBALIZATION PROCESS NEW HORIZONS IN CONTEMPORARY STRATEGIC INTELLIGENCE

by

GÖKHAN SARI

Submitted to the Graduate Institute of Social Sciences
In partial fulfillment of the requirements for the degree of
Master of
Business Administration
ISTANBUL, 2003

AFTER GLOBALIZATION PROCESS NEW HORIZONS IN

CONTEMPORARY STRATEGIC INTELLIGENCE

ISTANBUL

2003

T.C.

YEDİTEPE UNIVERSITY

GRADUATE INSTITUTE OF SOCIAL SCIENCES

AFTER GLOBALIZATION PROCESS NEW HORIZONS IN CONTEMPORARY STRATEGIC INTELLIGENCE

by

Gökhan SARI

Supervisor

Associate Prof. Mesut Hakkı CAŞIN

Submitted to the Graduate Institute of Social Sciences

In partial fulfillment of the requirements for the degree of

Master of

Business Administration

ISTANBUL, 2003

AFTER GLOBALIZATION PROCESS NEW HORIZONS IN CONTEMPORARY STRATEGIC INTELLIGENCE

by

Gökhan SARI

Approved by:

Associate Prof. Dr. Mesut Hakkı CAŞIN.....

(Supervisor)

Prof. Dr. Yaşar GÜRBÜZ .....

Prof. Dr. Ahmet YÜCEKÖK .....

Date of Approval by the Administrative Council of the Institute 28/02/2003

TABLE OF CONTENTS

Page

LIST OF ABBREVIATIONS

ACH	Analysis of Competing Hypotheses
ACOUSTINT	Acoustic Intelligence
AFSA	Armed Forces Security Agency
BC	Before Christ
BOS	Battlefield Operating System
CBRN	Chemical, Biological, Radiological, Nuclear
CFE	Conventional Armed Forces in Europe
CI	Counterintelligence
CIA	Central Intelligence Agency
COMINT	Communications Intelligence
DDP	Deputy Director for Plans
DI	Directorate Intelligence
DIA	Defense Intelligence Agency
DoD	Department of Defense
DPRK	Democratic People's Republic of Korea
ELECTRO-OPTINT	Electro-optical Intelligence
ELINT	Electronic Intelligence
EMP	Electro Magnetic Pulse
EW	Electronic Warfare
FEC	Far Eastern Command
FISINT	Foreign Instrumentation Signals Intelligence
FSU	Federation of Soviet Union
HUMINT	Human Intelligence
ICs	Intelligence Communities
IDA	Information, Decision Action
IG	Inspector General
IMINT	Imagery Intelligence
IO	Information Operations
IRINT	Infrared Intelligence

JCS	Joint Chiefs of Staff
KGB	Komitet Gosudarstvennoi Bezopasnosti (Committee for State Security)
LASINT	Laser Intelligence
LLC	Low-Intensity Conflict
MASINT	Measurement And Signature Intelligence
MICE	Money, Ideology, Compromise, Ego
MRBMs	Medium-Range Ballistic Missiles
NATO	North Atlantic Treaty Organization
NBC	Nuclear, Biological, And Chemical
NGOs	Nongovernmental Organizations
NIE	National Intelligence Estimate
NSA	National Security Agency
NUCINT	Nuclear Intelligence
OPTINT	Optical Intelligence
OSINT	Open-Source Intelligence
OSS	Office of Strategic Services
PHOTINT	Photographic Intelligence
PLA	People's Liberation Army
PVOs	private voluntary organizations
R&D	Research and Devolepment
RADINT	Radar Intelligence
RINT	Unintentional Radiation Intelligence
S&TI	Scientific And Technical
SAMs	Surface-to-Air Missiles
SIGINT	Signals Intelligence
TCA	Transnational Criminal Activity
TECHINT	Technical Intelligence
TELINT	Telemetry Intelligence
UAV	Unmanned Aerial Vehicle
UN	United Nations
US	United States

WMD	Weapons of Mass Destruction
WW	World War
WWW	World Wide Web

LIST OF FIGURES

LIST OF TABLES

LIST OF MAPS

ACKNOWLEDGEMENTS

I would like to express my deep gratitude to my supervisor Associated Prof. Dr. Mesut Hakkı CAŞIN for his invaluable comments, his advices and help throughout my study. His knowledge and guiding insights into strategic studies have provided me a new sound perspective. It was a great honor for me to study with him.

I want to thank Mr. Bedrettin DALAN, the founder and the president of the Istanbul Education and Culture Foundation, for his services to the Atatürk's Turkish youth, establishing opportunities in such a marvelous university with its precious academic personnel, contemporary educational system and modern buildings.

I would like to express my best regards to the Prof. Dr. Doğan ALTUNER, the dean of Yeditepe University Graduate School of Social Sciences, for his support throughout the master of business administration program, and to the Ret. Maj. Gen. Rıza KÜÇÜKOĞLU, The General Secretary of Yeditepe University, for his unique help. I would like to thank to all academic personnel of the university, Prof. Dr. Haluk ULMAN on Introduction to International Relations, Prof. Dr. Yaşar GÜRBÜZ to International Law, Prof. Dr. Nadir DEVLET to Military Strategy, Russia, Eastern Europe Center and on Turkish Foreign Policy, Prof. Dr. Ahmet YÜCEKÖK on Comparative Politics, Asst. Prof. Mehmet YAHYAGIL on Research Methodology and Data Analysis, Ret. Gen. Army Teoman KOMAN on Security and Intelligence Operations, Ret. Br. Gen. Nejat ESLEN and Author Ercan ÇİTLİOĞLU on National Security Systems, Dr. Adil Serdar SAÇAN on Organized Crimes and Smuggling, Dr. Giovanni ERCOLANI on International Terrorism for their endless desire for sharing the knowledge.

I also would like to express my best regards to the General Command of the Gendarmerie for providing this chance to attend the master of business administration program and improve myself. I believe that, as Atatürk has targeted, our nation will go beyond the level of contemporary nations with these well-educated personnel.

And consequently I would like to thank my wife Yeşim and my daughter Ece for their endless patience and precious support.

ABSTRACT

The need of information gathering as old as the history of humanity, combined with today's technology, produces the base of future structure. The adapting the need of information gathering, which is accorded to our purpose, in systematic and methodological form is intelligence.

States, which want to survive and attain well-being of their own people, require a dynamic intelligence system. The intelligence requirements, which are adapted national security strategies in macro dimensions such as ideology, national force, threat, deterrence, time and space, are met in functional mean by strategic intelligence activities.

In the period of the accelerated process of globalization, the analysis problem of dense information activities of international organizations, non-governmental organizations (NGOs) and private voluntary organizations (PVOs) beside the states, require presenting of true scenarios, which are consist of choices in different parameters, to decision makers.

However, in accordance with the structure, the term of strategic intelligence is affected by the factors of economic, military, politics, law and geopolitics, beside the dynamic variation process. In addition to this, the term of strategic intelligence has most sophisticated character, which contain most difficult and vital dimensions, because the actors, which take place in international system, have the different conjectural vital interests in their structures.

In this coherence of ideas, the main purpose of this academic research in the view of international relations is to assess the future strategic intelligence structure depending on international world order and conjectural breaking, and to bring intelligence concept to light from the complexity of literature.

In this research, it is intended to define basic intelligence concept and to assess the forthcoming progress in intelligence structure by using inductive method. To assess the future of strategic intelligence and to arrive a conclusion, the intelligence failures in the historical process are tried to examine and in this framework, the concept of intelligence is analyzed.

The technology and the new world order do not change the core of intelligence, but it is observed to have changed its techniques and affairs. The arriving assessments presented in conclusion.

ÖZET

İnsanlık tarihi kadar eski olan bilgi toplama ihtiyacı, günümüzün teknolojileri ile birleştiğinde geleceğimizi oluşturacak yapılanmanın esasını oluşturur. Bu bilgi toplama ihtiyacının amacımıza uygun olarak sistematik ve metodolojik hale getirilmiş şekli ise istihbarattır.

Devletler varlıklarını devam ettirmek ve daha iyi şartları temin etmek için dinamik bir istihbarat sistemine ihtiyaç duyarlar. İdeoloji, ulusal güç, tehdit, caydırıcılık, zaman ve mekan gibi makro boyuttaki ulusal güvenlik stratejilerine uygun olarak ihtiyaç duydukları istihbarat gereksinimleri, fonksiyonel anlamda stratejik istihbarat faaliyetleri ile karşılanır.

Küreselleşme sürecinin hızlandığı bu dönemde, devletin yanı sıra uluslar arası örgütler, hükümet dışı kuruluşlar (NGO) ile çokuluslu şirketlerin(ÇUŞ) yoğun enformasyon içerikli faaliyetlerinin analizi problemi, karar vericilere farklı parametrelerdeki seçenekleri içeren en doğru senaryoların arzını gerekli kılmaktadır.

Ancak stratejik istihbarat kavramı, yapısı gereği dinamik değişim sürecinin yanı sıra, ekonomik, askeri, siyasi, hukuki ve jeopolitik faktörlerden etkilenir. Bununla beraber, uluslar arası sistemde yer alan aktörlerin farklı konjektürel hayati çıkarlarını bünyesinde bulundurması sebebi ile uluslararası rekabetin en çetin ve yaşamsal boyutlarını içeren son derece sofistike bir karaktere sahiptir.

Bu bağlamda, akademik araştırmanın amacı, uluslararası dünya düzeni ve konjüktürel kırılmalara bağlı olarak gelecek stratejik istihbarat yapılanmasını uluslar arası ilişkiler açısından değerlendirmek ve mevcut anlam kargaşasından sıyrılarak istihbarat konseptini ortaya çıkarmaktır.

Bu araştırmada, metodolojik yöntem olarak tümevarım metodu uygulanmış, temel istihbarat kavramı tanımlanmaya ve istihbarat yapılanmasındaki muhtemel değişim süreci değerlendirilmeye çalışılmıştır. Stratejik istihbarat yapılanmasının geleceğini değerlendirmek ve bir sonuca varabilmek için tarihsel süreç içerisindeki istihbarat hataları incelenmeye çalışılmış, bu çerçevede istihbarat konsepti analiz edilmiştir.

Araştırma sonucunda genel konsept olarak, yüksek teknolojinin ve yeni dünya düzeninin istihbaratın özünü değiştirmediği ancak ilgi alanı ve tekniğinde değişiklik meydana getirdiği görülmüş, bu konuda varılan değerlendirmeler sonuç bölümünde açıklanmıştır.

"... it is surprising that there is not more general agreement and less confusion about the meaning of the basic terms. The main difficulty seems to lie in the word 'intelligence' itself, which has come to mean both what people in the trade do and what they come up with. To get this matter straight is crucial: intelligence is both a process and an end-product."

Sherman KENT[1]

INTRODUCTION

In this academic research I took a macro look at the Intelligence Phenomenon and tried to find the effects of Post World Wars Era on future intelligence structure, and specifically, future applicability of the Intelligence Needs Process. By the way I tried to open a window, which aimed to reach futures horizons and developments for new researchers. While arriving conclusion, I examined historically and conceptionaly evolution. Historically evaluation examined in two phases; First until collapse of Soviet Union, Second from the beginning Post Cold War Era until today. The aspects and forecast of the future intelligence examined in the chapter six and finally recommendations is presented in conclusion. This study provides academic guidelines to the Intelligence Communities (ICs) on how the requirements process should be structured to ensure that the Communities can meet national security needs of the 21st century and also a handbook for all users.

The main mission of the Strategic Intelligence is to supply policy makers with timely information and analysis that allows for informed, knowledgeable decision making. Strategic Intelligence indicates the way and lights the corridors, which are potential risks for policymakers. In order to fulfill this mission, the ICs must understand the prioritized intelligence requirements of policy makers. In an ideal world, ICs would be able to fulfill all actual and potential policy maker requirements in a timely, comprehensive manner.

The states have lacked a strategic vision defining its role in the world since the end of the Cold War. The requirements process, in fact, has been made even more difficult by the

[1] Kent, S., "Prospects for the National Intelligence Service," Yale Review, 36 (Autumn 1946), p. 117 in Warner, M., "Wanted: A Definition of Intelligence", Studies in Intelligence, Available on site http://www.cia.gov/csi/studies/vol46no3/article02.html

absence of any current political consensus on national security issues and their importance. As policymakers have struggled to define core national interests, they have turned to the ICs for increased coverage of diverse issues. Because of the changing nature of threats and intelligence needs which are requires and responses of intelligence consumers (push and pull)[2] since the end of the Cold War, the ICs themselves should force to examine their roles and missions. There is considerable disagreement among experts about whether the ICs should focus primarily on supporting national security policy makers or whether it should support other customers, such as law enforcement agencies, economic/trade officials, or environmental agencies. Still others argue that intelligence support to military operations should be the primary function of intelligence. These debates over national security priorities and the ICs' mission, requirements, and customer bases are not easily resolved. Nonetheless, the ICs' function in aiding the national security decision making process must be defined so that it can properly target its resources against the most important foreign policy challenges.

Maintaining an effective requirements process has been a continuous struggle for the ICs. During the Cold War, when a majority of Communities resources were targeted against the Soviet Union for NATO members, having an effective requirements process was less important than it is now. Since the end of the Cold War, the growing complication of new requirements, some of which are of the "highest priority" for only a short time, have left the ICs without clear guidance on which to base its resource allocation and planning. Lacking a cohesive foreign policy strategy to guide it and faced with declining resources and increasingly diverse customer demands, the ICs need a flexible, dynamic requirements process to help it fulfill its main mission.

Although the ICs have changed their focus and targeting since the end of the Cold War, they cannot hope to link strategic resource planning to future needs until it has a corporate understanding of what future intelligence needs will likely be and how its resources currently are used to meet intelligence requirements.

---

[2] Advanced explanation in page 98.

Although importance of intelligence is known everybody, there is known exactly what is it. “Everybody knows, nobody know.” What I mean with this phrase? While you talk about intelligence, everybody has something to say. And also every sector has own definitions. Generally speaking, “intelligence” refers to information about “things foreign” that is not available to the Government through conventional means-in other words, to information collected by “secret” or “clandestine” means. But the work of intelligence also involves collecting and analyzing information available through conventional means to the extent needed to understand what is otherwise gathered by “secret” means.

As the five senses of human, intelligence serve policymakers that are the brain of same human. So I preferred the start with what is intelligence? What is the relation of intelligence with the other components of national security?

DEFINITION OF THE PROBLEM

Although the concept of Intelligence is as old as the history of war, there is not a common understanding among the literature. The discussions especially focus on sub-concepts or assessment for a state. There isn’t a neutral and general literature, which can be use for all states and researchers.

And also the changing world how effects the intelligence structure and what will be future intelligence aspects, are second problem which we faced.

So for the purpose of this thesis, analysis of strategic intelligence and assess the future affects on national security and intelligence communities.

OBJECTIVES OF THE STUDY

A descriptive study is committed in order to determine the common characteristics of the intelligence evaluation and to assess the possible impacts of intelligence in national security by analyzing the means, strategies and the possible target set of intelligence.

The main objective of the study is to determine the priorities for the possible impacts of strategic intelligence on the national security. The other objective of the study is to make clarifications on the assessed priorities in order to construct a base for future studies.

SCOPE OF THE STUDY

The main scope of this study is to search for the characteristics of the intelligence and assessing the possible impacts of intelligence on the national security to find future strategic intelligence structure.

Therefore, the study begins with nature of intelligence in second chapter. To clarify the complexity of intelligence concept, it is searched what we understand from the term of intelligence in different sectors and to appear diverges between them. And also in this chapter, the relation between intelligence and other security terms is examined.

Chapter 3 is about the evaluation of intelligence. The chapter begins from 500 BC to 1991 when cold war ended with collapse of Soviet Union. Throughout the history of that period, most important wars are examined in detail in order to find out failures and lessons to emphasize the direction of evaluation. Subsequently, the discussions about the range, scope, and characteristics of the emerging intelligence are analyzed while the emphasis is given on the relationship between failures and the intelligence.

Chapter 4 presents the conceptual analysis of intelligence in every form. By the conceptual analysis the dimensions, missions components, disciplines, tenets and psychology of intelligence are examined and clarified the relation between them and national security. Initially, presents dimensions of intelligence in order to determine the borders and relations of them. Missions of intelligence identify what are necessary and appropriate missions for the Intelligence Communities as it enters the 21st century. Although each component and collection disciplines of intelligence has a large area, in this chapter definitions of components and disciplines are presented and assessed the relation with national security. At the end of chapter different forms of strategic intelligence and their relationship with the concept is discussed in detail by analyzing conceptual approaches of several authors. The chapter also aims to emphasize the impacts of strategic intelligence at the grand strategic level.

Chapter 5 presents changing face of intelligence by globalization and possible impacts of intelligence on the future security environment. Although globalization as a process which origins arrive until WW II, main change started with collapse of Soviet Union. So

globalization and its effect on intelligence is examined between 1991 and 11 September 2001 which terrorist attack changed the form of enemy. So the reflection of September 11th on Security Mentality is examined in this chapter.

Chapter 6 begins by outlining the sources of the need for change. It is not intended to be a comprehensive treatment of the whole of intelligence issues, but to bring to the attention of a new defense system and intelligence structure the handful of most important needs. These are outlined in this chapter, and a series of specific recommended actions are outlined in the conclusion. At the end, the new intelligence developments are also attached in the Appendix A.

Chapter 7, Conclusion and Recommendations, summarizes the findings about the priorities for the possible impacts of strategic intelligence on the national security and future structure of intelligence communities. Finally presents some suggestions for the determined priorities and points out the critical subjects that require future research.

METHODOLOGY

Descriptive study about strategic intelligence and its possible impacts on the national security is examined given subjects in 'Scope of the Study'. Intelligence cycle mentality is used, which is explained in chapter four (planning and direction, collection, processing, production and dissemination).

By the way in the first step, all interested areas have been selected, and program planned with time diagram. In the second step, in order to reach required information, literature review, Internet survey and interview have been used. Many books, articles, and military magazines have been examined to determine the characteristics of both the national security and strategic intelligence in order to reach the possible impacts of strategic intelligence on the national security.

In the third step, while analyzing, as the intelligence capabilities of nations are assessed as the secrets of that nation which is a critical component of national security, the emphasis is given on the conceptual approaches that are obtained by utilizing existing and uncovered academic resources. By taking into consideration the rational and objective methodological

criterion in the study, the possible parameters belonging to the strategic intelligence and the national security are tried to be uncovered.

In the fourth step, this thesis is prepared and in the last step, although there may be some deficiencies in this study as in all of the scientific studies, is presented to the future academicians. We hope that it will be helpful to all states and researchers.

"...all attempts to develop ambitious theories of intelligence have failed."

Walter Laqueur[3]

NATURE OF INTELLIGENCE

Initially, in order to create a wide range of the nature of intelligence, aimed to shape academic epistomologic dimensions. So we should understand what are intelligence and the other terms that are related with intelligence. Defining these terms are not easy to answer and, depending on whom you ask, you may get different answers. We should draw the framework in strategic perspective by using all kinds of definitions.

According to Kent[4], intelligence "has developed a recognized methodology; it has developed a vocabulary; it has developed a body of theory and doctrine; it has elaborate and refined techniques. It now has a large professional following. What it lacks is a literature.... The most important service that such a literature performs is the permanent recording of our new ideas and experiences." Kent saw this journal as a "rudimentary step towards making our findings cumulative." So let's look the terms, which are related with intelligence, beginning with the definition of intelligence.

WHAT IS INTELLIGENCE?

Many alternative approaches to intelligence have been suggested by a succession of authors. It is entirely possible that by asking "what is intelligence?". To answer this question I prefer the beginning with the definition of sociology. Because, human is as a social presence at center of the sciences. According to Universal English Dictionary, Intelligence is the facility of understanding, power of perceiving, knowing, reasoning; and Webster's Dictionary defines Intelligence as the ability to learn or understand from experience, the ability to acquire and retain knowledge; the ability to respond quickly and

---

[3] Laqueur, W., "A World of Secrets: The Uses and Limits of Intelligence" Basic Books Inc., New York, 1985, p. 8.

[4] Kent, S., "The Need for an Intelligence Literature" Central Intelligence Agency, Studies in Intelligence, 1955, Available on site http://www.cia.gov/csi/books/shermankent/2need.html

successfully to new situations; or the use of the faculty of reason in solving problems, directing conduct, etc., effectively.

By the way of this definition some words are related with intelligence (as an ability of comprehension) which are; knowledge & understanding, reasoning, thinking, calculating and logic skills, being able to communicate (language), perception ability (aware of environment). These occur core of intelligence science.

For the private sector, intelligence is the product of the collection, evaluation, analysis, integration, and interpretation of all available information (known as intelligence cycle[5]) that may affect the survival and success of the company. This information, which is well interpreted, can be immediately significant in the planning of corporate policy in all of its fields of operations which is stated in both operational and organizational terms, the main purpose of intelligence is to help the chief executive officer fulfill his wide-ranging responsibilities.[6]

But most people agree that intelligence is information needed by the nation's leaders, to keep their country safe[7]. With the way of this approach, since World War II, much effort has gone into defining "intelligence." This effort has even given rise to what is sometimes called intelligence theory, which can be traced to Sherman Kent's[8] desire to see intelligence programmatically examined, addressed, and included by the main stream social science tradition. His conviction that intelligence should he a broad-based analytical discipline is characterized in his maxim "intelligence is knowledge," which has set the precedent for most subsequent debate. [9]

---

[5] Intelligence cycle will explain in the chapter four.
[6] Eells, R.S., and Nehemkis, P. R., "Corporate Intelligence and Espionage: A Blueprint for Executive Decision Making" Macmillan, New York, 1984, p. 75
[7] CIA, "Who We Are and What We Do", Available on site http://www.odci.gov/cia/ciakids/spyguy /index.html
[8] During World War II Sherman Kent served in the Bureau of Analysis and Estimates of the US Office of Strategic Services, and later headed the office of National Estimates of the US Central Intelligence Agency (CIA). Almost all intelligence theory could be considered a footnote to Kent.
[9] Davies, P.H.J., "Ideas of Intelligence: Divergent National Concepts And Institutions", Hahvaro International Review, Fall 2002, pp.62-64

In this meaning, intelligence is a specialized information product that provides the states or an adversary with information required to further its national interests.[10]

One of the most important functions of intelligence is the reduction of the ambiguity inherent in the observation of external activities. In the most obvious case, adversary intelligence organizations may seek information concerning military capabilities or other matters that directly threaten the national security of the States. Karl von Clausewitz defines "By 'intelligence' we mean every sort of information about the enemy and his country— the basis, in short, of our plans and operations." [11]

The tendency of countries to employ differing definitions of intelligence has both conceptual and substantive implications. Substantively, it provides a particularly telling insight into how and why intelligence institutions take shape in specific ways. It is not, of course, the whole story; governmental, institutional, and even constitutional factors come into play but are significant in terms of why intelligence is conceived one way or another as well as in terms of what architectures are created and in what form.

Although definitions of this sort have their place within the world of intelligence, the full concept is much richer as inter-disciplinary field drawing upon contributions from history, political science, law, military science, sociology, mathematics, etc.

A useful starting point is the conceptual definition of the term ``intelligence'' which is direct related with our research is governmental approach. In this circumstance we should begin by looking at the definition by this glasses.

Intelligence is a body of evidence and the conclusions drawn from this point that is acquired and furnished in response to the known or perceived requirements of customers; it is often derived from information that is concealed or not intended to be available for use by the acquirer. It is the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign

---

[10] OPSEC Support Staff, "Operations Security Intelligence Threat Handbook" The Interagency OPSEC Support Staff Publishing, April 1996, Available on site http://www.fas.org/irp/nsa/ioss/threat96/

[11] Clausewitz, C., "On War" 1832, translated by Michael Howard and Peter Paret, Princeton University Press, Princeton, 1976/84, Compiled by Christopher Bassford, Bassford, 1998, Available on site www.clausewitz.com/CWZHOME/On_War/BK3ch01.htm.

countries or areas. [12] Or information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding[13] to decision-makers and to the production of intelligence as defined above.

The product resulting from collection, evaluation, analysis, integration, and interpretation of intelligence information about a foreign power that is significant to the national securing, foreign relations, or economic interests of the states, provided by a government agency that is assigned an intelligence mission (i.e., an intelligence agency).

Information should be relating to the ability of the states to protect themselves against actual or potential attack by, or other hostile acts of, a foreign power or its agents, or against the activities of foreign intelligence services.

If we look at the phenomena to which the term "intelligence" is applied; these phenomena include certain kinds of "information, activities, and organizations."[14] Intelligence applies to "information" related to a government's formulating and implementing policy to further its national security interests and to deal with threats to those interests from actual or potential adversaries. In the most clear and important case, this information has to do with military matters, such as an adversary's plans for military action. Potential or actual enemies typically do their best to keep this type of information secret. Also other types of secret information such as another country's diplomatic activities and intentions, as well as information about its intelligence activities may be equally important.[15]

In addition to information of this sort, many types of information about an actual or potential adversary may be useful to know, even though the adversary may not attempt to keep them secret. These could include information about internal political affairs and societal developments as well as economic and demographic statistics.

---

[12] GS-132, "Implementation of Army Occupational Guides (AOGs) for the Intelligence Specialist Series", Scientific and Technical Positions in Intelligence Production, 24 Apr 1991, p.20
[13] Joint Chiefs Of Staff, "Joint Doctrine Encyclopedia", U.S. Army Publishing, 16 July 1997, pp. 339-340
[14] Shulsky, A. N., "Silent Warfare: Understanding The World of Intelligence", (2nd edition), Revised by Gary Schimitt, Brassey's Publising, New York, 1993, p. 1
[15] Shulsky, A. N., Ibid, p. 2

Finally, intelligence information typically includes not only the "raw data" collected by means of espionage or otherwise, but also the analyses and assessments that may be based on it. It is this output, often referred to as the intelligence "product," which is typically of direct value to policymakers. To what extent this intelligence product should strive to present a comprehensive evaluation of a situation, based on all available data, both public and secret, may vary from one intelligence service to another. This is U.S. approach on information. Because; The United States approaches information as a specific component of intelligence, while Britain approaches intelligence as a specific type of information.[16]

As an "activity", intelligence includes the collection and analysis of intelligence information that related to the formulation and implementation of government national security policy. It also includes activities undertaken to counter the intelligence activities of adversaries, either by refusing them entry to information or by deceiving them about the facts or their significance.

Intelligence includes a wide range of activities. For example, there are various methods of collecting information, such as espionage, photography, intercepting communications, and research using publicly available documents and radio and television broadcasts. There also are different techniques for analyzing the information that has been collected: some of these may be similar to the methods the social sciences use, while others, such as the decryption of coded messages, are characteristic to the intelligence world. Similarly, refusing information to others includes various activities such as investigating suspected foreign intelligence agents to learn whether they are in contact with government officials.[17]

Looking at this wide variety of intelligence activities, it seems difficult to see any common thread running through them. Anyway, they have to do with obtaining or denying information. Therefore, intelligence as an activity may be defined as that component of the struggle between adversaries that deals primarily with information (as opposed to

[16] Davies, P.H.J., Ibid, pp. 64-66
[17] Shulsky, A. N., Ibid, p. 2

economic competition, diplomatic maneuvering or negotiations, or the threat or use of military force, etc.).[18]

Finally, the term intelligence also refers to the "organizations" that carry out these activities. One of the most notable characteristics of such organizations is the secrecy. Many of their methods of operation derive from this requirement such as the use of undercover agents or strict rules concerning access to information. Since intelligence agencies are organized to increase their capacity for secrecy, the responsibility of undertaking secret activities to advance their government's foreign policy objectives directly.

As you see intelligence is main instrument to defeat our adversaries or having a forward step from our rivals. As Frederick the Great indicated over two hundred years ago, "If you know the enemy's plans beforehand you will always be more than a match for him..." [19].

Intelligence has importance as Kent indicate, "there is no phase of the intelligence business which is more important than the proper relationship between intelligence itself and the people who use its products. Oddly enough, this relationship, which one would expect to establish itself automatically, does not do this. It is established as a result of a great deal of conscious effort"[20]which in every kind of administration.

In military, for a commander, intelligence is an essential element in planning and executing both combat and non-combat operations. It provides an assessment of an adversary's capabilities, vulnerabilities, and intentions, enabling the commander to employ combat power more effectively in attaining specific military objectives. Intelligence tries to reduce the uncertainty facing the commander, thus reducing risk to friendly forces. The commander's information requirements always must be the principal driver of the

---

[18] Shulsky, A. N., Ibid, p. 3
[19] Weinberg, G. L., "A World at Arms", Cambridge University Press, Cambridge, 1994, p. 25
[20] Davis, J., "A Policymaker's Perspective On Intelligence Analysis", (Sherman Kent, Strategic Intelligence for American World Policy, Princeton University Press, 1949, p.180.), Studies In Intelligence, 1995 edition, Vol. 38, No. 5, Available on site www.cia.gov/csi/studies/95unclass

intelligence effort. By clearly articulating his intent, the commander sets the tone for successful integration of intelligence within the command.[21]

On the other side in the interview with Ambassador Robert D. Blackwill indicate the relation between policymaker and intelligence analyst; "My job description called for me to help prepare the President for making policy decisions, including at meetings with foreign counterparts and other officials" and continues to describe a intelligence analyst as "should help key policymakers make the best game plan by telling them what they do not know or appreciate sufficiently.[22]

And intelligence in the meaning of collecting and analyzing information available through national security, "intelligence" may be contained in or derived from:

- Publicly available sources, including foreign and domestic broadcast and print media, government or private publications, and information available over computer networks;
- Personal observation or photographs taken by a person who is physically located at a particular point of interest;
- Privileged communications that officials have with their counterparts in other governments or international organizations;
- Photographs taken from air or space of areas that are otherwise inaccessible to persons on the ground;
- The interception of electronic signals or emanations, or the measurement of the physical attributes of things on the ground or in the air; or
- Persons who have access to places, persons, or things that are not otherwise available.[23]

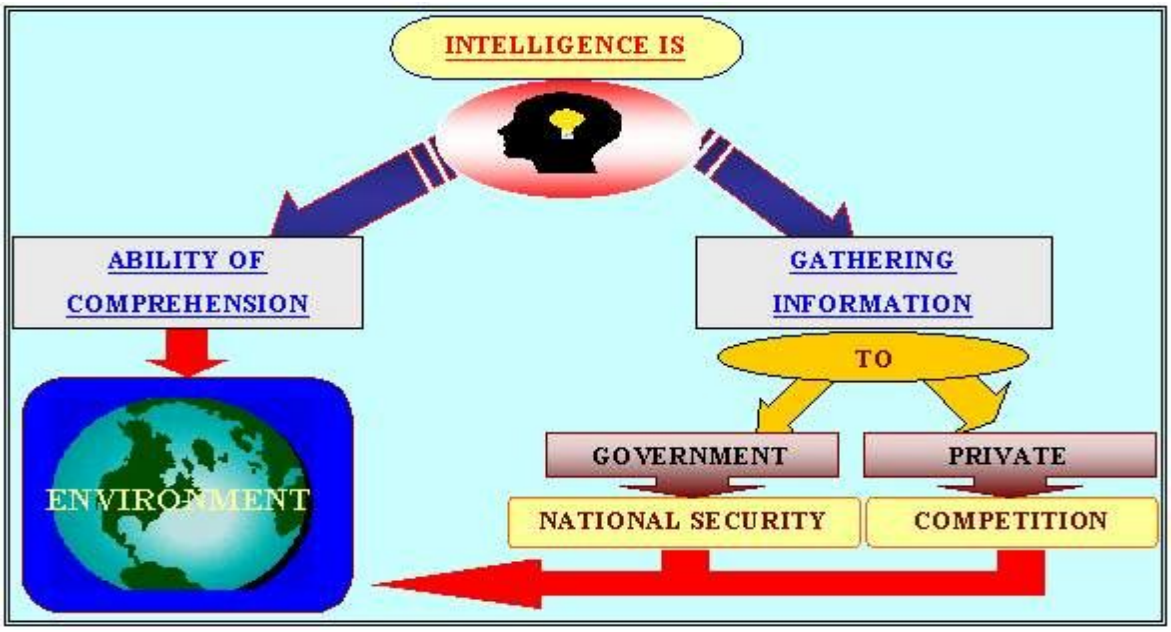
Until now we tried to describe what intelligence is in different fields. In sum we can say as Özdağ[24] said: " Today we should talk about a analyst who is S.Holmes, not 007 James Bond". So intelligence is intelligence. In other words, intelligence is a term as a gathering

---

[21] Department Of The Navy Office, "Naval Intelligence", Naval Doctrine Publication (NDP) 2, Washington, 1993, p.5
[22] Davis, J., "A Policymaker's Perspective On Intelligence Analysis", Ibid.
[23] US Government Print Office,"Preparing for the 21st Century: An Appraisal of U.S. Intelligence", March 1, 1996, Available on site http://www.access.gpo.gov/int/int023.html
[24] Özdağ, Ü., "Stratejik İstihbarat", Avrasya Dosyası (İstihbarat Özel), Summer 2002, No:2, Ankara, p.149,

of information by using the ability of comprehension. Summary of definitions about intelligence can be seen in figure 2.1.

Figure 0.1 Summary of Definition About Intelligence



DATA, INFORMATION AND INTELLIGENCE

Nothing is wrong with 'information' per se. Policymakers and commanders need information to do their jobs, and they are entitled to call that information anything they like. Indeed, for a policymaker or a commander, there is no need to define intelligence any further.

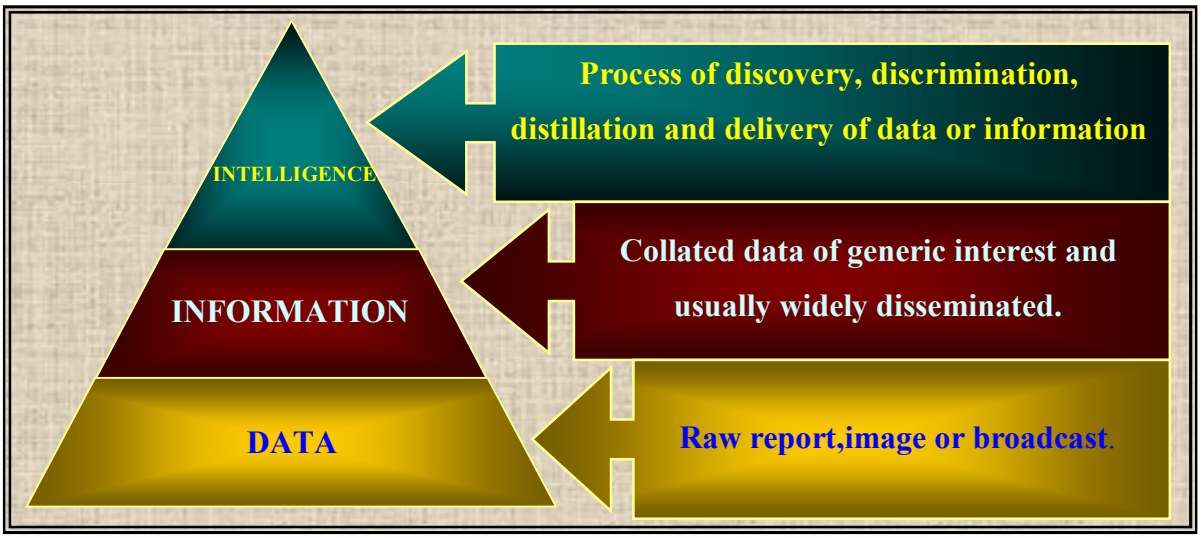
For producers of intelligence, however, the equation "intelligence = information" is too vague to provide real guidance in their work. To professionals in the field, mere data is not intelligence; thus these definitions are incomplete. Think of how many names are in the telephone book, and how few of those names anyone ever seeks. It is what people do with data and information that gives them the special quality that we casually call "intelligence."

Although we mentioned about intelligence and information, to arrive decisive point we should briefly draw the differences between data, information and intelligence as illustrated in figure 2.2.

“Data” is what you would expect. Raw data, collected from various sources (humans, communications, radars, and images), are fused by trained specialists and synthesized into a finished product. “Information” is generic collations of data, generally broadcast to large numbers of individuals. Information is collated data of generic interest and usually widely disseminated. “ Intelligence” is a process that answers questions for specific individuals and distinct from information in that it is the final product derived from data that has been closely scrutinized by human beings. By comparison, "Information is unprocessed data of every description which may be used in the production of intelligence."[25]

Using these definitions, we can assume the most of intelligence production, is actually classified information rather than classified intelligence. [26]

Figure 0.2 Data, Information and Intelligence



INTELLIGENCE IN NONGOVERNMENTAL ORGANIZATIONS

Although relation between intelligence and nongovernmental organizations (NGOs) has complex and deep subject, and today have a great affect on intelligence activities, I’ll briefly mention about meaning of intelligence in NGOs.

---

[25] Department of National Defence, “Joint Doctrine For Candian Forces Joint and Combined Operations”, B-GG-005-004/AF-000, Ottawa, Canada, 1995, p. 8-1

[26] Steele, R.D., “Overview of Open Sources & Services”, Available on site http://isuisse.ifrance.com/ emmaf2/96Vol1/ Chapter1.html

Information gathering in military operations other than war involving in depth coordination or interaction with nongovernmental organizations (NGOs) and private voluntary organizations (PVOs) and most UN operations, the term “information gathering” should be used rather than the term “intelligence.” The term “information gathering” is also appropriate in peacekeeping operations because peacekeepers must be overt, neutral, and impartial. Non-military organizations may resent being considered a source of intelligence.

These organizations may perceive that governmental forces are seeking to recruit members of their organizations for collection efforts, or turn the organizations into unknowing accomplices in some covert collection effort. NGOs and PVOs, by the very nature of what they do, become familiar with the culture, language, and sensitivities of a populace. This information is very valuable to military commanders as they seek to accomplish missions, which focus not on destroying an enemy, but on providing aid and assistance to the populace of a foreign country. By using the term “information gathering,” military forces may be able to foster better communications with other agencies, and thereby benefit from their valuable knowledge. [27]

THE SCOPE OF INTELLIGENCE

As we mention above not only governments but also many other types of organizations operate in an environment that takes place in a competitive struggle. The concept of intelligence might be applied to them as well as. For example, some researchers try to enlarge the concept to business corporations, treating intelligence as "organized information . . . designed to meet the unique policymaking needs of one enterprise."[28] Similarly, we could speak of the intelligence function of a political party or campaign in trying to figure out what the opposition is up to.

To make a frame the term of intelligence we should prefer a limit to its meaning. The limit of intelligence can be all information and activities relevant to the national security concerns of governments.

---

[27] Joint Chiefs Of Staff, “Joint Doctrine Encyclopedia”, U.S. Army Publishing, 16 July 1997, p. 330, Available on site www.fas.org/man/dod-101/dod/

[28] Meyer, H. E., “Real-World Intelligence”, Weidenfeld & Nicolson, New York, 1987, p. 6.

Also the nature of the regime affects the scope of intelligence is what is called domestic intelligence. Any government must be concerned not only with purely external threats but also with threats against its ability to govern, or its very existence, that arise from individuals or groups within the nation's borders. So a government defines also internal threats depends heavily on the type of government it is. [29]

Such as a totalitarian regime in which a dynasty or a single political party has a monopoly of power, is likely to regard any domestic political dissent as a security threat, and its intelligence service will focus a great deal of attention on detecting and thwarting it. In such states may regard all nonmembers of the ruling party as actual or potential enemies.[30] In the other side, in parliamentary and other democratic systems, implies that the government's domestic political opponents do not pose a security threat and hence are not a suitable concern of intelligence.[31]

There are questions concerning the function of intelligence agencies with respect to economic issues. As we mentioned before, much depends on the regime and its economic system. In a system under centralized government control, intelligence would be concerned with the economic aspects of the government's relations with foreign governments. In addition, intelligence can be used to increase the state's economic well-being. In a market economy, however, it is much less clear which economic issues have a national security dimension that justifies or requires the involvement of intelligence agencies.

Moreover, in a democratic society, economic policy is much more likely to be determined by the interplay of domestic economic interests than by any coherent view (whether or not based on intelligence information) of the future world economic environment. For these reasons, it is not clear whether the government in such a society would be an important consumer of such intelligence. Private economic interests could probably put it too much greater use, but

---

[29] Shulsky, A. N., "Silent Warfare: Understanding The World of Intelligence", (2nd edition), Revised by Gary Schimitt, Brassey's Publising, New York, 1993, p. 4
[30] Dziak, J.J., "Chekisky: A Story of the KGB", Heath&Co., Lexington Books, Lexington, 1988, p.42
[31] Mansfield, H.C., "Statesmanship and Party Government: A Study of Burke and Bolingbroke", University of Chicago Press, Chicago, 1965, pp .65-72

it is not clear how information gathered secretly at government expense would be distributed to individuals or corporations to further private interests. [32]

And also, the relationship between economic information and intelligence depends critically on the measure to which a nation sees its economic situation and relationships in national security terms. For some countries, in particular those with command economies, viewing economics in national security terms may be almost self-evident. For others, it depends on particular circumstances. For example, in wartime, intelligence means could be used to gain access to strategic materials, a key national security goal.

Similarly, in the course of negotiating with a foreign country on economic matters, a nation might use its intelligence capability to learn about its partners' negotiating positions. More generally, the appetite for economic intelligence on industrial, commercial, and financial activity in other countries would probably depend on whether a government has an industrial policy bureaucracy that could make use of it. As such, questions about the use of intelligence agencies to collect economic information is in large measure a surrogate for a more fundamental debate over government's role in directing economic future of a country. [33]

Finally, by the September 11th another related question deals with those transnational threats that do not appear primarily from a foreign government such as international terrorism or certain types of organized crime come in mind. These can be serious threats to a nation's well being, but they appear to be problems that come within the ambit of law enforcement with intelligence. Intelligence is often involved in the fight against them for several reasons. First, they involve activities in foreign countries. Intelligence may be called upon for information about the foreign aspect of these activities that would otherwise be unavailable.

Second, if a single incident, such as blowing up a passenger airplane in flight, may cause so much harm that it is necessary to prevent these crimes rather than merely solve them. Furthermore, a specific crime, such as attacking Twin Towers, in an international border, may be part of a criminal enterprise's operations; if the enterprise is large and well organized, arresting the perpetrators of a single crime may not have much impact on it. Finally, even if

---

[32] Shulsky, A. N., Ibid, p. 6
[33] Shulsky, A. N., Ibid, p. 7

agencies were content to wait until a specific crime occurred, the chances of solving it would depend heavily on their having a great deal of background information available about the organizations involved.

For these reasons, an intelligence approach is often adopted with these types of activity. Instead of waiting for a specific criminal act on which to focus, agencies gather information over a long time concerning various individuals and groups, their motivations, resources, interconnections, intentions, and so forth. Often it is necessary to use informers who penetrate the groups involved and who operate like spies. It also may be possible to intercept communications or use other technical methods of collecting information.

Thus, intelligence agencies are often involved in the fight against such groups. Depending on the regime, agencies' involvement may be limited to the foreign aspects of these activities while domestic aspects remain in the purview of law enforcement agencies. Even in these cases, however, law enforcement agencies often must resort to some intelligence techniques to deal with organized criminal groups. [34]

WHY STRATEGY IS NECESSARY?

Let us first be clear as to what is strategy. Clausewitz, in his monumental work, “On War”, defined it as the art of the employment of battles as a means to gain the object of war. In other words strategy forms the plan of the war, maps out the proposed course of the different campaigns, which compose the war, and regulates the battles to be fought in each.[35] The defects of this definition are:

- It intrudes on the sphere of policy, or the higher conduct of the war, which must necessarily be the responsibility of the government and not of the military leaders it employs as its agents in the executive control of operations.
- It narrows the meaning of “strategy” to the pure utilization of battle, thus transmitting the idea that battle is the only means to the strategically end.

It was an easy step for Clausewitz's less profound disciples to confuse the means with the

[34] Shulsky, A. N., Ibid, p. 6
[35] Clausewitz, C., Ibid.

end, and to reach the conclusion that in war every other consideration should be subordinated to the aim of fighting a decisive battle.[36]

So we can define strategy is the art and science of developing and using political, economic, psychological, and military forces as necessary during peace and war, to afford the maximum support to policies, in order to increase the probabilities and desirable consequences of victory and to reduce the chances of defeat.

Strategy is necessary for the strategic direction of the all forces. Chairman Of The Joint Chiefs of Staff Instruction describe these necessity areas as:

- Establishing policy
- Determining requirements
- Developing plans
- Allocating resources. [37]

National security strategy and national military strategy shaped by and oriented on national security policies. These strategies integrate national and military objectives (ends), national policies and military concepts (ways), and national resources and military forces and supplies (means). [38] National strategic directions (in figure 2.3.) show the relations between national strategy, policy, interest and plans.

Best strategy is important and difficult, because it is always to be very strong, first in general, and then at the decisive points.[39] There are three reasons why it is difficult to do strategy well:

- It is very nature, which endures through time and in all contexts
- The multiplicity and sheer variety of sources of friction
- It is planned for contexts that literally have not occurred and might not occur.[40]

---

[36] Liddell, H.B., "The Classical Book On Military Strategy", (2nd Edition), Meridian Publishing, New York, 1991, p. 319

[37] Joint Staff of US Navy, "Chairman Of The Joint Chiefs Of Staff Instruction", J-5, 1 September 1997, Available on site www.dtic.mil/doctrine/jel/training_pubs/3150_05.pdf, Enclosure, p. B-2

[38] Joint Chiefs Of Staff, "Joint Doctrine Encyclopedia", U.S. Army Publishing, 16 July 1997, p.628, Available on site www.fas.org/man/dod-101/dod/

[39] Jomini, A. H., The Art of War, Greenhill Books, London, 1992, p. 70

Figure 0.3 National Strategic Directions[41]

Clausewitz explains, "everything in strategy is very simple, but that does not mean that everything is very easy."[42] There are five reasons that are; first, strategy is neither policy nor armed combat; rather it is the bridge between them. Second, strategy is perilously complex by its very nature. Every element or dimension can impact all others. Third, it is extraordinarily difficult, perhaps impossible, to train strategists. Fourth, strategy accepts all aspects of the military instrument (among others), as well as many elements of the polity and society it serves, the maximum possible number of things can go wrong. Finally, it is critical to flag an under recognized source of friction, the will, skill, and means of an intelligent and malevolent enemy.

Andre Beaufre defines strategy as "the art of the dialectic of force or, more precisely, the art of the dialectic of two opposing wills using force to resolve their dispute."[43] Recall Clausewitz's idea: "War is thus an act of force to compel our enemy to do our will."[44]

---

[40] Gray, C. S., "Why Strategy Is Difficult", Joint Force Quarterly (JFQ), Summer 1999, p.6
[41] Joint Chiefs Of Staff, "Joint Doctrine Encyclopedia", Ibid, p.628
[42] Clausewitz, C., Ibid.
[43] Beaufre, A., "An Introduction to Strategy", Faber and Faber, London, 1965, p. 22.
[44] Clausewitz, C., Ibid.

It is vital to recognize potential tension in three sets of relationships: between politicians and commanders, between commanders and planners, and between commanders and theorists. Military professionals must simplify, focus, decide, and execute. Politicians, by virtue of their craft, perceive or fear wide branches of action and like to keep their options open as long as possible by making the least decision as late as possible.

The reasons for strategic success can be categorized:

- The forces must be internally coherent, which is to say competently joint,
- To be of a quantity and provide a strategic effect scaled to the tasks set by high policy,
- To be employed coercively in pursuit of military objectives that fit political goals.[45]

Because of the future is unexpectable, specifically, we plan to behave strategically in an uncertain future on the basis of three sources of practical advice: historical experience, the golden rule of prudence, and common sense. We can educate our common sense by reading history. But because the future has not happened, our expectations of it can only be guesswork. Historically guided guesswork should perform better than one that knows no yesterdays. Nonetheless, planning for the future, like deciding to fight, is always a gamble. So we can say intelligence without strategy is impossible.

NATIONAL SECURITY AND INTELLIGENCE RELATIONS

Since the term "national security" is itself unclear, the limitation does not sufficiently define the scope of intelligence. Its core meaning has to do with protecting a nation against threats, ultimately military, emerging from foreign nations. When a nation is or is about to be invaded, its national security concerns clearly center on preventing or defeating the invasion and securing itself against a similar situation arising in the future. In a less bad situation, it may be much less clear which foreign nations, events, or circumstances can threaten national security and therefore require attention by the nation's intelligence.[46]

---

[45] Gray, C. S., Ibid, p.7
[46] Shulsky, A. N., Ibid, p. 4

The problem is further complicated by the fact that national security interests and threats to them cannot be considered independently of the type of the regime and its ideological perspective. Although a nation's interests are determined by the objective factors of the international system, ideological views and a country's political culture more generally affect how a government perceives them. In particular, status quo and revolutionary powers are likely to have different views about what constitutes a threat to national security. [47]

In the frame of this scope, when we look the explanations; Defense Dictionary of U.S. define national security as "the condition provided by: (a.) a military or defense advantage over any foreign nation or group of nations, or (b.) a favorable foreign relations position, or (c.) a defense posture capable of successfully resisting hostile or destructive action from within or without, overt or covert." From the costly lessons of World Wars to recent transnational terrorist attacks, the world learned that its national security is dependent upon a wide spectrum of conditions and activities, both within a state and around the world. National objectives, closely related to national interests, support the national security by protecting and reinforcing those values. [48]

Defense of the national security rests first on the concept of deterrence. By demonstrating national decision and maintaining the ability will be successful to deal with threats to the national interests. [49] Readiness that can obtain with intelligence, reduce the all type of risks.

National security interests are those actions or conditions we feel are essential to the survival of a nation. Defense Dictionary of U.S. defines national security interests as those which preserve "...political identity, framework, and institutions; fostering economic well-being; and bolstering international order supporting the vital interests..."[50]Donald E. Nuechterlein[51] created a way of distinguishing the importance of different interests as "Intensity of Interest" model in Table 1.3.

---

[47] Richelson, J., "The U.S. Intelligence Community", Ballinger Publishing, Cambridge, 1985, pp. 5-16
[48] Joint Chiefs Of Staff, "Department of Defense Dictionary of Military and Associated Terms", Joint Pub 1-02, 23 March 1994, As Amended Through 7 December 1998, Washington, p. 318, Available on site www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf
[49] Joint Chiefs Of Staff, "Joint Doctrine Encyclopedia", U.S. Army Publishing, 16 July 1997, p. 542, Available on site www.fas.org/man/dod-101/dod/
[50] Joint Chiefs Of Staff, "Department of Defense Dictionary of Military and Associated Terms", Ibid, p. 319
[51] Nuechterlein, D. E., "America Overcommitted: United States National Interests in the 1980's", 1985, Available on site http://dde.carlisle.army.mil/authors/RSA%20_Aid2001.pdf

Table 0.1 Model of Intensity of Interest[52]

INTENSITY OF INTEREST				
BASIC INTEREST	SURVIVAL	VITAL	MAJOR	PERIPHERAL
Defense of Homeland				
Economic Well-being				
Favorable World Order				
Promotion of Values				

A Survival Interest exists when the physical existence of a country is in danger due to attack or threat of attack. Clearly, this is the most basic interest the state has. The second level of intensity is Vital Interest, which involve circumstances that would result in serious harm to the nation unless strong measures, including the use of force, are employed to protect the interest. The third level of interest is Major Interests where a country's political, economic, or social well-being may be adversely affected but where the use of armed force is not necessary. The fourth level of interest is Peripheral Interests, which involve some national interest but where the nation as a whole is not particularly affected by any given outcome.[53]

National security interests specify why a nation is involved in a given situation, but national objectives state what the nation wants. It is the national objectives that guide policy formulation.[54]

To executive the national security every state has different precaution. For example in U.S. there are over 180 federal agencies play for homeland security. From the Department of Agriculture to the Department of Transportation, lines of authority, responsibility and communication blend, blur and sometimes break. [55]

Effective homeland security isn't simply smart spies and cops. It requires switchboard operators (and very able computer jockeys) who know how to connect complex and time-

[52] Nuechterlein, D. E., Ibid.
[53] Drew, D.M., and Snow, D.M., "Making Strategy: An Introduction to National Security Processes and Problems", Air University Press, 1988, pp. 27-30
[54] National Intelligence Course (NIC) Textbook, Joint Military Intelligence Training Center, November 1999, Chapter 6, p. 1
[55] Bay, A., "Homeland Security: Disseminating the Information, No Easy Task", Aug 1, 2002 Available site on www.strategypage.com/ inetpub\strategypageroot\onpoint\docs\20020801.htm

critical conference calls.[56]In the Table 2.2 you can see the U.S. Critical Infrastructure in 2002.[57]

Table 0.2 Constitutes Critical Infrastructures Over Time[58]

Infrastructure	Criteria for Being Considered Critical. Vital to			
	national defense	economic security	public health and safety	national morale
telecommunications information networks	x	x		
energy	x	x		
banking/finance		x		
transportation	x	x		
water			x	
emergency services			x	
government			x	
health services			x	
national defense	x			
foreign intelligence	x			
law enforcement			x	
foreign affairs	x			
nuclear facilities, in addition to power plants			x	
special events				x
food/agriculture			x	
manufacturing		x		
chemical			x	
defense industry	x			
postal/shipping			x	
national monuments icons				x

Another term which is related with national security; national objectives[59] which are defined as "the aims, derived from national goals and interests, towards which a national policy or strategy is directed and efforts and resources of the nation are applied." Policies are designed and actions are taken specifically to meet our national objectives.

[56] Bay, A., Ibid.
[57] Report for Congress, "Critical Infrastructures: What Makes an Infrastructure Critical?", Library of Congress, p. CRS17, Available on site http://www.fas.org/irp/crs/RL31556.pdf
[58] Report for Congress, Ibid.
[59] National Intelligence Course (NIC) Textbook, Ibid, Appendix, p. 14

Occasionally, these objectives have been overly broad in nature and difficult to qualify or quantify.

Intelligence takes places at the bottom of national security house. Summary of all we explain about national security can be seen in figure 2.4.

Figure 0.4 Relation of Intelligence and National Security's Summary

LEVELS OF MODERN WARFARE

Intelligence locates in every phase of war. But depending intelligence level and aim have been called different names as level as war. To understand how appear these levels, we can look at levels of war and compare with them.

The levels of intelligence correspond to the established levels of war that is described in Joint Doctrine Encyclopedia as "doctrinal perspectives that clarify the links between strategic objectives and tactical actions. Although there are no finite limits or boundaries between them, the three levels, in general, are strategic, operational, and tactical."[60]

Levels of command, size of units, types of equipment, or types of forces or components are not associated with a particular level. National assets such as intelligence and communications satellites, previously considered principally in a strategic context, are an important adjunct to tactical operations. Actions can be defined as strategic, operational, or

[60] Joint Chiefs Of Staff, "Joint Doctrine Encyclopedia", U.S. Army Publishing, 16 July 1997, p.458, Available on site www.fas.org/man/dod-101/dod/

tactical based on their effect or contribution to achieving strategic, operational, or tactical objectives, but many times the accuracy of these labels can only be determined during historical studies.

Advances in technology, information ages media reporting, and the compression of time space relationships contribute to the growing inter-relationships between the levels of war. These levels can be explained as;

1.1.1 The Strategic Level

The Strategic Level of war at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) strategic security objectives and guidance and develops and uses national resources to accomplish these objectives. Strategy is the art and science of developing and employing armed forces and other instruments of national power in a synchronized fashion to secure national or multinational objectives. The National Authorities translate policy into national strategic military objectives. These military objectives facilitate theater strategic planning. [61]

1.1.2 The Operational Level

The Operational Level links the tactical employment of forces to strategic objectives. The focus at this level is on operational art — the use of military forces to achieve strategic goals through the design, organization, integration, and conduct of strategies, campaigns, major operations, and battles. [62]

1.1.3 The Tactical Level

The Tactical Level includes the ordered arrangement and maneuver of units in relation to each other and/or to the enemy in order to use their full potential.[63]

---

[61] Joint Chiefs Of Staff, "Joint Doctrine Encyclopedia", Ibid, p.458
[62] Joint Chiefs Of Staff, "Joint Doctrine Encyclopedia", Ibid, p.459
[63] Joint Chiefs Of Staff, "Joint Doctrine Encyclopedia", Ibid, p.460

In each level of war that can be seen in figure 2.4; intelligence takes place but also levels of intelligence change depend on the level of war, the aim of intelligence, the instruments that is used, can be change.

Figure 0.5 Levels of War[64]

[64] Joint Chiefs Of Staff, "Joint Doctrine Encyclopedia", Ibid, p.459

"During the Second World War, major encounters between Germany and its Western foes were, in almost all instances, profoundly affected by effective utilization, misreading or neglect of intelligence."

Harold C. Deutsch[65]

HISTORICAL PERSPECTIVE OF INTELLIGENCE EVOLUTION

It is difficult to understand the importance of intelligence in peace. But when war started, it is too late to gather intelligence. So to take lesson we should look in history.

To make informed decisions about what kind of intelligence system we need we must have a reasonably clear view of the character of the next phase in international politics and its implications. Historical analysis of intelligence revolution will open a new perspective on our minds.

I prefer to use four phases of this revelation, which are; until World Wars, during the World Wars, in the Cold War that is in two phase. And at the conclusion I analyzed all this period focusing especially on Cold War.

OVERVIEW ON PROBLEM

The way of future based on tree main factors that are; history, assessment of today's situation and forecast of future. The information is located in core of them.

The assessment of the information toward to our aim by using technology and sense of human is directly intelligence. A point to be made at the outset is the enormous difference between the scale on which you operate today and our own efforts through out the history, and so lessons based on the experiences must be drawn with caution.

---

[65] Deutsch, H.C, "Commanding Generals and the Uses of Intelligence," In Intelligence and National Security 3, No: 3, 1988, p 194.

In order for doctors to prescribe an appropriate remedy, they must first document the symptoms of an illness and establish a cause. A similar approach will be used for this paper. By examining a mixture of theory and historical evidence we will attempt to determine the causes of intelligence failure.

The stories of intelligence successes and failures are numerous indeed. In this chapter is highlighted only a few.

DEVELOPMENT PROCESS OF INTELLIGENCE UNTIL XXTH CENTURY

Although in my opinion history of intelligence arrive until first humanity, as we know the documents on intelligence have existed for thousands of years. One of the oldest references to the craft of intelligence can be found in The Art of War which is attributed to Sun Tzu who is a Chinese General, in circa 500 BC, is written as "to remain in ignorance of the enemy's condition simply because one grudges the outlay of a hundred ounces of silver in honors and emoluments, is the height of inhumanity."[66] In this passage, he was referring to spending for intelligence (or knowledge) proportionately to the spending for combat operations.

The first recorded Human Intelligence (HUMINT) dispatch can be found in 490 B.C., another example of the successful use of knowledge of the organization and fighting qualities of an opponent occurred. A force from the Greek city-state of Athens, led by Miltiades, who had at one time served with the Persians, faced a Persian force that outnumbered his own forces by two to one. Miltiades knew about the Persians light armor and their reliance on undisciplined mass formations. He supposed that if the Athenian forces did not immediately engage the Persians, then the Persians would break out of the coastal plain and overrun Athens and the surrounding area. His force of well-armored Athenians utilized long spears and tight formations. Miltiades believed that he could defeat the Persians on the coast, and by using coast watchers and runners to inform him when the Persians landed; he engaged the Persians and defeated them at Marathon.[67]

---

[66] Phillips,T.T., ed., "Roots Of Strategy, The Art of War", Stackpole Books Publishing, Pennysylvania, 1985, p. 60.
[67] Liddell, H.B., "The Classical Book On Military Strategy", (2nd Edition), Meridian Publishing, New York, 1991, p.7

Miltiades used a good intelligence database, accurate and timely intelligence reporting, and effective incorporation of dynamic intelligence data into tactical plans to defeat the Persians, the ultimate effect of which was to allow Greek culture to flourish and leave its mark on all Western civilization.

Another example that had been occurred by Julius Caesar in first landing in Britain in 55 B.C. Julius Caesar describes the intelligence gathering process and storied as:

> "Summer was now drawing to a close, and winter sets in rather early in these parts, as Gaul lies wholly in northern latitudes. Nevertheless I hurried on preparations for an expedition to Britain, knowing that Britain had rendered assistance to the enemy in nearly all my Gallic campaigns. Although it was too late in the year for military operations I thought it would be a great advantage merely to have visited the island, to see what kind of people the inhabitants were, and to learn something about the country with its harbors and landing places. Of all this the Gauls knew virtually nothing; for no one except traders makes the journey with any regularity, and even their knowledge is limited to the sea coast immediately facing Gaul. Interviews with numerous merchants elicited nothing as to the size of the island, the names and strength of the native tribes, their military and civil organization, or the harbors, which might accommodate a large fleet. Nevertheless it seemed essential to obtain this information before risking an expedition, and Caius Volusenus appeared to me the best man for the job. He traveled in a warship with orders to make a general reconnaissance and report back as early as possible. Meanwhile the whole army moved into Artois, where the mainland is nearest to the coast of Britain; and ships were ordered to assemble there from all neighboring districts, including the fleet, which had been built last year for the Venetian campaign. Meanwhile, however, some traders revealed our plans to the Britons, and a number of tribes sent envoys promising hostages and offering their submission. They were received in audience, promised generous terms, and urged to abide by their undertaking. They were accompanied on their return journey by Commius, whom I had appointed ruler of the Atrebates after the subjugation of that people, and of whose honor, discretion, and loyalty I had received abundant proof. Commius was greatly respected in Britain, and his

orders were to visit all the states he could, impressing on them the advantages of Roman protection, and to announce my impending arrival. Volusenus completed his survey as far as e was able without disembarking and risking a hostile reception from the natives. Five days later he returned and made his report....”[68]

Some examples of intelligence can be seen in holy books. For example in the Bible;

"Moses sent them (twelve men) to spy out the land of Canaan, and said to them, Go up this way by the South, and go up into the hill country; and see the land, what it is; and the people who dwell therein, whether they are strong or weak, whether they are few or many; and what the land is that they dwell in, whether it is good or bad; and what cities they are that they dwell in, whether in camps, or in strongholds; and what the land is, whether it is fat or lean, whether there is wood therein, or not…”[69]

In this reference, Moses sent twelve men to explore Canaan and report back to him what sort of land it was. To put this in perspective, imagine, if you will, the Israelites, a nomadic tribe, wandering the desert for many years.

The Israelites and the Canaanites had some type of military force to carry out their objectives. Their objectives were mutually exclusive. What Moses was really asking his explorers to do was to find out how well defended the people of Canaan were, how satisfied they were with their lot in life, their government or lack of it, their land, and to report to him their vulnerabilities. Moses wanted to know, as any military or political leader would, if he had to mount a massive or token campaign to achieve his objective.

This story contains most of the elements of strategic intelligence. The collection requirements included requests for information on the economic qualities of the land, the vitality of its people, and their military strength as a basis for policy judgments. This information produced disagreement show the importance of the historic uncertainties of major decisions.

---

[68] Hastings, Max, ed., “Military Anecdotes”, Oxford University Press, New York, 1985, pp. 41-42.
[69] “The World English Bible (WEB)”, The Book Of Numbers, Chapter 13, Available on site www.ebible.org/ bible/web/ webrft.zip

In 624 A.D., the prophet Mohammed fled from Mecca to Medina. The non-Muslim authorities at Mecca gathered some 10,000 men to attack and destroy him. Clandestine intelligence collectors were left behind to gather information about such movements and report them to him. Mohammed ordered defenses to be built at Medina, which surprised those who were pursuing him, since they expected an easy overrun of a minimally defendable position. Heavy rains fell as the attackers considered their course of action, and the rains disrupted the camp to such a degree that the army dwindled and finally departed without making any assault. As a result, Islam lived and flourished and has become a strong force in the world. [70]

In the 16th century, the rulers of the Ottoman Empire learned that there had been a major fire at the gunpowder factories in Venice, with vast explosions that destroyed the Venetian fleet. They decided to attack Venice while it was in a weakened military position, and to give an ultimatum to the Venetians. On receiving the ultimatum from the Ottoman Empire, the Venetians, who in fact had lost only four vessels to a fire, enlisted the support of other European powers. In 1571, a naval battle followed at Lepanto, and the Ottoman fleet suffered a decisive defeat. This event marked the end of the uninterrupted western expansion of the Ottoman Empire. With evident the Turkish campaign originated with inaccurate information that better communication could have excluded. The Turks acted on not verified information, and it led to their ultimate defeat. [71] As seen in this example; Bad intelligence is worse than no intelligence.

In 1759, the French Commander in Canada, Montcalm, planned his defenses against the English along the line of Lake Champlain and Fort Niagara. Montcalm learned from an intercepted letter of the British Commander, that the campaign against Quebec was to be by sea and the St. Lawrence River, instead of the western route as expected. With this warning, the French assembled their defenses at Quebec, which were then considered almost impregnable. The British Commander, knowing that he had lost the element of strategic surprise, resorted to tactical intelligence. He had in his army a man who was held prisoner by the French in Quebec, where he learned of a steep trail up the high embankment

[70] National Intelligence Course (NIC) Textbook, Joint Military Intelligence Training Center, November 1999, Chapter 1, p.1
[71] National Intelligence Course (NIC) Textbook, Ibid, p.2

from the river to the plain behind the fort. The French considered the trail too steep and narrow to be used by significant military forces and left it undefended. The British Commander moved his forces up the trail, took the French by surprise, and won the battle that followed on the Plains of Abraham behind the fortified city. [72]

On all scales of operation skilled the men and cooperative action were ingredient factors, but the balance of importance between them changed with scale. Similarly, in intelligence personal skill may be the paramount factor on the small scale, but the ability to coordinate the skills of many individuals may be predominant in large-scale operations.

STRUCTURAL EXCHANGE PHASES THE INTELLIGENCE PHENOMENA DURING THE GLOBAL WARS

The most disastrous events of humanity were World Wars. This period was a fortunate and exhilarating time to be involved in intelligence, when new channels of information were opening up, and when we could quickly see the effects of the work on the operation of war. By the wars importance of intelligence increased.

Although the state of technological developments over a wide range of fields was still elementary, have profound effects on warfare. Electronics, for example, was in transition from the "steam age" of radio to the sophistication of television, radar, and devices.

1.1.4 Intelligence Analysis of World War I

The period until WW I is awash with stories of intelligence operations, including one of the earliest military aerial photographic reconnaissance by balloonists. In beginning of the war the balloon is continued to use especially landing of agents by “free balloon”.

Silence therefore became an essential desideratum and it was eventually proved after experimental flights that it was a feasible operation to land agents by means of free balloons, provided weather, wind and other circumstances were favorable. But in the other side, at the same time, efforts had been directed towards the improvement of methods of communication such as the portable continuous wave set which was far ahead of anything

[72] National Intelligence Course (NIC) Textbook, Ibid, pp. 3-4

in wireless apparatus, was believed to be incapable of detection by any means of position finding and detective organization known to wireless experts either on one or other side.[73] Between 1913 and 1915 the U.S. Army in the Philippines and along the Mexican border flew visual and photographic reconnaissance missions.[74]

In the other hand the different ways of coding things became numerous in WWI. Coding could be found in combs, buttons, sheet music and even glass eyes. The all-purpose of coding was to give someone information and make sure that they could figure it out until the information had little or no value. French and British would dress up like civilians and be able to travel easier. The problem with dressing like a civilian is that if you are caught the Germans had orders to shoot you without delay. During WWI telephones were also use but instead of freely talking the soldiers would say phrases like "Looks like rain" and would know that meant move back or something of that sort. Most spies really were not spies until they helped someone. Once a Prussian found a bulletin about Russian too much deployment and in a cart of hay brought it to the Germans. [75]

In 1917 during the Middle East Battles, the information that the existing agents were able to provide was second-hand only, derived from visual observation of limited-mostly tactical-value, rumours or accidental contact with the German and Ottoman military. British Intelligence cryptanalysts failed to break the principal cipher used by the Ottoman Yıldırım Army Group, while the ottomans themselves relied extensively on wire-line communications, which the British were unable to monitor. The most significant development was enhanced visual air reconnaissance over Sinai and Palestine by the Royal Air Force squadrons and real-time tasks artillery and blinding topographic data reporting with aircraft and ground forces Royal although based on the Egypt-Sina-Palestine Airforce logistic operational supports.[76]

---

[73] Drake, R.J., Lieut. Colonel, General Staff., 5 May 1919, History of Intelligence (B), British Expeditionary Force, France, From January 1917 To April 1919, Available on site www.lib.byu.edu

[74] Burrows, W., "Deep Black: Space Espionage and National Security", Random House Publising, New York, 1986, pp. 28, 32.

[75] Albuquerque Public Schools, "Military Advancements During WWI", Available on site http://www.aps.edu/APS/EISENHOWER /Mercer/class/wars/ww1 /Matt.htm

[76] Caşın, M.H., "Strategic Effects of World War I to International Security and Power Balances In The Middle East", The First World War: Middle Eastern Perspective, Israel-Turkish International Colloquy, Tel-Aviv, April 2000, p.13

1.1.5 Intelligence Analysis of World War II

The main difference between the world wars, in technological mean, is the invention of the radar, which effected the direction of war. But especially in Second World War is opened a new way to technologic intelligence efforts by cryptology.

In 1929, a blow to states cryptologic efforts occurred. By the way in ten years continued the code-making and code-breaking operations. Especially during the period 1939-1945 with MAGIC[77] and ULTRA[78], the code name under which highly sensitive intelligence resulting from the solution of high-grade codes and cyphers was passed between selected allied individuals.

A decisive event in breaking the German cyphers and the subsequent evolution of ULTRA occurred when pre-war (1939) Polish intelligence officers, in concert with their government's attempts at defending against a German attack and therefore contributing to the cause of an Allied victory over Germany, turned over to the French and British duplicates of the German Enigma machine[79] used for encoding messages.

Although the procurement of the German Enigma machine proved to be the most noted event in the development of special intelligence, other factors contributed as well. In fact, by 1943 British cryptographers had also broken into the German "secret writing machine," (the geheimschreiter) a different encoding system from Enigma.

The specifics of the evolution of the special intelligence system not with standing, the ULTRA network proved highly reliable giving those trusted with the secret a clear view of the enemy's operations and intentions.

The ULTRA secret remained. In fact by the end of the war, the information became so complete and comprehensive--not merely of military significance, but also political and

---

[77] US code name given to intercepts of Japanese codes.
[78] Allied intelligence system that, in tapping the very highest-level communications among the Germen armed forces, as well as (after 1941) those of the Japanese armed forces, contributed to Allied victory in World War II.
[79] The Enigma is a cipher machine which was created by a native born German, Arthur Scherbuis. Its function is based on the principle of the rotor, which is a wired codewheel (for advance information Mody R., “The Enigma Machine”, http://militaryhistory.about.com/gi/dynamic/offsite.htm).

economic--that the enemy could scarcely make a move without the Allies knowing of it and thereby enjoying the advantage of meeting him at a controlled time and place. Indeed, without Special Intelligence the war most certainly would have been much more costly in terms of lives lost in the defense of freedom.[80]

The period between the wars non-only passed using single intelligence, and also the failures occurred. For example; failure of former Soviet Russian head of state Josef Stalin over Germany's invasion; Miscalculation of strategies in war planning; Significance of intelligence on the conduct of war.

Britain and France used intelligence on Germany to confirm that Hitler could be deterred and war averted by Western firmness; Hitler used intelligence on the West to confirm his view that in 1939 Poland could be brought to heel without a wider European war. The position of both sides was strengthened, so it was believed, by evidence that the Soviet Union would not be used by the other side to swing the balance of power in its favour. These were miscalculations, which in the end locked both sides into positions from which it was almost impossible to retreat, and determined that the crisis, when it reached boiling point in the last week of August 1939, would result in war. [81]

In 1939 the central problems in communicating and evaluating intelligence were organizational and political. In all the major states intelligence were gathered by a wide number of agencies and by the separate branches of the armed forces. In most cases assessment was neither systematic nor well integrated. The need for cooperation was greater in the case of intelligence, because at some point it had to be communicated to the highest level of decision-making. [82]

The failure of the West to construct a firm military front among the smaller states, revealed by regular reading of western diplomatic traffic with south-eastern Europe, Turkey and

[80] Weinberg, G. L., "A World at Arms", Cambridge University Press, Cambridge, 1994, p. 25
[81] Weinberg, G. L., Ibid, p.26
[82] Weinberg, G. L., Ibid, p.27

Poland, permitted Hitler to run greater risks over Danzig than he might otherwise have done.[83]

The German perception of Western attitudes to Poland hinged on two main kinds of intelligence: the German estimate of British and French military strength, and German analysis of the weak political situation of the democracies. Intelligence estimates of Western Military Powers consistently played down the achievements of Western rearmament.

Another example takes place in the Pacific Ocean on December 7, 1941. Japan was on the attack. Information from pointed to a Japanese strike being mounted somewhere in Southeast Asia on either November 30 or December 7.[84] US Naval Commanders reinforced this tactic by allowing their aircraft carrier battle group to be observed steaming south (perception and misperception of reality). This deception plan was planted in fertile soil. Japan took advantage of a perceived US military superiority arrogance that Hawaii was an impregnable fortress.

The US intelligence on Japan was not lacking intelligence reports from Japan reinforced rumours of an intention to attack. They were discounted. Similarly, submarine sightings near Hawaii, Communication intelligence (COMINT) ordering Japanese codes to be destroyed, radar information reporting approaching unidentified aircraft were all intelligence indicators that were dismissed.[85] According to the US Senate report on Pearl Harbor, "[Intelligence Officers'] efforts were unsuccessful because of the poor repute associated with intelligence, inferior rank, and the province of the specialist...."[86] The success of the Japanese operation speaks for itself. The element of surprise is the revenge

---

[83] Weinberg, G. L., Ibid, p.28
[84] Finley, J.P., "Nobody Likes to be Surprised: Intelligence Failures," In Military Intelligence, Vol 20, No. 1 (January-March), 1994, p. 15
[85] Wohlstetter, R., "Pearl Harbor: Warning and Decision", Stanford University Press, Stanford, 1965, pp 312-316
[86] United States Congress, "Senate Report of the Joint Committee on the Investigation of the Pearl Harbor Attack", US Government Press, Washington, 1946, Available on site http://www.ibiblio.org/pha/pha/congress/part_0.html

of intelligence. On the US side, Pearl Harbor was labeled as an intelligence failure and military intelligence was reorganized.[87]

Until the Cold War, most efforts went toward current intelligence such as studies of the enemy, weather, and terrain Army forces were likely to encounter. Prior to World War II, strong parochial and isolationist influences caused the Army to weigh factors other than intelligence (or strategic planning) in shaping Army decisions about technology, doctrine, and force structure.[88]

Between the wars, each command and department continued to supply its own intelligence to support individual command requirements. It was largely because of this "individuality" that warning of the attack on Pearl Harbor was not adequately disseminated. It was proposed that intelligence should be coordinated, by forming one Department of Intelligence reporting directly to the president.

To see the increasing importance of intelligence in the WWII, the other two examples, first is Manchuria operation of Soviet Army. In this operation 30 percent of total aircrafts of Soviet Air force which were used for intelligence and reconnaissance. [89]Second the agents that used by Britain in the war roughly 6,000. As far as is known at present, of these 98(a) was executed and 600(b) imprisoned. [90]

The Soviets didn't really invent anything new in the spying business, but they energetically improved upon ancient techniques and thus made the XXth century a golden age for espionage (see pages 31,32). Basically, the Russians realized that successful spying was all about developing a lot of personal relationships, and then exploiting as many as possible. Early on, in the 1920s and 1930s, the Soviets had a lot of capable and eager agents. And there were many communist sympathizers worldwide. Thousands of these pro-communists

---

[87] Finley, J.P., Ibid, p. 17

[88] Murray, W. and Millett, A.R., (eds.), "Military Innovation in the Interwar Period", Cambridge University Press, Cambridge, 1996, p. 58.

[89] Caşın, M.H., "Askeri İstihbaratın Politik ve Stratejik Yapısındaki Boyutsal Değişim", Strateji, Doğuş Matbaacılık Ltd.Şti., Ankara, No.1, 1996, p.98

[90] (a) Includes: 4 died in prison before execution, 2 shot and one electrocuted crossing the frontier. (b) Includes: 19 sentenced for life, 25 sentenced to unknown periods, 10 deported see Drake, R.J., Lieut. Colonel, General Staff., 5 May 1919, History of Intelligence (B), British Expeditionary Force, France, From January 1917 To April 1919, Available on site www.lib.byu.edu

were turned into valuable Soviet agents. Those that got caught were declared "martyrs." Nothing was wasted. [91]

Stalin's purges in the late 1930s brought this golden age to an end. Most of the excellent agents were executed. Many of the spies began to have second thoughts about working for the Soviet Union. But then World War II came along and made recruiting spies easier for a time. This continued for a while after World War II. But without the large number of skilled agents, some new enticements were used. The most frequently used tactic was to threaten the safety of relatives behind the Iron Curtain. Western counterintelligence soon caught on to this, and having relatives back in the old country kept a lot of people from getting security clearances or sensitive jobs. But the Soviets had many more techniques they could use. Sex and blackmail (often used together) were very successful. Attractive men and women were recruited, trained and sent forth to be romantic for the revolution. This worked particularly well in West Germany, where East German spy studs recruited a number of key female staff in NATO and West German organizations. But this pointed up another problem the Soviets were having, the collapse of communist idealism and Stalin's purges had eliminated a supply of agents who could "pass" for foreigners on their home ground. America was particularly difficult, with its multiplicity of customs and odd accents. [92]

COLD WAR TENSION AND BI-POLAR INTELLIGENCE COMPETITION PROCESS

Although the Cold War was the dominant characteristic of the post-1945 world, another momentous change in the international system took place concurrently: the end of Europe's five-century-long domination of the non-European world. Some one hundred new sovereign states emerged from the ruin of European colonialism, and Cold War competition was promptly extended to many of these new states.

---

[91] Cole, S. V., "How To Make War", Available On Site http://www.strategypage.com/search.asp?target=d:\inetpub\strategypageroot\fyeo\howtomakewar\docs\archives\htint01.htm
[92] Cole, S. V., Ibid.

Inspired by Winston Churchill's 1945 "Iron Curtain" speech[93] in Yalta, the entrance to the Cold War Era is closed with the Berlin Wall and collapse of Soviet Union.

Although when Summy defines the globalization as a process had begun earlier -after World War II - but the Cold War period masked "an awareness of the globalization"[94] process. But we assume Cold War period between 1945 and 1991.

As visitors walk through the corridor of Cold War Era, they see some important clues that point the evaluation of intelligence in the fog of history.

Following World War II the only remaining world powers were the United States and the Soviet Union. While the U.S. quickly disbanded its forces, the Soviets failed to demobilize their huge wartime army threatening. The North Atlantic Treaty Organization (NATO) and Warsaw Treaty Organization (Warsaw Pact) were created.

In 1948 The Soviets blockaded West Berlin, attempting to force out the Allies by starving the city into submission. On the other side of the world, the Communists under Mao Tse Tung defeated the Nationalist Chinese.

In 1950's following "Peaceful Coexistence" [95] is promoted by Nikita Kruschev, Premier of the Soviet Union, which is filled with bluster, a new war appeared which is Korean war. By the way the world faced with the new conflicts between intercontinental states and super powers like as inversion Bay of Pigs and Cuba crisis, Vietnam War, etc.

In recent history of Cold War Era, then, other factors besides intelligence or long-range planning predominated in shaping the States' strategic, acquisition, and force development plans. Using intelligence to support these activities is a recent and historically novel idea.

Since World War II, intelligence support to long-range planning has become big business. Through much of the Cold War, the emphasis in futures intelligence was on "getting the

---

[93] Yılmaz, V., "Siyasi Tarih", Harp Akademileri Basım Evi, İstanbul, 1998, p.376
[94] Summy, R., "Politics of Globalization," in Social Alternatives, 1996,Vol.15, Issue 1, pp: 18-21.
[95] National Intelligence Course (NIC) Textbook, Ibid, Chapter 6, p. 5

Soviets right" being able to forecast accurately how the Soviet ground forces would develop over time.[96]

This era includes a variety of espionage artifacts from all intelligence services. The Cold War section displays ingenious specialized cameras, audio transmitters and bugs, and secret tools. From camera lenses concealed behind buttons and belt buckles, to a cigarette lighter that conceals an audio device, the exhibit moves into the late Cold War with sophisticated concealment and microdot equipment, advanced communications gear, and counterintelligence devices. Seemingly ordinary items frequently conceal clever clandestine technology. For example, there is a walnut taken from a Soviet agent arrested in West Germany that he used to conceal his ciphers. Another more lethal item is a 4.5mm single-shot "lipstick" pistol the KGB manufactured and gave to an East German spy who was arrested while trying to enter West Berlin. [97]

The period also includes more information on the historical and operational context of the displayed artifacts. All in all, it will continue to serve as a reminder that the Cold War covered "fifty years of silent conflict," that fortunately never turned into a "hot" war.[98]

To understand the evaluation of intelligence in Cold war, we should examine some important wars. I prefer the beginning to examine with one of the important conflicts in that period as we mentioned above is Korean War.

1.1.6 Korean War

Korean War is the first war after the experiment of World War. It is not a local conflict; it is another world war with the characteristic of intercontinental. Direct or indirectly 22 nations participated this war.

So I examine this war with the steps of general view, Turkey's function and analyzing of intelligence failures and successes.

---

[96] Rosen, S. P., "Winning the Next War: Innovation and Modern Militaries", Cornell University Press, 1991, p. 250.
[97] Hiley, T., "Symposium on the Psychology of Intelligence Analysis," Center for the Study of Intelligence Bulletin 11, Summer, 2000, Available on site http://www.cia.gov/csi/bulletin/ csi11.html
[98] Hiley, T., Ibid.

1.1.6.1 Overview of Korean War

0n 25 June 1950, the North Korean People's Army of the Democratic People's Republic of Korea (DPRK) by the goal of to consolidating and controlling strategic areas of South Korea[99] swept across the 38th parallel and came close to uniting the Korean peninsula under the Communist regime of Kim II-Sung. Map 3.1 illustrated battlefront of Korean War in November 1950.

American military and civilian leaders were caught by surprise, and only the intercession of poorly trained and equipped US garrison troops from Japan managed to halt the North Korean advance at a high price in American dead and wounded. Four months later, the Chinese People's Liberation Army (PLA) intervened in massive numbers as American and UN forces pushed the North Koreans back across the 38th parallel. US military and civilian leaders were again caught by surprise, and another costly price was paid in American casualties. [100]

A total of 22 nations agreed to send either troops or medical units. Sixteen countries responded to the U.N. resolution by sending troops to halt the invasion of South Korea by the North Koreans. One of the first of the major participants to send a brigade was Turkey. Inexperienced but well trained and eager to show their character, the first Turkish troops arrived in Korea just in time to face the Chinese attack of November 1950, and in varying strengths remained until midsummer 1954.[101]The Turkish Brigade, which had no war experience, was affecting a great battle from its roots, was saving the friendly Army, which was starting to roll down a dangerous cliff, by stopping the superior numbers of enemy forces. Thus the Brigade was achieving fame in the world by playing an important role in the course of the war in its first battle. [102]

---

[99] Defense Intelligence Agency, "North Korea: The Foundations for Military Strength, Employing The Armed Forces", October 1991, Chap. 6, Available on site http://www.fas.org/irp/dia/product /knfms/knfms_chp6.html

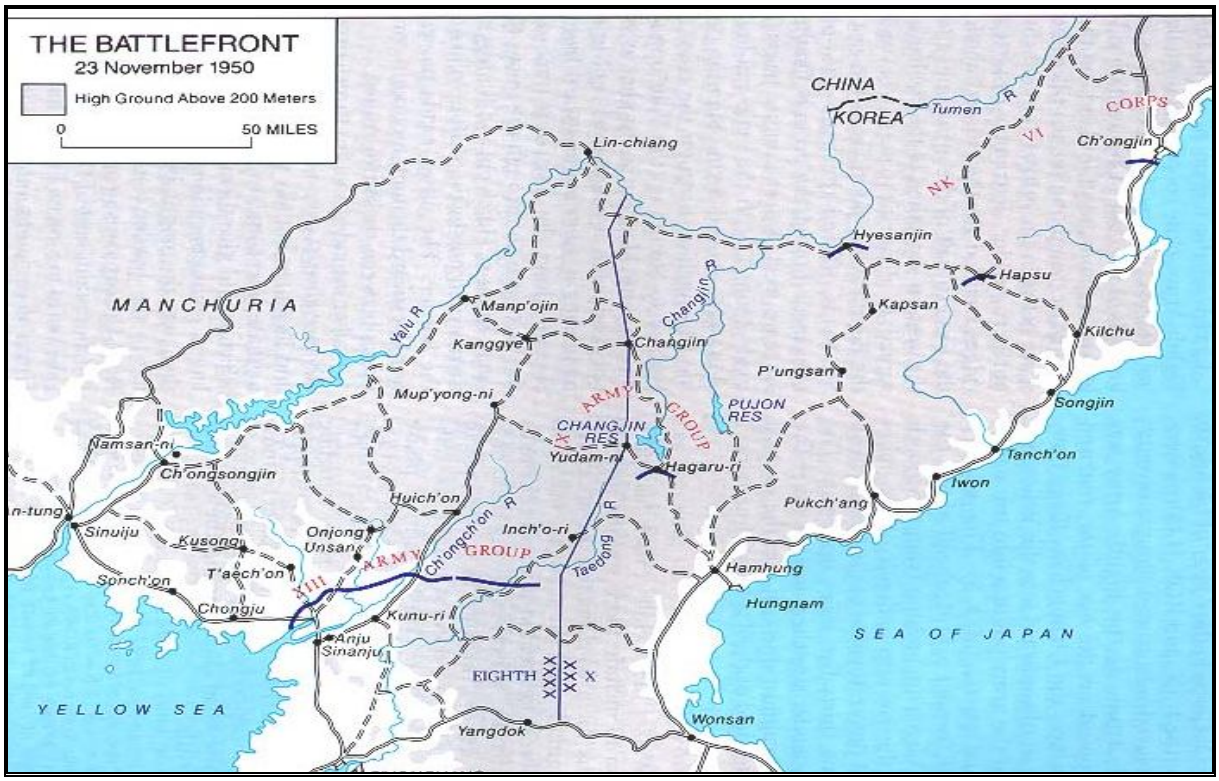
[100] Rose, P.K., "Two Strategic Intelligence Mistakes in Korea, 1950", Fall-Winter 2001, No. 11, Unclassified Edition, Available on site http://www.cia.gov/csi/studies/fall_winter_2001 /article06.html

[101]Dawson, A.K., "Turkish Brigade", Military History Magazine, December 1997, Available on site http://europeanhistory.about.com/library/prm/blturkishbrigade1.htm

[102]Korean War Home Page, "Turkey's Role in the Korean War", http://www.koreanwar.net/turkey.htm

Dwarfed by the total U.S. victory in World War II, the negotiated settlement in Korea seemed to many observers to be a defeat and at best a draw. Certainly it seemed no model for the future. [103]

Map 0.1Battlefront Map of Korean War[104]



1.1.6.2 Intelligence Analysis of Korean War

The document discloses for the first time the details of an espionage case known to National Security Agency (NSA) officials as "Black Friday" and the resultant failure of NSA analysts to uncover evidence of a North Korean invasion of South Korea in 1950.

In 1934, the Soviet Union's intelligence service, the Committee for State Security (KGB)[105], recruited William Weisband, a Russian linguist who had been working for Armed Forces Security Agency (AFSA). The KGB convinced him to divulge details of

[103] Summers, H.G., "The Korean War: A Fresh Perspective", Military History Magazine, April 1996, p.4
[104] Battlefront Map of Korean War, Available on site http://www.koreanwar.org/html/maps/map3_full.jpg
[105] Komitet Gosudarstvennoi Bezopasnosti [KGB], For details available on site http://www.fas.org/irp/world/russia/index.html

U.S. penetration of Soviet cipher systems. Then, two years before the start of the Korean War, “in rapid succession, every one of these cipher systems went dark,” according to the NSA document.[106]

The Soviets had conducted a massive change of all cryptological systems, denying U.S. intelligence critical communications intercepts. “This was perhaps the most significant intelligence loss in U.S. history,” states the NSA document. However, AFSA did score some successes. Although communications intelligence during the Korean War was "hampered by supply shortages, outmoded gear and equipment ill-suited to frequent movement over rough terrain," AFSA inadvertently discovered a new communications intercept tool. It soon became apparent that sound detection devices planted near enemy bunkers were capable of intercepting telephone calls. Known as "ground-return intercept," the new capability enabled collection of Chinese and Korean telephone traffic.[107]

Two strategic intelligence blunders within six months: yet the civilian and military leaders involved were all products of World War II, when the attack on Pearl Harbor had clearly demonstrated the requirement for “intelligence collection” and “analysis”. The answers to why it happened are simple, and they hold lessons that are relevant today. [108]

Mistakes started with CIA analytic reports in 1948, regarding the Communist threat on the peninsula. The first report, in a Weekly Summary dated 20 February[109], identifies the Soviet Union as the controlling hand behind all North Korean political and military planning. In the 16 July Weekly Summary[110], the Agency describes North Korea as a Soviet “puppet” regime. On 29 October, a Weekly Summary[111] states that a North Korean attack on the South is “possible” as early as 1949, and cites reports of road improvements

---

[106] Verton, D., **“**NSA Posts Declassified Intelligence From Korean War”, July 18, 2000, Available on site http://www.fcw.com/fcw/articles/2000/0717/web-nsa-07-18-00.asp
[107] Verton, D., Ibid.
[108] Rose, P.K., Ibid.
[109] Weekly Summary Excerpt, “ Soviet Expansionism in Korea”, 20 February 1948, p.172, Available on site http://www.cia.gov/csi/book/coldwaryrs/5563bod2.pdf
[110] Weekly Summary Excerpt, “International Communism; Establishment of Competing Regimes in Korea”, 16 July 1948, p.229, Available on site http://www.cia.gov/csi/books/coldwaryrs/5563bod2.pdf
[111] Weekly Summary Excerpt, “Prospects for Invasion of South Korea by the North” 29 October 1948, p.254, Available on site http://www.cia.gov/csi/books/coldwaryrs/5563bod2.pdf.

towards the border and troop movements there. It also notes, however, that Moscow is in control.

These reports establish the main theme in intelligence analysis from Washington that accounts for the failure to predict the North Korean attack that the Soviets controlled North Korean decision-making.

By the spring of 1950, North Korea's preparations for war had become readily recognizable. According to CIA reports DPRK forces could not mount a successful attack without Soviet assistance, and such assistance would indicate a worldwide Communist offensive.[112]

Although the CIA published reports, based primarily on human assets, concluding that the DPRK had the capability to invade the South at any time, a few days later, the DRPK invaded the South. Both Washington and the Far Eastern Command (FEC) in Tokyo were surprised and unprepared. So, on 30 June 1950, President Truman authorized the use of US ground forces in Korea. The United States was caught by surprise because, within political and military leadership circles in Washington, the perception existed that only the Soviets could order an invasion by a "client state" and that such an act would be a prelude to a world war. Washington was confident that the Soviets were not ready to take such a step, and, therefore, that no invasion would occur. [113]

By August, the Communist leaders in the USSR, China, and Korea recognized that the large-scale intervention by US forces would lead to the defeat of the North Korean forces.[114] This realization was particularly threatening to China. On 4 August, at a Chinese Communist Party Politburo meeting, Mao stated that if the United States won in Korea, it would threaten China. Therefore, China had to come to the assistance of the DPRK and

[112] Rose, P.K., Ibid.
[113] Rose, P.K., Ibid.
[114] Domes, J. and Te-huai, P., "The Man and the Image" Stanford University Press, Stanford, 1985, p. 60.

intervene.[115] This decision set in motion China's efforts on diplomatic, military, and propaganda fronts to defend itself from US aggression.

On 15 September, US Marines rushed ashore, captured the west coast city of Inchon, and began driving DPRK forces north toward their country. This strategic success was a clear signal that the invasion from the North had not only failed, but also that the DPRK forces could be destroyed by the US and UN forces. Two days later, a high-ranking Chinese delegation of intelligence and logistics officers arrived in North Korea to evaluate the military situation and prepare the battlefield for Chinese military action.[116]

Finally, on 5 November, Willoughby admitted, "Chinese forces in Korea had the potential to conduct a large-scale counteroffensive". Later that day, however, Macarthur advised the Joint Chiefs of Staff (JCS) that he still did not believe the Chinese would enter the war in force.[117]

On 24 November, however, National Intelligence Estimate 2/1 stated that China had the capability for large-scale offensive operations but that there were no indications such an offensive was in the offing.[118] That same day, the second Chinese offensive started and U.S. corps surrounded and threatened with destruction.

Finally, on 28 November, is reported that U.S. forces faced 200,000 PLA troops and a completely new war.

Consequently, in Korean War there are a little hard data on enemy weapon systems. That mean we realized that "to be able to develop effective countermeasures, especially on Technical Intelligence (TECHINT) because of an ongoing process."[119] In the other side the National Security Agency (NSA) has setup a World Wide Web site where it plans to post newly declassified documents outlining the successes and pitfalls of signals intelligence

---

[115] Shu, G. Z., "Mao's Military Romanticism: China and the Korean War, 1950-1953", Kansas University Press, Kansas, 1995, p. 63.
[116] Shu, G. Z., Ibid, p. 74
[117] Rose, P.K., Ibid.
[118] Washington File "Congressional Report on North Korean Threat", Available on site http://usembassy-australia.state.gov/hyper/WF991103/epf304.htm
[119] FM 43-54, "Battlefield Technical Intelligence", Headquarters Department of the Army, Washington, DC, 5 April 1990, Available on site http://www.fas.org/irp/doddir/army/fm34-54/Ch1.htm

(SIGINT) during the Korean War.[120] This means as Air Force Lt. Gen Michael Hayden (NSA's director) said: "In the coming weeks and months you can expect to see releases of newly declassified materials relating to SIGINT operations in Korea during 1950 [and] published articles detailing intelligence-gathering activities," in an introduction to the Web site."[121]

At the end as we see the importance of intelligence in the Korean War, if you don't care the information, and if you don't direct agencies and intelligence collectors toward the information, which you need, the surprises wait for you.

1.1.7 Bay of Pigs Invasion and Cuban Missile Crisis

"The crisis years" of 1960-1962 are remembered as a peak of the Cold War, a zenith of the bipolar confrontation. Many consider them even more dangerous than the Korean War, when the military forces of West and East clashed and almost slipped into a global conflict.

The early 1960s were all the more frightening since the two superpowers, the United States and the Soviet Union, were engaged in a fierce nuclear arms race, and two more states, Great Britain and France, had developed small nuclear arsenals of their own. By the end of the period the edge in this race clearly belonged to the United States such that, at the height of the Cuban Missile Crisis, Washington had at least nine times as many deliverable nuclear warheads as Moscow.[122]

The days of crisis, which begin Bay of Pigs invasion in 1961 and continue with the Cuban Missile Crisis as other than a period in which the world was on the brink of nuclear war, when the slightest miscalculation could have pushed either side over the edge.

The United States armed forces were at their highest state of readiness ever and Soviet field commanders in Cuba were prepared to use battlefield nuclear weapons to defend the island if it was invaded.

---

[120] Verton, D., "NSA posts declassified intelligence from Korean War", July 18, 2000, Available on site http://www.fcw.com/fcw/articles/2000/0717/web-nsa-07-18-00.asp
[121] Verton, D., Ibid.
[122] McNamara, R.S., " Blundering into Disaster: Surviving the First Century of the Nuclear Age", Pantheon Books, New York, 1986, pp. 44-45

1.1.7.1 Overview of the Crisis

Although crisis arrive in 1960 Eisenhower program, which designed to effectuate the downfall of the Cuba regime[123], to start with 1962, is suitable. In 1962 the Soviet Union was extremely behind the United States in the arms race. Soviet missiles were only powerful enough to be launched against Europe but U.S. missiles were capable of striking the entire Soviet Union.

In late April 1962, Soviet Premier Nikita Khrushchev conceived the idea of placing intermediate-range missiles in Cuba. A deployment in Cuba would double the Soviet strategic arsenal and provide a real deterrent to a potential U.S. attack against the Soviet Union. [124]

While the Bay of Pigs invasion met its ignominious end on the afternoon of 19 April 1961,[125] Fidel Castro was looking for a way to defend his island nation from an attack by the U.S. Ever since the failed Bay of Pigs invasion in 1961; Castro felt a second attack was inevitable. Consequently, he approved of Khrushchev's plan to place missiles on the island. In the summer of 1962 the Soviet Union worked quickly and secretly to build its missile installations in Cuba. Map 3.2 illustrated Missile Installations in Cuba.

For the United States, the crisis began on October 15, 1962 when reconnaissance photographs revealed Soviet missiles under construction in Cuba. Early the next day, President John Kennedy was informed of the missile installations. During the public phase of the Crisis, tensions began to build on both sides. Kennedy eventually ordered low-level reconnaissance missions once every two hours. [126]

---

[123] Blum, H.R., (ed.), "Surveillance and Espionage in a Free Society" A report by the Planning Group on Intelligence and Security to the Policy Council of the Democratic National Committee, Praeger Publishing, New York, 1972, p.222

[124]The Cuba Missile Crisis Main Page "An Overview of The Cuba Crisis", Available on site http://hyperion.advanced.org/11046/days/index.html

[125] Warner, M., "The CIA's Internal Probe of the Bay of Pigs Affair", Studies in Intelligence, Winter 1998-1999, Available on site www.cia.gov/csi/studies/winter98-99/art08.html

[126]The Cuba Missile Crisis Main Page "An Overview of The Cuba Crisis", Available on site http://hyperion.advanced.org/11046/days/index.html

Map 0.2 Missile Installations in Cuba[127]

By Khrushchev in an impassioned letter is proposed removing Soviet missiles and personnel if the U.S. would guarantee not to invade Cuba. October 27 was the worst day of the crisis. A U-2 was shot down over Cuba and a second letter from Khrushchev demanding the removal of U.S. missiles in Turkey in exchange for Soviet missiles in Cuba.

Tensions finally began to ease on October 28 when Khrushchev announced that he would dismantle the installations and return the missiles to the Soviet Union, expressing his trust that the United States would not invade Cuba. Further negotiations were held to implement the October 28 agreement, including a United States demand that Soviet light bombers be removed from Cuba, and specifying the exact form and conditions of United States assurances not to invade Cuba.[128]

Causes of the Crisis are Soviet insecurity, and the fear of losing Cuba in an invasion. According to Nikita Khrushchev's memoirs, in May 1962 he conceived the idea of placing intermediate-range nuclear missiles in Cuba as a means of countering an emerging lead of the United States in developing and deploying strategic missiles. He also presented the

[127] Warner, M., Ibid.
[128] The Cuba Missile Crisis Main Page "An Overview of The Cuba Crisis", Ibid.

scheme as a means of protecting Cuba from another United States-sponsored invasion, such as the failed attempt at the Bay of Pigs in 1961. [129]

The answers of intervention seen as;

- The Castro regime will not fall of its own weight.
- Within a matter of months the capabilities of Castro's military forces will probably increase.
- The Cuban paramilitary force if effectively used has a good chance of overthrowing Castro.
- Among the alternative courses of action here reviewed, an assault in force preceded by a diversionary landing offers the best chance of achieving the desired result. [130]

The critics of Cuba Crisis; according to Zegart (realist model) as "...does not make a convincing case..." and claims that the traditional models are inductive and thus do not offer testable hypotheses, and in the sum repeat such as "agencies act in their own best interest." And according to Graham Allison's analysis of bureaucratic politics in the Cuban missile crisis, she writes: "How John F. Kennedy approached the Cuban missile crisis sheds little light on how Jimmy Carter handled the Iranian hostage crisis." The old aphorism "Where you stand depends on where you sit" captures something about bureaucratic behavior. But the far more important questions are "How did you come to sit there in the first place?" and "What power will you bring to the table tomorrow?"[131]

An example of bias and how an analyst's own cultural values can result in failure occurred during the 1962 Cuban missile crisis.[132] In quoting a National Intelligence Estimate (NIE), one analyst stated that "...it was highly unlikely that the Soviet Union would pursue a policy of such high risk as the placement of offensive missiles in Cuba. This estimate was

---

[129] Soviet Archives, "Cuban Missile Crisis", Library of Congress's Documents from the Soviet Archives, Available on site http://www.ibiblio.org/pjones/russian/Cold_War__Cuban_ Missile_ Crisis.html
[130] Bundy, Mc G., Ed. Smith, L. J., Foreign Relations of The United States, 1961-1963, Volume X, Cuba, 1961-1962, Department of State, Washington, 1997 Available on site http://www.state.gov/www/ about_state/ history/frusX/index.html
[131] Berkowitz, B., "Intelligence Reform, The Third Act", Orbis, Elsevier Science Publishing, Winter 2001, Vol. 45, Issue 1, pp.152-162
[132] Codevilla, A., "Informing Statecraft: Intelligence For a New Century", Maxwell Macmillan, Canada, 1992, p 201,

made on the assumption that such a course of action would be irrational."[133] Placing it on a western bias on the situation flawed the analysis. Unfortunately, it is easy to recognize this as only a human failing.

Stockwell criticize this period and says "In 1959 the CIA did not recommend to President Eisenhower that we befriend Fidel Castro and learn to live with him in Cuba. No, it presented the violent option, noting that it had the essential ingredients for a covert action: angry Cuban exiles, a haven in Guatemala, a beach in the Bay of Pigs, intelligence that the people of Cuba would rise up in support of an invasion. Presidents Eisenhower and Kennedy were persuaded. The operation was run, and it was bungled. Today we are still haunted by it." [134]

1.1.7.2 Intelligence Analysis of Bay of Pigs

History is full with failures of intelligence agencies. Some of them cause important effects on policies of world. One of them is failed attempt of United States-sponsored invasion in Bay of Pigs. CIA made some mistakes on policy of U.S. in that invasion.

Warner mentions how grow events. "CIA officers who planned the assault gathered around a radio in their Washington War Room while the Cuban Brigade's commander transmitted his last signal. They had been pleading all day for supplies and air cover, but nothing could be done for them. Now they could see Fidel Castro's tanks approaching. "I have nothing left to fight with," he shouted. "Am taking to the woods. I can't wait for you." Then the radio went dead, leaving the drained and horrified CIA men holding back nausea."[135]

The disconnection between what CIA wanted Cuba's Army to do and how the Army would be persuaded to do it was a major flaw in the invasion planning. This defect, in turn, distorted the Agency's advice to President Kennedy, and thus contributed to the disastrous

---

[133] Handel, M., "Intelligence and the Problem of Strategic Surprise," in Douglas H.Dearth and R. Thomas Godden ed., "Strategic Intelligence: Theory and Application" Defense Intelligence Agency, Washington, 1995, p 225.
[134] Stockwell, J., "In Search of Enemies, The Third World Traveller", W.W. Norton, 1978, p. 250, Available on site http://www.thirdworldtraveler.com/Stockwell/In_Search_Enemies.html
[135] Warner, M., Ibid.

misunderstanding explored in Piero Gleijeses's[136] recent analysis. CIA officials did not spot this failure before the Bay of Pigs, and the controversy over the CIA's Inspector General (IG) Survey obscured the lesson and ensured that few Agency principals would understand what had gone wrong. [137]

The Deputy Director for Plans (DDP) would have served itself and CIA better by drafting a careful analysis of the operation, particularly the way in which the assumptions contained in intelligence plan evolved on their own without conscious revision and constant comparison with current intelligence and policy directives. Kirkpatrick[138] had approved a bad report and then mismanaged its presentation to CIA's principals, thus incurring lasting resentments and helping to ensure his report would not be heeded. Neither the IG nor the DDP prepared clear insights that could instruct Agency leaders and planners. More attention to the need to understand the Bay of Pigs invasion might have prevented a generation of CIA officers from believing that one more air strike would have saved the Brigade. As a result, CIA convinced itself because of this invasion [139]

1.1.7.3 Intelligence Analysis of Cuba Crisis

In fact, Cuba Crisis was part of a high-stakes game of prestige and influence played by the Soviet Union and U.S. Their motivations probably owed to strategic calculation and internal politics. What directed states to this crisis and who make mistakes? Is it only an intelligence failure?

Estimates of intelligence agencies of U.S. not only failed to predict this action, but also argued resolutely against its probability, right up to the moment that offensive missiles were discovered in Cuba. On the face of it, the system created because of the strategic surprise that began the Korean War had functioned no better than its predecessor.

---

[136] Piero Gleijeses is a historian whose researches on the White House and the CIA, to see Gleijeses, P., "Ships in the Night: The CIA, the White House and the Bay of Pigs," Journal of Latin American Studies, 27 Feb. 1995, pp. 37-42.
[137] Warner, M., Ibid.
[138] Kirkpatrick, L. B., "The Real CIA", The Macmillan Company, New York, 1968, Chap. 8, Available on site http://www.rose-hulman.edu/~delacova/bay-of-pigs/kirkpatrick.htm
[139] Warner, M., Ibid.

As it happened, the Board of National Estimates was reinforced in its preconceptions by the fact that offensive missiles were not deployed to Cuba until very late in the game. They were preceded over a three-month period by surface-to-air missiles (SAMs), coast-defense missiles, KOMAR-class missile boats and II-28 BEAGLE light bombers, all of which fit neatly into the concept of a defensive buildup in Cuba. [140]

At bottom, however, it was the lack of precedent for these Soviet deployments in the measured, action-reaction sequence of Cold War confrontation that led to the Board's failure to recognize the situation for what it actually was. Thus, although in estimates[141] patronizingly conceded that "the USSR could derive considerable military advantage from the establishment of Soviet medium- and intermediate-range ballistic missiles in Cuba," such a development "would be incompatible with Soviet practice to date and with Soviet policy as we presently estimate it." [142]

By the way, it would indicate the level of risk in US-Soviet relations than the USSR has displayed thus far, and consequently would have important policy implications with respect to other areas and other problems in East-West relations.[143]

At the end for Khrushchev to kept the Intelligence Community on track, and perhaps staved off war. In an unusual series of telegrams, written while he was on honeymoon in France, Mc Cone badgered his Agency with warnings of Soviet missile deployments. Returning in September, he demanded that reconnaissance flights against Cuba be resumed, despite the presence of ever more numerous SAMs on the island and despite the continued lack of evidence of anything beyond a defensive buildup. Finally, on 14 October, U-2 photographs revealed Soviet SS-4 medium-range ballistic missiles (MRBMs)

---

[140] Steury, D. P., "Sherman Kent and the Board of National Estimates", Collected Essays, Center for the Study of Intelligence, Available on site http://www.cia.gov/csi/books/shermankent/toc.html
[141] The White House, "The Cuban Missile Crisis", Special National Intelligence Estimate, Washington, September 1962, Available on site http://www.gwu.edu/~nsarchiv/nsa/publications/cmc/cmcdoc2.html
[142] Steury, D. P., Ibid.
[143] McAuliffe, M.S. ed., "CIA Documents on the Cuban Missile Crisis", Central Intelligence Agency, 1962, Washington, 1992, p. 93.

in the early stages of deployment in sites about 50 nautical miles to the west-southwest of Havana.[144]

According to Kent "There is no blinking the fact that we came down on the wrong side," and "When the photographic evidence of 14 October was in, there was the proof." There was also no question that the Office of National Estimates had misread Soviet intentions throughout the summer and fall of 1962; yet if Sherman Kent was willing to acknowledge in looking back that there were in fact a handful of indicators that ought to have warned the Board of National Estimates what the Soviets were about, he nonetheless stood by the intelligence judgments that were made. The problem, he argued, was the faulty judgment on the part of the Soviets, who had themselves misread US intentions with respect to Cuba in the months following the Bay of Pigs. In any intelligence estimate, he argued, the "other man's" decision will have been shaped by his diplomatic missions and intelligence service, which will have observed and reported the "things he must know prior to his decision." [145]

These and other phenomena very considerably narrow the area of a foreign statesman's choice, and once thus narrowed it is susceptible to fairly sure-footed analysis by studious intelligence types. As long as all the recognizable constants in the equation are operative the estimator can be fairly confident of making a sound judgment. It is when these constants do not rule that the real trouble begins. No estimating process can be expected to divine exactly when the enemy is about to make a dramatically wrong decision. Office of National Estimates was not brought up to underestimate the enemies.[146]

One consequence of the American failure to recognize the buildup of a Soviet military contingent was a serious underestimation of the number of Soviet military personnel in Cuba. In September and early October the number was estimated at 4,000 to 4,500. By October 22, after identifying the missile bases (through U-2 imagery) the total was revised at 8,000 to 10,000. Later, the estimates were revised again to 12,000 to 16,000 troops....

---

[144] Steury, D. P., "Sherman Kent and the Board of National Estimates", Collected Essays, Center for the Study of Intelligence, Available on site http://www.cia.gov/csi/books/shermankent/toc.html
[145] Steury, D. P., Ibid.
[146] Steury, D. P., Ibid.

Retroactive estimates in early 1963 raised the total to 22,000 and were never later revised."[147]

In this environment, Sherman Kent's detached approach to estimative intelligence seems old and the end of the Cold War has raised diverse new issues, while the changing of the global balance of power and the changes that seem to occur almost daily in the international arena have brought a new conception of intelligence.

1.1.8 Vietnam War

Another case, which helps to understand changes toward end of Cold War Era, is Vietnam War. Vietnam War full with intelligence failures, which are made especially by American Intelligence Agencies and policy makers.

As told General Frederick C. Weyand **"**One of the saddest legacies of the Vietnam War is the cruel misperception that the American fighting men there did not measure up to their predecessors in World War II and Korea. Nothing could be further from the truth."[148]

The Vietnam War, like the Korean War, was pursued on the strategic defensive the United States still not realizing that the best result possible was stalemate. In Korea, U.S. forces kept the external enemy at bay while giving local forces responsibility for counterguerrilla operations. But in Vietnam, this strategy was regarded as ineffective, even though the Korean War objective of preserving South Korea's independence had been attained. [149]

Vietnam had gained its independence from France in 1954. The country was divided into North and South. US involvement in Vietnam began during the administration of Dwight D. Eisenhower (1953-1961), which sent US military to South Vietnam. In 1957 Communist rebels -- Viet Cong -- began a campaign of terrorism in South Vietnam. They were supported by the government of North Vietnam and later by North Vietnamese troops. Their goal was to overthrow the anti-communist government in the South. Under

---

[147] O'Leary, J., " Surprise And Intelligence: Towards A Clearer Understanding", Airpower Journal, Spring, 1994, Vol. 8, Issue 1, p.34

[148] Frederick C.W., U.S. Army Ret. General, " Troops to Equal Any" Available on site http://www.vwam. com/vets/ equal.html

[149] Summers, H.G., "The Korean War: A Fresh Perspective", Military History Magazine, April 1996, p.4

President Lyndon B. Johnson (1963-1968), US intervention mushroomed both militarily and politically. Richard M. Nixon (1969-1974) was elected on the claim that he had a "secret plan" for honorably disengaging American troops, which succeeded initially only in intensifying the conflict. This last phase of American involvement in South Vietnam was carried out under a broad policy called Vietnamization.[150]

According to the Vietnamese military leaders, 1954 was a missed chance for peace. The French were withdrawing after military defeat by the Vietnamese people. A peace treaty at Geneva was signed. Yet, the United States was aloof at the Geneva meetings and according to McNamara, the reason was the United States did not care much. However, the British and French had already decided that partition of Vietnam was the best solution and agreed with the Soviets and Chinese." [151]

As you see, Vietnam passed a difficult way from 1954 to 1975. Maybe it is going on. But in my thesis, because of Vietnam War effects on the intelligence concept, I preferred it. Vietnam War has many examples of intelligence failures and lessons. So I'll try to examine this war.

1.1.8.1 Overview of Vietnam War

The Vietnam War was the legacy of France's failure to suppress nationalist forces in Indochina as it struggled to restore its colonial dominion after World War II. After a political and military struggle for Vietnamese independence resulted ultimately in two the region. The North had a communist government led by Ho Chi Minh. The South had an anti-communist government led by Ngo Dinh Diem. [152]

The Communist victory in the Chinese Civil War in 1949 and Chinese intervention against the United Nations in Korea made U.S.-China policy a captive of Cold War politics. Those events also helped to transform American anti-colonialism into support for the French protectorates in Indochina, and later for their non-Communist successors. American

---

[150] Summers, H.G., Ibid, p.5

[151] McNamara, R.S. et al, "Argument Without End: In Search of Answers to the Vietnam Tragedy", Public Affairs, New York, 1999, p. 71

[152] Military Analysis Network, "Vietnam War", Available on site http://www.fas.org/man/dod-101/ops/vietnam.htm

political and military leaders viewed the Vietnam War as the Chinese doctrine of revolutionary warfare in action. The overarching geopolitical aim behind the United States' involvement in Vietnam was to contain the spread of communism in Southeast Asia. To accomplish this aim, the United States supported an anti-communist regime. South Vietnam faced a serious, dual-tracked threat: a communist-led revolutionary insurgency within its own borders and the military power of its communist neighbor and rival, the Democratic Republic of Vietnam (North Vietnam). [153]

Although US involvement in Vietnam began during the administration of Dwight D. Eisenhower, which sent US military to South Vietnam, and was continued by John F. Kennedy until he was murdered. But intervention is accelerated both militarily and politically by Lyndon B. Johnson. In theory, Westmoreland's strategy of search and destroy would force the Communists to expend supplies and thus make the logistics establishment in North Vietnam all the more vulnerable to bombing. By the way in 1966, more than 200,000 troops were committed to Vietnam. The United States escalated its participation in the war to a peak of 543,000 troops in April 1969. In 1966 it became increasingly clear that this strategy of attrition was not working and could not work because of the enemy's capacity to replace losses far higher than those the allies were able to inflict. Lacking a single responsible air commander, a clear set of objectives, and a common concept of operations, even the most skilled operations of the separate components tended to work at cross-purposes and give respite to the enemy.[154]

Initially, most Americans backed Washington's Vietnam policy. A dangerous situation seemed to be developing, one which the US government referred to as the “domino theory” “If South Vietnam were allowed to fall to communism, so eventually would the rest of Southeast Asia.” But as the war took a long time and a military victory appeared more and more away, public opposition became more vocal. [155]

Opposition to the war and to the Administration's war policies led anti-war demonstrations to bigger and bigger. Johnson strongly defended the use of American soldiers in Vietnam.

---

[153] Military Analysis Network, Ibid.
[154] Military Analysis Network, Ibid.
[155] Military Analysis Network, Ibid.

In a speech to a group of lawmakers he said: "Since world war two, this nation has met and has mastered many challenges - challenges in Greece and Turkey, in Berlin, in Korea, in Cuba. We met them because brave men were willing to risk their lives for their nation's security. And braver men have never lived than those who carry our colors in Vietnam this very hour." [156]

By the spring of 1972 the Vietnam War was in a decline and beginning in late 1972, National Security Advisor Henry A. Kissinger's negotiations with North Vietnam began to move seriously towards a settlement. In early 1973 the United States, North and South Vietnam, and the Viet Cong signed an armistice. American military activities in Cambodia and Laos, which had continued after the cease-fire in South Vietnam, went into effect, ended in 1973 when Congress cut off funds. It was 21 years after the first advisors arrived in country and nearly three years after the last combat troops withdrew. [157] "More than three million people were killed in the Vietnam War." In other words, McNamara does not hide that the Yankee military killed 3.8 million Vietnamese, lost 58,000 Americans. [158] Map 3.3 illustrated Vietnam War between 1968-1975.

1.1.8.2 Intelligence Analysis of Vietnam War

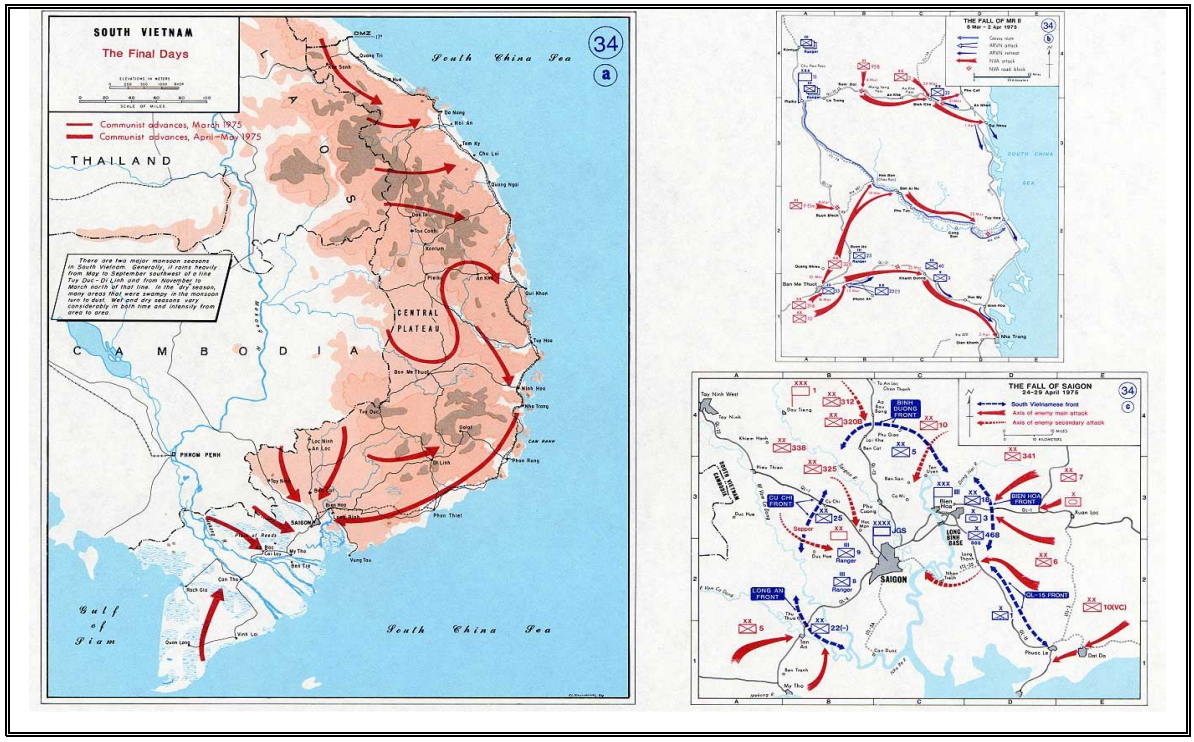
The setback suffered by the United States in the Vietnam War was rooted in a failure of strategy. Indeed, perhaps no war in American history shows more clearly both the difficulties of making sound strategic judgments and the dire consequences of a lack of clear strategic vision. The Vietnam War thus provides a warning tale for all state political and military decision makers about the crucial importance of thinking clearly about strategy.

Major H.R. Mc Master responds the question of "why did Johnson's middle-course strategy in Vietnam (graduated pressure and constrained attacks) represent no strategy at all? Is warfare by political consensus doomed to fail?" as **"**Johnson's strategy assumed, with no thought for the nature of the war, that any military action would constitute progress in the war effort. Without defining a strategic objective, he told the Joint Chiefs of Staff in

[156] Military Analysis Network, Ibid.
[157] Military Analysis Network, Ibid.
[158] McNamara, R.S. et al, Ibid, p. 1

the spring of 1965 to kill more Viet Cong, a tactical mission." And continues, "Lyndon Johnson pursued consensus, which is the absence of leadership. He so feared dissent that he excluded everyone but his most trusted advisers from discussions on Vietnam when the situation there demanded a full examination and debate. So feared a debate over Vietnam that he often refused to discuss the subject within his own circle. On one occasion he threatened to feign illness and leave town for his Texas ranch if his advisers pressed him further to confront the issue." And also according to him during the Vietnam War there isn't a clearly stated policy goal or objective, between Johnson and his advisers, the ideas are precisely the opposite. [159]

Map 0.3 Vietnam War Between 1968-1975[160]



When the United States finally and completely lost the Vietnam War in 1975, the general watchword was "mistake" and "learned its lesson." What was the mistake and lesson learned one would wonder. McNamara answered "so indecisively that President Reagan

[159] Young, R., "Lessons Of Vietnam: A Conversation With Major H.R. McMaster", Available on site http://www.pbs.org/wgbh/pages/frontline/shows/military/etc/lessons.html
[160] Maps of Vietnam War (1968-75), Available on site http://www.english.uiuc.edu/maps/vietnam/maps.htm

elected in 1980 popularized the myth that the Yankee imperialists could have won the Vietnam War if the military had been freed from corrupt politicians' control." [161]

Not only failures in strategy, and also American agencies made mistakes and had some lessons in Vietnam. Stockwell thinks "CIA managers arrogantly resistant to criticism of their own ranks" and give an example "when I spoke out about the most flagrant mismanagement that I knew about which occurred during the evacuation of Vietnam, I was politely and gently admonished."[162]

The criticized of National Intelligence Agency of U.S. in Vietnam War; first was the inability of the CIA to centralize all the intelligence collected by American government organizations. This led to the second, and more serious problem. The many other intelligence organizations (in particular the army, navy, air force and state department, plus just about every other arm of government) not only collected and interpreted information from overseas, but their analysts didn't always agree with the CIA's conclusions. This abundance of different conclusions allowed decision makers unhappy (for political or personal reasons) with the CIA's analysis to select another, more acceptable, conclusion. This defeated the basic reason for having a CIA in the first place. So CIA never quite worked as originally intended in war.[163]

Throughout the Vietnam War, the DIA and CIA analysis was often in a disagreement. The CIA reports were generally more pessimistic, but, in the end, proved to be more accurate. Unfortunately, the president wanted to win the war and the DIA analyses bent the facts in an attempt to keep the president happy, or at least optimistic. [164]

In another case of "no good deed goes unpunished", the CIA came out of the Vietnam era tainted with responsibility for a lot of the bad intelligence work it had not done. The DIA moved in hurry for the shadows while the CIA took the heat. The agency was attacked for

---

[161] McNamara, R.S. et al, Ibid, p. 2
[162] Stockwell, J., "In Search of Enemies, The Third World Traveller", W.W. Norton, 1978, p. 9, Available on site http://www.thirdworldtraveler.com/Stockwell/In_Search_Enemies.html
[163] Cole, S. V., "How To Make War", Intelligence 1999-2001, Strategy Page, Available on site http://www.strategypage.com/search.asp?target=d:\inetpub\strategypageroot\fyeo\howtomakewar\docs\archives\htint01.htm
[164] Cole, S. V., Ibid.

inaccurate analysis (a bad rap if there ever was one) and shady, and sometimes embarrassing, operations in foreign nations. For a while, the CIA even got nailed for intelligence gathering operations in the U.S. This, again, was a result of the agency trying to please its political bosses by helping out the FBI in digging up dirt on anti-Vietnam war protesters and assorted radicals during the 1960s. [165]

By the 1970s, most of the old Office of Strategic Service (OSS) operators were gone; fired or retired. The analysts were getting better, but their output was increasingly viewed with skepticism. Worse, the analysts were more frequently expected to put the right political spin on their studies. The one part of the CIA that was doing well was the technical branch. This is where the money went, and the techniques came up with enough fascinating photos (taken from space) or messages (often phone conversations) plucked out of the air over enemy territory. Who needed spies or analysts if you had dynamite visuals and tapped phone calls? [166]

In Vietnam, Filipinos had provided the CIA with extensive help, keeping radios, vehicles, and air conditioners running, managing warehouses and tending bar at cocktail parties-all the things that highly paid CIA staffers could not be expected to do with much enthusiasm. [167]

The American failure in Vietnam also resulted from trying to fight a traditional conventional war when the conflict's nature demanded a counterinsurgency effort. Top military commanders should be able to measure the problem, and should be able to refuse to implement such a strategy despite evidence of its effectiveness.

In another perspective as Young said: “The failure in Vietnam was not the result of impersonal forces but a uniquely human failure. The consequences of mistakes in war are most often unforeseen and disastrous.” [168] So with Vietnam, to think through the potential long-term costs and consequences associated with each decision to escalate the involvement in the war was appeared.

---

[165] Cole, S. V., Ibid.
[166] Cole, S. V., Ibid.
[167] Stockwell, J., Ibid.
[168] Young, R., Ibid.

If we say something about the technical situation of intelligence until the end of Vietnam War which following the Korean War, the United States did not disband its TECHINT capability completely, as it had at the conclusion of previous conflicts. In fact, when the Vietnam conflict began, the US TECHINT capability consisted of only a few experienced personnel. However, as combat forces were committed and increased, so did TECHINT capability and structure of U.S. [169]

The lessons learned from World War II, the Korean War, and finally the Vietnam War clearly indicated the need for a fully operational TECHINT system even in peacetime. To do otherwise was to invite a technological surprise that would give the enemy an unacceptable advantage on the next battlefield.

The TECHINT system had two goals: first, to keep a step ahead of threat battlefield weapon systems; and second, to create TECHINT units that could provide instant battlefield TECHINT capability in a war. TECHINT elements exploit foreign and threat materiel. They provide valuable studies, which forecast trends in all areas including armor, antitank rockets, and even chemical warfare.[170]

The world was changing; changing nature and importance of targets, especially after World Wars, Western States focused on the knowledge of the capabilities and decision-making processes in China, Cuba, Iraq, Libya, North Korea, and Vietnam (closed societies that have chosen to remain outside the emerging international order). [171] This phenomenon remains essential until end of Cold War.

BEYOND THE COLD WAR REVOLUTION IN MODERN INTELLIGENCE

In the period of a few short years, the world witnessed; the demise of communism in the Soviet Union and Eastern Europe, the dissolution of the Warsaw Pact, breaking the Soviet empire into newly independent states, the end of the Cold War. Intelligence unquestionably

---

[169] FM 43-54, "Battlefield Technical Intelligence", Headquarters Department of the Army, Washington, DC, 5 April 1990, Available on site http://www.fas.org/irp/doddir/army/fm34-54/Ch1.htm
[170] FM 43-54, Ibid.
[171] Berkowitz, B.D. and Goodman, A.E., "Why Spy--And How--In The 1990s?", Orbis, Spring 92, Vol. 36 Issue 2, p. 269

helped win the Cold War by balancing the imbalance between NATO and the Warsaw Pact.

The Cold War came to end by the withdrawing of Soviet troops from Afghanistan which had been meant to reassure the West and the East Europeans that they "would not be sent into another country."[172] For East Europeans, this meant that the so-called "Brezhnev doctrine" on the permanence of communist rule was a dead letter.

1990 was the year in which the Conventional Armed Forces in Europe (CFE)[173] Treaty, signed in November, changed the military face of the Warsaw Pact forever. And intelligence agencies signed that as the strategic implications of political and military changes in Eastern Europe changes which transformed the geopolitics of the Cold War.

Recent political events in Eastern Europe will further erode Soviet confidence in their allies. For the West, these dramatic changes signified a big reduction of the Soviet military threat in Europe.

Although the Intelligence Communities recorded the Soviet economy's stagnation and decline in the 1980s, and anticipated the failures of Perestroika and the break up of the USSR in a timely and accurate manner, even though the message was not always welcome.[174] The collapse of communist power in Eastern Europe was a windfall for the United States, especially in the military-strategic area.[175]

The consequences of collapse were ironic. These; first, in the 1970s, Soviet economists told their leadership that the final stage of the "crisis of capitalism" had begun.[176] That was

---

[172] Fisher, J., "At Cold War's End: US Intelligence on the Soviet Union and Eastern Europe, 1989-1991", September 1999, Available on site www.odci.gov/csi/books/19335/art-1.html
[173] Conference on Security and Co-operation in Europe, "Treaty on Conventional Armed Forces In Europe", Available on site http://www.osce.org/docs/english/1990-1999/cfe/cfetreate.htm
[174] Berkowitz, B. and Richelson, J., "The CIA Vindicated," National Interest 41, Fall 1995, pp. 36-47.
[175] Fisher, J., Ibid.
[176] Day, R.B., "Cold War Capitalism: The View from Moscow 1945-1975" M.E. Sharpe Publishing, New York, 1995, p. 275.

the real beginning of the final decline, not Gorbachev's Perestroika. Second, CIA studies of the Soviet economy, especially those studies on growth rate, and defense spending[177].

The last great drama of the Cold War unfolded in three acts between 1989 and 1991. These were; first Gorbachev had made major concessions on arms control, withdrawn Soviet troops from Afghanistan, pledged to reduce Soviet ground forces by half a million, and rejected class warfare in favor of "pan-human values" as the basis of Soviet foreign policy.

The second act the de facto collapse of the Warsaw Pact and East Germany was united with West Germany and integrated into NATO. The third act closed with the 1991 dissolution of the USSR. And the Cold War was over. [178]

1.1.9 Gulf War

Today while a new war appears in the same region, Middle East and Golf War save their impotence on the international politics. And also because of the last important war, which participated United Nations and affected Turkey directly, I decided to look at that war.

Although the hot period of war between 2 August 1990 and 3 March 1991 finished, effects of war still continue.

This region attracts many countries due to its naturals riches, and struggle goes until before the World Wars. Hopkirk tells the struggles of intelligence agencies in this region and give a name on this struggle as “great game”. In the same book Paul Rohrbach who is propagandist for German expansionism, says, “Where does Germany’s future lie? It lies in the East- in Turkey… in Mesopotamia …in Syria…”[179]

1.1.9.1 Overview of Gulf War

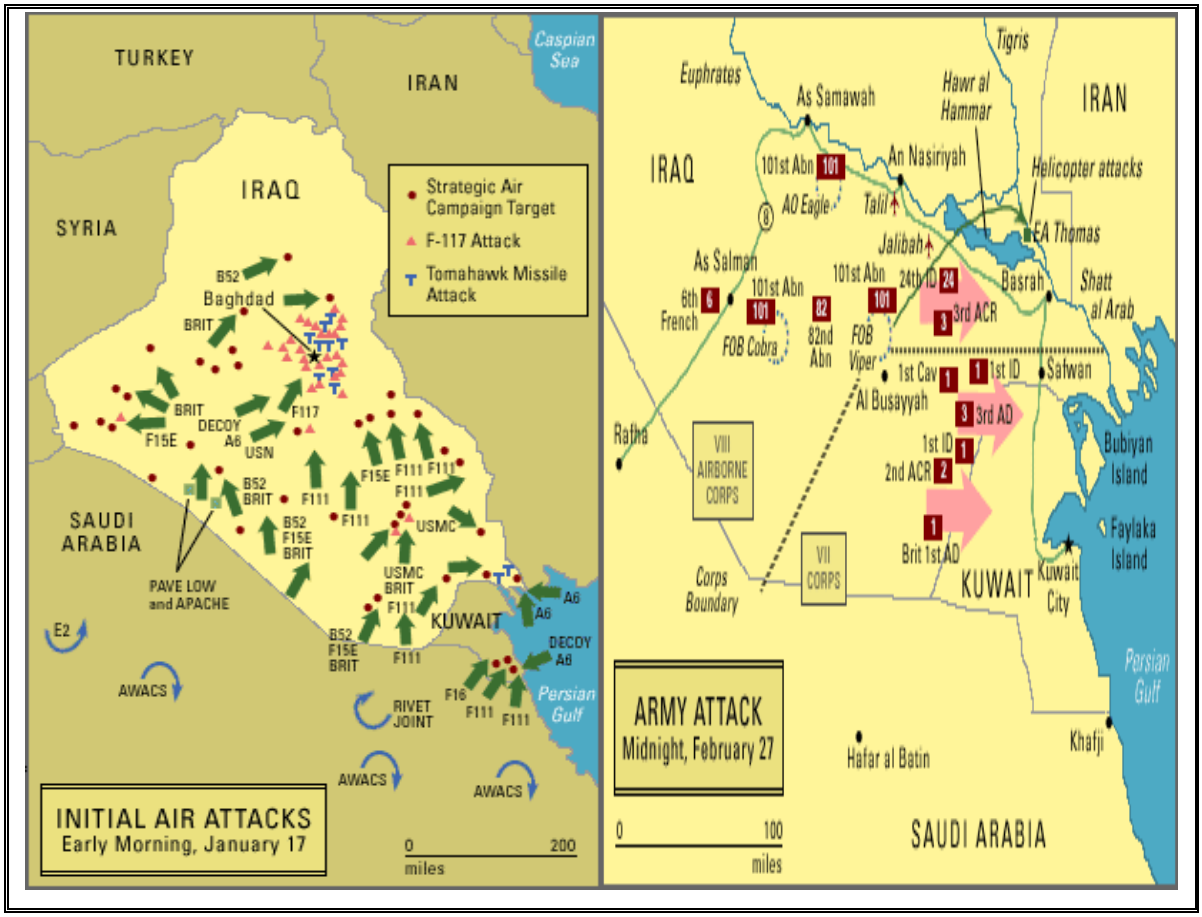
The Iraqi invasion of Kuwait on August 2nd 1990 has provoked a military response from the Western Powers unprecedented for over 20 years. The United Nations immediately

---

[177] Treml, V.G.,“Censorship, Access, and Influence: Western Sovietology in the Soviet Union” The University of California Publishing, Berkeley, 1999, pp. 36-37.
[178] Fisher, J., Ibid.
[179] Hopkirk, P., “On Secret Service East of Constantinople”, Oxford University Press, 1994, pp.1-7

condemned the invasion and imposed economic sanctions, By October 150,000 US troops were in the Arab Peninsula preparing for war.[180] On 16 January 1991, Operation Desert Storm commenced. By 10 March 1991, less than two weeks after combat operations in Desert Storm ceased, a total of 227,657 members of the deployment of US forces to the Persian Gulf was the largest logistics operation since the Vietnam Conflict. In the deserts of the Persian Gulf, Guards members and Reservists of combat, combat service, and combat service-support units were mobilized to participate fully with the active component in many essential aspects of the operation.[181] The air and army attacks of Allied Forces in Gulf War illustrated in map 3.4.

Map 0.4 The Air and Army Attacks of Allied Forces In Gulf War[182]



[180] White, J., and Gordon, M., "After The Peace Dividend Its War As Usual: Understanding The Gulf Crisis" Available on site http://flag.blackened.net/revolt/awg/gulf_crisis3.html

[181] Duncan, S.M., "Desert Shield/Desert Storm Employment or Reserve Component: Extracts of Lessons Learned", The United States Naval War College, p.84, Available on site www.fas.org/man/dod-101/ops/docs/p162.pdf

[182] Atkinson, R., "Crusade: The Untold Story of the Persian Gulf War" Houghton Mifflin Company, 1993, Available on site http://www.eskimo.com/%7Ektlange/MCOilFields.jpg

1.1.9.2 Intelligence Analysis of Gulf War

During Gulf War, which finished on 3 March 1991, the development and capabilities of the U.S. Intelligence Community from its inception during the early days of the Cold War to the end, along with the potential impact of intelligence upon warfare was most recently demonstrated.

The Coalition Forces enjoyed intelligence capabilities that far surpassed the sophistication of previous conflicts. As a result, Coalition Forces knew the enemy's strengths, weaknesses and the battlefield terrain exceptionally well. Schwartzkopf[183]directed the war effort using these superior intelligence resources.

The Gulf War demonstrated how intelligence could help win battles with minimal loss of life. However, as in all wars, mistakes occurred and intelligence resources contributed their share. One of the lessons of Desert Storm for the U.S. Intelligence Community was the need to better integrate advanced technology with intelligence and operations. This accelerated the development and exploitation of more advanced technology and sophisticated intelligence capabilities. Although technical intelligence is not a war winner ,[184] through the use of new technologies, future conflicts may make the Gulf War seem crude by comparison and may change the nature of warfare itself.

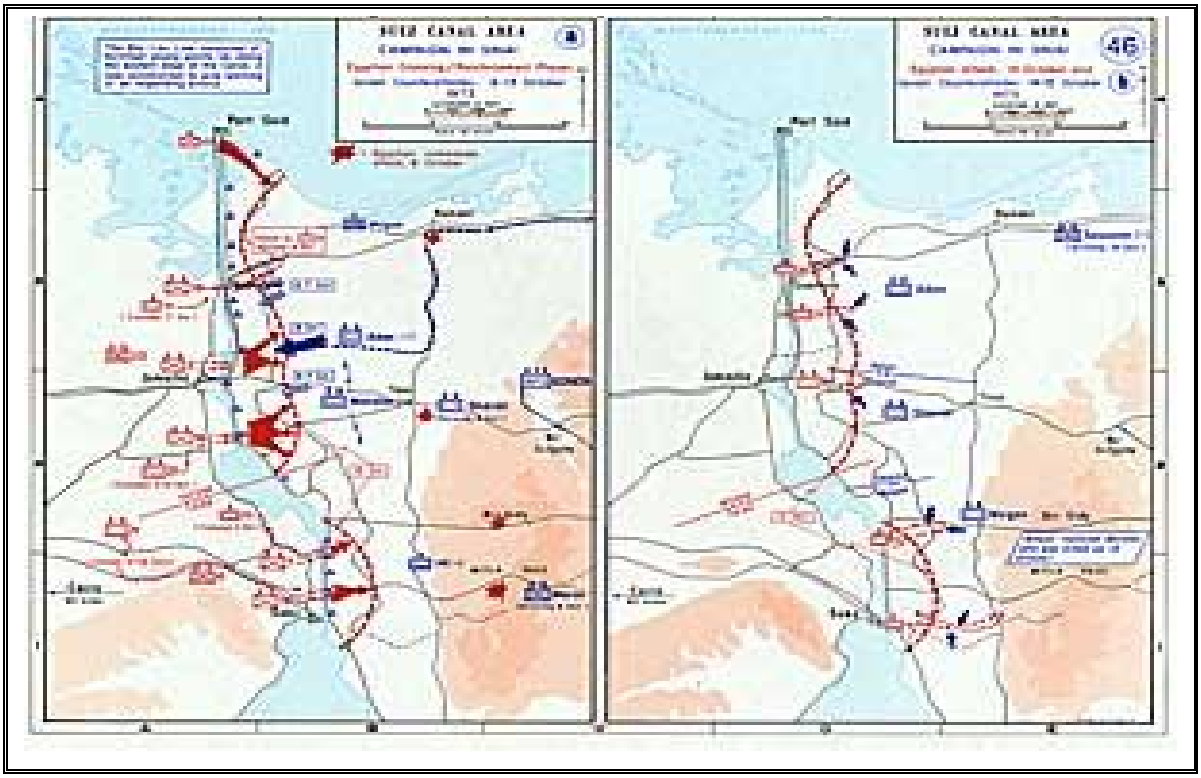
And also another problem, which appear in Golf War, is as the American commanders complained about difficulties to get timely access to all this great intelligence data. The commanders were also upset over the worthless conducts of the analysis. No one wanted to come right out and make a conclusion. So, after half a century, the intelligence is still not centralized, nor readily available to those who need it. Various government committees and oversight panels continue to look for solutions. But so far, there are no solutions, only a sad history.[185]

---

[183] General H. Norman Schwartzkopf, Jr., the Coalition Commander in Gulf War.
[184] Brian, F., and Wiersema, R., "Battlefield TECHINT: Support Of Operations Dessert Shields/Storm", Military Intelligence Professional Bulletin, Apr-Jun 1992, Vol. 18, Issue 2
[185] "How to Make War", Available on site http://www.strategypage.com/search.asp?target=d:\inetpub\strategypageroot\fyeo\howtomakewar\docs\archives\htint01.htm&search=history%20of%20intelligence

But the most obvious failure, of course, was that the intelligence community did not anticipate Iraq's invasion of Kuwait - just as it did not anticipate Israel's march to Beirut in 1982 and the Yom Kippur War in 1973 (seen at the map3.5). As intelligence failures go, failing to forecast a war in the Middle East is a big one. [186]

Map 0.5 Arab-Israel War in 1973[187]



Ambassador Wolfowitz's views "...on what works, what does not, and why regarding intelligence support to policymaking are illustrated by his perceptions of the relationship before and during the Persian Gulf crisis touched off by Iraq's invasion of Kuwait."[188]

In sum, the opportunities for failure are almost unlimited in intelligence. They may arise from a lack of sufficient information or too much information. They can be caused by the element of surprise, deception, or because an enemy acts irrationally. Even though our examination has by no means been scientific, nowhere has it been evident that

[186] Hadar, L.T., "Extricating America From Its Middle Eastern Entanglement, Policy Analysis No. 154, June 12, 1991, Available on site http://www.cato.org/pubs/pas/pa-154.html
[187] Map Library, "Maps of Arab-Israili War" Depertment of History, Available on site http://www.dean.usma.edu/history/dhistorymaps/Arab-Israel%20Pages/aitoc.htm
[188] Davis, D., "The Challenge of Managing Uncertainty - Paul Wolfowitz on Intelligence Policy-Relations", Available on site http://www.ci-ce-ct.com/article/showquestion.asp?faq=5&fldAuto=1278

organizational structures cause failures. It has been illustrated, however, that intelligence failures may be inevitable. Given this forecast, let us now refocus upon the primary contention of the thesis and search for a solution.

INTELLIGENCE ANALYSIS OF COLD WAR PERIOD

This period mostly can be called as a "spy vs. spy" story. Each side collected and used intelligence about their opponent to their advantage, until one came up with the critical information, which led to victory.

According to KGB documents in this period, as Khrushchev was told, 375 foreign agents were recruited, and 32 officers of the State Security were transferred abroad and legalized.[189]And only during one year alone 4,144 reports and 68 weekly and monthly informational bulletins prepared and presented to the Party's Central Committee and the USSR Council of Ministers.[190]

Soviet foreign intelligence appeared to have been particularly successful in "SIGINT" (signals intelligence) operations. During 1960 it reported deciphering 209,000 diplomatic cables sent by representatives of 51 states and the KGB's scientific-technical intelligence service reported that it stole, bought, and smuggled from the West 8,029 classified technologies, blueprints, and schemas, as well as 1,311 different samples of equipment.[191]

The Soviet Union, for all it's economic and political defects, was very good at one thing; keeping secrets. So difficult was espionage against the Soviet Union that the United States eventually came to rely mainly on "technical intelligence" to do most of their spying. Going into the 1980s, success caught up with the technical crew. America was increasingly dependent on spy satellites, and then the Space Shuttle Challenger blew up in 1986. There was suddenly no way to put new and replacement satellites up. [192]

---

[189] Kramer, M., "Archival Research in Moscow: Progress and Pitfalls," Cold War International History Project Bulletin 3, Fall 1993, 1, pp.18-39.
[190] Zubok, V.M., "Espionage, KGB, CIA, 1960-1962", CWIHP Bulletin, Washington, Available on site http://cwihp.si.edu/cwihplib.nsf
[191] Zubok, V.M., Ibid.
[192] "How to Make War", Available on site http://www.strategypage.com/search.asp?target=d:\inetpub\strategypageroot\fyeo\howtomakewar\docs\archives\htint01.htm&search=history%20of%20intelligence

The end of the cold war has produced a host of views on the future of intelligence. These views fit an unfortunate pattern in the history of decision-making concerning the intelligence communities. Both past experience and recent developments suggest that policy makers do not always understand the need for intelligence after the threat of war has passed. [193]

In the years of Cold War tension the intelligence services were more than just "eyes," they were powerful weapons in propaganda warfare between the ideological blocs. Furthermore, in a situation of mutual fear produced by the nuclear deadlock, when huge armies confronted each other in Europe and around the world, intelligence networks were the only mobile force in action, the "light infantry" of the Cold War: conducting reconnaissance, but also trying to influence the situation in the enemy's rear by means sometimes just short of military ones. [194]

The plans and instructions related to operational work and intelligence sources, in particular involving planting agents abroad and using double agents, justifiably belong to the most zealously guarded secrets of intelligence bureaucracies. [195]

Intelligence unquestionably helped Western States to win the Cold War by balancing the imbalance between NATO and the Warsaw Pact. Yet by the time that paradigm no longer applied, and defense intelligence moved on to more pressing matters. Primary among them was modifying a structure that would enhance the ability of the intelligence communities to address the challenges of a different, emerging, global environment. [196]

With wars in Afghanistan and Iraq, there was an intense need for intelligence, and for a while there were only a few working satellites available to get it. A bureaucracy evolved to tightly control who could use satellite and electronic ease dropping resources and who

---

[193] Berkowitz, B.D. and Goodman, A.E., "Why Spy--And How--In The 1990s?", Orbis, Spring 92, Vol. 36 Issue 2, p. 269

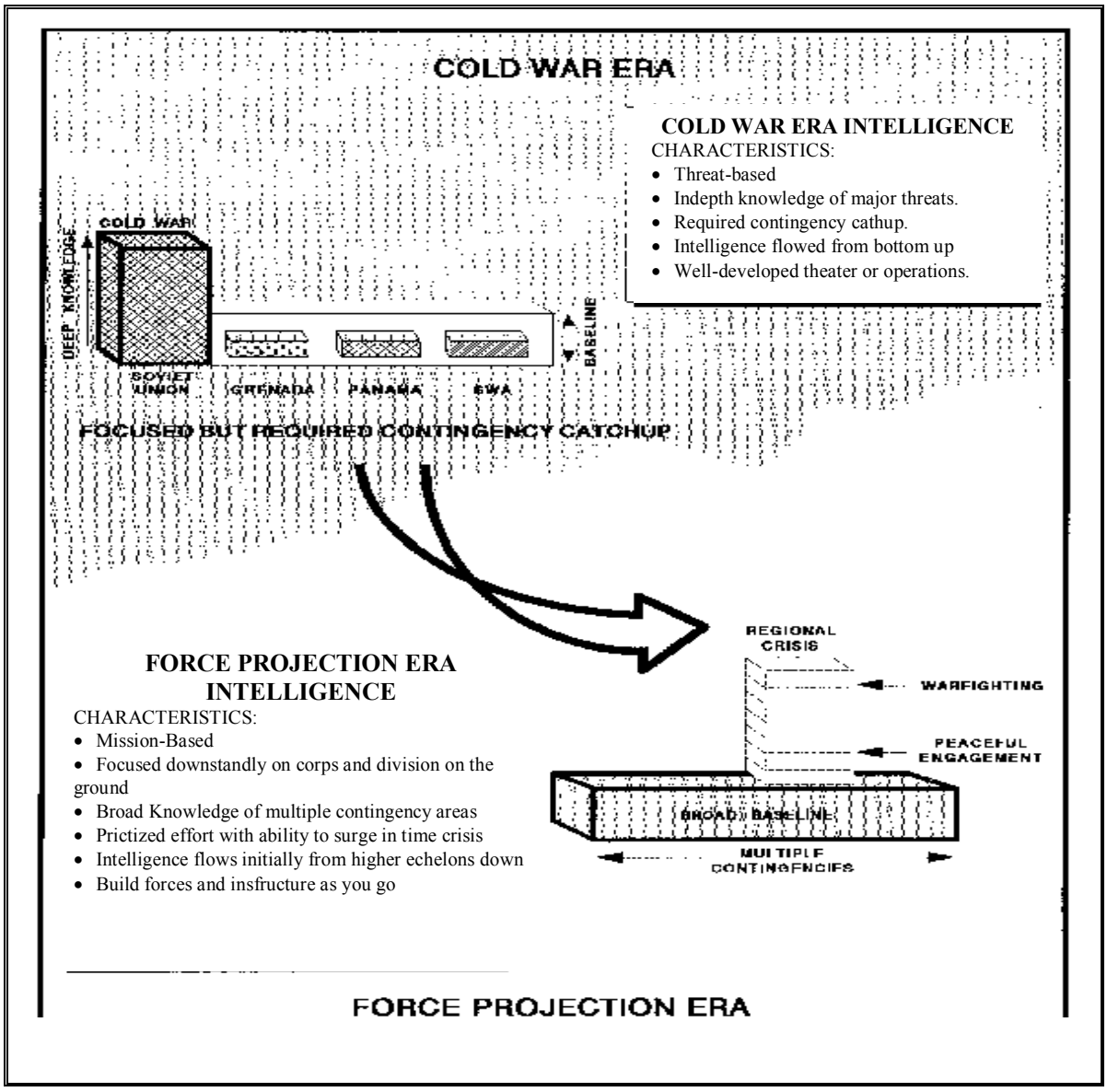
[194] Zubok, V.M., "Espionage, KGB, CIA, 1960-1962", CWIHP Bulletin, Washington, Available on site http://cwihp.si.edu/cwihplib.nsf

[195] Clapper, J.R., "Challenging Joint Military Intelligence", Joint Force Quarterly (JFQ), Spring 1994, pp. 92-99

[196] Zubok, V.M., Ibid.

could see the results.[197] Characteristics of intelligence and force projection are illustrated in Figure 3.1 Cold War Era.

Figure 0.1 Cold War Era[198]



[197] "How to Make War", Available on site http://www.strategypage.com/search.asp?target=d:\inetpub\strategypageroot\fyeo\howtomakewar\docs\archives\htint01.htm&search=history%20of%20intelligence

[198] FM 34-1, "Intelligence And Electronic Warfare Operations", Headquarters Department of the Army Washington, DC, 27 September 1994 Available on site http://www.fas.org/irp/doddir/dod/index.html

1.1.10 Reflections on Military Intelligence

While analyzing the intelligence evolution in the Cold War era, pointing out the effects in Military Strategy will be suitable. The fundamental elements of the mission of military intelligence to provide unique insight to operating forces reduce uncertainty for decision makers, and project future threat environments for the systems acquisition communities.

As Rosen observed, "the overall picture of American research and development in the period from 1930 to 1955 is one of technical innovation largely unaffected by the activities of potential enemies, a rather self-contained process in which actions and actors within the military establishment were the main determinants of innovation . . . Military innovation is much less bound up with foreign military behavior or civilian invention than is ordinarily thought."[199]

Throughout the Cold War, the Army focused on strategic programming (making decisions about the number and type of units in the force, their organization, and their equipment) rather than on strategic planning.[200] Therefore, intelligence support to their efforts had little influence because the planners themselves enjoyed little.

The fundamental elements of the mission of military intelligence have not changed in the Cold War era. What has changed very dramatically in several recent cases is the international military balance? By the late 1980s defense intelligence had evolved over a period of nearly forty years in response to the threat posed by powers; the proliferation of multiple, complex weapons systems and intelligence associated with their design and employment; and a corresponding increase in the size of the defense budget. [201]

During these four decades dynamic threats and responses to it increased large scale, capable service component and departmental intelligence organizations focused on intelligence problems related to this threat.

---

[199] Rosen, S. P., "Winning the Next War: Innovation and Modern Militaries", Cornell University Press, 1991, p. 250.
[200] Builder, C. H., and Dewar, J. A., "A Time for Planning? If Not Now, When?" Parameters, Summer 1994, pp. 4-5
[201] Clapper, J.R., "Challenging Joint Military Intelligence", Joint Force Quarterly (JFQ), Spring 1994, pp. 92-93

The intelligence communities were primarily concerned with adequate capabilities to support the mission of anticipating, monitoring, deterring, and containing adversaries' aggressions or advantages. So the Armies required thousands of intelligence personnel scattered across Europe as a critical force multiplier to help their States. But with great collapse, as many other things, and also that was changed. [202]

As seen in Gulf War, among precision-guided "smart" weapons, intelligence support to sophisticated weapons and others, the most critical was that such systems are voracious consumers of intelligence. For instance, in the past the identification of a specific targeted building sufficed. Today precision delivery capabilities require further identification — down to a particular room in that targeted building. This increase in the level of targeting detail demands exacting geo-positional data, near-real time imagery, and fused all-source intelligence. [203]

So defense intelligence faces a broad spectrum of global geopolitical changes that requires supporting new and increasingly complex missions. The military intelligence community is at the same time attempting to manage the transition from its Cold War posture to one appropriate for the new world disorder. This would be a strong challenge in and of itself. But in addition defense intelligence is embarking on this transition in a period marked by a reduction in resources, which far outstrips the annual increases required to build capabilities in the first place. [204]

CONCLUSION OF HISTORICAL ANALYSIS OF INTELLIGENCE

From the previous time to end of Cold War, importance of intelligence accelerates in administration, in battlefield, in every areas while human intelligence is saving importance, technical intelligence having importance day by day.

Although first documents about intelligence arrive until 500 BC, I believe it doesn't mean the others whose lived before Sun Tzu, didn't know the importance of intelligence.

---

[202] Clapper, J.R., Ibid, pp. 93-94
[203] Clapper, J.R., Ibid, pp. 94-96
[204] Clapper, J.R., Ibid, pp. 96-99

By Greek, Athens, Chinese, Turks, and others were used intelligence in battlefield to see the aim and arrangement of enemy. But their unique apparatus to gather information about enemy was human. By the way the characteristics of foreknowledge of that period; cannot be elicited from spirits, nor from gods, nor by analogy with past events, nor from calculations. It must be obtained directly from men who know the enemy situation.

Is Human Intelligence (HUMINT) a strategic or tactical intelligence? If you think these developments as in battlefield, maybe you can think as a tactical or operative intelligence. But if you think those periods' feasibility, maybe you can think as a strategic intelligence. I think it is a strategic intelligence. I explain it with an example; while determining the national waters in 18 century, states preferred the usage of a range of cannon that was a strategic weapon in this period. Today a cannon is not a strategic weapon.[205]So determine the boundaries between strategic, operative and tactical is relative.

This period contains most of the elements of strategic intelligence. The collection requirements included requests for information on the economic qualities of the land, the vitality of its people, and their military strength as a basis for policy judgments. In intelligence personal skill may be the paramount factor on the small scale, but the ability to coordinate the skills of many individuals may be predominant in large-scale operations. To say about a doctrinal development of intelligence in this period is unsuitable.

By the wars importance of intelligence increased. This period was a fortunate and exhilarating time to be involved in intelligence, when new channels of information were opening up, and when we could quickly see the effects of the work on the operation of war.

Although the state of technological developments over a wide range of intelligence fields was still elementary, have profound effects on warfare.

The period until WW I is awash with stories of intelligence operations. For gathering information about enemy by balloonists, different ways of coding things became numerous in WWI. By the code-making and code-breaking operations especially during the period 1939-1945 with MAGIC and ULTRA, a new intelligence era started.

---

[205] Tetik, A., "Devletler Hukuku", Harp Akademileri Basım Evi, İstanbul, 2001, p.53

By the end of the war, the information became so complete and comprehensive, not merely of military significance, but also political and economic, that the enemy could scarcely make a move without the Allies knowing of it and thereby enjoying the advantage of meeting him at a controlled time and place.

Especially failures caused to understanding of strategic intelligence absence such as Stalin's failure to accept that Germany was going to invade, American failure to recognize that Japan was embarking on a war policy, German miscalculations over D-Day, etc. Not so the outbreak of the war itself, where strategic intelligence arguably played a significant a part in producing a general war.[206] Intelligence used to provide a picture of the general political and military intentions of other states, is both the most difficult intelligence to procure and the most necessary.

Until the Cold War, most efforts went toward current intelligence. By the Cold War most of intelligence events and development takes place in the scene of superpowers. For Western States especially for U.S., during the Cold War period the most important estimates focused on the annual assessments of Soviet military forces. The major intelligence controversies of the 1960s and 1970s revolved around how well the community had assessed the Soviet threat.

The fact that the Cold War in the 1970s and the late 1980s looked more like a "long peace" appeared to have limited effect on the mentality of intelligence officials in Washington and Moscow.[207] By then, the KGB's First Directorate concentrated even more on technical-scientific espionage, which reflected, on the one hand, a long-standing living together between the Soviet intelligence services and the military-industrial connection, and, on the other, a distancing from "cloak and dagger" covert activities. The shady games and counter-games in which the two intelligence services had engaged all during the Cold War.[208]

---

[206] Overy, R., "War In History, Strategic Intelligence and the Outbreak of the Second World War", King's College Publising, London, 1998, p.451
[207] Gaddis, J. L., " The Long Peace: Inquiries into the History of the Cold War" Oxford University Press, New York, 1987, pp. 215-245.
[208] Zubok, V.M., Ibid.

There were failures and errors in these collection and analysis of information work, but, in general, the record shows considerable accuracy and consistent objectivity, at least as far as the specific actions and motives were concerned. But the darker side of intelligence activity, linked to the Cold War mentality and actions, always co-existed with the former, sometimes forming a long shadow. The resources spent on intelligence operations related to psychological warfare and deception had a dynamic of diminishing returns: the disruption caused by them in the enemy's camp rarely justified the money and efforts spent on them.[209]

With the collapse of the Warsaw Pact and the break-up of the Soviet Union, many of these specific issues are less important. However, the state of the former Soviet Union and what remains of its military is still a critical intelligence target, if only because of its uncertain future. The main development is not that the Soviet Union is less important, but that the information, which is needed, about the Soviet Union is different. These questions are; what will be the nature of the newly declared Commonwealth of Independent States? What will become of the Soviet military organization and its command structure? Will individual members of the Commonwealth successfully establish independent military forces, and, if so, what capabilities will they have? Who are the key leaders in each of the republics, and what are their policies? What are the dynamics of politics among the republics? Will the Commonwealth be able to organize a coordinated economic policy?

By the way intelligence aspects changed to find a solution to all these questions. In reality concept is similar, but format is changing depend on the changing face of world. Globalization, which started with collapse of Soviet Union, can suggest a new step to analysis intelligence prospectus.

Through out the corridor of intelligence, we see failures caused by human, organizational crookedness and appeared spontaneously. All analysts forced to put a schema to reduce the failures. Until collapse of Soviet Union all efforts are human centric. So if we look these phenomena, we see human is the main argument in the intelligence process and it doesn't change. It is blessed with the strengths of flexibility and judgment, and cursed with the

---

[209] Zubok, V.M., Ibid

inherent imperfection of man. If the imperfection should surface during a time of crisis, the ensuing advice may not match the leader's expectations. This mismatch of perceptions defines a failure. But, how should the failure be rectified? Should it be considered a system problem and fixed with bureaucratic action? Or, should this be treated as a human failing and fixed by adjusting expectations and adopting a risk management mentality? The recent example of the Gulf War provides some insight into a common response to these questions. It is evident from these examples that some perceive intelligence as a panacea. That perception is incorrect. Rather, it is the end product of a logical progression of human thought processes. Good intelligence is viewed as important to leaders. Intelligence plays a supporting role in assisting leaders to make informed decisions. Even the best intelligence in the world does not eliminate the burden of making difficult choices - that is a leadership role.[210]

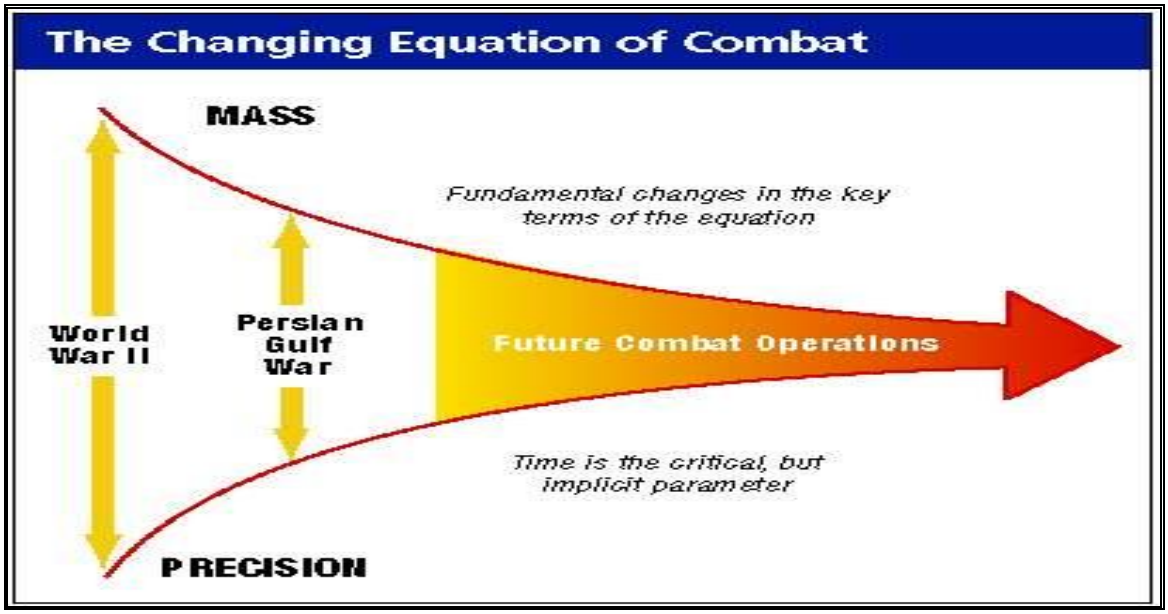
Second types of failures which can be seen also in two military examples such as Cuban crisis and Vietnam, help to demonstrate how intelligence failures continued to occur regardless of the organizational structure.

Conducting a pure comparative analysis of historical occurrences of failure and demonstrated responses will document a trend, but do little to suggest a solution. Prescribing a solution is obligated upon understanding the cause. For that reason, we need to investigate organizational theory and concepts, and the intelligence process. Only then will it be possible to prevent, predict or, at the very least, understand intelligence failures in the future.

Equation of intelligence is parallel to the changing equation of combat as illustrated in figure 4.5.

[210] Dearth, D. H.and Godden, R. T. (eds), "Strategic Intelligence: Theory and Application", (second edition), Defense Intelligence Agency, Washington, 1995, p. xi

Figure 0.2 The Changing Equation of Combat[211]



If we talk about on the future of intelligence at the end the Cold War, we should look the views fit an unfortunate pattern in the history of decision-making concerning the intelligence communities. Both past experience and recent developments suggest that policy makers do not always understand the need for intelligence after the threat (or reality) of war has passed. Historically, some policy makers favored reductions in intelligence as part of a general cutback in national security programs and as a way to realize a peace dividend. Others were against spying in principle or believed that it was inconsistent with the conduct of peacetime international relations. These views are reoccurring among policy makers. Recently, the press reported that major cutbacks are being sought for the intelligence community.[212]

According to Berkowitz "The reasoning behind these views is wrong. First, it mistakenly assumes that the Soviet threat was the reason for maintaining an intelligence community. In fact, the intelligence communities was necessary, and was established, because the formulation of national security policy, necessary, to protect their interests requires large

[211] Sheehan, J.J., "Next Steps in Joint Force Integration", Joint Force Quarterly (JFQ), Autumn 1996, pp.47
[212] Best, R.A., "Reforming Defense Intelligence", Congressional Research Service Report for Congress, Rev. ed. Library of Congress, Washington, 22 Jan. 1992, 91-475F, June 11, 1991 Available on site http://www.chem.au.dk/~db/fusion/alpha_P

amounts of information, tailored for its users and often difficult to obtain. Secondly, such reasoning assumes that some other organization --the media, academia and the military services, can provide whatever data the government needs." [213]

All government departments are reluctant to expend their resources to support information requirements beyond their own. Even if collection is technically feasible for the public media, the profit for collecting data is often too small to entice companies to make the necessary investment. The intelligence communities must gather much information that is not of current interest, but which might be critical for decision maker sometime in the future. Ultimately, people are the make-or-break factor for effective intelligence. Some analyst eventually has to write the report, develop the on-line database, or present the briefing that connects the intelligence communities to the intelligence consumer. To analyze all of the new targets, the intelligence communities will need more, not fewer people.[214]

At the end, history is full with intelligence failures from Carthage to Pearl Harbor, from Navarin to Normandia, from Cuba to Vietnam etc. The last one is the September 11th attack of terrorist, who's used a historical trick, which is known as Trojan.[215]

---

[213] Berkowitz, B.D.and Goodman, A.E., "Why Spy--And How--In The 1990s?", Orbis, Spring 92, Vol. 36 Issue 2, p. 269
[214] Berkowitz, B.D.and Goodman, A.E., Ibid, p. 270
[215] Caşın, M.H., "Stratejik İstihbarat", Avrasya Dosyası (İstihbarat Özel), No:2, Ankara, Summer 2002, pp. 255-256

"If intelligence is viewed as a panacea, as fortune-telling rather that as a complicated and inherently imperfect process, it is only too easy to turn it into a scapegoat. ... Even the best intelligence in the world does not eliminate the burden of making difficult choices…"

Micheal I. Handel[216]

CONCEPTUAL ANALYSES OF INTELLIGENCE

Implementing an effective intelligence program prevents the inadvertent compromise of sensitive or classified information concerning an organization's activities, intentions, or capabilities. For an intelligence program to be effective, personnel must be aware of intelligence concerns, implement intelligence countermeasures when appropriate, and be observant of potential collection activities directed at their organization. This is only possible if the members of the organization understand the range of threats affecting their organization and actively supports the intelligence program.

Why do we need to understand the intelligence process? A few decades ago, it was possible to predict conflict by monitoring military and civilian activity, especially changes in a country's military industrial output. Today an attack does not rebuke a massive mobilization and the corresponding telltale evidence. In this era of "instantaneous" attack, the intelligence community cannot wait until after the decision to attack has been made before warning our government. Warning must come as soon as possible, so that appropriate action can be taken.

To make informed decisions about what kind of intelligence system we need we must have a reasonably clear view of the character intelligence by analyzing it.

Because of the categories of intelligence threat, which provides an overview of worldwide threats in each category, and identifies available resources for obtaining threat information, and forecasting future structures, So in this chapter I will try to structural analyses of intelligence to assist the policymakers, directors, commanders and administrators in

---

[216] Handel, M. I., in Dearth, D. H.and Godden, R. T. (eds), "Strategic Intelligence: Theory and Application" (second edition), Defense Intelligence Agency, Washington, 1995, p xi.

gaining organizational support for intelligence countermeasures by providing data on the significant collection threat targeting the states and organizations activities and industry.

DIMENSIONS OF INTELLIGENCE

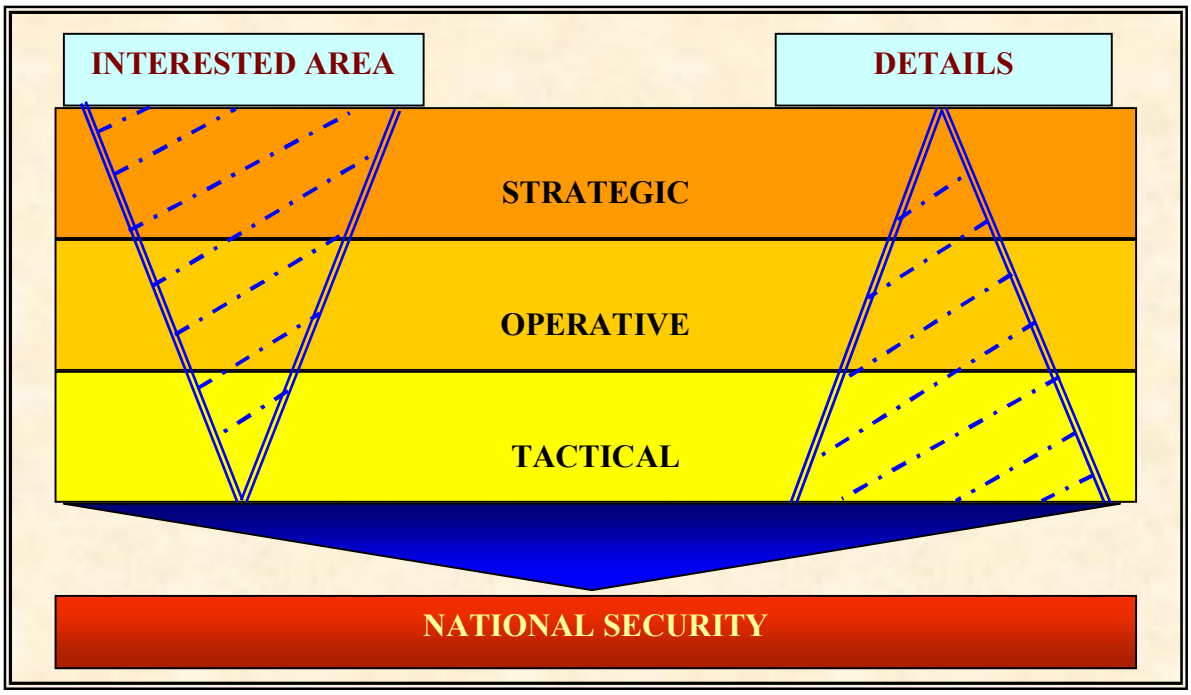
Until now we looked at the terms that are related with strategic intelligence. The dimensions of intelligence are not tied to specific ranks but rather to the intended outcome of the aims, which they support. We can describe intelligence in tree dimensions that are strategic, operative, and tactical intelligence.

Logically, strategic levels needs to be broader in its scope, address a wider variety of topics, and investigate more potentialities. Details will still be important, but they are details of a different kind. As illustrated in Figure 4.1 the relation between dimensions are not specific. Some called these dimensions as levels of intelligence[217]and describe these levels as,

- Strategic intelligence,
- Operational intelligence,
- Tactical intelligence.

[217] Joint Pub 2-0 "Intelligence Support to Operations", Joint Force Employment Briefing, Joint Chiefs of Staff (CJCS), p.vii, Available on site http://www.fas.org/irp/doddir/dod/jp2-0/index.html

Figure 0.1 Relation Between The Dimensions of Intelligence



1.1.11 Strategic Intelligence

Without interested with the analyses of strategic intelligence, if we wants to define strategic intelligence generally,

Strategic intelligence is required for the formulation of strategy, policy, and military plans and operations at national and theater levels. At the strategic level, intelligence is oriented toward national objectives and supports the formulation of policies and determination of priorities. Strategic intelligence focuses first on distinguishing the capabilities and intentions of potential adversaries as well as considering the strategic intentions of allies and other potential multinational partners. Strategic intelligence plays a central role in identifying an adversary's centers of gravity.[218] So strategic intelligence;

- Concentrates on the national political, economic, and military considerations of states or nations. It identifies the support for governments, the ability of states or nations to mobilize for war, the national political objectives, and the personalities of national leaders.

[218] Department Of The Navy Office, "Naval Intelligence", Naval Doctrine Publication (NDP) 2, Washington, 1993, p.6

- Identifies a nation's ability to support forces and operations (for example, ports and the transportation infrastructure).
- Predicts other nations' responses. [219]

Finally, it seeks to determine the identity and characteristics of each of the possible threats a strategic political or military objective may face and how each may have a compounding or canceling effect on the overall operation.[220]

1.1.12 Operational Intelligence

Operational intelligence is required for the planning and execution of campaigns and major operations, and reflects the nature of the theater of war itself. Intelligence at this level serves as a bridge between strategic and tactical levels. So operational intelligence;

- Supports friendly campaigns and operations by predicting the enemy's campaign plans, identifying their military centers of gravity, lines of communication, decisive points, pivots of maneuver, and other components necessary for campaign design.
- Focuses primarily on the intelligence needs of commanders from theater through corps and task force.[221]

1.1.13 Tactical Intelligence

Tactical Intelligence is required for planning and conducting tactical operations. Tactical intelligence supports the execution of battles and engagements. It provides the tactical leader with the intelligence he needs to employ combat elements against enemy forces and achieve the objectives of the operational leader. Tactical intelligence is distinguished from other levels by its perishability and ability to immediately influence the outcome of the tactical leader's mission. Tactical intelligence normally supports operations by ranks corps and below units. [222]

---

[219] FM 34-1 "Intelligence And Electronic Warfare Operations", Headquarters Department of the Army Washington, 27 September 1994, Available on site http://www.fas.org/irp/doddir/dod/index.html
[220] Medby, J., "IPB Considerations at the Strategic Level", Military Intelligence Professional Bulletin, Apr/Jun 2002, Vol. 28, Issue 2, p.26
[221] FM 34-1, Ibid.
[222] FM 34-1, Ibid.

1.1.14 Differences Between The Dimensions

Strategic intelligence provides information on the host nation's political climate; operational intelligence identifies key objectives; and tactical intelligence shows of where the adversaries can be decisively engaged. Advances in technology and the requirements also make the demarcation between strategic, operational, and tactical intelligence resources indistinguishable.[223]

Collection assets, which normally support strategic intelligence, can and often are tasked to support operational and tactical intelligence requirements. This blending of dimensions and resources is a characteristic of intelligence in the post-Cold War era, a characteristic that the Intelligence Battlefield Operating System (BOS) exploits. [224]

Shortly, strategic intelligence looks for what should build or direct for national security; Operative intelligence put the directions in objectives; Tactical intelligence try to realize these objectives. So strategic intelligence is upper dimension of intelligence and contains the others.

THE MISSIONS OF INTELLIGENCE ON INTERNATIONAL SYSTEM

In this section, is identified what are necessary and appropriate missions for the Intelligence Communities as it enters the 21st century. Many are traditional missions that require little explanation. A few, however, raise issues needing elaboration.

1.1.15 National Diplomacy and Intelligence Requirements

This support entails providing advance warning of developments in other countries that will or could affect national interests. Such advance warnings give policymakers the time to frame an appropriate response and, if possible, to avoid conflicts that might require the introduction of national forces.

---

[223] FM 34-1, Ibid.
[224] FM 34-1, Ibid.

Intelligence can also provide information that assists policymakers in determining which of several diplomatic steps may be most effective.

Even if we know in our bones of the great weight which such issues have carried in many a foreign policy decision, we do not readily and consciously acknowledge it. Our wish, is, of course, to have our knowledge and wisdom about the foreign trouble spot show itself so deep and so complete that it will perforce determine the decision. The nature of our calling requires that we pretend as hard as we are able that the wish is indeed the fact and that the policymaker will invariably defer to our findings as opposed to the cries of some domestic lobby.

Ideally, the best intelligence is precisely that information that provides policymakers with the leverage to achieve national objectives in international affairs without the commitment of national forces. [225] Intelligence also provides information that serves as the basis for diplomatic initiatives in bilateral and multilateral treaty negotiations.

1.1.16 Monitoring of Treaties and Other Agreements

Intelligence is also essential for monitoring the multitude of treaties, agreements, and sanctions. For example, put in place of the weapon arsenal of Greek in Aegean Islands.

1.1.17 Military Operations and Intelligence Support

Another traditional mission of the Intelligence Communities is to provide support to military operations. This mission encompasses not only warning of attack on national territory and installations, but also providing information needed to plan for and carry out military operations of all kinds. In the past, this has largely involved the provision of order of battle information on opposing military forces: their size, nature, location, morale and capabilities. In recent years, however, this mission has been rapidly expanding.[226]

---

[225] Kent, S., "Estimates and Influence ", Sherman Kent and the Board of National Estimates, Collected Essays, Available on site http://www.cia.gov/csi/books/shermankent/toc.html

[226] Vector 21, "The Defense Intelligence Architecture", A Strategic Plan for the Defense Intelligence Agency, Available on site http://www.fas.org/irp/dia/vector21/

Recent years have also seen radical change in the nature of warfare. The 1991 Persian Gulf War continued only a few weeks, but signaled a quantum leap in military capability. The world saw weapons fired from aircraft, ships, and land batteries far from the point of impact and delivered with pinpoint precision and devastating consequences. The war ended quickly, and U.S. casualties were minimal.[227]

1.1.18 Defense Planning, Modern State and Intelligence Levels

Intelligence should also continue to support defense planning, another traditional mission. This mission causes providing information on foreign military capabilities in order for defense planners to shape the size, nature, and disposition of national military forces. It also includes necessary information to guide military research and development activities and future military acquisition decisions. It encompasses information about foreign military tactics and capabilities, which can then be used to train and protect national forces.[228]

1.1.19 Importance of Economic Intelligence

Although this subject is explained in previous sections, it is a mission for intelligence. This activity focused on national interests, including the economies of foreign countries, worldwide economic trends, and information to support trade negotiations. While much of this information was available from public sources, there were many countries where such information was restricted or not readily available. Intelligence filled a considerable space.

Now, after the Cold War, far more economic information is openly available, causing some to urge that the Intelligence Communities abandon or cut back its historical role in economic intelligence, particularly macroeconomic collection and analysis. Some recipients of this analysis complain that it adds little to what they already know. Intelligence analysts concede that approximately 95 percent of the analysis on economic topics now comes from open sources. On the other hand, there remains the five percent

---

[227] Teke, M., "Priorities for the Possible Impacts of Information Warfare on The Future Battlefield", Unpublished Master Thesis, Yeditepe University, Istanbul, 2002, p.112

[228] Cadena, L., "Rethinking the Missions and Priorities of the Intelligence Community", 1997. Available on site http://www.fas.org/irp/eprint/snyder/priorities.htm

added by intelligence. Reliable information about economic conditions in certain countries continues to be unavailable. In these cases, accurate information could be crucial to decision making. In some contexts, policy agencies may need to rely on intelligence agencies to perform economic analysis to preserve confidentiality even if open sources form the principal basis of such analysis, for example, in supporting trade negotiations.[229]

1.1.20 Countering Activities Abroad That Threaten National Interests

For the last ten years, changing trends in environments, also affected threats. This can be national or international threat. These new missions include: Counterterrorism, Counternarcotics, Countering International Organized Crime, etc.

In all of these cases, intelligence information has provided the basis for diplomatic initiatives, supported national law enforcement efforts to prevent and prosecute such activities, served as the basis for military responses in some cases, and has often been key to the efforts of other governments to bring such activities under control. Frequently, intelligence agencies provide assistance to other governments beyond mere information, for example, by providing training or specialized equipment to cope with certain threats. On occasion, intelligence agencies are authorized to undertake covert operations to counter them.

1.1.21 Support to Criminal Justice and Regulatory Agencies

In addition to providing information to law enforcement agencies about terrorism, drug trafficking, international organized crime, and weapons proliferation, intelligence agencies also frequently are asked to collect or provide information they may have regarding foreign persons or entities who are the subject of criminal investigations within the territory. Responding to these requests ordinarily requires only a part of intelligence effort or resources. It does, however, raise concerns about the protection of intelligence sources and methods, and, given the much information that is ordinarily developed by, or available to, criminal justice or regulatory agencies, the search of intelligence records may produce little

---

[229] Potter, E.H.,"Economic Intelligence and National Security", Carleton University Press, Canada, 1998, pp.15-30

of value. Moreover, regulatory agencies often have difficulty using classified intelligence information because their actions must be based on a public record. [230]

1.1.22 Collecting and Analyzing Environmental Information

The unique collection capabilities of the Intelligence Communities are occasionally put to use to obtain information on threats to national and the world's environment, such as the dumping radioactive substances in territory or seas. Environmental hazards can directly threaten the security of states and their citizens, and environmental conditions in other countries can have an indirect effect by causing regional conflicts over rare resources, and destabilizing foreign governments. Analysis of this environmental information is performed on a limited basis. [231]

But these affords primarily are executed by powerful states which are have technical equipments.

1.1.23 Information Warfare Idea and Intelligence Dimensions

"Information warfare" refers to activities undertaken by governments, groups, or individuals to gain electronic access to information systems in other countries either for the purpose of obtaining the data in such systems, manipulating or fabricating the data, or perhaps even bringing the systems down, as well as activities undertaken to protect against such activities. Intelligence agencies have been involved in aspects of information warfare, both offensive and defensive, for many years. New momentum has recently been given to these roles by the explosion in information systems and information systems technology.

Government and public communications, transportation, financial, energy, and other industrial systems have become critically dependent on a complex set of interconnected automated information and control systems. Many of these systems are potentially vulnerable to computer-based disruption, manipulation, or corruption by hostile individuals, groups, or countries.

---

[230] Cadena, L., Ibid.
[231] Cadena, L., Ibid.

Collecting information about "information warfare" threats posed by other countries or by non-governmental groups to national systems is, however, a legitimate mission for the Intelligence Communities. Indeed, it is a mission that has grown and will become increasingly important. It also is a mission which the Commission believes requires better definition. While a great deal of activity is apparent, it does not appear well coordinated or responsive to an overall strategy. [232]

CONCEPTUAL ANALYSES OF STRATEGIC INTELLIGENCE

By the light of these definitions, I'll try to describe what strategic intelligence is. We should think strategic intelligence as one dimension of intelligence. By recording different concepts of strategic intelligence, and different contexts in which these are applied, the idea of intelligence is not restricted to national security, or corporate competition. It can apply at the level of the individual citizen, company, community, or country; we focused on the conceptual analyses.

According to Kent, Strategic Intelligence's subject "the sinews of national life". In its most elevated form, it considers the nation-state to the depth and breadth of its being. This is what Sherman Kent called a nation's strategic altitude: "not just the means it possessed to wage war, but its total potential for war-the resources that are available, or might be made available; the population, industrial plant, and transportation net; the political and social structure, their stability, and the moral quality of the people and their strength of values…and, lastly, the political leadership, their strength and genius (or want of it) for organizing men and materials into a community of life and strength."[233]

Strategic intelligence is intelligence that is required for the formulation of strategy, policy, and military plans and operations at national and theater levels. [234] Operational intelligence is intelligence required for planning and conducting campaigns and major operations to

---

[232] Teke, M., "Priorities for the Possible Impacts of Information Warfare on The Future Battlefield", Unpublished Master Thesis, Yeditepe University, Istanbul, 2002, pp.197-205

[233] Kent, S.,"Intelligence and the Problem of National Foreign Policy," Sherman Kent and the Board of National Estimates Collected Essays, CIA Progress Report, Office of National Estimates, Section I, 26 December 1951, p. 2.

[234] National Intelligence Course (NIC) Textbook, Joint Military Intelligence Training Center, November 1999

accomplish strategic objectives within theaters or areas of operations. Tactical intelligence is intelligence that is required for planning and conducting tactical operations.

This definition and interpretation of intelligence does not take into account the work of the intelligence services, and implies that corporate intelligence is distinct from that gathered by government agencies. This assumption is, in fact, correct in the sense that intelligence agencies such as the CIA, KGB, MI5 have a clear mandate which does not include supplying commercially sensitive data to their national companies. [235]

"There is no phase of the intelligence business that is more important than the proper relationship between intelligence itself and the people who use its products. Oddly enough, this relationship, which one would expect to establish itself automatically, does not do this. It is established as a result of a great deal of conscious effort . . ." [236]

Despite guidance from Kent and numerous subsequent authors, the terms of engagement between intelligence, policymaker, national security, strategy and war are still ill-defined doctrinally and thus practiced as much to suit the immediate preferences of the players on both sides of the relationship as to meet the fundamental demands of sound policymaking. In the forward section about psychology of intelligence, I will mention about these doctrinal approaches.

TENETS OF INTELLIGENCE[237]

The tenets of intelligence, which is seen in figure 4.2, are the fundamental standards against which performance of intelligence personnel and organizations must be judged. The tenets of intelligence offer qualitative objectives for intelligence used to support all activities and standards against which intelligence activities and products are evaluated. A failure to achieve any one of these fundamental attributes may contribute to a failure of

---

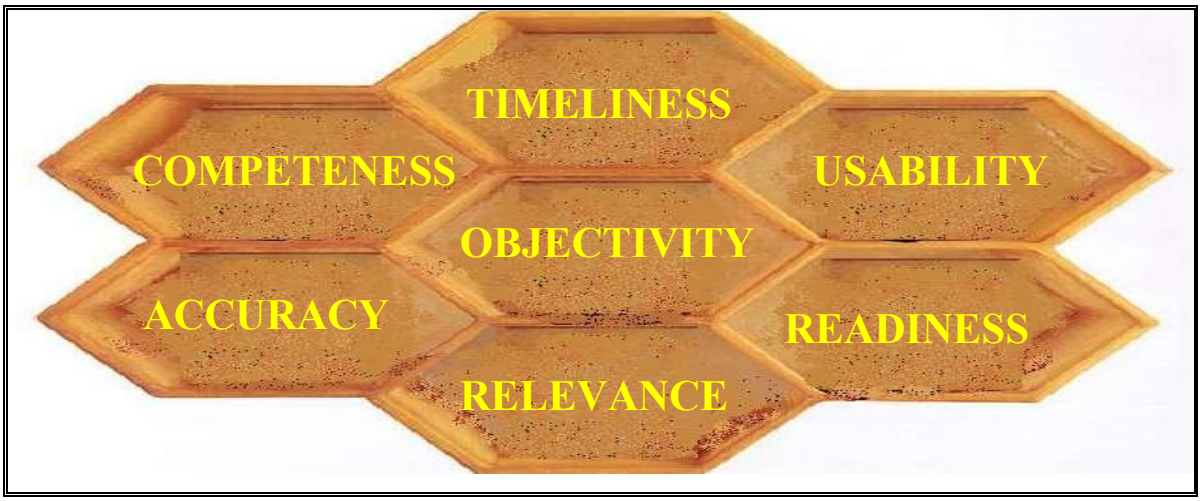
[235] Trim, P.R., "The Company-Intelligence Interface and National Security", International Journal of Intelligence, Vol 13, No: 2, p.204-214

[236] Davis, J., "A Policymaker's Perspective On Intelligence Analysis", Studies In Intelligence, 1995 edition, Vol.38, No. 5, Available on site www.cia.gov/csi/studies/95unclass

[237] Joint Staff, "Joint Doctrine for Intelligence Support to Joint Operations", Office of the Joint Chiefs of Staff, Washington, 05 May 1995, pp. IV-14, IV-16

operations. The bottom line is whether the user's priority information requirements are being satisfied.

Figure 0.2 The Tenets of Intelligence



1.1.24 Timeliness

Intelligence must be available when the users require it. Late intelligence is as useless as no intelligence. Timely intelligence enables the commander to anticipate events in the operational area. This enables the users to time operations for maximum effectiveness and to avoid being surprised.[238]Timeliness is influenced by the intelligence process of developing essential elements of information, identifying and stating requirements, and collecting and producing intelligence.

1.1.25 Objectivity

For intelligence to be objective, it should be unprejudiced, undistorted, and free from political or other constraints. The methodology, product, and use of intelligence must not be directed or manipulated to conform to a desired result, preconceptions of a situation or an adversary, institutional position, predetermined objective, operation, or method of operations. Intelligence concerning a situation is one of the factors in determining policy, but policy must not determine the intelligence.

---

[238] Joint Pub 2-0 "Intelligence Support to Operations", Joint Force Employment Briefing,, Joint Chiefs of Staff (CJCS), p.6-7, Available on site http://www.fas.org/irp/doddir/dod/jp2-0/index.html

1.1.26 Usability

Intelligence must be tailored to the specific needs of consumers and provided in forms suitable for immediate comprehension. The form in which intelligence is provided to the users should be tailored for particular applications or be suitable for general use without additional analysis or manipulation. As much as practicable, intelligence must be in a form suitable for application when it is received. Provision of useful intelligence requires producers to understand the circumstances under which their products are used.

1.1.27 Readiness

Intelligence structures, databases, and products must be responsive to the existing and contingent requirements of all users' levels. Intelligence assets and resources oriented to areas where there is a high probability of operations must be maintained in a high state of readiness, understand potential adversaries, and be capable of producing and disseminating intelligence usable by all elements.

1.1.28 Completeness

Complete intelligence answers the all questions about the adversary to the fullest degree possible. It also tells what remains unknown. When justified by the available evidence, intelligence must forecast future adversary actions and intentions. For example the answers meet all questions about adversary's intent and capabilities.

1.1.29 Accuracy

To be accurate, intelligence must be objective. It must be free from any political or other restriction and must not be distorted by pressure to conform to the positions held by higher levels of command. Intelligence products must not be shaped to conform to any perceptions of the commander's preferences. While intelligence is a factor in determining policy, policy must not determine intelligence. To the extent possible, intelligence should correctly identify threat intentions, capabilities, limitations, and dispositions. It should be derived from multiple sources and disciplines to minimize the possibility of deception or

misinterpretation. Alternative or contradictory assessments should be presented, when necessary, to ensure balance and bias-free intelligence. [239]

1.1.30 Relevance

For intelligence to be truly relevant, it must also meet the qualitative criteria of being complete, accurate, timely, objective, and usable. Intelligence should be relevant to determining, planning, conducting, and evaluating operations. It must contribute to user's understanding of the adversary and own situation relative to the adversary. Intelligence must be appropriate to the purposes for which it is needed and how it will be applied for the operation.

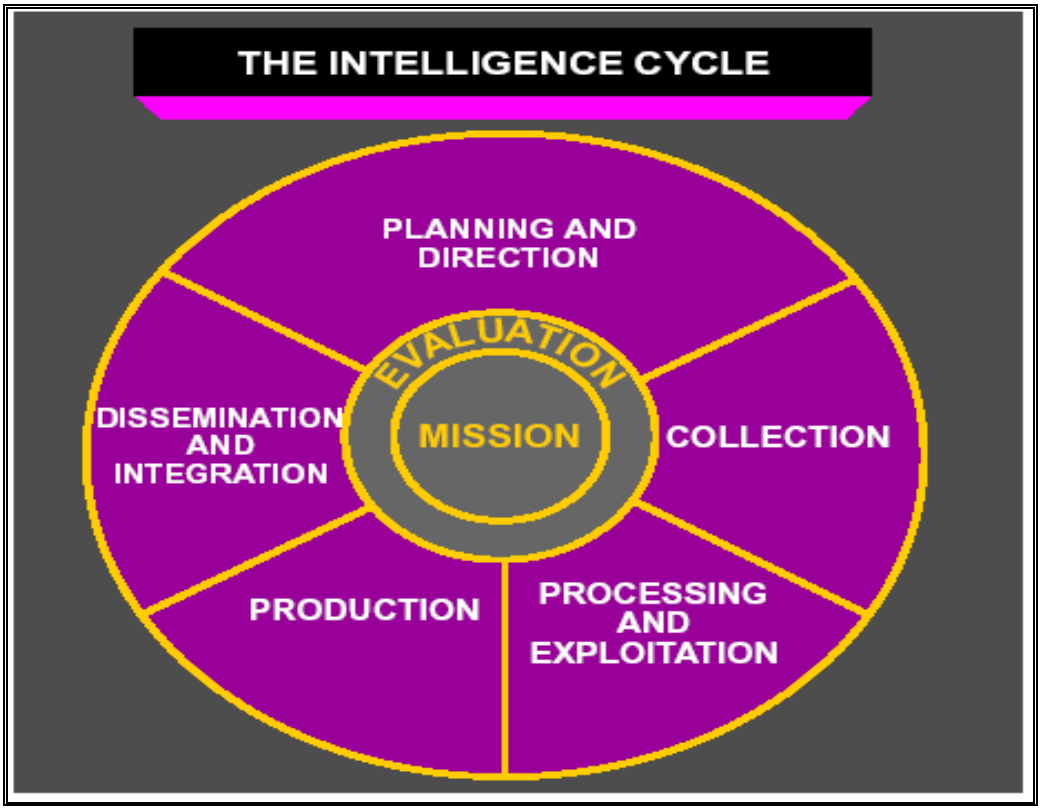
THE INTELLIGENCE CYCLE

Historically, the process of intelligence production has been cyclical. The intelligence cycle is the process through which intelligence is obtained, produced, and made available to users. In describing this cycle, I prefer using a five-step process that is changing between four or five steps. For example in Turkish Army[240] and Canadian Army[241] are using four steps (Planning and Direction, Collection, Processing, Dissemination). But in U.S. Army it is five. [242] Other nations may describe this cycle differently; however, the process is largely the same. The steps by which information are converted into intelligence and are made available to users, in the intelligence cycle are described in figure 5.3 illustrations:

---

[239] FM 34-1 "Intelligence And Electronic Warfare Operations", Headquarters Department of the Army Washington, 27 September 1994 Available on site http://www.fas.org/irp/doddir/dod/index.html
[240] MD 37-1C, "Stratejik İstihbarat Analizi", Silahlı Kuvvetler İstihbarat Okul Komutanlığı, Ankara, 2001, pp. 1-9
[241] Office of the Auditor General of Canada, "The Canadian Intelligence Community", Available on site http://www.oag-bvg.gc.ca/domino/reports.nsf
[242] Joint Staff, "Joint Doctrine for Intelligence Support to Joint Operations", Ibid, p. II-2

Figure 0.3 Intelligence Cycle[243]



So the methodology behind turning raw, single source information into multi-discipline, all-source intelligence is referred to as the Intelligence Cycle.

Shortly the steps of cycle be composed of five steps which are the first step; is the identification of intelligence gaps, the second step; analysts translate these gaps into intelligence requirements, the third step; the strategic debriefed fulfills those requirements, the fourth step; involves preparation of an intelligence report, the fifth and last step; is the preparation of an intelligence report evaluation by the originator of the requirement.[244]

1.1.31 Planning and Direction.

The first step in the cycle, planning and direction, involves the management of the entire intelligence effort, from the identification of a need for data to the final delivery of the

---

[243] Joint Staff, "Joint Doctrine for Intelligence Support to Joint Operations", Ibid, p. II-3
[244] FM 34-52, "Intelligence Interrogation", Headquarters Department of the Army, Washington, 8 May 1987, Available on site http://www.globalsecurity.org/intell/library/policy/army/fm/fm34-52/chapter7.htm

intelligence product to the consumer. The process consists of identifying, prioritizing, and validating intelligence requirements, translating requirements into observable, preparing collection plans, issuing requests for information collection, production, and dissemination, and continuously monitoring the availability of collected data. In this step specific collection capabilities are tasked, based on the type of information required, the susceptibility of the targeted activity to various types of collection activity, and the availability of collection assets.[245]

There are no firm boundaries delineating where each phase of the cycle begins or ends. The intelligence cycle provides a process to understand and order the many activities involved in intelligence and is useful for understanding the interrelationships of the intelligence phases. The intelligence process may not continue through the entire cycle. For example, during the processing and exploitation phase data may be passed directly to the user from an unmanned aerial vehicle (UAV) or other source, instead of being processed or exploited first. [246]

1.1.32 Collection

Collection refers to the gathering of data, through espionage, technical means (photography, interception of electronic communications, and so on), or in any other manner; thus, it comes closest to what is popularly considered intelligence activity. While collection is obviously fundamental to intelligence work, opinions differ regarding the relative importance of the various methods.[247]

Collection includes both acquiring information and provisioning that information to processing and production elements. The collection process encompasses the management of various activities, including developing collection guidelines that ensure optimal use of available intelligence resources. Intelligence collection requirements are developed to meet the needs of potential consumers. Based upon identified intelligence, requirements

---

[245] OPSEC Support Staff, "Operations Security Intelligence Threat Handbook" The Interagency OPSEC Support Staff Publishing, April 1996, Available on site http://www.fas.org/irp/nsa/ioss/threat96/

[246] Joint Pub 2-01, "Joint Intelligence Support to Military Operations", 20 November 1996, pp. III-2, III-45, Available on site www.dtic.mil/doctrine/jel/new_pubs/jp2_01.pdf

[247] Shulsky, A. N., "Silent Warfare: Understanding The World of Intelligence", (2nd edition), Revised by Gary Schimitt, Brassey's Publising, New York, 1993, pp. 1-9

collection activities are given specific taskings to collect information. These taskings are generally unnecessary and may use a number of different intelligence disciplines for collection activities. Tasking redundancy compensates for the potential loss or failure of a collection asset. It ensures that the failure of a collection asset is compensated for by duplicate or different asset capable of answering the collection need. The use of different types of collection systems contributes to redundancy. It also allows the collection of different types of information that can be used to confirm or disprove potential assessments. Collection operations depend on secure, rapid, redundant, and reliable communications to allow for data exchange and to provide opportunities for cross-cueing of assets and tip-off exchanges between assets. Once collected, information is correlated and forwarded for processing and production. [248]

Collection of foreign intelligence relies heavily on technical means. The most of the intelligence budget is for acquisition and operation of technical systems, most of which are related to collection.

1.1.33 Processing

The third step, processing, is the conversion of collected information into a form suitable for the production of intelligence. In this process, incoming information is converted into formats that can be readily used by intelligence analysts in producing intelligence. Processing may include such activities as translation and reduction of intercepted messages into written format to permit detailed analysis and comparison with other information. Other types of processing include video production, photographic processing, and correlation of information collected by technical intelligence platforms.[249]

1.1.34 Production

The fourth step, production, is the process of analyzing, evaluating, interpreting, and integrating raw data and information into finished intelligence products for known or anticipated purposes and applications. The product may be developed from a single source

---

[248] Nelson, H., "The U.S. Intelligence Budget in the 1990s," International Journal of Intelligence and Counterintelligence, Volume 6, 1993, pp. 195-198.
[249] Nelson, H., Ibid, p. 198-201

or from all-source collection and databases. To be effective, intelligence production must focus on the consumer's needs. It should contain the tenets of intelligence.

As part of the production process, the analyst must eliminate information that is unnecessary, erroneous, or inapplicable to the intelligence requirement. As a result of the analytical effort, the analyst may determine that additional collection operations are required to fill in gaps left by previous collection or existing intelligence databases. The final intelligence product must provide the consumer with an understanding of the subject area, and draw analytical conclusions supported by available data. [250] Also applied to as the prediction phase. [251]

To better understand the exact needs of the consumer and the best way of answering the requirements, the producer needs to know who will use the intelligence at what dimensions, the user's mission, the general intelligence requirements and responsibilities, and purpose of the intelligence products. Producers must be objective, unbiased, and avoid any tendency toward preconceived ideas. Users need all available appropriate intelligence, including conflicting or contradicting information and opinion.

Intelligence analysts should use information available from multiple sources, integrate it, and provide the decision maker with a clear picture. Intelligence production should be coordinated from strategic through tactical dimensions. Intelligence produce at higher echelons[252] is derived from both collection assets organic to that echelon or higher and a refinement and compilation of intelligence received from subordinate units and external organizations. Production Guidelines can be seen in figure 5.4.[253]

---

[250] Nelson, H., Ibid, p. 201-205
[251] National Intelligence Course (NIC) Textbook, Joint Military Intelligence Training Center, November 1999
[252] International SIGINT collection effort is known as Echolon.
[253] OPSEC Support Staff, "Operations Security Intelligence Threat Handbook" The Interagency OPSEC Support Staff Publishing, April 1996, Available on site http://www.fas.org/irp/nsa/ioss/threat96/

Figure 0.4 Production Guidelines[254]

In the vast majority of cases, the collected information is fragmentary, ambiguous, and susceptible to widely divergent interpretations. Thus, the process of analyzing the available information to make judgments about the capabilities, intentions, and actions of another party is a vital part of the intelligence process. Even more difficult is the process of forecasting the future capabilities, intentions, and actions of a foreign government or political organization. [255]

1.1.35 Dissemination

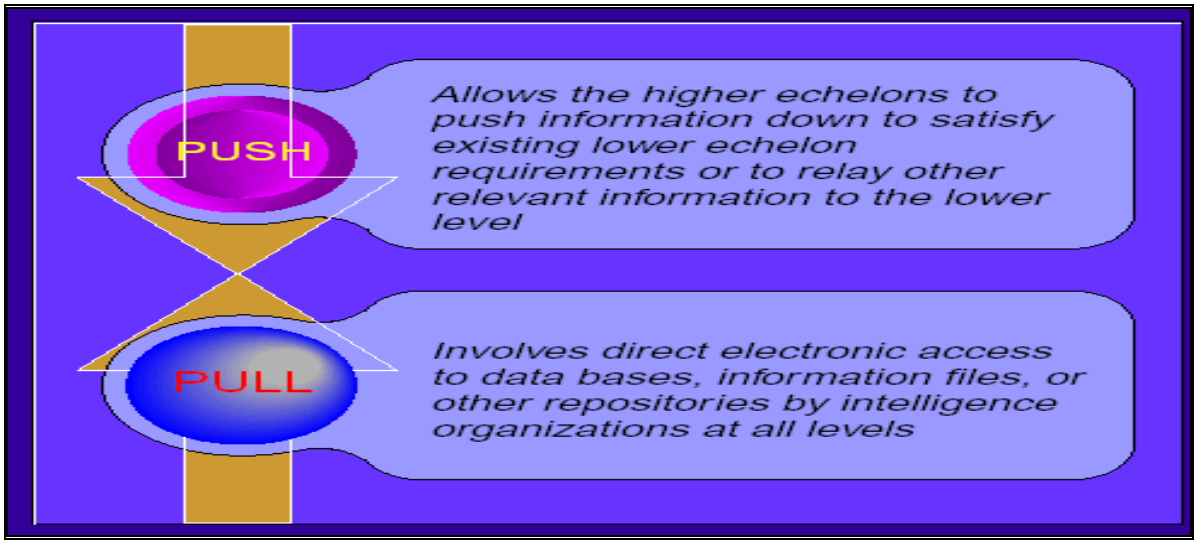
The final step of the intelligence cycle is dissemination. Dissemination is the transfer of intelligence to the consumer in a usable form. Intelligence can be provided to the consumer in a wide range of formats including verbal reports, written reports, imagery products, and intelligence databases. Dissemination can be accomplished through physical exchanges of data and through interconnected data and communications networks.[256]

---

[254] OPSEC Support Staff, "Operations Security Intelligence Threat Handbook", Ibid.
[255] Shulsky, A. N., "Silent Warfare: Understanding The World of Intelligence", (2nd edition), Revised by Gary Schimitt, Brassey's Publising, New York, 1993, pp. 1-9
[256] Joint Staff, "Joint Doctrine for Intelligence Support to Joint Operations", Ibid, p. II-7

Dissemination consists of both "push" and "pull" control principles in figure 4.5. The "push" concept allows the higher echelons to push intelligence down to satisfy existing lower echelon requirements or to relay other relevant information to the lower level.[257]

Figure 0.5 "Push" and "Pull" Control Principles



We should be aware of the intelligence cycle for three reasons. First, this awareness allows us to play a role in the production of intelligence required to support our program. We must be aware of the range of threats that confront our program, or we will not be able to implement countermeasures to deny the adversary access to data that may provide critical information. Knowledge of the intelligence cycle and the various ICs allows us to determine how to access intelligence needed for conduct of the intelligence process.

Second, knowledge of the intelligence cycle allows us to develop protective measures to prevent adversary collection activities. Knowledge of an adversary's collection methods and patterns allows the program manager to develop effective countermeasures that hide or deform indicators.

Finally, knowledge of the adversary's analytical biases can be used to develop deception programs that deceive the adversary by confirming incorrect perceptions.[258]

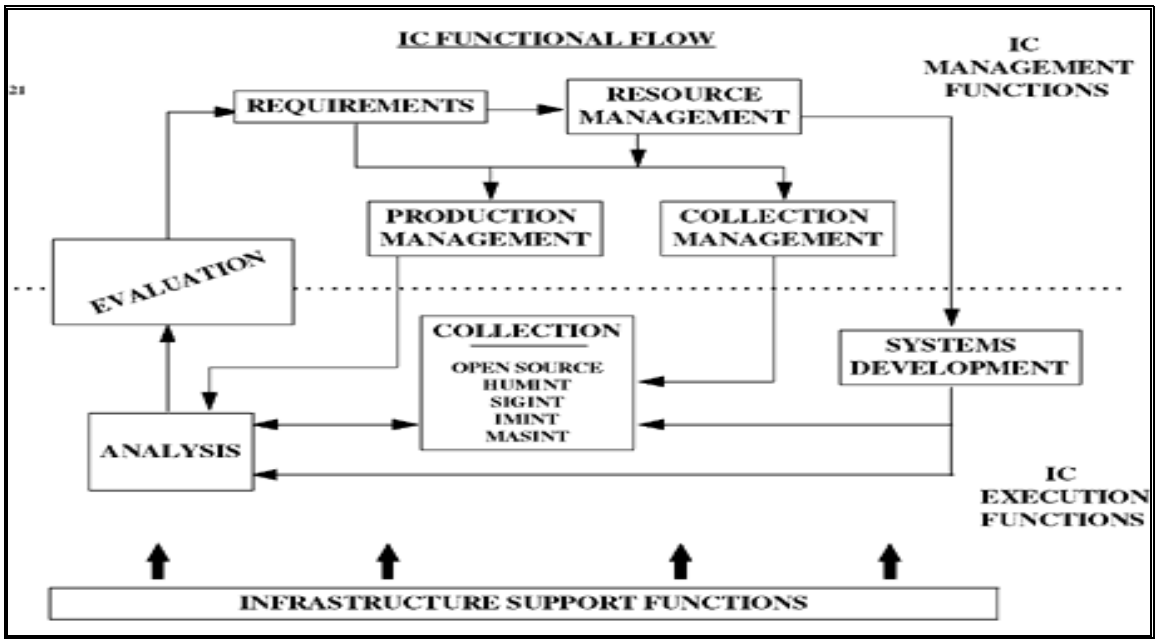
---

[257] Joint Pub 2-01, "Joint Intelligence Support to Military Operations", Ibid, pp. III-2, III-45

The cyclic nature of this process represents continuous review as it moves from one phase to the next. The human being that established the initial requirement in the Direction phase initiates subsequent repetition of this cycle.

Finally, as illustrated in figure 4.6 Intelligence Community functional flow show the some relation of intelligence disciplines which structure shaped after Cold War. Some of them are static but most of them change in the evaluation of world.

Figure 0.6 Intelligence Community Functional Flow[259]



1.1.36 Information And Intelligence

Although I defined briefly main differences between data, information and intelligence in the second chapter, I need the detailed explanation on information and intelligence in the intelligence cycle.

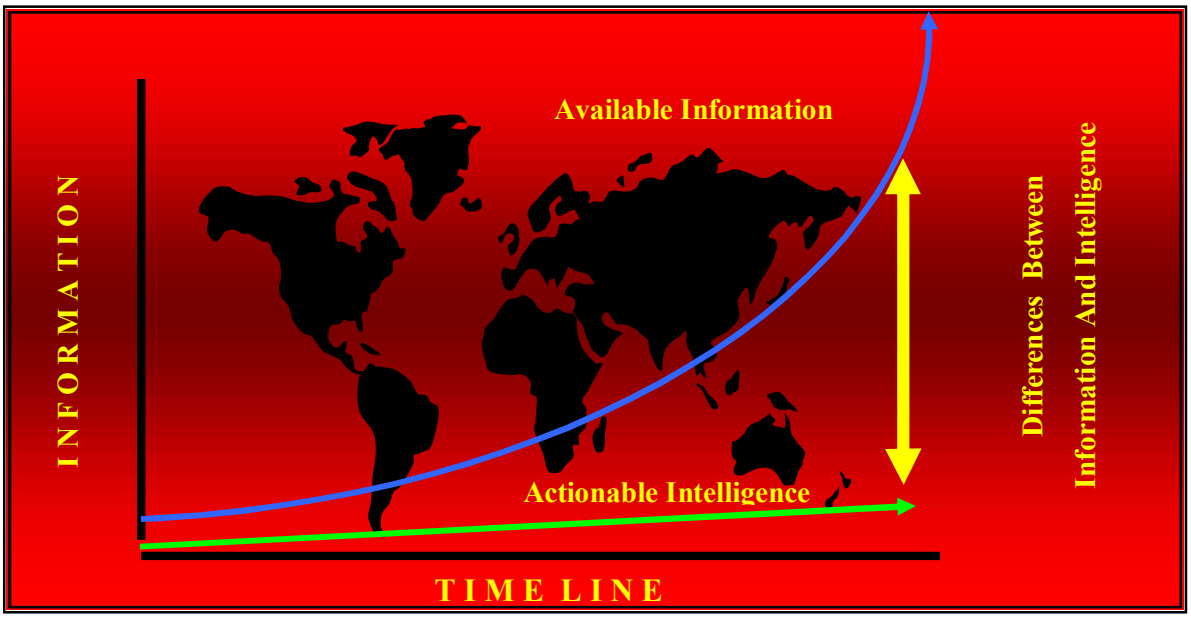
The dimension of time began to be recognized as more important, and conscious efforts were made to reduce the time required to gather information, disseminate it, make a

---

[258] OPSEC Support Staff, "Operations Security Intelligence Threat Handbook" Ibid.
[259] Government Printing Office, "IC21: The Intelligence Community in the 21st Century", Staff Study Permanent Select Committee on Intelligence, House of Representatives One Hundred Fourth Congress, Washington, 1996, Available on site http://www.access.gpo.gov/congress/ house/intel/ic21/ic21_toc.html

decision, and follow it up by action[260]. So time has an important affect on available information and actionable intelligence as illustrated in figure 4.7.

Figure 0.7 Time-Information and Intelligence



And we can explain it in the intelligence cycle. The intelligence cycle is the process by which information is converted into intelligence and made available to users. To better understand intelligence and its cycle, it is important to recognize the clear and critical distinction between information and intelligence. Information is data that have been collected but not further developed through analysis, interpretation, or correlation with other data and intelligence. The application of analysis transforms information into intelligence. Both information and intelligence are important, and both may exist together in some form. They are not, however, the same thing, and thus they have different connotations, applicability, and credibility.

Information and intelligence from all sources, including counterintelligence, must be evaluated, correlated, and integrated into products that present the most complete, accurate, and objective views possible.

Having access to and using all sources of information and intelligence is essential to understanding the actual situation. Single-source intelligence analysis may lead to

[260] Singh, J., "Time: The New Dimension in War", JFQ, Winter 1995–96, p.57, Available on site www.dtic.mil/doctrine/jel/jfq_pubs/1510.pdf

incomplete assessments. Use of the all-source concept and methodology will reduce the risks of deception. It will also become the basis for the nomination and development of countermeasures against hostile intelligence and operations. All-source intelligence fusion must begin with collection and production planning. Each source can provide useful information and cues for collection and exploitation through other sources.[261]

1.1.37 Leaders Role In The Intelligence Cycle

Leaders have a dual role in the Intelligence Cycle. First, as initiators of the cycle, they have a responsibility to provide precise direction to focus available resources. Second, as consumers of the intelligence, they have a responsibility to provide feedback to the producers and force a re-assessment.

If decision-makers do not get actively involved in providing well-defined, clear direction, the intelligence process is unlikely to produce the undesired results. Since, by definition, leaders are part of the Intelligence Cycle, their lack of involvement should be considered an intelligence failure. At the very least such negligence should be considered a leadership failure.

Failures also occur when the leader is a consumer. If a consumer is not willing to accept the message being passed, the unrealistic intelligence available will not prevent failure.

The receptivity of policy-makers to intelligence varies inversely with their prior commitment to a given policy or course of action. The lower the receptivity is the greater the risk of failure and surprise. The more ingrained in time the policy commitment is, the more and better information is required to change the commitment.[262]

It would be inappropriate not to recognize that culpability for this situation does not lie solely on the management. It would be equally inappropriate and counter-productive to entirely blame management for the greater failures of the intelligence process. The salient observation is that both producers and consumers of intelligence often share the blame for

---

[261] Joint Chiefs Of Staff, "Joint Doctrine Encyclopedia", U.S. Army Publishing, 16 July 1997, p.328, Available on site www.fas.org/man/dod-101/dod/

[262] Poteat, G.H. "The Intelligence Gap: Hypotheses on the Process of Surprise," International Studies Notes, No. 3, 1976, p. 17, Available on site www.ndu.edu/library/ic6/96-E-14.pdf

failure. Thus, solutions that include education and accountability are more appropriate to human failings than organizational disruption. It would be appropriate at this point to define a failure.

A failure is most easily defined as a lack of success. What is not so easy is reaching a consensus as to whether a particular incident was a success or not. Mission success criteria are generally not available to assist in the evaluation. Even on those occasions when such criteria is available, grading and measuring the action against the criteria are often just as subjective as the original judgment.[263] The other often refers to what might be called a military operational success by one side as an intelligence failure.

Intelligence will never be as effective as we might wish, nor can all surprise be eliminated. Nor should we be willing to accept or overlook poor performances, avoidable errors, or repeated shortcomings. But it is the very acceptance of the real limits of intelligence that would give both producers and consumers more confidence and put the concept of intelligence failure into its proper perspective.

In other words, if leaders recognize that they play a key role in the Intelligence Cycle, and accept the inherent risks involved with humans doing analysis, perception of failure can diminish. However, given the fallibility of human beings and the requirement for man to be involved in the process of turning information into intelligence, intelligence failures will continue to occur. As fatalistic as that this assessment is, all is not lost. Strong, fully engaged human leadership offers the only possible solution to protect against the coming intelligence failure.

INTELLIGENCE COLLECTION DISCIPLINES

Despite extraordinary changes in the world geopolitical environment in recent years, many nations and non-governmental organizations are actively engaged in intelligence operations against the others. Most of the intelligence operations range from classic human intelligence operations to technical intelligence collection capabilities. Intelligence

---

[263] Lowenthal, M.M., "The Burdensome Concept of Failure," in Maurer, A.C,et. al., (eds.), "Intelligence Policy and Process", Westview Press, Boulder, 1985, p 51,

collection activities range from the traditional political and military collection activities to the collection of economic and proprietary data. The intelligence organizations involved in collection activities use a wide range of collection capabilities to obtain information on targeted activities in adversary states. Intelligence operations can be categorized in terms of the collection discipline or sources used. [264]

Intelligence sources are the means or systems used to observe, sense, and record or convey information of conditions, situations, and events. As illustrated Intelligence sources in the figure 5.2, there are seven primary source types: imagery intelligence, signals intelligence, human intelligence, measurement and signature intelligence, open-source intelligence, technical intelligence, and counterintelligence.[265]

[264] OPSEC Support Staff, "Operations Security Intelligence Threat Handbook", Ibid.
[265] Joint Chiefs Of Staff, "Joint Doctrine Encyclopedia", Ibid, p.342

Figure 0.8 Intelligence Sources

1.1.38 Human Intelligence (HUMINT)

HUMINT is the oldest of the intelligence disciplines. Although HUMINT can be a sole collection discipline, it is normally employed to confirm, refute, or increase intelligence derived through other disciplines. [266] The examples of HUMINT can find in the corridor of history trough 500 BC as I explain in chapter 3. HUMINT is the intelligence collection discipline where humans are both the collector and the collection platform. This non-technical intelligence collection discipline declined during the 1970s following several scandals related to HUMINT.

[266] FM 34-1 "Intelligence And Electronic Warfare Operations", ibid.

Human intelligence is derived from human sources.[267] To the public, HUMINT remains synonymous with espionage and clandestine activities, yet, in reality, most HUMINT collection is performed by overt collectors such as diplomats and military attaches. HUMINT is the oldest method for collecting information about a foreign power. Until the technical revolution of the mid to late twentieth century, HUMINT was the primary source of intelligence for all governments. HUMINT includes overt, sensitive, and clandestine activities and the individuals who exploit, control, supervise, or support these sources.

There are two main methods of HUMINT collection: overt and clandestine. Overt collection is obtained through personal observation, from knowledgeable human sources or openly available media. These activities are conducted openly. Some overt collection may be sensitive when compromise of the information or source could embarrass the collector. The resulting information obtained through overt means might then be classified. Disclosure of the sponsor's identity may result in political embarrassment, compromise of other intelligence operations, or security threats to the sponsoring nation.[268]

The opposite of overt collection is clandestine collection (not to be confused with covert action). Clandestine collection requires increased security to insure plausible deniability. Some typical examples of clandestine efforts involve the use of false identities, adopting the appearance of commercial activity, etc. In clandestine collection, the activity is unseen by design. Also Clandestine HUMINT sources include agents who have been recruited or have volunteered to provided information to a foreign nation, and foreign nationals who successfully infiltrate an organization with a cover story.[269]

Human intelligence gathering is performed either by interviewing a subject with knowledge of the target area, via the "tailing" of a subject of investigation, or by using a combination of "black" techniques to gain confessions or involuntary disclosure of information. For example, the KGB considered (in the cold war days) the following as standard practice and even have defined the "MICE" acronym to help Soviet agents

---

[267] Interagency OPSEC Support Staff, “Compendium of OPSEC Terms”, Ibid.
[268] Department of the Air Force, “Target Intelligence Handbook: Unclassified Targeting Principles”, 200-18, Washington, October 1, 1990
[269] Wood, S., ed al., “American Espionage, 1945-1989”, Defense Personnel Security Research and Education Center, Monterey, 1990, pp.46-49

remember the "tricks of the trade": (M) Money...buy the agent; (I) Ideology...turn dislike of his own country's system, or use a passion for socialism or communism; (C) Compromise...trick the target into a compromising situation or use the person's past as a means of blackmail; (E) Ego...appeal to the target who feels they deserve better treatment than they are getting, and/or make them feel more important in their own eyes. [270]

Even with the explosion of technical capabilities, HUMINT can still provide information that even the most proficient technical collectors cannot, such as access to internal memoranda and to compartmented information. Most importantly, human collectors can provide key insights into the intentions of an adversary, whereas technical collection systems are often limited to determining capabilities.[271] HUMINT can be used to reveal adversary plans and intentions, or uncover scientific and weapons developments before they are used or are detected by technical collection systems. HUMINT can also provide documentary evidence such as drafts of facilities, copies of adversary plans, or copies of diplomatic or policy documents. Finally, HUMINT is extremely cost effective compared with technical collection systems and does not require a significant technological production base for support.

1.1.39 Signals Intelligence (SIGINT)

SIGINT is intelligence derived from the intercept and exploitation of foreign electromagnetic emissions. SIGINT results from collecting, locating, processing, analyzing, and reporting intercepted communications and noncommunications (for example, radar's) emitters. [272]

David Kahn[273] describes how a scripture writer carving hieroglyphics on a tomb wall over 4000 years ago, unintentionally gave birth to the science of Cryptology. Cryptology began with the study of secret writing and now includes both cryptography and cryptanalysis.[274]

---

[270] Richelson, J. T., "The US Intelligence Community", Ballinger Publishing Company, Cambridge, 1985, pp. 1-3
[271] Richelson, J. T., Ibid, pp.3-5
[272] FM 34-1 "Intelligence And Electronic Warfare Operations", Ibid.
[273] Kahn, D., "The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet", Simon & Schuster Inc, 1997, pp.3-5
[274] Conversion of code into plain text by a person who does not have the key or system.

By the invention of telegraph, making it inevitable that intelligence would eventually intrude into the world of electronic communications. And by the invention of wireless telegraphy and radio, SIGINT was born. Most famous SIGINT is known as Zimmermann telegram that caused U.S. participation in WWI and defeat of Germany. This is one of many examples how communications intelligence was used with powerful consequences. Many times communications triumphs result from the communications failures of an adversary.

Signals intelligence collection can be performed from a variety of platforms. Examples include overt ground collection sites, such as the Russian facility at Lourdes, Cuba; ships and aircraft; and covert locations inside the states. SIGINT facilities can monitor transmissions from communications satellites, as well as terrestrial facilities. [275] Signal intercepts comprising, individually or in combination, all communications intelligence (COMINT), Foreign Instrumentation Signals Intelligence (FISINT) and electronic intelligence (ELINT).[276]

1.1.39.1 Communications Intelligence (COMINT)

COMINT, one of the primary SIGINT disciplines, includes information derived from intercepted communications transmissions. COMINT targets voice and teleprinter traffic, video, Morse code traffic, or even facsimile messages. Assuming access is possible, COMINT can be collected from the airwaves, cable, fiber optics, or any other transmission medium. Usually the most desired type of traffic is clandestine or private. But clearly there is a role in monitoring and analyzing traffic sent in the "clear" as military protocol does sometime fail and information of incredible worth is sometimes sent without the usual coding.[277]

1.1.39.2 Electronic Intelligence (ELINT)

ELINT is the collection of electronics intelligence, typically the collection of the target's electronic countermeasures capabilities, including such things as jamming capability,

---

[275] Rosenau, W.,"A Deafening Silence: U.S. Policy and the SIGINT Facility at Lourdes," Intelligence and National Security Publishing, October 1994, pp. 723-734.
[276] Intelligence Community Staff, “Glossary of Intelligence Terms and Definitions”, ICS, Washington, June 1989, pp.128-129
[277] Richelson, J. T.,“The US Intelligence Community”, Ibid, pp. 4-5

electronic deception capability, and other electronic emanations. ELINT overlaps the areas of RADINT (Radar Intelligence), COMINT (Communications Intelligence), and TELINT (Telemetry Intelligence...i.e. intercepts of space vehicle telemetry during launch, in orbit, or during terminal stages) since these areas are also concerned primarily with electronic emissions. ELINT can be gathered by means of airborne platforms, ships on or below the sea, and in rising numbers via satellites.[278] Also ELINT is used to identify the location of an emitter, determine its characteristics, and infer the characteristics of supported systems.

1.1.39.3 Foreign Instrumentation Signals Intelligence (FISINT)

FISINT consists of intercepts of telemetry from an opponent's weapons systems as they are being tested. Telemetry units provide designers with information on a prototype's guidance system operation, fuel usage, staging, and other parameters vital for understanding operational characteristics. These data enable the designer to evaluate the performance of the prototype. However, if intercepted, they also provide an adversary with the ability to estimate the capability of the prototype. [279]

1.1.40 Imagery Intelligence (IMINT)

Imagery includes representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media. Imagery can be derived from visual photography, radar sensors, infrared sensors, lasers, and electro-optics. IMINT includes the exploitation of data to detect, classify, and identify objects or organizations. It can be produced from either hard or soft copy (digital) imagery. Hard copy imagery is synonymous with film, while soft copy imagery is displayed on electronic terminals. Both types of imagery sources can be analyzed and interpreted for various purposes by different users. IMINT is the product of imagery analysis. [280]

---

[278] Richelson, J. T., Ibid, p.5
[279] Federal Standart 1037 C,"The Glossary of Telecommunication", 1996, Available on site http://www.its.bldrdoc.gov/fs-1037/dir-033/_4879.htm
[280] FM 34-1 "Intelligence And Electronic Warfare Operations", Ibid.

Historical background of IMINT goes before the WW I. But the effective use of imagery interpretation is demonstrated during WW II, Korea, and the Cuban missile crisis. In WW II, almost eighty percent of intelligence is derived from aerial photography.[281] Improvements go until today.

The proliferation of space-based imagery systems permits a much greater use of imagery products by nations that previously did not have access to them. An additional factor that must be considered is the growing availability of sophisticated imagery workstations, and analytical tools. These capabilities will allow adversaries to conduct in-depth analysis for targeting and technical intelligence gathering.[282]

The 1992 Open Skies Treaty also poses an imagery collection threat. Using the imagery derived from Open Skies flights analysts will be able to identify particular types of equipment by type and capability, and perform detailed analyses of rail, port, industrial, and military facilities.[283]

Finally, imagery intelligence collection usually requires a technologically oriented infrastructure. While this requirement may be reduced to some extent in the future, effective use of imagery will still require well-educated, technically competent analysts.

1.1.41 Measurement and Signature Intelligence (MASINT)

"Measurements" (in MASINT) refers to the data collected in order to obtain precise parameters, such as height, weight, distance, depth, etc. MASINT techniques can derive parameters that are not directly measurable by the sensor.

MASINT is scientific and technical intelligence information obtained by quantitative and qualitative analysis of data derived from specific technical sensors for the purpose of identifying any distinctive characteristics associated with the source emitter or sender. This information is then used to facilitate the subsequent identification or measurement of the same type of equipment. The term measurement refers primarily to the data collected for

---

[281] FM 34-1, Ibid.
[282] Sibbet, D.B., "Commercial Remote-Sensing," American Intelligence Journal, Spring/Summer 1993, p. 37
[283] On-Site Inspection Agency, "Fact Sheet: The Open Skies Treaty," May 1993, U.S. Arms Control and Disarmament Agency, Treaty on Open Skies (Official Text), April 10, 1992 Available on site http://www.usinfo.state.gov/topical/pol/arms/02081499.htm

the purpose of obtaining finite metric parameters. The term signature refers primarily to data indicating the distinctive characteristics of phenomena, equipment, or objects as the collection instruments sense them. The signature is used to recognize the phenomenon, equipment, or object when its distinctive characteristics are detected. [284]

As future adversaries develop new technologies to avoid some of the SIGINT and IMINT collection systems, MASINT will be used as another means of sensing the enemy.[285]

Two important distinctions between MASINT and other intelligence systems are the maturity and diversity of the component systems. MASINT technologies are both immature and diverse. The R&D support emphasis that has characterized past MASINT collection and processing is shifting with the fielding of modern weapons systems. Few MASINT systems fielded prior to 1991 used embedded libraries, signatures or templates to perform autonomous detection, classification, tracking or engagement functions. This has changed markedly over the past years, with the fielding of new aviation and fire support weapons. Numerous MASINT-based systems are used in roles as varied as intruder detection, strategic missile launch warning, and nuclear weapons test monitoring.[286] Today's we are witnessing best example of MASINT in Iraq. MASINT includes some subdiciplines.

1.1.42 Acoustic Intelligence (ACOUSTINT)

ACOUSINT is the collection of acoustical information underwater such as sonar "signatures" or sound signatures. One example of the gathering technique and implementation is the SOSUS line, which is a long line of hydrophones, laid under the Bering Straight. The mission of this sensor line is to note the passing of Soviet ships leaving their waters through the Straight. For instance, a massive movement of submarines across the line would indicate a possible move to wartime footing. The data from the

---

[284] "MASINT" Available on site http://www.fas.org/irp/program/masint.htm
[285] FM 34-1, "Intelligence And Electronic Warfare Operations", Ibid.
[286] FM 34-1, "Intelligence And Electronic Warfare Operations", Ibid.

SOSUS network is used to identify a number of submarines by their unique acoustical signature. Thus a nation's Navy is able to track individual submarines.[287]

1.1.42.1 Electro-optical Intelligence (ELECTRO-OPTINT)

Electro-optical intelligence is the collection, processing, exploitation, and analysis of emitted or reflected energy across the optical portion (ultraviolet, visible, near infrared, and infrared) of the electromagnetic spectrum. Electro-optical intelligence may provide detailed information on the radiant intensities, dynamic motion, spectral and spatial characteristics, and the materials composition of targeted objectives. Electro-optical data collection provides broad applications to variety military, civil, economic, and environmental issues. [288]

1.1.42.2 Laser Intelligence (LASINT)

LASINT is a fairly new category in TECHINT, dealing with the collection of information on the target's laser capability. This may include such items as laser designators (used to guide "smart" weapons onto target via illumination with an infrared laser), laser weapons (ala the Strategic Defense Initiative), or anti-laser capabilities (as in rejection or absorption of laser light to prevent successful laser designation). As this is a recent "INT", there are few details, with much of the activity still remaining classified. LASINT can, of course, be gathered by space-borne or airborne reconnaissance and surveillance platforms.[289]

1.1.42.3 Nuclear Intelligence (NUCINT)

Nuclear Radiation Intelligence is information derived from the nuclear radiation and physical phenomena associated with nuclear weapons, processes, materials, devices, or facilities. Nuclear, monitoring includes nuclear radiation detection, identification, and characterization of sources and events. Data exploitation results in nuclear signature of weapons or materials.[290]

---

[287] Richelson, J. T., Ibid, p. 4
[288] U.S. Military WEB Page, “Glossary of Military Terms”, Available on site http://usmilitary.about.com/ library/glossary/i/ bldef03160.htm
[289] Richelson, J. T., Ibid, p. 5
[290] U.S. Military WEB Page, “Glossary of Military Terms”, Ibid.

Today US insist on Nuclear Weapons that were gathered by Iraq while inspectors didn't find any sign of these weapons. What is the meaning of this? US detected them by using of NUCINT or didn't detect. Probably we will learn in few days but I suggest US detected them.

1.1.42.4 Unintentional Radiation Intelligence (RINT)

Unintentional Radiation Intelligence (RINT) is the integration and specialized application of multiple MASINT collection, processing, and exploitation subdisciplines and techniques against unintentional radiation sources that are incidental to the design propagation and operating characteristics of military and civil propulsion units, power sources, weapons systems, electronic systems, machinery, equipment, or instruments. These techniques may be valuable in detecting, tracking, and monitoring a variety of activities of interest.[291]

1.1.43 Open Source Intelligence (OSINT)

Information of potential intelligence value available to the general public such as papers, books, periodicals, and other printed information. It also includes information derived from radio and television transmissions, press agencies, publications, maps, and photography. [292] But OSINT is not a collection of news clippings, and is not the Internet, and also is not a substitute for spies or satellites or other sensitive collection capabilities.

OSINT is often the only intelligence available during routine times and as the necessary first body of knowledge when the national intelligence communities and policy makers are shifting toward the increased coverage required by crises. OSINT is widely acknowledged as an essential element on: "Tip-off" for regarding intentions, new weapons systems, and emerging crises, "Context" for the expertise and historical knowledge to assess a situation rapidly (can be tapped on a "just enough, just in time" basis), "Collection Management" for the focus of classified capabilities on the hard stuff, "Cover" for to protect sources and methods.[293]

---

[291] U.S. Military WEB Page, "Glossary of Military Terms", Ibid.
[292] National Intelligence Course (NIC) Textbook, Ibid, Chapter 10, p.9
[293] Defense Daily Network Report, "Open Source Intelligence: Private Sector Capabilities to Support DoD Policy, Acquisitions, and Operations," 5 May 1998, Available on site http://www.fas.org/irp/eprint /oss980501.htm

Open source intelligence involves the use of materials available to the public by intelligence agencies and other adversaries. Some analysts have estimated that the Soviet Union derived up to 90 percent of its intelligence from open source information. With the proliferation of electronic databases, it has become easier to collate large quantities of data, and structure information to meet the needs of the adversary collector. Open source information can often provide extremely valuable information concerning an organization's activities and capabilities. Frequently, open source material can provide information on organizational dynamics, technical processes, and research activities not available in any other form. When open source data is collected, it is often possible to derive classified data or trade secrets.

Open source intelligence collection does have limitations. Often articles in military or scientific journals represent a theoretical or desired capability rather than an actual capability. Censorship may also limit the publication of key data needed to arrive at a full understanding of an adversary's actions, or the press may be used as part of a conscious deception effort.

Open Source Intelligence results from the analysis of Open Source Information, and the comparison of it with other sources. OSINT is not new but since the advent of the Internet has been recognized as a growing source in support of all-source intelligence.

Open sources may rapidly orient both analyst and consumer, and are useful to increase an awareness of possible collection requirements, but they do not substitute for the other intelligence disciplines. Analysts must never rely exclusively on open sources, because many are motivated by a variety of agendas unrelated to accurate, objective reporting. Conclusions based upon the exclusive use of open sources that report persuasive, but misleading or slanted information can be profoundly embarrassing to a professional intelligence analyst. An equally dangerous result may occur by relying upon a narrow range of both open and classified sources that can mislead the analyst into accepting a narrow interpretation of events.

There are different views regarding the importance to which intelligence agencies should give to open source information. According to George Tenet recognition, “In every possible case, we will provide intelligence at the lowest permissible level of classification,

including 'sensitive, but unclassified.'" Pointedly, he did not include open source information. [294]

There has been a longstanding discussion of the role of intelligence agencies in collecting and analyzing OSINT. Some observers argue that the Intelligence Communities should devote more resources to exploiting information that is available publicly, collecting materials that do not circulate widely, and assigning a significant analytical effort to monitoring OSINT. Others argue that the fundamental responsibility of intelligence agencies is secret information and that an extensive OSINT effort would detract from that assignment.

Finally, open source information is generally timelier and may be the only information available in the early stages of a crisis or emergency.

1.1.44 Technical Intelligence (TECHINT)

TECHINT is the end product of a complex process. It is the result of collecting, analyzing, and processing information on foreign technological developments. It is also the result of studying the performance of foreign materiel and its operational capabilities.

Intelligence agencies focus on the TECHINT requirements of strategic policy and the decision makers. TECHINT is a multidiscipline function and its products support consumers and users during the preparation stage by either identifying or countering adversaries' momentary technological advantage, or by maintaining a friendly technological advantage.

Historical background of TECHNIT arrives in the 1920's Germany. By the WW II developments in TECHNIT especially advances of Germany, triggered the other nations to give importance on TECHNIT.

The lessons learned from World War II, the Korean War, and finally the Vietnam War clearly indicated the need for a fully TECHINT system even in peacetime. To do otherwise

---

[294] Best, R.A., "Homeland Security: Intelligence Support", CRS Report for Congress, August 7, 2002, p. 6, Available on site http://www.usembassy.at/en/download/ pdf/homelandsec_intell.pdf

was to invite a technological surprise that would give the enemy an unacceptable advantage. By the way Cold War period passed with TECHNIT struggle.

For point out the importance of TECHNIT when a glance at Pentagon reports "… notes a sudden increase in the number of foreign attempts to obtain US military technology. Companies and governments from a total of 63 nations, many of them allies, have been detected spying on US defense contractors. Targets include information technology, sensors, lasers, aerospace systems, weapons, energetic materials, and electronics. Components and subsystems are a specific target, indicating that the espionage is aimed at upgrading existing weapons and equipment..."[295]

The TECHINT system we have today especially after September 11 the advances in Internet and cryptography (secret codes) technology need the security agencies to hire many of the new generation of computer programmers. For security agencies it is difficult to keep on top of computer and crypto technologies available to terrorists.

1.1.45 Counterintelligence (CI)

If there is intelligence, it is obviously that there will be counterintelligence. The proper scope and nature of counterintelligence is less well defined and more controversial than the other intelligence elements. In its most general sense, counterintelligence refers to the protection of a society and particularly its own intelligence capability from the actions of hostile intelligence services. In the first place, counterintelligence means; information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, persons, or terrorist activities. [296]

This protection is accomplished by programs of *security* actions which is taken to keep information away from those not authorized to have it; and by counterespionage actions which is taken to apprehend or otherwise neutralize foreign agents to prevent them from

---

[295] Cole, S. V., "How To Make War", Available On Site http://www.strategypage.com/search.asp?target=d:\inetpub\strategypageroot\fyeo\howtomakewar\docs\archives\htint01.htm

[296] Department of Energy, "Acquisition Regulation, Classification, Security and Counterintelligence", Rules and Regulations, Vol. 62, No. 192, 1997, Available on site http://www.fas.org/sgp/othergov/doecont.html

acquiring and communicating secret information. In addition, a society could attack its adversary's intelligence analysis as well as its collection capability; this is done using deception operations that provide false or deliberately misleading information to the adversary to induce him to reach an incorrect analysis.

However, protecting a society or oneself against an adversary's intelligence capability, understood broadly, would require other activities as well. It may be necessary to take steps to ensure that you are not deceived by misleading information deliberately provided by the other party. Thus, counterintelligence must safeguard the integrity of the collection and analytic functions. You would also want to know about a foreign government's covert action aimed at influencing your society and government. Ultimately then, the breadth of counterintelligence activities is determined by the threat an adversary or competitor's intelligence activities pose. All these activities can be called in one word, this is, counterintelligence.[297]

By its nature, CI is a multidiscipline (counter-HUMINT, counter-IMINT, and counter-SIGINT) function designed to defeat or degrade threat intelligence and targeting capabilities.[298]

Olson describe Ten Commandments of counterintelligence, as "Be Offensive, Honor Your Professionals, Own the Street, Know Your History, Do Not Ignore Analysis, Do Not Be Parochial, Train Your People, Do Not Be Shoved Aside, Do Not Stay Too Long, Never Give Up." [299]

ALL-SOURCE INTELLIGENCE

Each discipline has its own unique characteristics, capabilities and limitations. It is extremely important to avoid the traps of depending on a single source for either reporting observations or drawing conclusions. Instead, use an all-source approach that will provide a greater probability of accuracy and a better awareness of uncover events.

---

[297] Intelligence WEB Page "Counterintelligence" Available on site http://www.angelfire.com/ca7/Security/INTELLIGENCE.html
[298] FM 34-1 "Intelligence And Electronic Warfare Operations", Ibid.
[299] Olson, J.M., "A Never-Ending Necessity: The Ten Commandments of Counterintelligence", Studies in Intelligence, Fall-Winter 2001, No. 11, Available on site http://www.cia.gov/csi/studies/fall_winter_2001/

Intelligence products and/or organizations and activities that incorporate all sources of information, which include, most frequently, HUMINT, IMINT, MASINT, SIGINT, and open source data. In intelligence collection, a phrase that indicates that in the satisfaction of intelligence requirements, all collection, processing, exploitation, and reporting systems and resources are identified for possible use and those most capable are tasked.[300]

The culmination of the intelligence cycle is the development of all source intelligence. The intention of this type of effort is to develop reinforcing information and to use multiple sources to corroborate key data points. The advantage of an all source approach is that each of the intelligence disciplines is suited to collecting a particular type of data, which allows the intelligence organization to examine all facets of an intelligence target, and gain a better understanding of its operation. Fortunately, only a few nations have the ability to mount such efforts.

Information and intelligence from all sources, including counterintelligence, must be evaluated, correlated, and integrated into products that present the most complete, accurate, and objective views possible. Having access to and using all sources of information and intelligence is essential to understanding the actual situation. Single-source intelligence analysis may lead to incomplete assessments. Use of the all-source concept and methodology will reduce the risks of deception. It will also become the basis for the nomination and development of countermeasures against hostile intelligence and operations.[301]

All-source intelligence fusion must begin with collection and production planning. Each source can provide useful information and cues for collection and exploitation through other sources.

The architecture provides access to data from national, theater and tactical intelligence organizations and sources primarily from a “push-pull” system, which figure, located in dissemination section. A “pull” concept will result in receiving only high-quality, relevant intelligence based on their mission and phase of the operation. The “pull” capability is

---

[300] U.S. Military WEB Page, “Glossary of Military Terms”, Ibid.
[301] Joint Chiefs Of Staff, “Joint Doctrine Encyclopedia”, Ibid, p.30

designed to prevent communications circuit saturation. In addition, time-sensitive intelligence will be “pushed” to consumers and components via dedicated broadcasts in response to preplanned essential elements of information.[302]

COVERT ACTION

Covert action is only one of the tools of foreign policy and so one of the usages of intelligence agencies. In certain conditions it may be decisive.

It is not an option to be chosen lightly but in the absence of such an option a global power may be doomed to impotence. Most people, albeit reluctantly, have reached the conclusion that a covert action capacity should exist as long as international politics remains what it pretty much always has been. There is yet another argument against covert action.[303]

Conceptually, covert action differs from the other elements of intelligence in that, while the others are concerned with seeking and safeguarding knowledge, covert action seeks to influence political events directly. In terms of intensity, covert action can range from persuasion or propaganda to paramilitary action; it has been described as "an activity midway between diplomacy and war."[304]

While the techniques for exerting this influence are many, they have the common characteristic of anonymity, that is to say, the role of the government conducting the activity is not readily apparent or publicly acknowledged. For this reason, an intelligence agency's ability to act secretly often brings it the assignment of carrying out covert action as well. But because it involves implementing policy rather than informing policymakers, there have been occasional suggestions in many states that covert action not be a function of the same intelligence agencies that collects and analyzes intelligence. On the other hand, both the United States and Great Britain have discovered through experience that having two organizations involved in running clandestine operations (one for espionage

---

[302] Joint Chiefs Of Staff, “Joint Doctrine Encyclopedia”, Ibid, p.31
[303] Laqueur, W., “The Future of Intelligence” Society, Jan/Feb 1998, Vol. 35, Issue 2, p. 301
[304] Shulsky, A. N., “Silent Warfare: Understanding The World of Intelligence”, (2nd edition), Revised by Gary Schimitt, Brassey’s Publising, New York, 1993, pp. 1-9

and the other for covert action) can result in energy-sapping rivalries, duplication of effort, or mutual interference.[305]

FINISHED INTELLIGENCE

The Intelligence Communities provides many different kinds of finished intelligence analysis in formats driven by the needs of its varied consumers. According to the CIA's website, "analysis may be delivered as written reports, oral briefings, or other forms tailored to the needs of the intelligence consumer, including maps, charts, photographs, or models."[306] The written products remain the primary vehicles for finished intelligence, however, and according to a CIA publication are organized into four categories: Current Intelligence, Research Intelligence, Estimative Intelligence, Warning Intelligence.[307]

1.1.46 Current Intelligence

The current intelligence oversight system arose from a view that intelligence had to be handled in a manner that was extraordinary when compared to other functions of government.

Current Intelligence; "addresses day-to-day events, seeking to apprise consumers of new developments and related background, to assess their significance, to warn of their near-term consequences, and to signal potentially dangerous situations in the near future."[308]

1.1.47 Research Intelligence

Research Intelligence; is more in-depth than current intelligence and can be used to support specific operations or decisions, or address a new development in greater detail. Research intelligence can also provide a "structured compilation of geographic, demographic, social, military, and political data on foreign countries," known as "basic intelligence."[309]

---

[305] Shulsky, A. N., Ibid, pp.1-9
[306] CIA, "Analytical Products of the DI", Available on site http://www.odci.gov/cia/di/work/major.html
[307] Central Intelligence Agency,"A Consumer's Guide to Intelligence", September 1993, (Undated) October 29, 1997, p. 4 Available on site http://www.odci.gov/cia/publications.htm
[308] Central Intelligence Agency,"A Consumer's Guide to Intelligence", Ibid, p. 26
[309] Central Intelligence Agency,"A Consumer's Guide to Intelligence", Ibid, p. 26

1.1.48 Estimative Intelligence

Estimative Intelligence; "deals with what might be or what might happen. … (It) starts with the available facts, but then it migrate into the unknown, even the unknowable. The main roles of estimative intelligence are to help policymakers navigate the gaps between available facts by suggesting alternative patterns into which those facts might fit and to provide informed assessments of the range and likelihood of possible outcomes." Estimative intelligence can appear in current intelligence or research intelligence, but is highlighted in National Intelligence Estimates (NIEs).[310]

1.1.49 Warning Intelligence

Warning Intelligence; is a subset of estimative intelligence focusing on "developments that could have sudden and deleterious effects in US security or policy" such as "impending crises" or "long-term dangers. Warning intelligence can be provided through regular current and research intelligence and a number of IC "products specifically devoted to warning."[311]

COMPONENTS OF STRATEGIC INTELLIGENCE

To put intelligence in form and write about types, components, and disciplines is not easy. Because depending to your approach it change numerically and conceptuality. While we talk about components, most favorable approach is military approach that dividable in eight components. It is adoptable on every sector but in national security have most mean full respect to others.

Strategic intelligence covers a sufficiently wide range of inquiry that it is necessary to divide it into components, to make discussion manageable. Members of the intelligence communities are responsible for one or more of the components, which are through the use of acronym BEST MAPS:

- (B) Biographic intelligence
- (E) Economic intelligence

---

[310] Central Intelligence Agency,"A Consumer's Guide to Intelligence", Ibid, p. 27
[311] Central Intelligence Agency,"A Consumer's Guide to Intelligence", Ibid, p. 28

- (S) Sociological intelligence
- (T) Transportation and telecommunications intelligence
- (M) Military geographical intelligence
- (A) Armed forces intelligence
- (P) Political intelligence
- (S) Scientific and technical intelligence.

Each of these components can further be divided into a number of subcomponents. These components and subcomponents are not all-encompassing or mutually exclusive. This approach is merely a means to enhance familiarization with the types of information included in strategic intelligence.[312]

As I mentioned in previous section about Scientific and Technical Intelligence (S&TI), it touches upon all of the other components of strategic intelligence. The names of some of the components (economic, geographic, political, and sociological) appear as though they belong exclusively to academia. Academic disciplines indeed mirror those divisions, since World War II intelligence capability was hastily built employing University scholars. The other components have emerged out of specific needs of military commanders and government decision-makers.

While these eight components exhaust the range of intelligence inquiry, they are not mutually exclusive. An in-depth study by Intelligence specialist, for example, would involve most of the other components. Division of intelligence into its components is merely a mental and administrative convenience and too much should not be made of it beyond that regard. In fact, one arbitrary division, the structuring of intelligence production into geographic areas (e.g., Eastern Europe, Western Europe, the Middle East, Africa, etc.) brings together people with different academic backgrounds so that they may consider all aspects of a problem.[313]

---

[312] FM 34-52, "Intelligence Interrogation", Headquarters Department of the Army, Washington, 8 May 1987, Available on site http://www.globalsecurity.org/intell/library/policy/army/fm/fm34-52/chapter7.htm
[313] Garst, R.D., "A Handbook of Intelligence Analysis", 2d ed., Defense Intelligence College, Washington, 1989, pp.45-47

These parameters cannot be changed easily in short or medium periods. But their weights or effects can be evaluated in the changing international conjecture. Davutoğlu make a formula to estimate the power balance. According to him geography, history, population and culture are constant parameters; economic capacity, technologic capacity and military capacity are potential parameters.[314]

Although it is not a component of intelligence, the historical setting is an integral part of all intelligence analysis. We must understand the antecedents to the current situation in order to understand the present and to project into the future.

1.1.50 Biographic Intelligence

Biographic intelligence is the study of individuals of actual or potential importance through knowledge of their personalities and backgrounds. This component can be divided into a number of subcomponents:

- Educational and occupational history-including civilian and military backgrounds of individuals.
- Individual accomplishment-notable accomplishments of an individual in professional or private life
- Idiosyncrasies and habits-including mannerisms and unusual life styles.
- Position, influence, and potential present and future positions of power or influence.
- Attitudes and hobbies-significant interests that may affect an individual's accessibility. [315]

Biographic Intelligence focuses on individual foreign personalities of current or potential importance. Biographers contribute to the intelligence effort by keeping dossiers on large numbers of foreign persons, publishing biographic compendiums on foreign military or political leaders, members of narcotics-trafficking and terrorist organizations, and contribute biographic sketches to other intelligence reports. Due to the necessity of gathering intelligence

[314] Davutoğlu, A., "Stratejik Derinlik", Küre Yayınları, İstanbul, 2001, pp.17-29
[315] FM 34-52, "Intelligence Interrogation", Ibid.

concerning people of potential importance, as well as those currently in the limelight, the intelligence biographer must rely on all sources, and sift through a tremendous amount of information to extract a few nuggets of intelligence value. [316]

Some intelligence problems can be solved only by biographic intelligence. Biographic intelligence on a successful revolutionary leader may be the only means of determining whether a new government will be friendly or hostile to the United States. Moreover, if an envoy were replaced at a delicate phase of bilateral negotiations, the background of the new delegate may provide a valuable key to the probable courses of action to be expected. Knowledge of the background and associations of individuals is the essential contribution of biographic intelligence.

Extensive biographic dossiers can be maintained on only a tiny fraction of the world's population. Maintaining such a database is labor intensive and requires constant attention. In the case of prominent persons, information is often readily available in considerable detail. A wealth of data should not lead to complacency. The intelligence biographer must seek to unearth obscure but important information, which may be the key to understanding personalities and assist in making predictions about their behavior.

Collection of biographic information is simplified by the universal and intense interest in personalities. The press reports much information, and still more appears as the by-product of other intelligence collection. However, simple compilation is not enough. Imaginative and painstaking techniques must be applied to the analysis of this information to turn it into useful strategic intelligence.

The use of a law enforcement technique called link analysis has helped to make biographic intelligence more useful to the narcotics or terrorist analyst. This technique allows the S&TI analyst to connect scientists and developers in foreign nations together. Knowledge of the actions of one scientist may assist in defining the scope of an R&D project. Simply stated, it is a graphic display of "who knows whom" that allows one to trace connections between people and organizations.

---

[316] US Army Home Page, “Biographic Intelligence” Available on site http://www.dl.army.mil/portals/geopolitical/com/com205.htm

Finally, biographic intelligence is the product of technology, analysis and covert operations which help to estimate adversaries and their leaders.

1.1.51 Economic Intelligence

Although I mentioned about economic intelligence in previous section, I preferred to look again on economic intelligence as a component of Strategic Intelligence.

Economic intelligence studies the economic strengths and weaknesses of a country. Its subcomponents are;

- Economic warfare-information on the diplomatic or financial steps a country may take to induce neutral countries to cease trading with its enemies.
- Economic vulnerabilities-the degree to which a country's military would be hampered by the loss of materials or facilities.
- Manufacturing-information on manufacturing processes, facilities, logistics, and so forth.
- Source of economic capability-any means a country has to sustain its economy. [317]

Economics is the study of the production, distribution and use of wealth, the material means of satisfying human needs and desires. It analyzes production factors and how they are used to produce the things that people need and want. Economics focuses not only on domestic production, but also on international trade relations, especially where there is stiff competition for the world's scarce resources since this has been a major cause of international conflict.

Economic Intelligence focuses on the use of natural and human resources, and especially on the functioning of national economies and economic relations between countries[318]

---

[317] FM 34-52, "Intelligence Interrogation", Ibid.
[318] Laquer, W., "A World of Secrets: The Uses and Limits of Intelligence" Basic Books Inc., New York, 1985, pp.38-48

The raising importance of economic power after WW II, caused focus of the states on Economic Intelligence. Policy planners use Economic Intelligence for three major purposes. These are;

- To estimate the magnitude of military or other threats to themselves and their allies.
- To provide indications and warning of the intentions of any potential enemy. Despite the simplicity of the concept, this task is elusive and difficult.
- To estimate the relative strength of all foreign economies over the next few years.

The relationship between economic and military power is close, but analysts must know more than the size of an economy. They must know what it can produce, what it must purchase, and where it is vulnerable. To this end, economic intelligence analysts study not only the basic statistical data on the functioning of a nation's economy, but also the mines that produce the minerals and the factories that convert the raw materials into finished products. Strategic minerals, crucial to the production of high performance military weaponry are especially important.

The availability of raw materials within a country's borders is an important asset. Those supplies that in peacetime may be imported, in war may be blocked. Thus, estimates must consider the possibility of disruption of foreign raw materials supplies.

The degree to which a nation's industrial capacity can be converted to wartime production is related to its peacetime economic policies. A free-market economy focused primarily on consumer goods may not easily, rapidly or cheaply adapt to military production. On the other hand, command economies, such as the former Soviet Union, achieved a close approximation of a war economy even in peacetime.[319]

Even a consumer economy may prepare for the adjustment of its industry to war needs by stockpiling strategic materials and establishing long, slow production runs of important military equipment to keep the production facilities operating. In the world of high technology the relationship between civilian and military production has grown closer. This is not to say that the

[319] Renwick, R., "Economic Sanctions" Center for International Affairs, Harvard University, Cambridge, 1981, pp.12-15

products demanded by each sector are the same, but rather that the technology of manufacturing is similar, and quick conversion to military production is possible.

What about economic mobilization? At least four steps are required for economic mobilization. First, all available personnel must be utilized to staff the armed forces and simultaneously allow sufficient workers for the production of war materials and essential civilian goods. Second, raw materials must be controlled to ensure that military production is adequately supplied. Third, price controls aid in financing the war effort and ensure the smooth operation of the economy. Fourth, the rationing of civilian goods is imperative to ensure efficiency and to boost morale (of the population by insuring availability of most consumer goods, and of troops; by requiring civilians to share the cost of war).

1.1.52 Sociological Intelligence

Sociology is the study of the way people organize their lives, and includes groups within society, their composition, organization, purposes and habits, and the role of the individual in society and its institutions. Sociology differs from psychology in that it focuses on group behavior while psychology concentrates on individual behavior. Each country should be viewed as a distinct entity, with a unique culture (history, language, values, and perceptions) even though the differences may be difficult to discern, as in the case of countries that share cultural traits due their proximity or former status as colonies, etc.

Group behavior is studied through careful examination of social institutions, social stratification and mobility, religions, folkways (including social codes and taboos), national traditions, and the pace of and reaction to change. Particularly important are the factors that affect social stability; such as the way a society deals with information, influence, and authority.

For strategic intelligence purposes, sociological factors are studied under six main headings:

- Population-including location, growth rates, age and sex structure, labor force, military manpower, and migration.
- Social characteristics-including ethnicity, tribalism, social stratification, formal and informal organizations, and social mobility.
- Public opinion including perceptions of the government and the international picture.

- Education-including educational attainment, expenditures on education, and the relationship between education and other social and political characteristics.
- Religion-including the role of religious groups in the government decision-making process and conflict between religious groups.
- Public welfare and health-including governmental and informal welfare systems, health care delivery, and the general health of the population. [320]

All of these subcomponents can be handle one by one. But I preferred to concentrate the general perspective of Sociological Intelligence.

Strategic planners must have a basic understanding of the cultural, political, and religious aspects of each of these population groups. Once those aspects are understood, then analysts can make a determination of the impact of each group. Will they help or hinder the operation? Particularly at the strategic level, the answer to this question means more than a simple parsing of the population into only three categories--the doctrinal friendly, neutral, and enemy. Rather, analysts should assess each group against its capabilities and interests and in the context of the current situation and ultimate objective. Armed with this information, planners and analysts can determine how we can actively influence each of the many population groups within the objective areas to contribute to mission success, or at a minimum, how to minimize their interference.

We can also use the information to assess and predict which groups would most likely impede mission objectives.

At the strategic level, the intent of population analysis is to develop a good understanding of the culture and context of the operational area. This will ensure that by the time the information reaches the tactical level, it is consciously part of plans, force protection measures, rules of engagement, and all instructions to individual soldiers. [321]

At the end sociological intelligence bring policymakers estimative decision near true by clearing the characteristics of nations and their leaders.

---

[320] FM 34-52, "Intelligence Interrogation", Ibid.
[321] Medby, J., "IPB Considerations at the Strategic Level", Military Intelligence Professional Bulletin, Apr/Jun 2002, Vol. 28, Issue 2, p.26

1.1.53 Transportation and Telecommunications Intelligence

The developments in the transportation and telecommunication sectors increased the importance of Transportation and Telecommunications Intelligence, and made it very complex. The size and sophistication of these systems are generally tied to the nation's level of economic development. Highly developed countries have systems that are larger, denser, more complex, flexible, interconnected, and unnecessary. Sophistication and interconnectivity may make them vulnerable to temporary disruption, but flexibility and redundancy will mitigate that vulnerability. Cellular telecommunications systems and the worldwide computer network are largely decentralized making them less vulnerable to conventional disruption or destruction than traditional systems. Generally, extensive, well-integrated transportation and telecommunications systems are less vulnerable to attack by conventional means. Conflict in the information age, however may involve manipulating information itself rather than disrupting its pathways.

"Transportation intelligence" focuses on the facilities and operations of foreign transportation systems, including railways, highways, inland waterways, pipelines (especially petroleum and gas), ports, the merchant marine, and aviation.

"Telecommunications intelligence" focuses on the facilities and operations of civil and fixed military communications systems in foreign countries, including radio, television, telephone, telegraph, submarine cable, and related communications media. The primary purpose is to determine (1) the capabilities and vulnerabilities of the system and (2) the compatibility with own state or allied equipment.

A well-integrated transport network requires more than the simple connection of regional networks. For example, in a railroad network, the gauges, weight-carrying capacities, and operational techniques must be common to the entire system. The overall vulnerability of a transportation system is reduced by availability of alternate means, such as an inland waterway. The same holds true of telecommunications. The ability to reroute communications in case of war damage is essential.

Analysts should evaluate the effectiveness of a transportation and telecommunications system from the military perspective. In time of war, military requirements will be superimposed on domestic requirements. If normal domestic requirements impede the war effort, military

requirements will take precedence, thus impacting the operation of the civilian economy. Excess capacity, redundancy, and massive integration are essential if national telecommunications and transportation systems are to absorb the simultaneous impact of potential war damage and added demand.

Transportation and telecommunications systems tend to be geographically similar. Major telecommunications routes almost invariably follow the basic pattern of the transportation system because (1) historically telecommunications followed the development of the transportation system, (2) the locations of major cities determined the routes of both transport and telecommunications systems, and (3) access to telecommunications installations generally requires placement along roads.

The major exception to the above mentioned pattern is in radio and telephone microwave relay systems, which do not necessarily follow transport routes. In mountainous terrain individual towers can be placed miles apart on high vantage points, by helicopter. Line-of-sight radio relay systems tend to march straight across the landscape, deviating only around the highest mountains and avoiding circuitous roads.

Telecommunications have increased the capacity of transportation systems by providing easier scheduling, coordination, and control of shipments. Control lines along rail routes may provide additional communications circuits in a military emergency. These factors should maintain the interest of transportation and telecommunications analysts.[322]

1.1.54 Military Geographical Intelligence

All strategists should give importance to Military Geographical Intelligence since the beginning of peace; otherwise they will not success as Collins said, " history punished to whom didn't give importance geography."[323]

Military geography is the evaluation of all aspects of the physical and cultural environment, which may influence military operations. It concerns position, size, shape, boundaries, weather,

---

[322] FM 34-52, "Intelligence Interrogation", Ibid.
[323] Collins, J.M., "Military Geography" in Özdağ, Ü., "Stratejik İstihbarat", ASAM Yayınları, Ankara, 2002, p. 130

climate, terrain, drainage, vegetation and surface configuration, and artificial or man-made characteristics. Military geography is frequently the foundation upon which other intelligence efforts build.[324]

Görgülü define this approach as geographic power instead of military geography. According to him geographic power is necessary for national policy, national strategy, national purpose; but military geography is necessary for military strategy, doctrine, concept.[325] Although there isn't a same approach the definition, I preferred all these definitions in the form of military geography.

The military geographer must evaluate the effect of the physical landscape on military operations. Analysis of significant geographic characteristics helps to determine strategic objectives and their access routes. Those characteristics include economic centers (transportation, manufacturing, mining, and storage facilities), political focal points (centers of decision making), sociological clusters (population concentrations), and military bases, associated facilities and areas of movement. Vulnerability and defensibility of military objectives are determined by evaluating the following factors:

- Location, size, shape, and boundaries
- Coasts and landing beaches
- Weather and climate
- Topography
- Urban areas
- Military geographic regions
- Strategic areas, approaches and internal routes.[326]

The geographer's major tool for analysis and presentation is the map, which portrays the spatial arrangement of sources of national power (fuel and mineral resources, transportation facilities, manufacturing capacity, and, above all, people). Geographers make extensive use of computers for both analysis and data management, and for digitized

---

[324] FM 34-52, "Intelligence Interrogation", Ibid.
[325] Görgülü, İ., "Askeri Coğrafya", Harp Akademileri Basımevi, İstanbul, 1992, p.10
[326] Mackinder, H.J., "The Geographical Pivot of History," Geographical Journal, Vol. 23, 1994, pp. 421-444, Available on site http://iserit.greennet.gl/jknuni/geopolit.htm

cartography. With these tools, geographers can provide a systematic, graphic assessment of the war potential of nation or religion.

1.1.55 Armed Forces Intelligence

Armed Force Intelligence is important. Because; most of the history passed with wars as Caşın said "The history of civilization shows us the 87 years of every hundred period passed with wars, others for preparing to wars."[327]

Armed Forces Intelligence integrates the study of the organized land, sea, and air forces of foreign nations. It concerns both actual military power and potential military power. A nation's armed forces are its means for advancing policy by force. Since there are also economic, political and psychological instruments applied both in war and peace, their balanced development, integration and application are instrumental to a nation's ability to achieve its strategic goals.[328]

Total national power results from a combination of military, geographic, economic, social and political factors. Examining only a nation's armed forces cannot reveal the complete picture of its strategic capabilities or vulnerabilities. Economic resources, political alignments, the number, education and health of its people, and national objectives are all important in determining the ability of a nation to exert international influence through peaceful or forceful means.

In addition to analyzing the internal workings of the armed forces, we must consider the national context in which the military operates. Critical to the equation of national power is a country's reputation for its willingness to use military force to achieve policy goals. A militarily powerful nation with a demonstrated unwillingness to use that power soon develops a reputation as a "paper tiger." That reputation also contributes to the difficulties facing the analyst, for the "paper tiger" may unexpectedly seek to change its reputation.

Elements of all other components enter into the equation of military power.

---

[327] Caşın, M.H., "Çağdaş Dünyada Uluslararası Güvenlik Stratejileri ve Silahsızlanma", SSM Yayınları, No. 17, Ankara, 1995, p. 39-40

[328] Dunnigan, J.F., "How To Make War", Quill Publishing, New York, 1983, pp.48-49

For example, military hardware depends on the economy's ability to either produce the hardware or to generate the revenue to pay for it. In turn, the productive capacity of an economy depends on its resources, and scientific and technological capabilities. The latter, in turn, is largely a function of the human resources and the economic policies that may promote or hinder technology. Finally, the political and cultural philosophy of a nation and its international context influences the amount, of effort devoted to the military.

The political status of a nation's armed forces must be evaluated along with the details of organization, staffing, and armaments. Factors affecting the status of the armed forces include the constitutional and legal basis for its existence, the degree to which the military influences political decisions, military traditions of the nation and the attitude of the people toward the military. These are all essential to obtain an acceptable comprehension of any military establishment.

Armed forces intelligence is the integrated study of the ground, sea, and air forces of a country-often referred to as Operational Battlefields. It is concerned with military alternatives in terms of position, terrain, economics, politics, and so forth.[329]

1.1.56 Political Intelligence

Political intelligence studies all political aspects, which may affect military operations. Its subcomponents are;

- Government structure-organization of departments and ministries.
- National policies-government actions and decisions.
- Political dynamics-government views and reactions to events.
- Propaganda- information and disinformation programs.
- Policy and intelligence services- organizations and functions.
- Subversion-subversive acts sponsored by the government. [330]

Political intelligence begins with knowledge of a state's history and internal politics. What is the distribution of political power? Is it a democracy, an oligarchy, or a dictatorship? What

[329] FM 34-52, "Intelligence Interrogation", Ibid.
[330] FM 34-52, "Intelligence Interrogation", Ibid.

are the sources of political power? Is authority based on a legitimate constitution and the will of the people, political magnetism, skill and competence of leaders, or brute force? It is particularly important for western analysts to develop an understanding of non-western culture, values, beliefs, priorities, and political processes.

Knowledge of the decision-making process is essential to understanding how certain decisions are taken, and is critical to any attempt at forecasting policy decisions. The formal and informal decision-making process is influenced by (1) assigned responsibilities, (2) personalities and professional backgrounds and motivations of leaders, (3) mechanisms of decision-making, and the information on which policy makers act.

In some countries, institutions that on the surface seem western in nature may in fact operate quite differently. For example, civil and military bureaucracies may not be neutral agents of policy, but may operate almost entirely in their own self-interest. Armies may function as political parties, as economic institutions or administrators rather than as guardians of national security. Parliaments may have a developmental or honorary role, rather than a legislative role. The political intelligence officer must discern the difference between the political systems as it actually operates, from the way it theoretically should operate.

Adequate political intelligence provides indications of probable courses of action by foreign nations. The constant ebb and flow of political power requires constant monitoring of the changes in institutions, personalities and procedures.

Political intelligence starts with analysis of the formal political structures and procedures of a foreign nation. It includes the constitution, legal system, the prerogatives and responsibilities of the legislative, judicial and executive branches, and the civil and religious rights of the people. A thorough analyst should also know the depth and breadth of national devotion to constitutional and legal principles.

An analysis of government operations determines their efficiency, integrity, and stability. Widespread inefficiency and corruption, especially if it is a new development, may be an indication of an impending change in government. Continued inefficiency and corruption may indicate popular apathy or a populace unable to effect change. Restrictions on the electoral process and on other human rights may mean the government is growing fearful of civil action.

The careful analyst will separate form from substance to obtain clues about the probable future of a political system.

Since nations differ in goals and means, their foreign policies may encompass their local neighbors or the entire globe. Each nation, large or small, pursuing its own national interests must consider the interests of other nations likely to be affected by its policies in order to avoid conflict. It is the responsibility of the intelligence analyst to determine those interests each nation considers "vital" to its security. The cultural values and interests of the analyst should not obscure the result.[331]

Foreign political intelligence is gathered from a variety of sources. Most important is on-the-scene collection by diplomatic and military personnel. Other sources include data from technical collection systems, official statements by foreign governments, the press, public opinion polls, international businessmen, and the work of academic researchers.

Nations' political landscapes range from those with no political parties, through those with one party to those with so many parties that one can rarely win enough support to govern without creating a coalition. Therefore, depending on the country, analysts must determine the interests, platforms, and degree of popular support, financial backing and the personalities of each political party. Special interest parties, representing labor, religious, ethnic groups, or industry need to be studied in conjunction with the interest group they represent.

With few exceptions, most states have some type of formal or informal pressure groups. Examples include political parties, associations, religious or ethnic organizations, labor unions, even officially illegal organizations (e.g., a banned political party). The analyst must identify these pressure groups and their goals, methods, power, sources of support, and leadership. Pressure groups may have international connections, and in some cases, may be externally controlled.

Increasing attention is being directed at the following non-traditional pressure groups: terrorists, narcotics traffickers and other international criminal organizations. Because of their small numbers, their need to operate secretly, their ability to bribe officials, and quickly

---

[331] Feld, W. J. and Boyd, G., "Comparative Regional Systems", Pergamon Press, New York 1980, pp.23-25

and constantly adapt to government measures, they are among the most difficult entities on which to obtain good intelligence. Their increasing danger to the world communities demands ever-increased vigilance.

Elections range from "stage shows" of limited intelligence significance to a means of real, peaceful change. In democratic states they are more important and are a way for national issues to be debated (even if they are not always intelligently discussed). In addition to parties, personalities and policies, the intelligence analyst should consider whether the balloting process is free and fair and, very importantly, if there are changes from the historical norm.

In many countries clandestine organizations or guerrilla groups attempt to overthrow or destroy the government. These organizations typically conduct their activities in secret, making the intelligence analyst's job more difficult. Analysis may be limited due to the scarcity of information. Intelligence on subversive movements should include size, character of membership, affiliated organizations, key figures, funding, and methods of operation.

A country's international influence is determined in part by its international goals and policies, its leadership, stability, economic strength, population, physical resources, military power, international trade position, the strength and commitment of its allies.[332]

1.1.57 Scientific and Technical Intelligence

After the WW II seven technologies stand out. These are fiber optics, computers, human-computer interaction, digital transmission and digital compression, communication satellites, cellular technologies and last one networking.[333]

Scientific and technical intelligence studies the country's potential and capability to support objectives through development of new processes, equipment, weapons systems, and so forth. The subcomponents are weapons and weapon systems, missile and space program,

---

[332] Maurer, A.C.,et. al., (eds.), "Intelligence Policy and Process", Westview Press, Boulder, 1985, Chapters 1-4
[333] Papp, D., " The Impacts of Advanced Information and Communication Technologies on International Actors and the International System", in Strategic Environment, Air Command and Staff College Publishing, Alabama, 1996, pp.1-2

nuclear energy and weapons technology, NBC developments, basic applied science, research and development systems. [334]

Scientific and technical intelligence (S&TI) is the study of the scientific and technical capacities and activities of all nations. As weapon systems become more sophisticated, it is increasingly important to know about the activities of foreign military scientists, their research and development programs and even their civilian scientific establishment of foreign nations, and the details concerning their funding, discoveries, and inventions. [335]

Military research and development activities are most interesting to the intelligence analyst, but since applied and theoretical scientific research are the key to future potential they should not be ignored.

A sophisticated scientific establishment is a result of extensive, quality scientific education and sustained funding of scientific research. The public attitude toward science is critical in influencing the caliber of people entering the field. A sustained history of innovation and discovery is the surest indicator of a similar future.

1.1.57.1 New Weapons and Equipment

The Scientific and Technical Intelligence analyst evaluates new weapons and equipment of foreign armed forces and predicts which merit careful study. Careful review of Research and Development (R&D) efforts will allow estimations of deployment dates while analysis of basic research efforts will indicate the potential and characteristics of new weapon systems.[336] S&TI efforts should not be confined to the obvious. Prudence dictates observation of all areas where there may be potential for new technology to substantially alters the military landscape. In the search for the novel however, the S&TI analyst must not forget such old standbys as chemical industries. Synthetics or substitutes have enabled nations to wage war despite shortages of materials previously considered essential, e.g., fuels, lubricants, and

---

[334] FM 34-52, "Intelligence Interrogation", Ibid.
[335] Joint Chiefs Of Staff, "Joint Doctrine Encyclopedia", Ibid, p.628
[336] AFIO Intelligence Notes, "Current Intelligence" Issue 43, 10 November 1998, Available on site http://www.afio.com/sections/wins/1998/notes43.html

rubber. The potential of genetic engineering for novel military uses or the overall enhancement of an economy to sustain a war effort also merits concern by the S&TI analyst.

1.1.57.2 Collection

National collection systems are useful in monitoring the final stages of weapon system testing, but of little value when it comes to the early stages of research. Open sources, particularly translations, are a useful source of data. The scientific intelligence analyst should observe the activity of trained fieldworkers since military researchers depend upon them for raw data.

The scientific intelligence analyst must understand the bureaucracy of scientific research in the country being investigated. That includes identification of the main research and development organizations, interrelationships and coordination between organizations, where and how projects originate, obtain funding, and are controlled by government.

Foreign academies of science not only publish membership rosters, but also frequently publish scholarly papers that reveal research trends. Technical publications offer insight into the topics and sophistication of research.

Foreign universities, especially those with recognized scientific programs, can offer insights into future developments. The types of science stressed in their curricula may yield valuable information on those items that the nation is emphasizing in its research and development programs.

Privately owned research facilities, large and small, their relationship with the government, their significance, and type of research should be studied. Funding sources for conspicuous research projects may provide useful insights. Additional sources of information include funding received by individual scientists or specific projects. Citations, which accompany awards often, recite the accomplishments of the recipient.

Other hints that important scientific and technical developments are taking place include:

Imports of materials or equipment for a specific type of scientific research project

- Construction or expansion of facilities for specific types of scientific investigation
- Unusual security precautions
- Higher wages or incentives for a certain type of scientists or workers.

The location of key scientists may provide an indication of the type of research at a specific installation. Exchange visits between scientists can also yield intelligence on who is doing what and where.[337]

1.1.57.3 Internet

Internet or World Wide Web (WWW) is another source, which transform the world in a sanal world, for Electronic Intelligence. Its boundaries haven't known exactly.[338]

It is unclear to what extent foreign intelligence services are using computer hackers to obtain proprietary data or sensitive government information, or whether they have developed the capability to use computer intrusion techniques to disrupt telecommunications activities. The KGB did, however, sponsor computer intrusion activities by the Hannover Hackers, and there is no reason to believe that these efforts have ceased. The Hannover Hackers were able to access at least 28 Government computer systems, and obtain data from them. They sold this data to the KGB. While none of this data was classified, much of it was sensitive, and classified information could potentially be derived from comparing this information with other data. It has also been alleged that the KGB has been involved in similar efforts with other hacker groups and that these operations included the remote introduction of logic bombs and other malicious code.[339] There is little doubt that many foreign intelligence services could obtain these capabilities if they wished.[340] The ability of a group of Dutch hackers to obtain sensitive information from U.S. Army, Navy, and Air Force computer networks during Operations Desert Shield and Desert Storm serves as an example of this potential for access. Between April 1990

---

[337] National Intelligence Course (NIC) Textbook, Ibid, Chapter 5, pp.18-19
[338] Ersanel, N., "Siber İstihbarat", Jeopolitik-Strateji-Terör Dizisi, ASAM yayınları, Ankara, 2001, p.21
[339] Warren, P., "Technoterrorists: Growing Links Between Computer Technology and the Seedy Underworld of Terrorism, Organized Crime, and Spying." Computer Talk, 1989, p. 52, Available on site www.fas.org/irp/nsa/ioss/threat96/part02.htm
[340] Interview: DISA Center for Information System Security, November 3, 1993, Available on site www.fas.org/irp/nsa/ioss/threat96/part02.htm

and May 1991, this group was able to penetrate computer systems at 34 different facilities. The group obtained information on logistics operations, equipment movement schedules, and weapons development programs. Information from one of the penetrated computer systems directly supported Desert Shield/Desert Storm operations. In a review of this incident the General Accounting Office concluded that a foreign intelligence service would have been able to derive significant understanding of U.S. Operations in the Persian Gulf from the information that the Dutch hackers were able to extract from DoD information systems.[341]

PSYCHOLOGY OF INTELLIGENCE ANALYSIS[342]

As an interdisciplinary science, some intelligence scientist researched Psychology of Intelligence Analysis or another description researched quality of intelligence analysis. Most famous of them is Sherman Kent whose approach to intelligence concept is "analytic pyramid" characterizing a wide base of factual information and sides comprised of sound assumptions, which pointed to the most likely future scenario at the apex. And in Strategic Intelligence Kent, took account of the coming computer age as well as human and technical collectors in proclaiming the centrality of the analyst: "Whatever the complexities of the puzzles we strive to solve and whatever the sophisticated techniques we may use to collect the pieces and store them, there can never be a time when the thoughtful man can be supplanted as the intelligence device supreme." In his proselytizing and in practice, Kent battled against bureaucratic and ideological biases, which he recognized as impediments to sound analysis, and against imprecise estimative terms that he saw as obstacles to conveying clear messages to readers. Although he was aware of what is now called cognitive bias, his writings urge analysts to "make the call" without much discussion of how limitations of the human mind were to be overcome.

Another one is Robert Gates whose ideas for overcoming what he saw as insular, flabby, and incoherent argumentation featured the importance of distinguishing between what

---

[341] Committee on Governmental Affairs, "A Lesson of the Gulf War: National Security Requires Computer Security", Subcommittee on Government Information and Regulation, Washington, June 19, 1991, Available on site www.fas.org/irp/nsa/ioss/threat96/part02.htm

[342] Heuer, R.J., "Psychology of Intelligence Analysis", Central Intelligence Agency, Washington, 1999, Available on site http://www.cia.gov/csi/books/19104/index.html

analysts know and what they believe--that is, to make clear what is "fact" (or reliably reported information) and what is the analyst's opinion (which had to be persuasively supported with evidence). Among his other tenets were the need to seek the views of nonexperts, including academic specialists and policy officials, and to present alternate future scenarios. More than one participant in the process observed that a lack of guidelines for meeting Gates's standards led to a large amount of "wheel-spinning." Gates's impact, like Kent's, has to be seen on two planes. On the one hand, little that Gates wrote on the craft of analysis is read these days. But even though his pre-publication review process was discontinued under his successors, an enduring awareness of his standards still gives pause at jumping to conclusions to many managers and analysts who experienced his criticism first-hand.

Doug MacEachin sought to provide an essential ingredient for ensuring implementation of sound analytic standards: corporate tradecraft standards for analysts. This new tradecraft was aimed in particular at ensuring that sufficient attention would be paid to cognitive challenges in assessing complex issues. He came away from this experience with new insights on what constitutes "value-added" intelligence usable by policymakers. MacEachin advocated an approach to structured argumentation called "linchpin analysis," to which he contributed muscular terms designed to overcome many CIA professionals' distaste for academic nomenclature. The standard academic term "key variables" became drivers. "Hypotheses" concerning drivers became linchpins--assumptions underlying the argument--and these had to be explicitly spelled out. MacEachin also urged that greater attention be paid to analytical processes for alerting policymakers to changes in circumstances that would increase the likelihood of alternative scenarios.

Richards Heuer’s impact on the quality of Agency analysis arguably has been at least as important as theirs. Heuer received a degree in philosophy in 1950 from Williams College, where, he notes, he became fascinated with the fundamental epistemological question, "What is truth and how can we know it?" Dick Heuer's writings make three fundamental points about the cognitive challenges intelligence analysts face:

- The mind is poorly "wired" to deal effectively with both inherent uncertainty (the natural fog surrounding complex, indeterminate intelligence issues) and induced uncertainty (the man-made fog fabricated by denial and deception operations).

- Even increased awareness of cognitive and other "unmotivated" biases, such as the tendency to see information confirming an already-held judgment more vividly than one sees "disconfirming" information, does little by itself to help analysts deal effectively with uncertainty.

- Tools and techniques that gear the analyst's mind to apply higher levels of critical thinking can substantially improve analysis on complex issues on which information is incomplete, ambiguous, and often deliberately distorted. Key examples of such intellectual devices include techniques for structuring information, challenging assumptions, and exploring alternative interpretations.

His ideas were similar to or compatible with MacEachin's concepts of linchpin analysis. According to him “Given the difficulties natural in the human processing of complex information, a prudent management system should:

- Encourage products that (a) clearly delineate their assumptions and chains of inference and (b) specify the degree and source of the uncertainty involved in the conclusions.
- Emphasize procedures that expose and elaborate alternative points of view--analytic debates, devil's advocates, interdisciplinary brainstorming, competitive analysis, intra-office peer review of production, and elicitation of outside expertise.”

Heuer emphasizes both the value and the dangers of mental models, or mind-sets. And he notes that: “[Analysts] construct their own version of "reality" on the basis of information provided by the senses, but this sensory input is mediated by complex mental processes that determine which information is attended to, how it is organized, and the meaning attributed to it. What people perceive, how readily they perceive it, and how they process this information after receiving it are all strongly influenced by past experience, education, cultural values, role requirements, and organizational norms, as well as by the specifics of the information received.”

In essence, Heuer sees reliance on mental models to simplify and interpret reality as an unavoidable conceptual mechanism for intelligence analysts--often useful, but at times hazardous. What is required of analysts, in his view, is a commitment to challenge, refine, and challenge again their own working mental models, precisely because these steps are central to sound interpretation of complex and ambiguous issues.

Heuer sees mirror-imaging as an example of an unavoidable cognitive trap. No matter how much expertise an analyst applies to interpreting the value systems of foreign entities, when the hard evidence runs out the tendency to project the analyst's own mind-set takes over. Heuer observes: “To see the options faced by foreign leaders as these leaders see them, one must understand their values and assumptions and even their misperceptions and misunderstandings. Without such insight, interpreting foreign leaders' decisions or forecasting future decisions are often nothing more than partially informed speculation. Too frequently, foreign behavior appears "irrational" or "not in their own best interest." Such conclusions often indicate analysts have projected American values and conceptual frameworks onto the foreign leaders and societies, rather than understanding the logic of the situation as it appears to them.”

Heuer's concept of "Analysis of Competing Hypotheses" (ACH) is among his most important contributions to the development of an intelligence analysis methodology. At the core of ACH is the notion of competition among a series of plausible hypotheses to see which ones survive a gauntlet of testing for compatibility with available information.

Heuer's advice to Agency leaders, managers, and analysts is pointed: To ensure sustained improvement in assessing complex issues, analysis must be treated as more than a substantive and organizational process. Attention also must be paid to techniques and tools for coping with the inherent limitations on analysts' mental machinery. He urges that Agency leaders take steps to:

- Establish an organizational environment
- Expand funding for research
- Foster development of tools

CONCLUSION OF CONCEPTUAL ANALYSIS OF INTELLIGENCE

The need for 21st Century global information superiority is critical to the successful execution of the strategy. This entire issue deserves more careful study, although we recognize that classification requirements limit what can be covered in public reports. Nonetheless, it is important to note that the strategy makes it imperative to collect, analyze and disseminate strategic and tactical intelligence anytime and anyplace.

This imperative should include Human Intelligence (HUMINT), imagery and Signals Intelligence (SIGINT) as well as ground, airborne and space systems. The integration of these systems to provide a comprehensive assessment of a potential or actual enemy remains a weakness. This is especially true at the strategic and operational levels. As the asymmetric challenges of the future increase the complexity of warfare, the importance of HUMINT and other intelligence disciplines will likely grow.[343]

Requirements and collection must be managed coherently across the disciplines, with increasingly difficult resource trades made at the communities level in an informed, all-source process. Improved synergy during collection operations, which will become more and more critical to success in the 21st century, requires movement away from the traditional stovepipe approach to collection. Research and Development (R&D) needs to be more closely coordinated with requirements and a contingency fund should be established to take advantage of technological targets of opportunity.[344]

Changes in the nature of the world, the sole focus of intelligence agencies, have required a shift in the purposes and goals of the Intelligence Communities. Gone is the relentless focus on Soviet submarines, missile silos, and conventional military capabilities; new threats include terrorism, transfers of Weapons of Mass Destruction (WMD), and political, ethnic, and social upheavals in a variety of regions. Gone also is the massive military infrastructure of the Soviet Union that could be observed by overhead imagery platforms.

---

[343] National Defense Panel, "Assessment of intelligence", Quadrennial Defense Review, May 1997, Available on site http://www.defenselink.mil/topstory/ndp_assess.html

[344] Government Printing Office, "IC21: The Intelligence Community in the 21st Century", Staff Study Permanent Select Committee on Intelligence, House of Representatives One Hundred Fourth Congress, Washington, 1996, Available on site http://www.access.gpo.gov/congress/ house/intel/ic21/ic21_toc.html

Intelligence agents must be able to move beyond contacts with foreign government officials and tap into political sects and terrorist cells often having no perceptible infrastructure. [345]

As a result, some observers believe that intelligence agencies may be in for a period of transition and adaptation exceeding the one that followed immediately upon the dissolution of the Soviet Union and the Warsaw Pact. In particular, it is argued that the three major "INTs," the major intelligence disciplines [signals intelligence (SIGINT), imagery intelligence (IMINT), and human intelligence (HUMINT)] will have to be fundamentally reinvented and this process will have major technical and organizational ramifications.[346]

SIGINT intercepts communications worldwide in order to provide economic intelligence to states corporations. Agencies assist states corporations competing with foreign firms. They acknowledge, however, that intelligence agencies collect information regarding the use of bribery and other illegal efforts by foreign firms in competition with states corporations. [347]

A second major intelligence discipline, IMINT is also facing profound changes. Imagery is collected in essentially three ways, satellites, manned aircraft, and unmanned aerial vehicles (UAVs). The demise of the Soviet Union and experience in the Persian Gulf War have indicated that there is likely to be a greater number of collection targets than in the Cold War and that more maneuverable satellites may be required. At the same time, the advent of high-quality commercial satellite imagery has raised many questions about whether at least some coverage can be obtained less expensively from the private sector. Intelligence from human contacts (HUMINT) is the oldest intelligence discipline and the one that is most often written about in the media. Agencies, which are responsible for most HUMINT collection, had important successes during the Cold War; disaffected Soviets and others provided invaluable help in providing information about weapons programs and political intentions that were not obtainable from any other source. Today, however, the challenge is making contacts with influential figures in heretofore obscure third world states, clandestine groups, or narcotics traffickers who speak a variety of foreign

[345] Best, R. A., Intelligence Issues for Congress, Foreign Affairs and National Defense Division, June 4, 2001, Available on site http://www.fas.org/irp/crs/IB10012.html
[346] Best, R. A., Ibid.
[347] Best, R. A., Ibid.

languages. HUMINT regarding such sources can be especially important as there may be little evidence of activities or intentions that can be gathered from imagery and their communications may be carefully limited. [348]

A fourth INT, measurement and signatures analysis (MASINT) has received greater emphasis in recent years. A highly technical discipline, MASINT involves the application of more complicated analytical refinements to information collected by SIGINT and IMINT sensors. It also includes spectral imaging by which the identities and characteristics of objects can be identified on the basis of their reflection and absorption of light. A key problem has been retaining personnel with expertise in MASINT systems that are offered more remunerative positions in private industry. [349]

The widespread use of computers and new communications systems means that although there is a greater need for coordinating the INTs at the strategic level, intelligence products are used at many different levels of government and that quite low-level users can access information. In addition, there has been increased availability of tactical intelligence collectors (SIGINT systems, aircraft and UAVs) that are operated by military commanders who are also the immediate recipients of the information acquired. Some observers express concern about excessive emphasis on tactical intelligence, arguing that national priorities may be downgraded. Observers suggest that there will be increasing needs to share national and tactical intelligence and for organizational and individual flexibility. [350]

A superficial trend analysis of the data contained at Table 4.1 provides a listing of possible causes of intelligence failures over time. The listing is not all-inclusive but does help to reveal areas that may require further focus. The first trend is that technological advancements have been significant, but efforts to develop all- encompassing artificial intelligence systems to cope with this increased volume have failed. Automated data handling systems have been programmed to collate or sort selected material, to maintain dynamic databases, and to sound the alarm if key indicators are encountered. While these technology enablers are useful, the thinking is done by human beings in the time

[348] Best, R. A., Ibid.
[349] Best, R. A., Ibid.
[350] Best, R. A., Ibid.

consuming, and often-subjective task of analysis. Currently, the flow of information outstrips the analytic communities' ability to thoroughly sift through the masses of data.[351]This fact alone bodes poorly for future intelligence successes but other analytic challenges are more pervasive and problematic.

Tablo 0.1 Intelligence failures compared over time[352]

POSSIBLE CAUSES OF INTELLIGENCE FAILURES	PRE-MODERN INTELLIGENCE	MODERN INTELLIGENCE
Sources of information	Almost exclusively HUMINT,	Effective usage of SIGINT, IMINT, OSINT; and HUMINT
Reliability	Reliability low; difficult to verify; prone to be used for deception.	Relatively high; can be verified "objectively"; can be corroborated by different types of intelligence.
Availability	Slow; often too late to be relevant; overtaken by events.	Quick; can be available in real time when needed.
Demand for and importance assigned to intelligence	Demand is moderate; important, but not perceived as critical; in general, a pessimistic & negative evaluation of intelligence.	High to very high; important in both peace and war; seen as critical for survival and success; in general a positive evaluation of intelligence.
Organization	Primarily ad hoc; no permanent organization; not a distinct profession; small numbers of exclusive participants involved.	Large professional, permanent organizations; complex collection means; analysis coordination activities.
Intelligence Cycle	Basic four step (direction, collection, processing, dissemination); entirely manual.	Basic five step (added production,); increasingly automated.
Analysis	Limited information; done by humans; manpower intensive.	Ever increasing amount of information; thinking done by humans and aided by machines; manpower intensive.

[351] Dearth, D. H.and Godden, R. T. (eds), "Strategic Intelligence: Theory and Application" (second edition), Defense Intelligence Agency, Washington, 1995, p. x
[352] Dearth, D. H.and Godden, R. T. (eds), Ibid, p.x

"It is only when we demand a solution with no cost that there are no solutions."

Lester Thurow

GLOBALIZATION IS THE NEW FORM OF WORLD

Globalization is an idea whose time has come. From obscure origins in French and American writings in the 1960s, the concept of globalization finds expression today in all the world's major languages.

Globalization has taken its place in politics and economic discourse especially from the beginning of the 1990s. The globalization process had begun earlier -after World War II - but the Cold War period masked "an awareness of the globalization"[353] process. Although the origins arrive before the collapse of Soviet Union, I preferred to start with 1991 in which main revolution started in every sector and especially in mentality of security.

GLOBALIZATION AS A PROCESS

Today the word or the phenomenon 'globalization' has a wider use in every fields of our life such as politics, economy, military, culture, inner and foreign affairs, technology, communication, sports, security, etc. Every good or bad development in the world is seen to interrelate with globalization. So globalization is a fact of life and unpreventable process.

Before the analyzing intelligence failures and structure of the new face of world, which I assumed to start with globalization, we should look in definition of Globalization.

1.1.58 Definition of Globalization

Although globalization is the 'big idea' of the late twentieth century there isn't precise definition. Globalization describes the era that is emerging from the pieces of the Cold War. Globalization is not only a period, and also a process, which continue until today.

[353] Summy, R., "Politics of Globalization," Social Alternatives, 1996, Vol.15, Issue 1, pp. 18-21.

Defined broadly, globalization is the process of growing international activity in many areas that is creating closer ties, enhanced interdependence, and greater opportunity and vulnerability for all. Events at the far corners of the earth are now affecting each other, countries and regions are being drawn closer together, key trends are interacting as never before, and the speed of change is accelerating. Because of it, the 21st century will be the first truly Global Century.

What is globalization? Globalization is the "erosion of national borders, decline of the power of national governments, and the rise of organizations (such as transnational corporations) that operate across national borders" [354], "decline in costs of doing business internationally"[355], "advances in information technology, widespread use of air freight, speculation in currencies, increased capital flows across borders, Densification of culture, mass marketing, global warming, genetic engineering, multinational corporate power, new international division of labor, International mobility of labor, reduced power of nation-states, postmodernism, or post-Fordism, a particular form of capitalism"[356], "integration of technologies, finance, markets and nation states"[357], "movement of ideas"[358], "intensification of economic, political, social, and cultural relations across borders; historical period (or historical epoch) launched since the end of the Cold War; transformation of the world economy epitomized by the anarchy (literally defined) of the financial markets; the triumph of US values, through the combined agenda of neoliberalism in economies and political democracy; an ideology and an orthodoxy about the logical and inevitable culmination of the powerful tendencies of the market at work; technological revolution, with social implications; inability of nation-states to cope with global problems that require global solutions, such as demography, ecology, human rights, and nuclear proliferation"[359] , etc...

---

[354] Justino, P., "The Impact Of Globalisation And Trade Liberalisation On Household Poverty Dynamics", Poverty Research Unit Seminar on Globalisation University of Aarhus, 23 November, 2001, Available on site www.ulandslaere.au.dk/NOTICES/Events/ Oneday_seminar2001/ PatriciaJustino.htm

[355] Kym, A., "Globalization, WTO, and Asean," Asean Economic Bulletin, 2001, Vol.18, Issue 1, p. 12

[356] Marcuse, P., "The Language of Globalization," Monthly Review: An Independent Socialist Magazine, Jul/Aug2000, Vol.52, Issue3

[357] Moustafine, M., "Globalization and the Changing Role of Government," Australian Journal of Public Administration, 1999, Vol.58, Issue 4, pp; 126-127.

[358] Cameron, J., "Globalization and the Ecological State,"Review of European Community & International Environmental Law, 1999, Vol.8, Issue 3, p. 243

[359] Kacowicz, A.M., "Nationalism: Convergent, divergent or overlapping?," Alternatives: Social Transformation & Humane Governance, 1999, Vol.24, Issue 4, pp.527-529.

Four types of change characterize globalization. First, it involves a "stretching" of social, political and economic activities across frontiers, regions and continents. Second, it is marked by the "intensification" of interconnectedness and flows of trade, finance, migration, culture, etc. Third, it can be linked to a "speeding up" of global interactions and processes, as the development of worldwide systems of transport and communication increases the velocity of the diffusion of ideas, goods, information, capital and people. And, fourth, the growing "extensity, intensity and velocity" of global interactions can be associated with their deepening impact such that the effects of distant events can be highly significant elsewhere and specific local developments can come to have considerable global consequences. In this sense, the boundaries between domestic matters and global affairs become increasingly fluid. Globalization, in short, can be thought of as the widening, intensifying, speeding up, and growing impact of world wide interconnectedness. [360]

Moreover, globalization will continue to interact with old and new geopolitics to help lessen some tensions but aggravates others. The key challenge is shaping the interplay of globalization, old geopolitics, and new transnational threats.

1.1.59 Tendencies of Globalization[361]

Three broad accounts of the nature and meaning of globalization can be identified, referred to here as the hyperglobalist, the sceptical, and the transformationalist views. These define the conceptual space of the current intensive debate about globalization. The three dominant tendencies in the globalization debate are summarized in table 5.1. Identifying the critical issues in the debate creates an intellectual foundation for thinking about how globalization might best be conceptualized and the particular grounds on which any assessment of competing claims about it might be pursued.

---

[360] Held, D., et. al., "Global Transformations", Executive Summary, March 1999, Available on site http://www.polity.co.uk/global/summary.htm

[361] I summarized the ideas, which can be find for vast explanation in Held, D., et. al., "Global Transformations", Executive Summary, March 1999, Available on site http://www.polity.co.uk/global/summary.htm

For The Hyperglobalists, contemporary globalization defines a new era in which peoples everywhere are increasingly subject to the disciplines of the global marketplace and globalization defines a new epoch of human history in which 'traditional nation-states have become unnatural, even impossible business units in a global economy. Hyperglobalists argue that we live in an increasingly global world in which states are being subject to massive economic and political processes of change. These are eroding and fragmenting nation-states and diminishing the power of politicians. In these circumstances, states are increasingly the "decision- takers" and not the "decision-makers".

For the Sceptics, by comparison the sceptical position is much more cautious about the revolutionary character of globalization and drawing on statistical evidence of world flows of trade, investment and labour from the nineteenth century, maintain that contemporary levels of economic interdependence are by no means historically unprecedented.

For the Transformationalist Analysis, at the heart of the transformationalist thesis is a conviction that, at the dawn of a new millennium, globalization is a central driving force behind the rapid social, political and economic changes that are reshaping modern societies and world order.

Five principal issues constitute the major sources of contention among existing approaches to globalization. These concern matters of conceptualization, causation, periodization, impacts and the trajectories of globalization.

In exploring each of these in turn a cumulative picture will develop of the requirements of a rigorous account of globalization, a picture which will help move us beyond the debate between the three approaches outlined above.

Table 5.1 Comparing of three tendencies[362]

	Hyperglobalists (Kenichi Ohmae)	**Sceptics** (Held and Thompson)	**Transformationalists** (Held et al.; Cerny; Evans)
What's new?	A global age	Trading blocs, weaker geogovernance than in earlier periods	Historically unprecedented levels of global interconnectedness

[362] Held, D., et al., Ibid, p.10

Dominant characteristics	Global capitalism, global governance, global civil society	World less interdependent than in 1890s	"Thick" (intensive and extensive) globalization
Power of national governments	Declining or eroding	Reinforced or enhanced	Reconstituted, restructured
Driving forces of globalization	Capitalism and technology	States and markets	Combined forces of modernity
Pattern of stratification	Erosion of old hierarchies	Increased marginalization of South	New architecture of world order
Dominant motif	McDonalds, Madonna, etc.	National interest	Transformation of political community
Conceptualization of globalization	As a reordering of the framework of human action	As internationalization and regionalization	As the reordering of interregional relations and action at a distance
Historical trajectory	Global civilization	Regional blocs/clash of civilizations	Indeterminate: global integration and fragmentation
Summary argument	The end of the nation-state	Internationalization depends on state acquiescence and	Globalization transforming state power and world politics

1.1.60 Globalization After September 11th

There is nothing new about globalization. There have been many phases of globalization over the last two millennia including:

- Development of world religions,
- Age of Discovery,
- Spread of empires.

But having recognized this, it is important to note that there is something new about globalization today; that is, important to return to 9/11 and to say what it means.

First of all, there is a new concept occurred with September 11th, which there was no state invulnerable and it was reflection of hatred which globalization caused.

One cannot accept the burden of putting justice right in one realm of life without at the same time seeking to put it right elsewhere. If the political and the security, the social and

the economic dimensions of justice are separated in the long term the prospects of a peaceful and civil society will be bleak indeed. Popular support against terrorism, as well as against political violence and exclusionary politics of all kinds, depends upon convincing people that there is a legal, responsive and specific way of addressing their injustice. Without this sense of confidence in public institutions the defeat of terrorism and intolerance becomes a hugely difficult task, if it can be achieved at all. Globalization without cosmopolitanism could fail. [363]

GLOBALIZATION ON GLOBAL SECURITY MENTALITY

Globalization will exacerbate local and regional tensions, increase the prospects and capabilities for conflict, and give force those who would do harm. For instance, the globalization of technology and information will increasingly accord smaller states, groups, and individuals destructive capabilities previously limited to major world powers. Encouraging and consolidating the positive aspects of globalization, while managing and containing its "downsides," will be a continuing challenge.

Globalization is independent of any national policy and can weaken the power of governments to control events within and beyond their borders. This dynamic of globalization and the global reactions, will underpin many of the security challenges we face during the first two decades of the 21st century. Globalization is characterized by the compression of distance and the increasing permeability of traditional boundaries to the rapid flow of goods, services, people, information, and ideas. It is a multifaceted, transnational phenomenon. [364]

---

[363] Held, D., "Globalization After September 11th", Available on site http://www.polity.co.uk/global/after_sept11.htm

[364] Haass, R.N., "Policymakers and the Intelligence Community in This Global Era," Remarks to CIA Strategic Assessments Group Annual Conference, Wilmington, 2001,Available on site http://www.state.gov/s/p/rem/6423.htm

Wilson interprates, "Not everyone shares our particular view of the future and disaffected states, groups, and individuals will remain an important factor and a key challenge for policy."[365]

Numerous scholars, diplomats, politicians, journalists, generals, admirals and marshals, management gurus, economists and philosophers have attempted to come to grips with the emerging outliners of the New World Order. Many hypotheses and assumption have been advanced, analyzed, commented upon and criticized. While Fukayama has called it the "End Of History", Huntington foresees a "Clash of Civilisations". Krauthammer revels in the "Unipolar Moment". Sakakibara terms it the "End of Progressivism", Ohmae prefers to see it as the "End of the Nation-State" and the Tofflers argue that it is the "End of Equilibrium" (Not History)". They classify the present world into the distinct and potentially clashing super-civilisations. First Wave agrarianism, Second Wave industrialism and the emerging Third Wave post-modern civilisation.[366]

Defense Intelligence is confronted with a variety of new conditions and circumstances as the 21st century approaches. These challenges are marked by an historic reordering of international relationships, a process that is unlikely to stabilize soon; an unprecedented explosion of technology, carrying with it the potential to alter radically personal and institutional relationships and to change the nature and conduct of warfare; and, persistent global and transnational problems, some of which seem solvable and others that seem very difficult to solve. These challenges will compel the Intelligence Agencies to perform the combat support mission in ways that, in many cases, will be revolutionary.

These circumstances confront not only the Intelligence Agencies, but also policymakers and military commanders. Todays have seen an increase in the frequency of limited employment of military forces, unilaterally and in temporary, multinational coalitions, for operations other than war. These operations focused principally on humanitarian

---

[365] Wilson, T.R., "Global Threats and Challenges Through 2015", Statement for the Record, Senate Select Committee on Intelligence, 7 February 2001, Available on site http://www.dia.mil/Public/Press/statement01.html

[366] Kanwal, G., "The New World Order: An Appraisal—II", Strategic Analysis: A Monthly Journal of the IDSA, Vol. XXIII, No. 4, July 1999, Available on site http://www.ciaonet.org/srchfrm.html,

assistance, peacekeeping, and deterrence; require an indepth understanding of the threat and the operational environment.

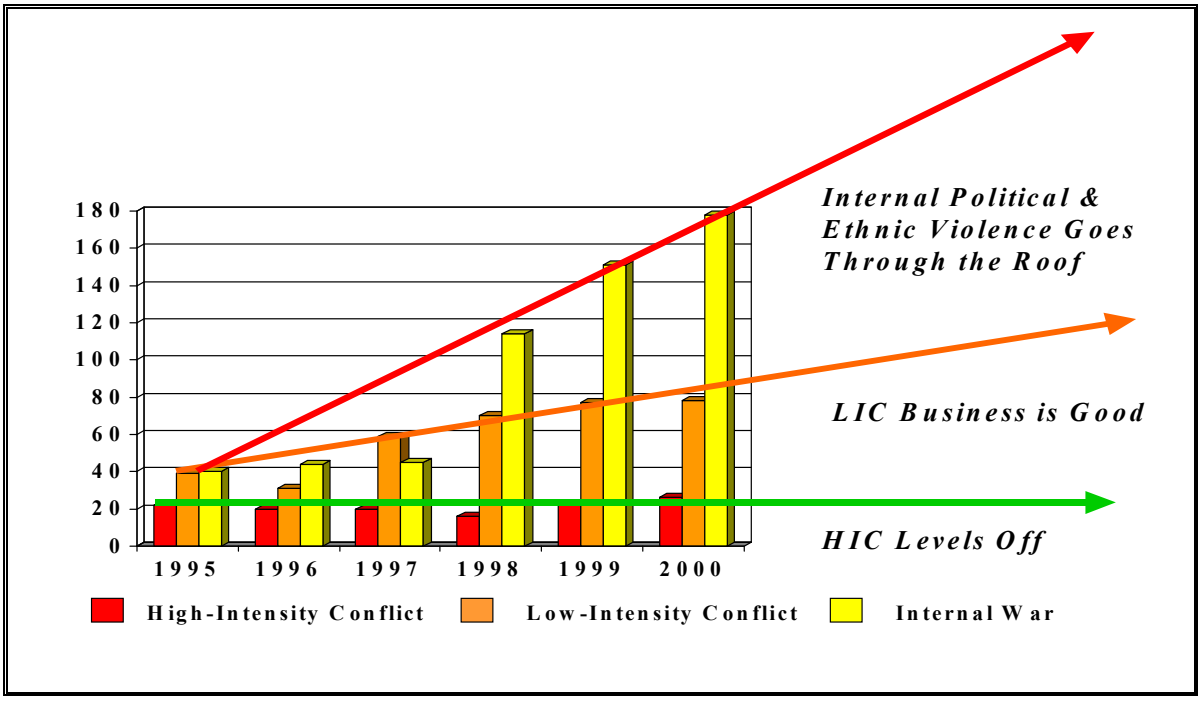
The fact of a smaller military force, coupled with rapid advances in weaponry and related technology. The national security policy of engagement and enlargement has caused to redouble efforts to solve global problems, such as proliferation of weapons of mass destruction, international terrorism, international narcotics trafficking, organized crime, and threats to our information infrastructure and related systems. These are the new threats of our century.

These global challenges and nation's responses provide insight into what the focus of intelligence will be at the beginning of the 21st century: regional orientation, the application of sophisticated technology and a rapidly adaptive approach to all aspects of developing policy and conducting military operations. But main problem is to find the relation between globalization and national security.

1.1.61 Globalization and Need for Security

In our minds the Cold War meaning remain as; odd combination of nonwar (between superpowers) and nonpeace (conflicts and wars which are continued after cold war as illustrated in Figure 5.1) forced the merging of states security roles for maintain and protect economic networks and also for defend against direct threats to national territory.

Figure 0.1 Trends of Wars and Conflicts[367]

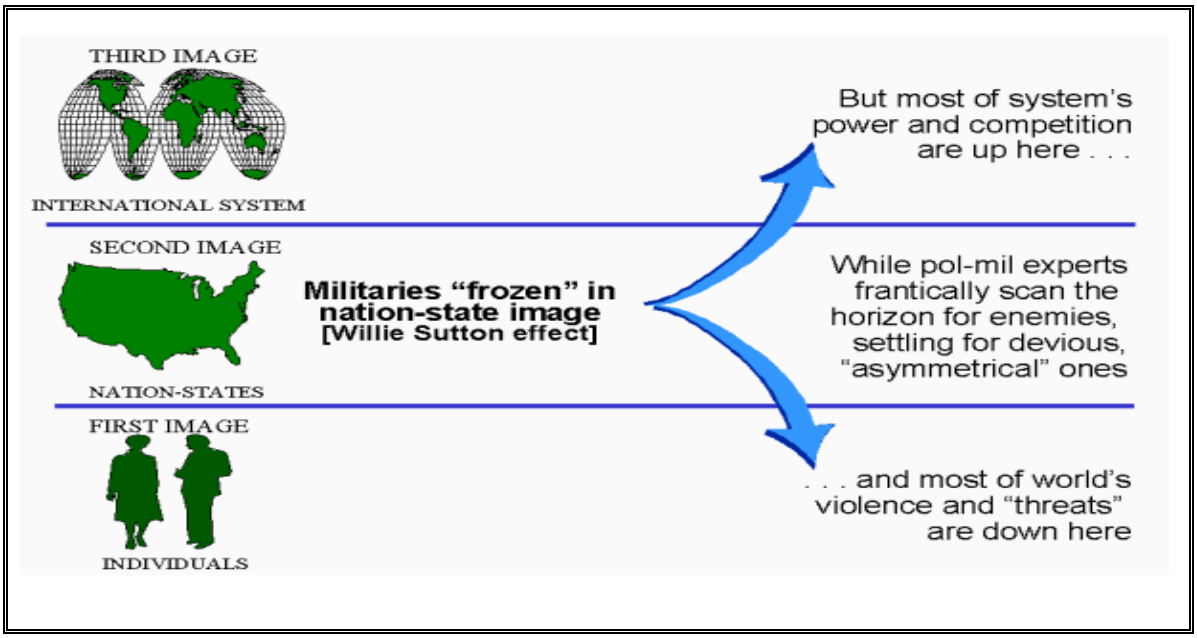


The two functions became one in the Cold War strategy known as containment. Thus subordinating economic rationales to security imperatives. But that strategy died with the start of the globalization era. Now, with the end of the Cold War, the mix of factors affecting national security is changing.[368]

As in Kenneth Waltz's "three images: Man, the State and War" framework in which he investigated the causes behind interstate war across three distinct levels (Figure 5.2: Individual, State, International system.[369]

[367] Steele, R.D., "Threats, Strategy, and Force Structure: An Alternative Paradigm for National Security in the 21st Century", Available on site www.oss.net/Papers/white/Strategy21.doc.
[368] Katzenstein, P., (ed.),"Introduction: Alternative Perspectives on National Security" in The Culture of National Security, Colombia University Press, New York, 1996, p.3
[369] Waltz, K. N., "Man, the State and War: A Theoretical Analysis", Columbia University Press, 1965, in Barnet, T.B.," Life after DoDth: How the evernet changes everything", Available on site http://www.geocities.com/ResearchTriangle/Thinktank/6926/LifeafterDoDth.htm

Figure 0.2 Man, The State and War[370]



In the Cold War, things were fairly straight forward, as both the international system through blocs and individuals through ideologies, were kept in strict subordination to the state centered superpower conflict.

Nation-states have long served as the superior collection point for collective security efforts, but that has begun to change. Two biggest security trends of the globalization era:

- Power and competition have shifted upward, from the state to the system (in the form of the global economy, culture, and communications grid).
- Violence and defense spending have replaced downward, from the state to the individual.[371]

So where can a military fit in this new global environment, where almost all the important crises are either too global or too local for most states to deal with military force? In a world featuring both integrating globalization and disintegrating localization, the great

[370] Waltz, K. N., Ibid.
[371] Barnet, T.B.," Life after DoDth: How the evernet changes everything", Available on site http://www.geocities.com/ResearchTriangle/Thinktank/6926/LifeafterDoDth.htm

challenge facing governments is raising compromises between the two, otherwise known as globalization adapting the local to the global in ways that improve the former's living standards.

Did the end of the Cold War entail the end of the Soviet system?[372] Or was it the other way around? It is possible to imagine a cold war without the USSR, but it is difficult to imagine a Soviet Union without the Cold War. "The Soviet empire was created and built for the arms race, confrontation, and even war with the rest of the world," according to civilian defense expert and Duma deputy Aleksey Arbatov.[373] As long as it existed, a return to the Cold War was still possible and perhaps inevitable.

And in the other side since the end of the Cold War, the number of states undergoing violent disorder and major human-rights problems affecting important sectors of the population has increased substantially. In several instances, internal unrest has generated high tension or conflict with neighboring states, while the flood of refugees has created serious internal socioeconomic and political problems for these states.[374]

International and regional organizations have responded to increased internal violence with a corresponding increase in external intervention, with the goal of mitigating the effects of the internal problems and resolving the some internal conflict. Weapons of mass destruction spread, rogue states threatened their neighbors, and several former soviet client states experienced militant nationalism and ethnic and religious conflicts.[375]

Some of the multinational coalitions of military forces' interventions have been successful, but others have not. Evidence as of 1996 suggests that, once a state has failed, peace does not easily return. The country becomes a battleground for heavily armed factions, many

---

[372] Hobsbawm, E., "The Age of Extremes: A History of the World, 1914-1991", Pantheon Publishing, New York, 1994, p. 250.
[373] Arbatov, A., "The National Idea and National Security", Mirovaya Ekonomika i Mezhdunarodnyye Otnosheniya, 5 May 1998, p. 8.
[374] Institute For National Strategic Studies "1997 Threat Assessment: Flash Points and Force Structure", Chapter Nineteen, Available on site http://www.ndu.edu/inss/sa97/sa97ch19.html
[375] National Intelligence Course (NIC) Textbook, Ibid, Chapter 6, p. 7

with commercial agendas and external connections, who have the unarmed citizenry a their mercy. [376]

It is not clear that the process of change is complete, but three important characteristics are evident. First, the global security environment in diverse and unpredictable than that experienced during the long years of the Cold War. Second, many of the traditional threat activities have not gone away, but remain, even although in a changed or changing form. Third, new types of threats are emerging, as described last year, particularly for the more developed democracies, which have the most to lose from instability.

While the democratic world prospers, much of the rest of the world struggles with increasing instability, which can lead ultimately to threats to the national security and public safety of the countries and citizens of the developed world. Some of the causes and symptoms of instability include the following:

- A lack of democracy and the rule of law in many countries;
- Too many failed and failing states;
- Existing or suspended wars between and within states;
- Numerous cases of potential ethnic and religious conflict;
- Economic disparities between and within states;
- Many examples of territorial and border disputes;
- Migrations of people dislocated from their places of origin;
- Many cases of torture and other violations of human rights;
- Exportable health problems and communicable diseases;
- Food and water availability and scarcity;
- Depleted and depleting environments;
- Exports and imports of weapons of mass destruction;
- The continued use of espionage to gather vital information;
- The increased use of terrorism to further political goals;
- The rise of transnational organized crime; and
- An information environment with many security problems. [377]

---

[376]Institute For National Strategic Studies "1997 Threat Assessment: Flash Points and Force Structure", Ibid.

In this unstable environment, approximately 23-million people are registered with the UN High Commissioner for Refugees, and several times that number are dislocated from their countries of origin. A recent and disturbing trend in countries where the worst population dislocations have occurred is the deliberate targeting of unarmed volunteer relief workers.[378]

Caşın indicates the miscalculation of terrorism, as a theocratic separation instead of ideological hatred of Cold War Era, will not get the peace.[379]

Shortly we can say national security form changed from black and white to gray. Who is my friend or foe and how I struggle with them are the new question marks in our minds? To find a solution I examine this problem in forward sections.

1.1.62 Threat Analysis in 21st Century

While specific threats are impossible to predict, and new threats and challenges can arise almost without warning in today's environment, over the next 12-24 months. The threat in the 21st Century is more complex than ever before and cannot be defined in strictly.

If we want to put this complex structure of future treats as illustrated in figure 5.3 than can be find four threat structure.

The kind of these treats are the traditional nuclear and conventional forces sponsored by a state; those that are violent but not necessarily associated with a state including both transnational criminals terrorists or warlords able to acquire weapons of mass destruction; those that are non-violent and often stateless, including environmental conditions imposing a high "magnitude of human suffering" as well as the refugees from those conditions, the child soldiers bound into armed slavery, and the women and children traded for money and often laden with disease, finally those threats to home defense, be they state-sponsored or not, that surround our critical infrastructures and the core of our economic well-being. At

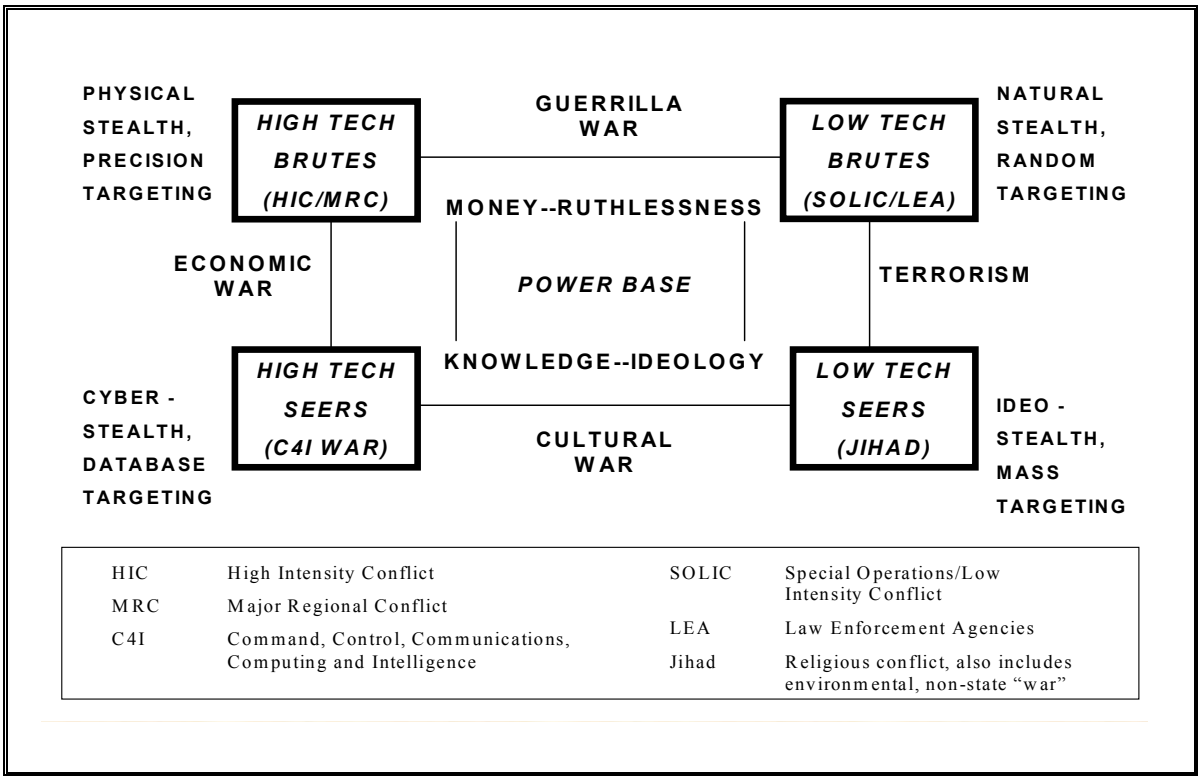
---

[377] Canadian Security Intelligence Service, "1996 Public Report", Available on site http://www.csis-scrs.gc.ca/eng/publicrp/pub1996_e.html
[378] Canadian Security Intelligence Service, "1996 Public Report", Ibid
[379] Caşın, M.H., "Rus İmparatorluk Stratejisi", ASAM Yayınları, Ankara, 2002, p. 408

times, it is ourselves that we have to blame for the scope and imminence of our vulnerability, as is the case with public health.

Seen another way, these four threat classes confront us with four distinct "ways of war": Systemic War, Dirty War, Peacewar, and Cyberwar.[380]

Figure 0.3 Four Threat Classes Requiring Strategic Consideration[381]

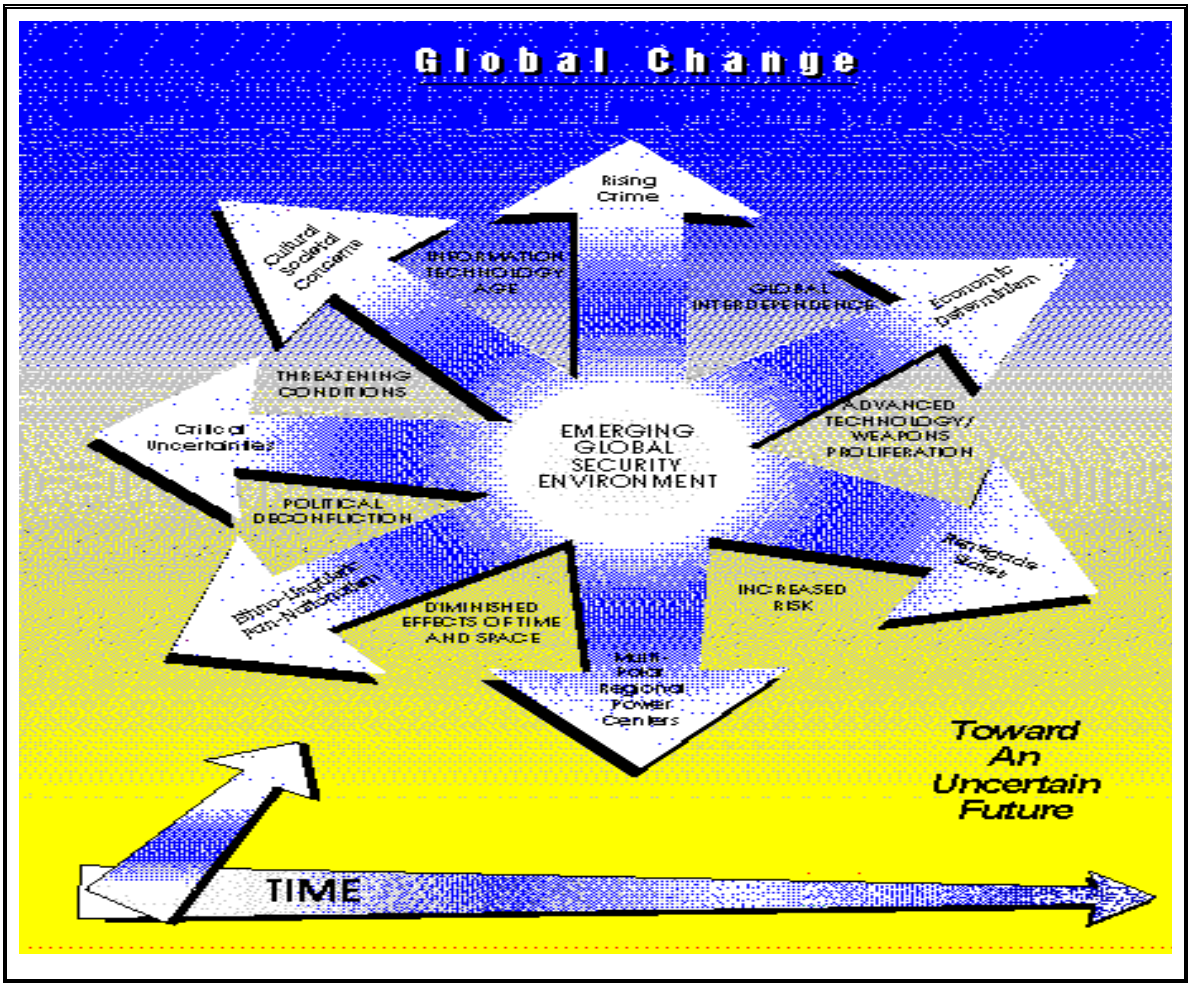


1.1.62.1 Threat Identification

The complexity and variability of threat present us uncertain future as illustrated in figure 5.4. To prevent the danger before existed can be execute by threat identification.

[380] Steele, R.D., "Threats, Strategy, and Force Structure: An Alternative Paradigm for National Security in the 21st Century", Available on site www.oss.net/Papers/white/Strategy21.doc.
[381] Steele, R.D., Ibid.

Figure 0.4 Future of Unpredictable Threat[382]



At the strategic level, the responsibility will be on the intelligence organizations to identify the real and potential threats. In any given operation and location, there are often diverse population groups and other elements that may impact our ability to operate there. In a worst case, these population groups may pit two or more ethnic or religious groups against one another and fight in the midst of drought, disease, or economic collapse. Any demographic mix, especially if compounded by additional environmental threats, can threaten the ability to successfully complete our mission. Therefore, needs to evaluate the big picture, the national or at least regional capabilities and limitations of each potential

[382] Vector 21, "The Defense Intelligence Architecture", A Strategic Plan for the Defense Intelligence Agency, Available on site http://www.fas.org/irp/dia/vector21/

threat, and identify those most likely to threaten the mission. Once we have identified these strategic capabilities, limitations, and threats.[383]

1.1.62.2 Media Analysis [384]

There is no longer any doubt that the most of the nation's audience has the proven ability to force the withdrawal of troops from an area because of its intolerance for casualties and collateral damage. This is the result of civilization and technologic developments such as telecommunication and media sectors.

Strategic planners must ensure they consistently relay the mission's objectives and methodology to the relevant domestic audiences. Accomplishing this requires an understanding of the culture, as discussed above, to ensure that hostility is not bred by accident. It also requires extensive investigation into who controls the media and how they propagate messages throughout a population. For instance, does the population draw most of its information and perceptions from locally owned newspapers or electronic media or do they rely on the international media such as CNN or Al-Jazeera satellite TV? (We saw the effectiveness of these channels in Afghanistan). Is there one person or a few in the locale that help mold these messages? What is the current theme to which the population adheres or listens, and, if necessary, how can we counter this theme?

There are many more considerations that analysts could and need to investigate during the conduct of strategic level. The three identified above are among the most important and except for threat; there is little approved supporting doctrine.

I don't give details about media. This subject should be taken especially with the terrorism. But today's world has much influence under the media devices. It is obviously effect the form and structure of intelligence.

Shortly I can say before media influences the intelligence, intelligence should give a direction and orientate the information.

---

[383] Medby, J., "IPB Considerations at the Strategic Level", Military Intelligence Professional Bulletin, Apr/Jun 2002, Vol. 28, Issue 2, p.26
[384] Medby, J., Ibid, p.26

1.1.63 Future Conflicts

Through 2015, internal conflicts will pose the most frequent threat to stability around the world. Interstate wars, though less frequent, will grow in lethality due to the availability of more destructive technologies. The international communities will have to deal with the military, political, and economic dimensions of the their adversaries or potential risky states for themselves.

1.1.63.1 Internal Conflicts[385]

Many internal conflicts, particularly those arising from communal disputes, will continue to be vicious, long-lasting and difficult to terminate leaving bitter legacies in their wake.

- They frequently will spawn internal displacements, refugee flows, humanitarian emergencies, and other regionally destabilizing dislocations.
- If left to fester, internal conflicts will trigger spillover into inter-state conflicts as neighboring states move to exploit opportunities for gain or to limit the possibilities of damage to their national interests.
- Weak states will spawn recurrent internal conflicts, threatening the stability of a globalizing international system.

Internal conflicts resulting from state repression, religious and ethnic grievances, increasing migration pressures, and/or indigenous protest movements will occur most frequently in Sub-Saharan Africa, the Caucasus and Central Asia, and parts of south and southeast Asia, Central America and the Andean region.

1.1.63.2 Transnational Terrorism[386]

States with poor governance; ethnic, cultural, or religious tensions; weak economies; and porous borders will be prime breeding grounds for terrorism. In such states, domestic groups will challenge the entrenched government, and transnational networks seeking safehavens.

---

[385] CIA, "Global Trends 2015", Available on site http://www.odci.gov/cia/publications/globaltrends2015/index.htm

[386] CIA, "Global Trends 2015", Ibid.

At the same time, the trend away from state-supported political terrorism and toward more diverse, free-wheeling, transnational networks will continue. Between now and 2015 terrorist tactics will become increasingly sophisticated and designed to achieve mass casualties. We expect the trend toward greater lethality in terrorist attacks to continue.

1.1.63.3 Interstate Conflicts[387]

Over the next 15 years, the international system will have to adjust to changing power relationships in key regions:

- **China's potential**. Estimates of China beyond five years are fraught with unknowable. Some projections indicate that Chinese power will rise because of the growth of its economic and military capabilities. Other projections indicate that the array of political, social, and economic pressures will increasingly challenge the stability and legitimacy of the regime.
- **Russia's decline**. By 2015, Russia will be challenged even more than today to adjust its expectations for world leadership to the dramatically reduced resources it will have to play that role. The quality of Russian governance is an open question as is whether the country will be able to make the transition in a manner that preserves rather than upsets regional stability.
- **Japan's uncertainty**. In the view of many experts, Japan will have difficulty maintaining its current position as the world's third largest economy by 2015. Tokyo has so far not shown a willingness to carry through the painful economic reforms necessary to slow the erosion of its leadership role in Asia. In the absence of an external shock, Japan is similarly unlikely to accelerate changes in security policy.
- **India's prospects**. India will strengthen its role as a regional power, but many uncertainties about the effects of global trends on its society cast doubt on how far India will go. India faces growing extremes between wealth and poverty, a mixed picture on natural resources, and problems with internal governance.

These regions were determined by U.S. So every state has a plan or evaluates the regions according to their geo-politic and geo-strategic situation.

---

[387] CIA, "Global Trends 2015", Ibid.

1.1.63.4 Transnational Criminal Activity (TCA)

The impact of transnational criminal activity (TCA) is a global concern, and one that is growing stronger and becoming more pervasive. Acting from bases around the world, TCA organizations have the power and wealth to project their influence globally, regardless of borders or sovereignty. [388] These powerful criminal syndicates and the illicit funds generated from their illegal activities pose a significant threat to states' national and economic security. TCA organizations can undermine the integrity of public and private institutions, adversely affect financial markets and the banking sector, and threaten key sectors of national economies. [389]

1.1.64 Changing The Nature of Strategy

Fundamental strategic thinking should include an appreciation for the fact that a national security strategy must be holistic managing all sources of national power including diplomacy, economic assistance, cultural outreach, and information operations, not just the military simultaneously. "War proper" is not just about military force, but rather about imposing one's will and assuring one's security in a complex world. Within this larger context, power without purpose is wasted, time is priceless, technology is not a substitute for strategy or thinking, asymmetric threats must receive co-equal attention with symmetric threats, and strategic culture matters.

Determining national security strategy for the 21st Century must therefore be guided by two related principles: co-equal standing for asymmetric versus symmetric threats; and co-equal structure and funding, or at least some semblance of a rational balance, between military forces designed for the traditional symmetric threat, and largely unconventional or non-military forces designed to deal with the asymmetric threat.

On this basis, "forward engagement" and "shaping" of the theater environment make a great deal of sense, but with two caveats: there must be a force structure as well as funding for non-military investments, and we are probably better off talking about "nurturing"

---

[388] CIA, "Global Trends 2015", Ibid.
[389] Canadian Security Intelligence Service, "2001 Public Report" Available on site http://www.csis-scrs.gc.ca /eng/publicrp/pub2001_e.html

peaceful environments instead of the more imperial "shaping." At a minimum a strategy that is seriously committed to force protection through economic, cultural, and information peacekeeping must recognize the vital role played by the non-governmental organizations (NGO), the critical importance of being able to communicate and cooperate with indigenous organizations that are not part of a military force, and the overwhelming influence on any situation of environmental conditions including the availability of clean drinking water, sufficient food for the children, and such medical provisions as might be needed to at least keep disease from spreading through epidemics.

New national security strategy must actually have five elements that are in complete harmony with one another: global intelligence strategy, for ensuring that we can maintain global coverage and global warning; interoperability strategy, for ensuring that what we build and buy is interoperable with both military and civilian coalition partners in a wide variety of "come as you are" circumstances; force structure strategy for ensuring that we build to both the most likely as well as the worst case threats while balancing the relative roles of our military, the reserve force, the private sector, and external allies or coalition partners; preventive diplomacy strategy for directly addressing conditions around the globe that spawn conflict and crises; and finally, home front strategy for fully developing and integrating the defensive capabilities of state & local governments and the private sector.

1.1.65 Terrorism is the New Enemy

There are some who claim intelligence never met a threat it did not like. The true situation is that intelligence only reluctantly gives up threats it knows best. Today's threats are different from yesterdays and in many respects considerably less predictable. These uncertain threats (regional, low-intensity conflict, terrorism, nuclear proliferation, and chemical and biological weapons) have emerged as defense intelligence's new priorities. Equally important is supporting the expanding involvement of military forces in efforts to alleviate global stress points, whether they involve the use of force or the provision of assistance.[390]

---

[390] Clapper, J.R., "Challenging Joint Military Intelligence", Joint Force Quarterly (JFQ), Spring 1994, pp. 92-95

The ICs are still responsible for providing the best possible intelligence on regional force capabilities, plans, dispositions, and objectives. It also retains the requirement to understand the conflict environment, whether the mission is containing aggression, keeping the peace, or feeding the starving.[391]

The indicator of new enemy is started at 1997; trends in international terrorism mix the old and the new and included the following:

- Continued sponsorship of terrorist organizations by a few states;
- Intractable conflicts in the Punjab, Middle East and elsewhere;
- The continued rise of Islamic and other forms of religious extremism;
- Increasing right-wing extremism in developed countries;
- Declining left-wing extremism, except in opposition to the right;
- Rejection of what is perceived elsewhere to be Western cultural imperialism;
- Nationalism and separatism as primary motivators for terrorism;
- The use of terror by alienated groups, less understood and less predictable;
- Hostage-taking to extort money from governments and multi-nationals;
- The search by terrorists for weapons of mass destruction; and
- The exploitation of communications technology for cyber-terrorism. [392]

Activities are selected and used by terrorists in proportion to their demonstrated success or failure, as reported instantaneously by the worldwide news media. The hostage-taking at the Japanese embassy in Lima, Peru is one example. The challenge for governments is to devise responses appropriate to the given crisis that will be neither an overreaction nor a violation of democratic values. [393]

---

[391] Clapper, J.R., Ibid, pp.95-99
[392] Canadian Security Intelligence Service, "1996 Public Report" Available on site http://www.csis-scrs.gc.ca/eng/publicrp/pub1996_e.html
[393] Canadian Security Intelligence Service, "1996 Public Report", Ibid.

1.1.65.1 The Changing Face of Terrorism and Technology[394]

The political symbolism of successful terrorist attacks is also often far greater than the casualties, and even an empty threat can help to undermine the fabric of social trust upon which the democracy is based.

This is also one area where the world has really changed since the end of the Cold War. To predict what capabilities terrorist organizations, hostile states, extremists and movements will acquire over the next 15-25 years. Today we can, however, predict that there are several major areas of technological change that can radically alter the effectiveness of asymmetric and terrorist attacks and which require care attention from the intelligence communities:

- The vulnerability of critical infrastructure is changing: The financial systems, communications systems, utilities, and transportation nets are far more tightly integrated than in the past, and we rely far more on national and regional systems, rather than large autonomous local ones. This reduces vulnerability in some ways, but increases vulnerability in others. Systems netting and integration involves shifts in technology that need careful examination.
- Information systems create new vulnerabilities: It is all too possible to grossly over-exaggerate dependency on information systems, their vulnerability, and the difficulty in finding work-arounds, and reconstituting critical systems. Many statements are being made that have no real analytic underpinning and the importance of given systems is poorly researched. The Internet, in particular, is being glamorized to the point of absurdity. Nevertheless, information systems have become part of our critical infrastructure, and virtually invisible cyber attacks may prove to be more lethal in some cases than high explosives. New physical methods of attack, such as EMP weapons, may also be becoming more practical.
- Chemical weapons and toxins are changing: It is impossible to discuss fourth generation chemical weapons in an unclassified forum. The technology and equipment for

---

[394] Cordesman, A.H., "The Changing Face of Terrorism and Technology, and the Challenge of Asymmetric Warfare", Center for Strategic & International Studies, Available on site http://www.csis.org/hill/ts010327cordesman.htm

older types of chemical weapons is also proliferating at a civil level and becoming steadily more available to governments, extremist movements, and individuals.

- Biological weapons are changing: It has been possible to make dry storable biological weapons with nuclear lethality since at least the late 1950s. Advances in biotechnology, food processing equipment, pharmaceuticals, and other dual-use facilities and technologies are also proliferating at a civil level and becoming steadily more available to governments, extremist movements, and individuals. These problems are compound by the rapid spread of expertise and equipment for genetic engineering. The end result is that the technology of attacks on humans, livestock, and crops is becoming steadily more available, and in forms which not only can be extremely lethal and/or costly, but difficult to attribute to a given attacker.
- The availability of nuclear weapons may change: It is far too soon to say that broad changes are taking place in the nuclear threat. Nevertheless, the break up of the FSU, and proliferation in India and Pakistan, does create a growing risk that fissile material may become more available for "dirty" and low yield weapons, and the knowledge of how to make crude nuclear devices, handle the high explosives, provide neutron initiators, and deal with the complex triggering problems is also spreading.
- The risk from radiological weapons may change: Radiological weapons have not been particularly attractive options in the past. There is, however, a steadily growing mass of nuclear waste, and some studies indicate that the long-term genetic effects of such weapons may be more serious than their short-term effects.
- The ability to exploit the media and psychological dimension of new technologies has grown: Far more is involved than body counts, physical damage, and economic loss. The spread of mass communications, and use of tools like the Internet and Satellite TV, also increases the impact of attacks.

It is all too easy to exaggerate today's threat in each of these areas, but it is equally easy to exaggerate the difficulties that individual terrorist movements and extremists now face in using such technologies. There is a clear need to examine how states can use such weapons covertly or through proxies, and forecast how widely spread each of these threats is likely to become in the future.

1.1.65.2 Intelligence and Low-Intensity Conflict (LLC)

A new concept appeared “Low-Intensity Conflict (LLC)” which threats include insurgency and counterinsurgency, terrorism, peacekeeping operations, "show of force" operations, and counter narcotics, among others. Prior to Desert Storm, the threats from LIC were attracting significant attention. These threats have not gone away, and the arguments made concerning the intelligence problems presented by LIC still apply.

LIC military forces are generally different from conventional military forces. Thus, intelligence resources previously effective against the USSR are neither appropriate nor effective when dealing with LIC. For example, detecting a single small aircraft transporting terrorists or drugs requires different equipment and different skills from those used in tracking waves of attacking military aircraft. [395]

Similarly, people who need intelligence to deal with LIC are likely to have different operational requirements and constraints. During a full-scale war, for instance, any vehicle detected in a designated free-fire zone would generally be considered hostile and destroyed. In contrast, in a short-of-war combat situation avoiding collateral damage or friendly-fire casualties is critical. As a result, precise identification of individual targets is essential.

Finally, the intelligence communities are witnessing a growth in demands for information having little or nothing to do with military operations. The most obvious nonmilitary threats are terrorists and corrupt business or political figures who are beyond the legal jurisdiction of the states but who can still harm states interests.[396]

Additionally, less malevolent but equally significant developments will require intelligence, such as population trends, the refugee problem, international economics and natural phenomena, such as the global spread of disease and pollution.

---

[395] Berkowitz, B.D. and Goodman, A.E., Why Spy--And How--In The 1990s?, Orbis, Spring 92, Vol. 36 Issue 2, p. 269

[396] Gries, D.D., "Intelligence in the 1990s," Studies in Intelligence 35, Spring 1991, p. 9.

1.1.65.3 Reflection of September 11th on Security Mentality

The magnitude of the September 2001 attacks changed the nature of the threat environment in the world, demonstrating the ability of a terrorist network to strike anywhere within its possibilities. International terrorist networks, including the superior threat of terrorist organizations, present complex global security implications. Terrorist operations conducted by extremists, exemplified by Osama Bin laden and the Al Qaida network; continue to demonstrate their willingness to use lethal force, inflicting mass casualties with no distinction between civilian and military personnel.

Although terrorism have great impact on states, in the other hand the proliferation of weapons of mass, transnational criminal activity have also directed administration of states.

All struggles with these concepts accelerated with attack on US. But in reality some states like Turkey had problems to find the international support until this event. But new phase of union struggle with international terrorism and its supporters started with this attack and indicator of this union struggle is Afghan war.

The events of September 11th, 2001 precipitated not only a significant shift in the global threat level, but also in the ensuing response by the Service. Public safety and safeguarding against the possibility of a terrorist attack occurring in, or originating from, all states were already the highest priorities of the Service, with terrorist organizations being the lead investigation within the Counter Terrorism program. [397]

In addition to the threat posed by the terrorist network, which undertook the attacks, other traditional and emergent issues also occupy the Service in the areas of public safety and national security. The global security environment remains unstable given the continued willingness of groups, individuals and states to use serious violence in support of political, religious or ideological agendas. [398]

---

[397] Canadian Security Intelligence Service, "2001 Public Report" Available on site http://www.csis-scrs.gc.ca/eng/publicrp/pub2001_e.html

[398] Canadian Security Intelligence Service, "2001 Public Report", Ibid.

To examine this new form firstly we should look the new enemy "terrorism" and its effect on national security and intelligence structure.

1.1.65.4 Struggle With Terrorism (Counter Terrorism)

Terrorism today is more complex, more extreme, more sophisticated and more transnational than ever before. The capacity of the modern terrorist has been enhanced by advanced communications technology and the speed and ease of international travel. Geographic constraints on the spread of terrorism have become almost non-existent. Today's terrorists are often well educated, more operationally adept and technically sophisticated, taking advantage of encryption devices and other communications technology such as cell phones and satellite communications. They are less predictable, willing to forge alliances of convenience and to use extreme violence, with large-scale destruction, to achieve their aims.[399]

So struggle with terrorism need much information and effective intelligence. To make terrorism from unclear to clear can only be by intelligence.

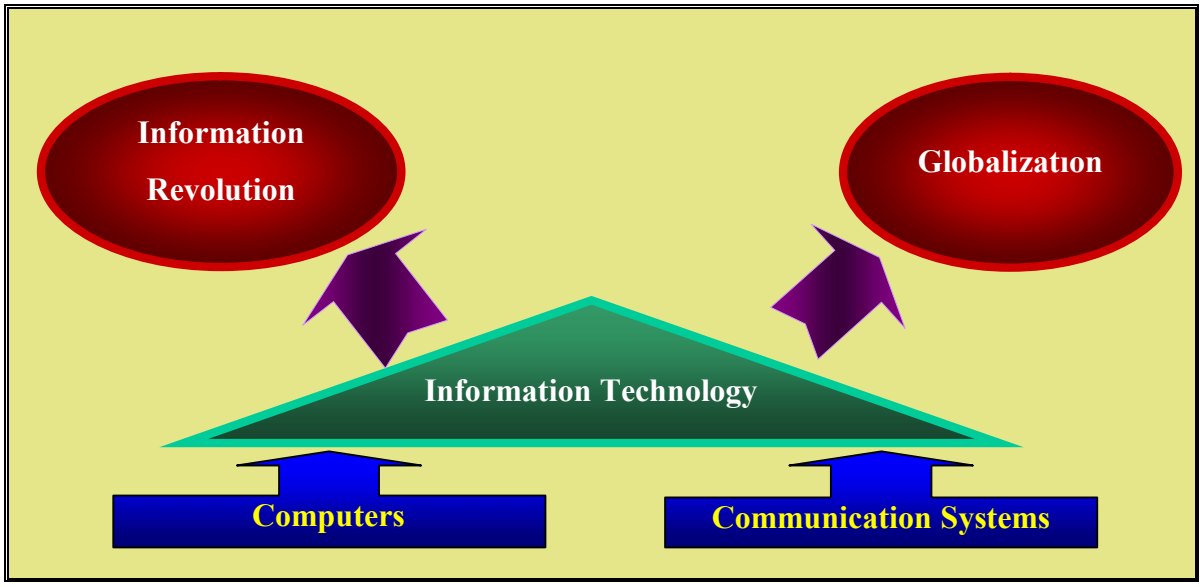
1.1.66 Information Revolution and Defense Industry

Spectacular advances in information technology over the last decade are changing the whole nature of political governance and its relation to defense industry and national security. Indeed, world itself has been materially affected by the arrival of the information superhighway, the Internet, the impact of multi-media on all sectors. By the world have turned into a global village virtually overnight. Gajendra Upadhyay declared 1996 as the year of Internet.[400] The Internet is gradually moving people towards the "one people, one planet" point of evolution. Internet is an information technology which relation with globalization and information revolution can be seen in figure 5.4.

---

[399] Canadian Security Intelligence Service, "2001 Public Report", Ibid.
[400] Upadhyay, G., "Will 1996 Be The Year of Internet?" Business World, January 24, 1996, pp. 144-145

Figure 0.5 Information Systems With Globalization



The globalization of technology, the integration and fusion of various technological advancements, and unanticipated applications of emerging technologies, make it difficult to predict the technological future. Regarding military technology, two other trends – constrained global defense spending, and the changing global armaments industry – will affect the nature of future conflict.[401]

The reliance of the modern world upon information infrastructures—the vast interconnected networks of computers and telecommunications equipment—has created vulnerabilities that are of significant national security concern. [402]

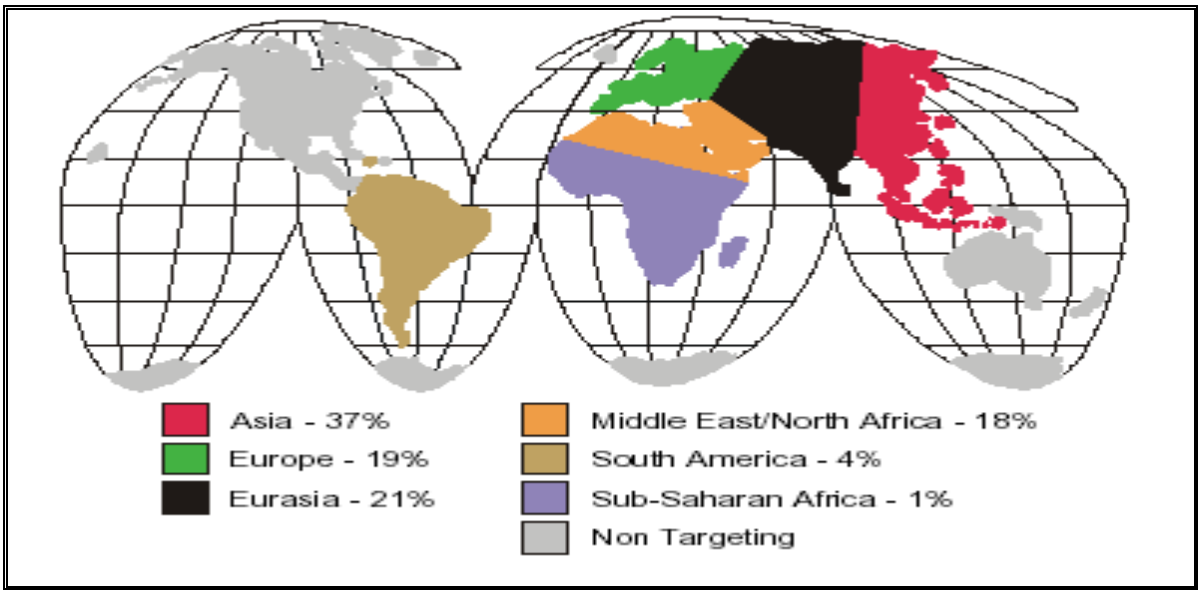
Due to the increased denial and non-response by cleared defense industry to foreign requests for information, foreigners will employ other collection methods and target different cleared facilities. This highlights the importance of reporting suspicious activity across the nation and overseas. Information Systems remained the most sought militarily critical technology category in 2003.

In figure 5.6 illustrated denotes regions of the world from where collection efforts reportedly originated. The percentages indicate the level of collection activity reported in

[401] Wilson, T.R., "Global Threats and Challenges Through 2015", Statement for the Record, Senate Select Committee on Intelligence, 7 February 2001, Available on site http://www.dia.mil/Public/Press/statement01.html
[402] Canadian Security Intelligence Service, "2001 Public Report", Ibid.

2000. The map does not imply national level support of the collection activity. The collector may have based their operation in a third country to conceal intentions such as the ultimate end-user of the research or technology. [403]

Figure 0.6 Worldwide Targeting Effords [404]



Now, surfing the Internet provides access to an exploding amount of information. By one estimate, stored information is doubling every two years.[405] The challenge for intelligence is new only in magnitude. But the change in magnitude is awesome. There is so much more information out there, and so much more of it is misleading because, in effect, anyone with a computer can now produce or "publish" anything. The risk that hackers, who may be simply curious kids but who also may have more evil motives, can enter restricted databases is well known if not yet well addressed. But in some respects, the harder problem for intelligence arises simply from volume, not evil intent: As "publishing" gets easier, standards of verification go down. Collecting information is less of a problem, and verifying it is more of one. This means that policymakers will be more, not less, reliant on information brokers. The images that are sometimes evoked of policymakers surfing the

---

[403] Mooney, M., Norvell, J., and Smith, S., "2001 Technology Collection Trends in the U.S. Defense Industry", Defense Research and Technology Horizontal Protection Publication, p. 32
[404] Mooney, M., Norvell, J., and Smith, S., Ibid, p. 32
[405] Simonds, L., "Magnetoelectronics Today and Tomorrow," Physics Today, April 1995, Available on site www.aip.org/pt/cont9504.html

Net themselves, in direct touch with their own information sources, are very misleading. Most of the time, as their access to information multiplies, their need for processing, if not analysis, will go up. If collection is easier, selection will be harder.

The more-open world is blurring the distinction between collection and analysis. The best looker is not a spymaster, much less an impersonal satellite, but someone steeped in the substance at hand in short, an analyst. By the same token, while reference librarians used to be able to point scholars toward reliable sources, the sources on the Net are many, but their reliability is dubious. So consumers need to beware of those who surf the Net but are not themselves experts: Who knows what such people might make of the Net's mix of fact, fancy, and pure error? To be sure, those who do the surfing or the looking need to be connected to the rest of intelligence.[406]

1.1.66.1 Trends in Global Defense Spending and Armaments

Defense-related technologies will advance rapidly over the next 15 years (particularly precision weapons, information systems and communications). The development and integrated application of these technologies will occur mostly in the advanced countries.

The most critic process to gather national competition is to gather technologic advances process.[407] Given the high costs and complexity of technical and operational integration, few nations will assign high priority to the indigenous development of such military technology. Such as;

- Non-US global defense spending has dropped some 50 percent since the late 1980s. "Military modernization accounts," particularly procurement, have been hit hard.
- The global arms market has decreased by more than 50 percent during the same period.

---

[406] Treverton, G. F., "Reshaping National Intelligence for an Age of Information" Cambridge University Press, Cambridge, 2001, pp.45-46

[407] Yetiş, N., "Ulusal Güvenlik Sisteminin Geliştirilmesinde Stratejik Teknoloji İşbirlikleri", 2000'li yıllarda Uzay, Havacılık ve Savunma Teknolojilerinin Öncelikleri Sempozyumu, Bildiriler, İstanbul, 29-30 Nisan 1999, Cilt: 1, p.71

- Indications are that global defense spending may be recovering from mid-1990s lows; part of East Asia, for example, could experience rises in defense spending over the next decade, but, overall, long-term spending patterns are uncertain.

Over the past decade, a slow but persistent transformation has occurred in the arms procurement strategies of states. Many states are attempting to diversify sources of arms for reasons that vary from fears of arms embargoes, to declining defense budgets, or to a desire to acquire limited numbers of cutting-edge technologies. Their efforts include developing a mix of indigenous production; codeveloping, coproducing, or licensing production; purchasing entire weapon systems; or leasing capabilities. At the same time, many arms-producing states, confronted with declining domestic arms needs but determined to maintain defense industries, are commercializing defense production and aggressively expanding arms exports. Together, the above factors suggest:

- Technology diffusion to those few states with a motivation to arm and the economic resources to do so will accelerate as weapons and militarily relevant technologies are moved rapidly and routinely across national borders in response to increasingly commercial rather than security calculations.
- Technological superiority will be difficult to maintain for very long. In an environment of broad technological diffusion, nonmaterial elements of military power (strategy, doctrine, and training) will increase in importance over the next 15 years in deciding combat outcomes.
- Export regimes and sanctions will be difficult to manage and less effective in controlling arms and weapons technology transfers. The resultant proliferation of WMD and long-range delivery systems would be destabilizing and increase the risk of miscalculation and conflict that produces high casualties.
- Advantages will go to states that have a strong commercial technology sector and develop effective ways to link these capabilities to their national defense industrial base. States able to optimize private and public sector linkages could achieve significant advancements in weapons systems.

The twin developments outlined above, constrained defense spending worldwide combined with increasing military technological potential, preclude accurate forecasts of which

technologies, in what quantity and form, will be incorporated in the military systems of future adversaries. In many cases, the question will not be which technologies provide the greatest military potential but which will receive the political backing and resources to reach the procurement and fielding stage. Moreover, civilian technology development already is driving military technology development in many countries.[408]

1.1.67 Managing the Risk

Security intelligence is a risk-management enterprise. There is no realistic number of personnel or financial resources that could ensure all possible scenarios involving threats to national security are covered. The task of addressing the spectrum of potential threats involves ongoing threat and risk analysis, priority setting and the flexible application of available resources. [409]

Management flexibility, however, is limited by the pace at which new resources can be brought on board. It takes time for new personnel to be recruited and fully trained. For example, a new intelligence officer follows a five-year training and development program. Once the new employees are fully trained and functioning, the Service will be better positioned to return to the equilibrium it maintained among the forces that impinge upon risk management of the global threat environment. [410]

1.1.68 Spy Is Still Going On?

Thirteen years after glasnost and more than nine years after the breakup of the Soviet Union, Russians and Americans still spy on each other with Cold War era gusto. Computers, spy satellites, tunnels under embassies and super sensitive microphones have updated the game. But as the evidence unveiled in the Hanssen case indicates, much of the "tradecraft" of today's spy could have been lifted from a 1950s potboiler.

"The only thing that has changed in this business in 2,500 years is the technology," says Rusty Capps, a former FBI counterintelligence specialist who teaches at the private Center

---

[408] CIA, “Global Trends 2015”, Ibid.
[409] Canadian Security Intelligence Service, “2001 Public Report”, Ibid.
[410] Canadian Security Intelligence Service, “2001 Public Report”, Ibid.

for Counter Intelligence and Security Studies, a private intelligence training facility in Alexandria, Va. "And some of that hasn't changed much." [411]

The Soviet Union collapsed in 1991, but the Russians had several reasons to keep on peeping." You're talking about something that's engrained, that goes back to at least Peter the Great," says Cannistraro, referring to the nation's first Romanov czar who reigned in the 17th and 18th centuries. "That doesn't change overnight." But former Russian intelligence officers cite another reason to keep their spy work going: job security. [412]

"Technology may tell you basically everything about an opponent's capabilities," Capps says. "But the only way to divine his intentions is to develop a human relationship." Shvets sees the issue differently but comes to the same conclusion." At the Russian Embassy (in Washington) today, you've got maybe 50 spies, and 45 of them are drinking coffee and reading the paper," he says. "If you stop (spying) entirely, everybody's out of work. And so the show must go on." [413]

1.1.69 Intelligence In The Information Era

This kind of information from commercial satellite companies, combined with the increasing volume of data passed via cell phones, the Internet and other electronic sources, is making an unprecedented amount of security information much more easily collectible and available for any interested observer.

By all accounts, the role of information in both statecraft and warfare is growing. Information technologies are creating greater "transparency" in political and military affairs. The word in this sense refers to the fact that is fewer and fewer secrets: Information about the characteristics of a government or military entity (or the location and condition of a downed plane, for example) is available to any foreign government, non-governmental organization or individual. And the rapid availability of the data increases the pressures on decision makers, who need to identify which information is relevant in any given situation

---

[411] Willing, R.," Little changes in world of spying, experts say", Available on site http://www.ci-ce-ct.com/article/showquestion.asp?faq=5&fldAuto=1260

[412] Willing, R., Ibid.

[413] Willing, R., Ibid.

and respond faster than ever to a public and other governments that have access to virtually the same material. [414]

The challenge for intelligence is different than during the Cold War. There are many more potential adversaries, and the targets are increasingly informed and witting of traditional intelligence methods. Where it is possible to have them, secrets are more important than ever for maintaining a security edge in the world.

This opens the door to the need for radically new types of intelligence gathering and analysis. Rather than try to compete with the new technologies and the information they provide, intelligence services can specialize in providing data and analysis that is unavailable by any other means. Among the many ways to do this are to reinvigorate the use of intelligence agents, increase long-term analysis, fuse together complex intelligence data and pursue the state of the art in remote sensing, whether from aircraft, space or elsewhere. While various studies have identified weaknesses in these areas, there needs to be more strategic vision about how to fix them. [415]

Rather than revisit the stale debate about whether the country should be investing more in satellites or spies, we would be wise to recognize the value of a diverse, creative and continuously updated strategy of collecting and analyzing security information, using a combination of people and technology.

In the face of the power of technology to gather raw data very rapidly, the intelligence agencies would do best to focus on exploiting open sources of information, collecting specialized data and on the broader view that good analysis can bring to bear. Rather than perpetuate a recent debate about whether intelligence focuses too heavily on short-term military threats at the expense of longer-term strategic problems. Among these are the needs to increase funding for intelligence and emphasize analysis over collection.

Intelligence agencies need to spend fewer resources exploiting conditions in foreign countries and end the current tendency to chase breaking news in an attempt to be responsive to policy-makers. While some of this is necessary, too much leaves the intelligence communities unable to support important, long-term missions such as strengthening homeland defense and curbing nuclear arms proliferation and terrorism.

---

[414] O'Connell, K.M., "Intelligence in the Information Age: Spy Data for Sale", Newsday, April 8, 2001, Available on site http://www.rand.org/hot/op-eds/040801ND.html

[415] O'Connell, K.M., Ibid.

Whatever the merits of the programs, the new administration's embrace of missile defense and space control will require enormous investments in intelligence information gathering and analysis. [416]

1.1.69.1 Counterintelligence

Counterspies will be forced to adapt and accelerate the use of digital tools in an effort to catch foreign spies. Hostile services will resort to powerful neural networks and massive databases to analyze information about individuals to identify and apprehend foreign spies.

Imagine the difficulties in establishing "legend" and "cover" in the digital world. Traditional identity details such as address, profession, association membership, etc. are now subjected to a new level of scrutiny using the Internet. However, simple details can be quickly challenged by using the Internet to search local property tax records, voting records, professional association memberships, etc. Establishing an effective cover and legend now requires the investment of additional resources and planning in the digital age.[417]

INTELLIGENCE AND POLICY

Intelligence and policy are such different cultures that it is a surprise that they ever connect at all. Intelligence analysts still work in a world of paper, while policy is mostly an oral culture. Analysts think analytically of what can go wrong, while policy officials tend to think wishfully of what might go right. Analysts, focused on events abroad, take a long view and tend to presume that the world is largely impervious to actions. Policy officials, by contrast, have a perspective that is dominated by the short term and by their own personal stakes.[418]

Tactical puzzles where secrets matter are both fewer and more varied today than they were in the Cold War, but they are still important. For solving puzzles, analysts need to be close

---

[416] O'Connell, K.M., Ibid.
[417] Cadena, L., "Rethinking the Missions and Priorities of the Intelligence Community", 1997. Available on site http://www.fas.org/irp/eprint/snyder/priorities.htm
[418] Treverton, G. F., "Reshaping National Intelligence for an Age of Information" Cambridge University Press, Cambridge, 2001, p. 17

to the collectors of secrets. In a world of too much information, policymakers will want to "pull" up what they need, not have information "pushed" upon them[419]; they will want to pull up puzzle solutions when they need them, not receive a torrent of information whether they ask for it or not. Yet solving the puzzle is often important enough that getting policy officials to pay attention is not a problem. [420]

This is very different from puzzle solving. For it, analysts need access to secrets, but their crucial partnerships are those with colleagues outside intelligence and outside government, in the academy and think-tank world, in NGOs, and in the world of private business. Intelligence needs to be opened wide, not cosseted in secret compartments. For these purposes, a kind of government wide designated reader, a version of the Congressional Research Service, could help. New government institutions are not much in fashion these days; nor are new connections of public and private, at least not in what is still called the "national security" realm, though that will change in the era of the market state. [421]

This is based on the recognition that intelligence's business is information, not secrets, and that its product is people, experts, not paper.

A successful foreign policy, however, depends upon bridging this intellectual gap between the imperatives of the present and the potential of the future. In turn, this often depends upon bridging the gap between policymakers and the intelligence communities. Policymakers need to ensure that you in the intelligence community are not working in a vacuum, that you know what is on our minds and what questions we need answered. At the same time, you in the intelligence community have the responsibilities of seeking out policymakers, understanding their concerns, and telling them what they should be paying attention to. It is important to tell policymakers what they need to hear, not what they want to hear. [422]

---

[419] For "push" and "pull" control principles see at chapter 4, p.101.
[420] Treverton, G. F., Ibid, p. 17
[421] Treverton, G. F., Ibid.
[422] Haass, R.N., "Policymakers and the Intelligence Community in This Global Era," Remarks to CIA Strategic Assessments Group Annual Conference, Wilmington, 2001,Available on site http://www.state.gov/s/p/rem/6423.htm

ATTACK OF SEPTEMBER 11TH ON AMERICAN SOIL IS NOT INTELLIGENCE FAILURE

Is it really surprise for US? Many researchers ask this question. I think it is not surprise. Because on US congress report seven months before the attack warn all decision makers as "The combination of unconventional weapons proliferation with the persistence of international terrorism will end the relative invulnerability of the U.S. homeland to catastrophic attack. A direct attack against American citizens on American soil is likely over the next quarter century. The risk is not only death and destruction but also a demoralization that could undermine U.S. global leadership. In the face of this threat, our nation has no coherent or integrated governmental structures.[423] So instead of to talk about the intelligence failures about this event, to talk how this attack occurred, will be appropriate.

But in self-criticism of US agencies we get some lessons. What Sept. 11 reminds us, as various failings come to light, is that collaboration is not a one-way street. It really is not even a two-way street. Intelligence collaboration is like a traffic circle with many roads (organizations or data points) feeding in information that mingles with other bits of information entering or already in the circle. Like a police officer directing and smoothing the flow of traffic, analysts integrate the various information streams, forming, breaking apart and reforming, and refining the mosaics described above. The products then are made available to participating agencies to use to carry out their particular mandate (political, military, economic, social, environmental/energy, anti-terrorism). Done properly, this is never-ending ebb and flow, one that should be occurring simultaneously at multiple horizontal and vertical levels within and among agencies. [424]

---

[423] Commission on National Security, "Road Map for National Security: Imperative for Change", The Phase III Report, February 15, 2001, Available on site http://www.nssg.gov/PhaseIIIFR.pdf

[424] Smith, D., "Intelligence and Sept. 11", The Defense Monitor, Washington, Volume XXXI, Number 6, June/July 2002, pp.1-4

1.1.70 Other Problems In Intelligence[425]

If we talk on several comments focused on the problem of intelligence coverage of terrorism and asymmetric warfare, there are some things that never seem to change:

- It is far easier to call for strategic warning than to get it, or get policymakers to act on it of they do receive it. It is always easy for decision-makers to demand prophecy and attack intelligence analysis when they don't get it. This may explain why there are so many calls for improved strategic warning and so few calls for improved decision-maker response.

- It is far easier to call for better HUMINT than it is to get it. In practice, however, it remains as underfunded as ever, and partly because it is so difficult to make cost-effective investments and to be sure they pay off. Far too often, successes are matters of chance and not of the scale of effort. An improved HUMINT is both a confession of the severe limits of national technical means and a substitute for serious planning and effort.

- New intelligence toys are not new systems, and systems always have limitations. The other side of this coin is that we probably face growing limitations in the imagery and signals intelligence capabilities in many of the areas that affect vulnerability to asymmetric warfare and terrorism. However, it is far from clear that some of the extremely expensive improvements we plan in National Technical Means will really pay off in the areas we are discussing today, or that some of the new tactical detectors and sensors being developed are integrated into effective systems. There may well be a need for independent net intelligence assessment of our probable future capabilities in these areas.

- We need more focus on weaponization, weapons effects, and different kinds of vulnerability. Proliferation and changes in information warfare are creating major new challenges in how the communities should assess the weapons available to state and extremist actors. This is particularly true of biotechnology and information warfare, but it also involves the risk of "dirty," unsafe, and unpredictable nuclear weapons. Most weapons

---

[425] Cordesman, A.H., "The Changing Face of Terrorism and Technology, and the Challenge of Asymmetric Warfare", Center for Strategic & International Studies, Available on site http://www.csis.org/hill/ts010327cordesman.htm

effects analysis is badly dated, and related to use against military targets. Weaponization analysis often does not address the acute uncertainty that may occur in weapons effects, and most vulnerability analysis is now dated. The technical issues of what attackers can really do, the problem intelligence may face in characterizing their resources, and the risk of combinations of new methods of attack - combining information systems and Chemical, Biological, Radiological, Nuclear (CBRN) attacks, cocktails of biological weapons, etc. needs more attention.

- We need an effective bridge between foreign intelligence and law enforcement that responds to the scale of the emergency.

One final point, whenever new threats emerge, there is a natural tendency to call for new organizations, czars, and interagency structures. It is far easier to say that a new organization is needed than to get into the nitty gritty of actually having to improve existing capabilities or develop new ones. A set of problems involving this many uncertainties and new skills may or may not require new federal organizations, and new organizations within the intelligence communities,

Ultimately, however, what improving capability to deal with terrorism and asymmetric warfare requires most is resources and improving collection, analysis, and fusion at sophisticated technical levels. The real issue is one of how to improve depth, give the communities the right perspective, and how to improve "quality," and not how to change organization or leadership. This requires both serious planning and a serious program and supporting budget. Changing the name on the door is almost mindlessly easy, but changing the capability within is what counts.

"Nimitz's concept of intelligence was dynamic: Facts were high grade ore to be sifted carefully, the pure metal of knowledge extracted and forged into a weapon to defeat the enemy."

Gordon W. Prange, Miracle at Midway[426]

ASSESMENT OF FUTURE INTELLIGENCE

The burden of global engagement brings with it a need for global scale sensors and the capacity for processing, analysis, reporting, and dissemination of the information they collect. This wide-ranging intelligence apparatus is essential for making national policy and conducting the affairs of state, and to support the deployment and employment of military forces on a global scale. The cost of these capabilities, however, is such that they will have to be shared by all functions and echelons of the national security structure, which creates major organizational challenges. This problem is already with us, and must be solved if the objectives of states are to be achieved. Significant deficiencies must be addressed in current intelligence and related capabilities, the analytic exploitation of these capabilities, and the integration of these systems with national forces.

This chapter begins by outlining the sources of the need for change. It is not intended to be a comprehensive treatment of the whole of intelligence issues, but to bring to the attention of a new defense team the handful of most important needs. These are outlined in this chapter, and a series of specific recommended actions are outlined in the conclusion.

THE NEED TO MAINTAIN AN INTELLIGENCE CAPABILITY

The need for changes in intelligence structure is driven by several factors. Chief among them is that the national intelligence structure created in the shadow of World War II and developed during the Cold War has not kept up. Moreover, it is dominated by collection activities, while assessment of the information thus collected is inadequate to present and future needs.

---

[426] Department Of The Navy Office, "Naval Intelligence", Naval Doctrine Publication (NDP) 2, Washington, 1993, p.3

Whether the intelligence structure can meet the requirements of the post-cold war world depends on several questions which are; "Will the intelligence structure have adequate resources?" , "Will the intelligence structure's resources for collecting and analyzing intelligence be suited to the new targets and new questions?", "Will the intelligence structure be organizationally capable of meeting the priorities and needs of intelligence users?", "Will the intelligence structure be intellectually capable of understanding the changing players and issues that comprise the international scene in the New World Order?", etc.

Today, intelligence, after all, is required not only for spying purposes, but for many other needs that vary from biological warfare to microchip industry.[427]

The intelligence structure will have difficulty addressing these tasks because it has not yet resolved basic issues concerning how to plan intelligence programs and its own organization. This has resulted in intelligence gaps in the past, and is likely to hamper intelligence operations in the future.[428]

The information revolution has brought with it the means of proliferation of information and new technologies that fuel the economic and industrial growth of other nations around the globe. This has stimulated the global economy within which each nation must compete for survival and well-being. It has also affected the technological and industrial base from which military systems, intelligence systems, and target information systems are drawn, permitting revolutionary approaches in each of these domains that have not yet been fully exploited.[429]

The advances in technology, particularly information technologies, have provided the basis for major changes in weapons systems, targeting systems, communications systems, intelligence systems which some of them can be seen in appendix.

---

[427] Atay, M., "Stratejik Ulusal Güvenlik İstihbaratı", Strateji, Doğuş Matbaacılık Ltd.Şti., Ankara, No.1, 1996, p.79

[428] Berkowitz B.D. and Goodman, A.E., "Strategic Intelligence for American National Security", Princeton University Press, Princeton, 1989, pp. 45-47

[429] Kanwal, G., "The New World Order: An Appraisal-II", Strategic Analysis: A Monthly Journal of the IDSA, Vol. XXIII, No. 4, July 1999, Available on site http://www.ciaonet.org/srchfrm.html

At the end without question, states needs information about the world outside its borders to protect its national interests and relative position in the world, whether as a Cold War superpower or a nation that remains heavily and inextricably engaged in world affairs. It needs information to avoid crises as well as respond to them, to calibrate its diplomacy, and to shape and deploy its defenses.

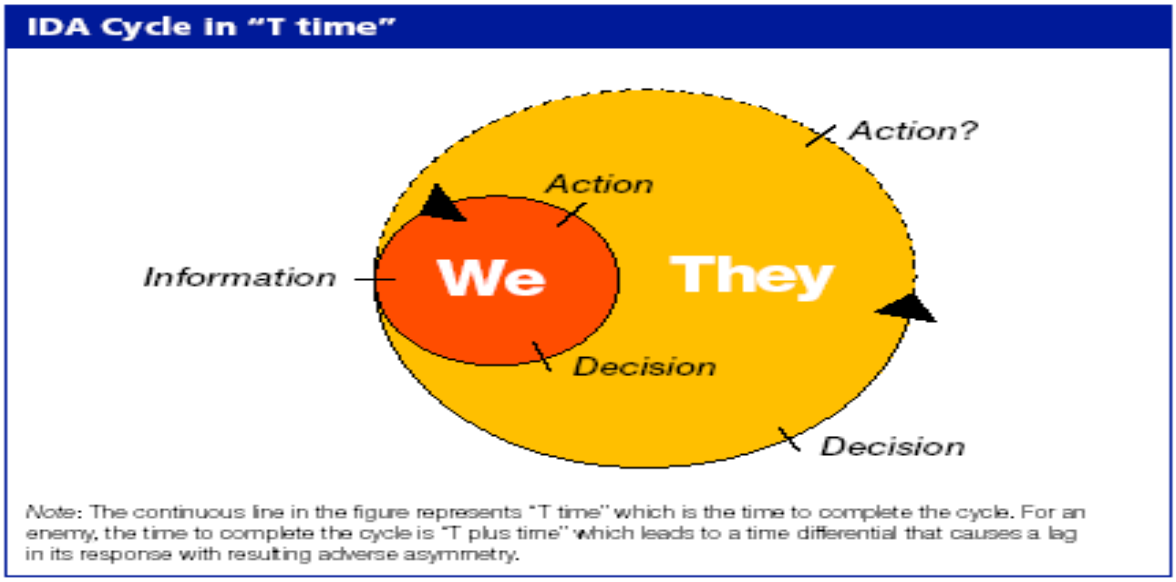
The governments' need for information, and the possible roles for intelligence in providing it, can be conceived along several dimensions, which are secret sources or open ones, tactical purposes or strategic ones, and questions that are puzzles or ones that are mysteries. [430] In those terms, the Cold War legacy of intelligence was a vast capacity to solve strategic puzzles, primarily about terrorist organizations, undemocratic states, imperialist states, and etc.

Much of that information is openly available, but much of it is not. Intelligence agencies attempt to fill the void. Their capabilities are costly. At times their activities are a source of embarrassment, even consternation. But they continue to provide information crucial to states interests.

So the need to maintain an intelligence capability is evitable, and time as a fourth dimension (at figure 6.1), reshape intelligence structure.

[430] Steury, D.P., "Sherman Kent and the Board of National Estimates", Collected Essays, Center for the Study of Intelligence, Available on site http://www.cia.gov/csi/books/shermankent/toc.html

Figure 0.1 Information-Decision-Action (IDA) Cycle[431]



THE COMING REVOLUTION IN INTELLIGENCE ANALYSIS

Constructive self-assessments are important to any organization. This effort will improve reorganizing of structure parallel to developments in our competitive world. It is unavoidable reality, which will happen in intelligence world.

Medina argues that revolution in intelligence as "…the Directorate Intelligence's (DI) current model of intelligence analysis is failing to respond to rapid changes in consumer needs and preferences. The DI is insufficiently focused on the consumer and is devoting its resources to increasingly useless syntheses of intelligence reporting." She recommends what she calls a revolutionary model that would shift analysis from a focus on day-to-day "developments" to forward-leaning, conceptual thinking that is "less independent and neutral" and more tailored to the policymakers' specific needs. She recommends that intelligence should have a continuity structure and surge a new model for intelligence in the future. [432]

---

[431] Singh, J., "Time:The New Dimension in War", JFQ, Winter 1995–96, p.57, Available on site www.dtic.mil/doctrine/jel/jfq_pubs/1510.pdf

[432] Medina, C., "The Coming Revolution in Intelligence Analysis: What To Do When Traditional Models Fail," Studies in Intelligence, Vol. 46, No. 3, pp. 24-26

Policymakers' intelligence demands in the wake of 11 September 2001 show the enduring value of analysts providing support that, at least in part, responds to the "old" assumptions laid out by Medina: officials needed help keeping current on, and interpreting, "developments" related to global terrorism. In any crisis, consumers' need for intelligence support is intensified.

Between October 2001 and April 2002, analysts working on Afghanistan were inundated with requests from policymakers to track developments in the region. The resulting high-level, event-driven "current intelligence" was shown to be an essential, but not necessarily the essential part of a successful model of intelligence analysis.

One can argue that crisis support is sufficiently different from routine support to policymakers that it only temporarily tips the balance in favor of a focus on developments at the expense of the provision of more conceptual, policy-relevant products. Policymaker requests support the view that a focus on developments is fundamental to intelligence analysis under any conditions in any century. [433]

To maintain credibility, an analyst would be wise to be as conversant in developments and disseminated raw intelligence as the policymaker being served. Few things undermine a policymaker's confidence as rapidly as an analyst's lack of familiarity with widely available information about developments in countries and issues relevant to ongoing policy discussions.

In 2002, Feder argued that the use of a specific analytic model produced more precise forecasts than conventional intelligence analysis without sacrificing accuracy, yet "despite the advantages of (the models) the vast majority of analysts do not use them."[434] Feder speculates that the models are not used because "this kind of systematic analysis does not fit into an organizational culture that sees an "analyst" as someone who writes reports, often evaluating and summarizing available information. In contrast, people who use models and quantitative techniques are considered "methodologists."

---

[433] Medina, C., Ibid, pp. 26-27

[434] Feder, S.A., "Forecasting for Policy Making in the Post-Cold War Period." Annual Reviews: Political Science, 2002, Available on site http://polisci.annualreviews.org/cgi/content/full/5/1/111

According to Arthur Hulnick, "methodologists discovered that their new techniques were unpopular with analysts because they had no time to absorb these systems in the face of tight deadlines."[435]

Richards Heuer observed "the initial attitude of country analysts toward our unconventional proposals typically ranged from skepticism to hostility. Equally typical, however, has been their post-project appraisal that the work was interesting and well worth doing."

The most of intelligence agencies have instituted several programs intended to increase the expertise of their analysts, but the quality and accuracy of finished intelligence could be further improved through the incorporation of new tools and techniques. However, this will require understanding the current DI culture and analytic practices and either working with them or changing them.

A PLAN TO CORRECT PAST SHORTCOMINGS

Parallel to changing environment a plan to correct these past shortcomings and prepare the intelligence structure to deal with the post-cold war era must be based on the following principles:

- Authority and responsibilities within the intelligence communities should be clear-cut and based on statute, so as to have support and legitimacy,
- Intelligence requirements are a function of the data requirements of national security policies and the programs intended to carry out these policies. Thus, intelligence planning must be built into these policies and programs when they are formulated,
- The resources necessary to meet these requirements must be analyzed and allocated objectively, rather than as an arbitrary portion of the total funding devoted to defense or other national security programs,
- The primary rule for effective intelligence is that what is collected and how it is provided must be determined by the needs of the user. [436]

---

[435] Hulnick, A.S., "Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century", Praeger, Westport, 1999, p.53.

With these general principles in mind, some specific recommendations can be made for preparing the intelligence structure to deal with the new world.

Improve relations between producers and consumers of intelligence. The traditional, carefully crafted and coordinated certain report may have made sense when the intelligence communities served only a small group of consumers. But the number of government officials needing tailored information has grown, and the intelligence communities must learn to mass market its product. It must understand the needs of a wide range of users and meet those needs with products.

Also, the ICs need to respond to the arrival of new information-processing technology and the corresponding habits of a new generation of intelligence users. The military services too have made progress in providing data directly to the commander on the battlefield. But the ICs has made less progress in taking advantage of this technology to get political and economic intelligence out of the house and into the hands of the consumer.

In addition, the categorization of finished intelligence must be minimized and the product exposed to wide examination among cleared individuals. As for protecting sources and methods, this is much more important for raw cables, intercepts, and agents' reports than for finished political analyses.

Finally, not only do intelligence users need better access to intelligence producers, the producers need better access to users. In the past, new weapons systems have been built with only superficial input from the ICs. Links between operational commanders and line diplomats are often poor. Intelligence obtained under these conditions has often been naive at best, useless at worst.

At the end according to me, perfect intelligence should obtain from coordinated structures. Otherwise by confirming the failures and by ineffective double effort, we arrive the uncorrectable results.

---

[436] Berkowitz, B.D., Goodman, A.E., Why Spy--And How--In The 1990s?, Orbis, Spring 92, Vol. 36 Issue 2, p. 269

THE ROLE OF INTELLIGENCE

The roles and missions of intelligence are not static. They are affected by changes in the world, in technology, and in the Government's needs. Each states' administration must decide where intelligence agencies should concentrate their efforts.

For the important role of Intelligence, firstly require for stable policy guidance, which created to perform, their functions often have foundered due to lack of involvement by officials. Otherwise this has resulted in inconsistent, infrequent guidance, and sometimes no guidance at all, leaving intelligence agencies to fend for themselves. Sometimes security forces illegally make collaboration with illegal organizations to obtain intelligence.[437]

There are complexities in each of the functional intelligence roles. Intelligence support to states' diplomacy, military operations and defense planning should continue to constitute the principal missions of the ICs. Countering illicit activities abroad, which threaten states' interests, including terrorism, narcotics trafficking, proliferation of weapons of mass destruction, and international organized crime are also increasingly important missions as we mentioned above.

The increase in the availability of publicly available information may permit some diminution in the current level of effort to analyze the economies of other countries. Administration strongly supports the current policy prohibiting intelligence agencies from engaging in "industrial espionage," i.e., using clandestine means to obtain information from foreign commercial firms for the benefit of a competitor. It is appropriate, however, for intelligence agencies to report to related officials, evidence of unfair trade practices being undertaken by or with the knowledge of other governments to the disadvantage of their firms.

---

[437] OSS, "Ireland Police Found to Have Collaborated with IRA in Raid on Police Intelligence Files" Available on sitehttp://www.oss.net/extra/news/?module_instance=1&id=188

Support to law enforcement and regulatory agencies is a legitimate mission but requests for such support must be rigorously evaluated to ensure that intelligence agencies are able to make a useful contribution.

REORGINIZING OF FUTURE INTELLIGENCE ARCHITECTURE

The Intelligence architecture provides the general structure for intelligence support. While not strictly hierarchical, formal relationships exist among the national, theater, and task force intelligence organizations and elements. These relationships facilitate requirements management and optimize complementary intelligence functions by echelon without obstructing the timely flow of intelligence to an information grid connecting all echelons. The national intelligence agencies maintain systems and organizations that respond directly, and provide intelligence, to any echelon for time sensitive support.

The objective for the future system is to provide the Intelligence Communities' analytical workforce the cognitive tools and automated capabilities necessary to ensure successful mission accomplishment in tomorrow's high information environment. This future architecture will ensure transparent, virtual, and uninterrupted electronic connectivity in all levels. The objective is to better enable the intelligence consumer to understand the environment and synthesize relevant facts from a complex information domain. For the ICs, the goal is to significantly accelerate and make the intelligence cycle more meaningful.

Advanced knowledge-based tools will target areas of information visualization, presentation, analysis, multisource information fusion, information management, and final delivery techniques. Coupled with preparedness and virtual collaboration with multiple users. This evolution will eliminate the physical limitations posed by location, classification levels, and mobility requirements, while using the capabilities of a more capable world-class analytic and associated support workforce. Subcomponents key to the architecture of the future system based on tree main factors, which are people, system, technology.

1.1.70.1 People

At the national level, to meet the needs of the warfighters, decisionmakers, and policymakers, the ICs is organized along major functional lines of collection operations, analysis and production, dissemination systems, services, and policy and administrative support.

The increasing tempo of events and quantity of information; instability in global affairs; the expanded potential for world-wide; and the technologies available to decision makers and operating forces to influence international activities, demand a more flexible, highly skilled and experienced work force than ever before. The very complex geopolitical and battlespace environments of the future will compel nations not only to keep pace with, but to anticipate, expanding and demanding requirements, and to fuse rapidly, apply, "visualize," and disseminate a full range of intelligence support.

The necessary training for all Intelligence is provided in a timely, efficient manner any time or place there is a demand. Training is provided in management, analysis, collection management, and automated systems as well as basic skills training for all positions within the ICs. [438]

ICs are firmly committed to utilizing their most valuable asset, their people, by developing and maintaining a diverse, well-trained cadre with the talent, energy, and vision necessary to meet the challenges of dynamic support requirements in the future.

The analysts, collectors, and information technologists can perform all-source fusion of complex information using knowledge-based tools. They are people who possess solid knowledge and understanding of the military art, science, and operations and key foreign forces. And also these people with expert technical knowledge, including an understanding of automated data processing and telecommunications required to collect, process, produce, and disseminate intelligence to users and consumers.

---

[438] Vector 21, "The Defense Intelligence Architecture", A Strategic Plan for the Defense Intelligence Agency, Available on site http://www.fas.org/irp/dia/vector21/

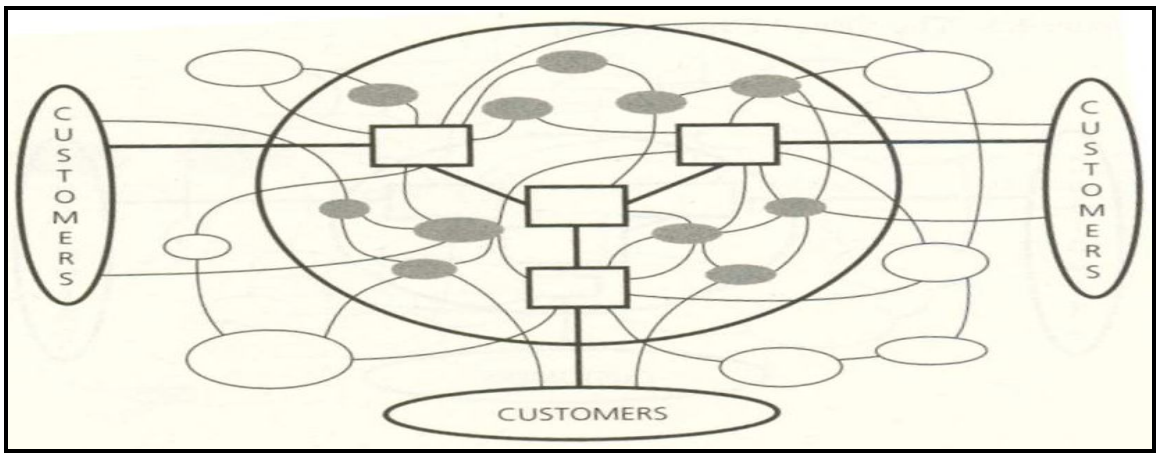
New talent will be gained by recruiting, developing, training and retraining the highest quality analysts. Specialists will be developed from within the Agency by providing rewarding and well-defined career paths from the entry level to the most senior technical, analytical, and managerial levels. [439]

By demanding professional certification, offering professional development opportunities in all intelligence fields and throughout the intelligence communities, providing currency training, sponsoring active programs, and promoting cross training, they will achieve and maintain this future cadre.

1.1.70.2 Systems

All intelligence made available to the intelligence network is communicated to users throughout the system. The data are stored and accessed on a standards automated system that interfaces with the communications network. (In the figure 6.2 illustrated a simple example of intelligence network complexity.)

Figure 0.2 The Intelligence Network Organization[440]



The Intelligence architecture is a dynamic, flexible structure providing global access to an information grid that consists of all intelligence sources at all echelons. [441] The Intelligence

[439] Vector 21, "The Defense Intelligence Architecture", Ibid.
[440] Pinchot, G., "Creating Organizations with Many Leaders", (ed.), Hesselbein, F., et.al., " The Leader of The Future" Drucker Foundation, New York, 1996, p.36
[441] Vector 21, "The Defense Intelligence Architecture", Ibid.

architecture is configured to provide access to all intelligence sources from anywhere on the globe and to provide essential data that the consumers will need to support their missions.

The Intelligence architecture is a network of integrated workstations, file servers, and communications links. These elements must work together, consistent with common standards, to create the interoperable information environment required to support military operations, defense planners, and policymakers. The network includes direct connectivity by communications links and broadcast capability to support time-sensitive needs. An important aspect of the information grid is its ability to make all intelligence, including direct collector to user information, accessible via standardized file servers to standards compliant workstations.[442]

Another important subject in systems is security, which the agencies have implemented a technical risk-management rather than a risk-avoidance policy that guarantees the security, integrity, and availability of national intelligence assets and capabilities. This policy will evolve to a multiple-level security system in which appropriate information can be accessed from a single workstation via a single physical communications network. Information dominance will be the most important phase, for the virtual architecture and for technical risk management. The physical environments will characteristic advanced security technologies, such as biometrics, high-speed data encryption cards, and data labeling. [443]

Advanced knowledge-based tools the keystones for predictive intelligence and accurate estimates. They will allow the analysts to achieve their missions perfectly.

To maximize the utility of the architecture, all systems must meet standards of connectivity using standard communications protocols and standard security devices available at all echelons.

---

[442] Vector 21, "The Defense Intelligence Architecture", Ibid.
[443] Vector 21, "The Defense Intelligence Architecture", Ibid.

All-source intelligence dissemination employs a variety of means to deliver high-quality, related intelligence to consumers. In support of operations at the national, theater, and subordinate force levels. The Intelligence Architecture provides access to data from strategic, operative, and tactical intelligence organizations and sources primarily from a "push-pull" system. The "pull" refers to the consumer's ability to query or select from intelligence databases relevant intelligence based on their mission and need for information. The "pull" capability is designed to prevent communications circuit saturation while permitting multiple users access to important information. Additionally, intelligence will be "pushed" to selected consumers in response to established requirements and essential elements of information. The up, down, and across echelon interface among strategic, operational, and tactical intelligence organizations is the backbone for intelligence dissemination.

1.1.70.3 Technology

Intelligence Agencies will maintain an open systems architecture that will allow the rapid integration of knowledge-based tools and that will achieve the blending of discrete activities of the intelligence cycle into a homogenous intelligence situation. The new architecture will help to create a collaborative electronic workspace for information technologists to eliminate the physical limitations imposed by location, classification level, and mobility requirements.

The Agencies will recapitalize their technology in leading edge information and communications capabilities by carefully managing technological change. This requires an awareness of technological developments, users' requirements, fiscal restraints, and technological insertion strategies that translate into new technical capabilities.

Successful technology insertion requires a proactive customer requirements awareness and management process to anticipate new mission needs that will drive applications for new technology. A revolving, rapid recapitalization based on a periodic cycle is required to stay ahead of technology oldness.

IMPROVING INTELLIGENCE ANALYSIS

Unless intelligence is concerning to users and reaches them in time to affect their decisions, the effort to collect and produce it has been wasted. Consumers in policy agencies in particular express dissatisfaction with the intelligence support they receive. While consumers often are uncooperative and unresponsive, producers must attempt to engage them.

Relationships with consumers cannot be sustained, however, unless intelligence producers can over time demonstrate they bring something of value to the table. While the administration found that intelligence analysis consistently adds value to that which is available from public sources, improving the quality of such analysis and ensuring it reaches users in a timely manner are continuing concerns.

A greater effort also should be made to intelligence the vast universe of information now available from open sources. The systems establishing electronic links between producers and consumers currently being implemented should be given a higher priority. Estimative, or long-term, intelligence came in for particular criticism from consumers.

Although there have been substantial personnel reductions in virtually every intelligence agency since the end of the Cold War, personnel costs continue to crowd out investments in new technologies and operational initiatives. In some agencies, this phenomenon is beginning to reach crisis proportions. Agencies find themselves with workforces that are not well aligned with their needs but lack the legal authority to streamline and reorient their workforces to current and future requirements.

While improving intelligence analysis, preventative intelligence, however, requires significantly greater investment, most noticeably in terms of skilled personnel who are capable of interpreting material and deciding which of the many warnings received each day represent a real and credible threat. Contrary to popular fantasy, fuelled by the image portrayed in movies of the James Bond style, a career in most Western intelligence services is not overly well paid and often involves boring, routine analysis of low-level material. As one renegade intelligence officer observed, "Ninety per cent of the work I did involved probably the most boring tasks I have ever performed in my life." It is not hard to

see why many able high-fliers wouldn't even consider a career in intelligence.[444]So instead of to talk about only action, we should talk about firstly mind, after action.

MILITARY INTELLIGENCE

As the most important function of national security, military intelligence also needs to adapt the changing world. To achieve changing need firstly information dominance. And also for information dominance, force commanders will need a detailed understanding of the situation over the full range of their respective areas of responsibility, as well as of the situations affecting their ability to execute their specific missions.

Military commands are agreed in their expressed need for more analytic support. [445] The access provided by the current set of global and organic sensors has improved and does a better job at meeting the needs of operational commands; the shortfall is in the analysis of the data coming from these systems. The global reach of forces and the variety of threats and problem sets they must address require at least as broad a set of analytic skills, languages, and specialized knowledge as were required during the Cold War, but since its end, the resources for this realm have been substantially reduced.

Most intelligence money is spent to acquire collection and processing systems, rather than analysis. While some imbalance might be natural, it is exaggerated in part by bureaucratic factors.

Another issue is the increasing availability of valuable information in the public domain. During the Cold War years, the period during which many of the organizations, processes, and habits of the intelligence communities were developed, most strategic intelligence information was derived from secret sources. The primary targets of intelligence activities were closed societies, and the questions needing answers required secret sources and methods.

---

[444] Janes News, "Where does US intelligence go from here - and were they really to blame?", 27 September 2001, Available on site http://www.janes.com/security/international_ security/ news/jiaa/jiaa020704_1_n.sht

[445] Blair, D., US Rear Admiral, "Associate Director Of Central Intelligence For Military Support", 28 October 1995, Available on site http://www.janes.com/security/international_security/news/jiaa/jiaa 020704_1_n.sht

In our current world, by contrast, many of the most important uncertainties for the states are not so dominantly defined by secret data from closed societies. While estimating the future adversaries may require some access to secret sources and methods, the dominant prerequisite is knowledge of the society and familiarity with its public behavior.

Changes in assignment of analytic responsibilities would help facilitate these improvements. Ways to improve on the quality of the current system include improvements in linkages between collection activities and policy consumers, in support to military operations, and in covert and clandestine operations; greater use of open-source information; reduction of the number of organizations; establishment of a more realistic requirements process; and creation of a systematic assessment process.

Changes are necessary to support the strategic objectives of maintaining national dominance in intelligence, improving integration of intelligence into operational capabilities, and expanding international cooperation in intelligence.

Support of policy decisions and support to military operations needed for leadership will require a superior intelligence, reconnaissance, and surveillance capability. Dominance in global awareness and in ability to apply military force intelligently is a primary national capability with a geopolitical impact in its own right.

Changes are necessary to support the strategic objectives of maintaining national dominance in intelligence, improving integration of intelligence into operational capabilities, and expanding international cooperation in intelligence.

Support of policy decisions and support to military operations needed for leadership will require a superior intelligence, reconnaissance, and surveillance capability. Dominance in global awareness and in ability to apply military force intelligently is a primary national capability with a geopolitical impact in its own right.

One of the most difficult management challenges both now and in the future, is how to share the extremely capable sensor, processing, and analysis systems that are now available under the rubrics of intelligence, reconnaissance, and surveillance.

A military commander must have a good picture of his or her area of interest. This "situation awareness" is derived from a wide variety of information sources, only a few of which are labeled "intelligence." Others, nominally "reconnaissance" or "surveillance," includes air traffic control radars, warning radars, and command and control radar systems.

This formulation of the issue and solution are identical to the "joint" elements of command and control which already has a significant role in the joint force development process, will take on the responsibility of establishing a Joint Office, to be charged with developing a common, adaptive, and agile command and control infrastructure including the elements of intelligence, reconnaissance, and surveillance. The Office would provide an essential framework for the evolution of "joint" functions. They also support joint demonstration, experimentation, and exercise activities, which are including intelligence. These are all steps in the right direction.

CONCLUSION AND RECOMMENDATIONS

CONCLUSION

Change is a constant in the intelligence analysis profession. Technologies change, organizational structures change, and procedures change. Yet the core of intelligence is a constant in the production of finished intelligence. In order to access informal knowledge from collectors throughout the ICs, benefit from the comments of analytic counterparts, and produce analysis relevant to policymakers, personal relationships are crucial to protect Homeland Security. Environmental changes in perceived threat, direct our needs to restructure intelligence architecture. For example Turkey after Cold War noticed intelligence deficiency when the NATO didn't share some of the intelligence products with her[446]and new threat appeared her circle.

As I realized in previous chapters that just as a human head depends on sense of human, which are sight, sound, smell, and touch as channels for gathering data about the external world for processing and interpretation by the brain, so an intelligence system depends on spies, electronic and photographic reconnaissance, and so forth. So I came to see the battle between intelligence and deception as the efforts on one side to establish as many channels as possible through which to observe the opponent, in the hope that he may fail to block at least some of these channels, while the opponent may in addition try to send false, and preferably consistent, signals in as many channels as possible.

To succeed in any such exchange, you should therefore aim to establish your channels of observation, and to deepen the sophistication in each individual channel so that if your opponent tries to send false signals in that channel they may fail to match a genuine signal in their sophistication.

---

[446] Fidan, H., "Intelligence and Foreign Policy: A comprasion of British, American and Turkish Intelligence Systems" Unpublished Master Thesis, Bilkent University, Ankara,1999, p.78

The changes in the world that are already apparent are more than enough to require a complete reshaping of intelligence, and the extension of those changes into the future of the market state will only sharpen that need.

The primary functions of intelligence will not change; they deal with warning, monitoring, and forecasting. The priority of estimates intelligence relative to current intelligence has declined significantly in the past fifteen years, although estimates intelligence provide one of the few connecting links in the intelligence communities. History we indicated who have technology or in another word, who spend for R&D, will win all kind of war.

It is not quite true that there is no point in producing intelligence of any sort if it cannot be used. A case can be made for producing "pure intelligence" just as a case can he made for doing basic research in science. An institute bringing together some of the best brains in the U.S. with an annual budget of $100 million would provide basic intelligence which for all known, might be superior to anything produced at present; but it could not provide the practical information that politicians need most: whether or not Argentina will actually land on the Falkland Islands at a certain date, whether the Soviets are massing troops for an operation against an unruly satellite, and so on. Roberta Wohlstetter has provided an excellent illustration in her study, Pearl Harbor. [447]

The business of knowing what is going on in the world, where things are and what leaders intend to do, is essential for the states which are intended to leadership in a region or in the world. Intelligence activities are an important part of meeting those needs for security strategy, diplomacy, development of economic policies and practices, and support of deployed and employed military forces. The roles of the current intelligence institutions need to change in response to the new environment and new technologies.

And most of important role is coordination between administrative organs and inside intelligence structures. Without coordination, most of affords, which can be response to national interests or global threats, go in vane. Because of that appropriate strategies

[447] Wohlstetter, R., “Pearl Harbor: Warning and Decision”, Stanford University Press, Stanford, 1965 in Laqueur, W., “The Future of Intelligence” Society, Jan/Feb98, Vol. 35 Issue 2, p.301

should be developed such as; there should be a coordinator, the sharing of relevant information, the coordination of law enforcement and intelligence activities.

Today one-step before another war in Iraq, which may be a new world war, the newspapers say much more then we can aspect.

As Toffler said, " Maybe you are not interested with war, but war interested with you",[448] some events are unpreventable and inevitable. There is a unique solution to estimate and to prepare before the events occurred. That is good and timely intelligence.

Good intelligence is the key to preventing attacks on the homeland and homeland security should become one of the intelligence community's most important missions. Better human intelligence must supplement technical intelligence, especially on terrorist groups covertly supported by states. As noted above, fuller cooperation and more extensive information-sharing among the states will also improve the chances that would-be perpetrators will be detained, arrested, and prosecuted before they ever reach their aims. Terror is important, and the other threats also important.

But there is something much more important than all for powerful states, that is "economic interests". So economic intelligence and open intelligence have importance day-by day.

At the end while information gathering conserve importance, to direct information, which we want to be, will have great influence on the mission of strategic intelligence.

RECOMMENTATIONS

This research is designed in order to determine the future structure of intelligence and impacts on national security. But findings of research suggest that there are several critical issues that require further research such as;

- Finding the affects of NGOs and media on new intelligence structure
- The new physiology of intelligence
- State centric approaches on intelligence concept.

---

[448] Toffler A. and H., "Savaş ve Savaş Karşıtı Mücadele", translated by Harmancı, M., Sabah Kitapları, Temmuz 1994, p.249

APPENDIX

This resource is a comprehensive alphabetical listing of intelligence programs. It is an extremely mixed bag that includes major hardware programs, medium-sized software implementations by the year 2000. For detail explanation of them can be find in FAS WEB page.

Table A.1 Intelligence Programs and Systems[449]

ABI	Airborne Broadcast Intelligence
ABI	AWACS Broadcast Intelligence
ACDBU	Automated Counter drug Database Update
ACC GOC	ACC Global Operations Center
ACCES	Advance Cryptologic Carry-on Exploitation System
ACIPS	Acoustic Intelligence Processing System
ACS	Aerial Common Sensor
ADARS	Airborne Digital Audio Recording System
ADARS	ASAS Data Recording and Summary System
ADNET	Anti-Drug Network
ADS	Advance Deployable System
AEOS	Advanced Electro-Optical System
AEPDS	Advanced Electronic Processing and Dissemination System
AFMSS	Air Force Mission Support System
AFINTNET	Air Force Intelligence Network
AHFEWS	Army HF Electronic Warfare System AN/TLQ-33
AIRTAPS	Aerial Imagery Reconnaissance Tracking and Plotting System
AIS	ACCINTNET Implementation Support
AIRES	Advanced Imagery Reqs & Exploitation System
ALE RMS	Aires Life Extension
AMHS	DODIIS Automated Message Handling System

[449] "Intelligence Programs and Systems" Available on site http://www.fas.org/irp/program/list.htm

AMOS	Air Force Maui Optical Station
AMSS	Automatic Met. Sensor System
AN/ALQ-151	Quickfix / Advanced Quickfix [AQF]
AN/BQH-5	Submarine Support Equipment
AN/FLR-9	High Frequency Direction Finding System
AN/FSQ-111	WHITE CLOUD
AN/FSQ-144	TROJAN CLASSIC
AN/FYK-16	WHITE CLOUD
AN/GSQ-187	Remote Battlefield Sensor System (REMBASS)
AN/GYQ-21	Intelligence Data Handling System
AN/GYQ-50	Intelligence Host Processing System
AN/MYQ-7	IAS - Intelligence Analysis System
AN/MYQ-8	TCAC PIP - Technical Control and Analysis Center Product Improvement Plan
AN/SRS-1	Combat DF [Combat Direction Finding]
AN/SSQ-108	CLASSIC OUTBOARD Direction Finding System
AN/TLQ-17	TRAFFICJAM / SANDCRAB
AN/TLQ-33	Army HF Electronic Warfare System AHFEWS
AN/TRQ-32	Teammate
AN/TSQ-105	Surveillance Information Processing Facility
AN/TSQ-108	Radar Sonar Surveillance Center (RSSC)
AN/TSQ-114	TRAILBLAZER
AN/TSQ-130	Tactical Control and Analysis Center
AN/TSQ-132	JSTARS Ground Station Module
AN/TSQ-134	Advanced Electronic Processing and Dissemination System
AN/TSQ-134	Enhanced Tactical Users Terminal (ETUT)
AN/TSQ-138	TRAILBLAZER
AN/TSQ-152	TRACKWOLF
AN/TSQ-156	Top Gallant

AN/TSQ-161	CLASSIC OWL
AN/TSQ-163	Top Gable / Top Graphic
AN/TSQ-176	Surveillance Integrated Processing Facility
AN/TSQ-181	CLASSIC OWL
AN/TSQ-190	TROJAN/TROJAN SPIRIT II
AN/TSQ-191	TROJAN Air Transportable Electronic Reconnaissance System
AN/TSQ-199	Enhanced TRACKWOLF
AN/TYQ-63	ASAS Communications Control Set (CCS) (unsheltered)
AN/ULR-21	Classic Troll ESM for NSSN Submarine
AN/USC-55	Joint Tactical Terminal-Hybrid
AN/ULQ-20	Battle Group Passive Horizon Extension System [BGPHES]
AN/USQ-123	Common High Bandwidth Data Link - Surface Terminal
AN/USQ-124	TACINTEL II - Tactical Intelligence Information Exchange Subsystem-Phase II
AN/WLR-8	Electronic Warfare Support Measure (ESM) Receiver
ANCHORY	ANCHORY
ANG GES	Air National Guard Ground Exploitation System
ANNULET	Cryptologic Maintenance System
Anvil	Automated Target Recognition on Multi-Spectral Imagery
AQUATONE	U-2
AQUILINE	1960s UAV Development Project
AQM-34L FIREBEE II	COMPASS BIN Unmanned Aerial Vehicle [UAV]
AQM-34N Firebee	Unmanned Aerial Vehicle [UAV]
Aquila UAV	Aquila Unmanned Aerial Vehicle [UAV]
AREAS	Airborne Reconnaissance Evaluation and Analysis System
ARGUS	Army Intelligence Database
ARL	Airborne Reconnaissance - Low
ARMISS	Agency Resources Management Information
ASARS-I	Advanced Synthetic Aperture Radar System

ASARS-II	Advanced Synthetic Aperture Radar System
ASAS	All Source Analysis System
ASTECS	Advanced Submarine Tactical ESM Combat System
ASSET	All Source Satellite Evaluation Tool
ATARS	Advanced Tactical Reconnaissance Airborne System
ATR	Automatic/Aided Target Recognition
ATS	Automated Tasking System
ATV	Advanced Tethered Vehicle
AUSS	Advanced Unmanned Search System
AVS	Airborne Video Surveillance
BARNACLE	Special Naval Collection Program (SNCP)
BGPHES	Battle Group Passive Horizon Extension System AN/ULQ-20
BEARTRAP	Acoustic Data Collection and Processing
BINOCULAR	NSA Signals Intelligence Product
BIRDSNEST	NSA High-Performance Workstation, UNIX-Based Desktop Computer
BLACKER	NSA End-to-End Encryption System
C4ISR	Capstone C4ISR Architecture
CAMS	COMIREX Automated Management System
CARS	Contingency Airborne Reconnaissance System
CARS/DGS	CARS Deployable Ground System
CATIS/IESS	Computer Aided Tactical Information System/Imagery Exploitation Support System
CAWS	Commercial Analyst Workstation
CCDB	Common Cryptologic Database
CCOP	Cryptologic Carry-On Program
CDIS	Counter Drug Intelligence System
CENTERBOARD	HF/DF Central Processor Computers
CES	Collection Evaluation System
CGS	JSTARS Common Ground Station

CHAINWORK	Crytptologic Support System
CHARIOT	S-Band Satellite Terminal
CHAALS	Communications High Accuracy Airborne Location System
CHASIS	CI/HUMINT All Source Integration System
CHATS	AN/PYQ-3 (V1) (CI/HUMINT) Automated Tool Set
CHBDL-ST	Common High Bandwidth Data Link - Surface Terminal
CHIMS	CI/HUMINT Information Management Systems
CIAP	Command Intelligence Architecture Planning Program
CIGSS	Common Imagery Ground/Surface System
CI/HUMINT	Counterintelligence/Human Intelligence
CIRAS	Corporate Information Retrieval and Storage
CIRC	Central Information Reference and Control System
CIS	Combat Intelligence System
CIWES	Common Information Warfare Exploit Sensor [Navy]
CLARINET MERLIN	Special Communication System
CLASSIC AERIE	Naval Security Group Command program
CLASSIC BULLSEYE	FLAGHOIST
CLASSIC OUTBOARD	AN/SSQ-108 (V) Direction Finding System
CLASSIC OWL	AN/TSQ-161 (V) and AN/TSQ-181 (V)
CLASSIC TROLL	AN/ULR-21 ESM for NSSN Submarine
CLASSIC TRUMP	Navy Counternarcotics Cryptologic System
CMSRR	Classified Modeling and Simulation Resource Repository
CMST	Collection Management Support Tools
COBLU	AN/SSQ-108 (V) Cooperative OUTBOARD Logistics Update
COBRA BALL	Tracking Aircraft
COBRA BRASS	Space-Based Multispectral Data
COBRA EYE	RC-135X TELINT Aircraft
COBRA GEMINI	Sea- and Land-Based Radar System
COINS	Community On-line Intelligence System [NSA]

COLISEUM	Community On-Line Intelligence for End-Users and Managers
COMBAT CATIS	Combat Computer-Aided Tactical Information System
Combat DF	Combat Direction Finding AN/SRS-1
COMBAT SENT	RC-135U
Communications Central	TROJAN/TROJAN SPIRIT II
COMPASS ARROW	Unmanned Air Vehicle
COMPASS BIN	AQM-34L FIREBEE II Unmanned Aerial Vehicle [UAV]
COMPASS COPE	Unmanned Air Vehicle
COMPASS JADE	NATO SIGINT Real-Time Air Situation Display
Condor	Unmanned Air Vehicle
CONFERM	Conventional Forces Europe in Reduction Monitoring System
CONSTANT SOURCE	WC-135W Aircraft
CONSTANT WATCH	Korean Air Intelligence System [IOC 1981]
CORNERSTONE	CORNERSTONE (Infrastructure Product)
CROSSHAIR	All-Service DF Requirements
CR-TUAV	Close Range - Tactical Unmanned Aerial Vehicle
CR-UAV	Close Range - Unmanned Aerial Vehicle
CSE-SS	Client Server Environment-System Services
CSIL	Commercial Satellite Imagery Library
CSP	Communications Support Processor
CSP-HOL	Communication Support Processor - Higher Order Language
CSP	Communication System Processor [TENCAP]
CUB	Cryptologic Unified Build
CUBIC	Common User Baseline for the Intel Community
CURV	Cable-controlled Undersea Recovery Vehicle
DATM	DISA ATM network
DAIRS	DIA Advanced Imagery Reproduction System
DARTS	Design and Analysis of Reference Threat Signature
DAWN	Defense Attaché Worldwide Network

DAWS	Defense Automated Warning System
DCIIS	Defense Counterintelligence Information System
DCPDB	Distributed Characteristics and Performance Database
DDN	Defense Data Network
DDS	Defense Dissemination System
DE	DDS Dissemination Element (DE)
DEWDROP	Digital Geocoordinate Point Mensuration System
DGS	Deployable Ground System
DIEPS	Digital Imagery Exploitation and Production System
DII COE	Defense Information Infrastructure Common Operating Environment
DISN	Defense Information Systems Network
DITDS	Defense Intelligence Threat Data System
DMFE	Defense Automated Warning System Message Front End
DODIIS	DOD Intelligence Information System
DODIMS/COLISEUM	DoD Intelligence MS/Community On-Line Intelligence for End-Users and Managers
DPPDB	Digital Point Positioning Data Base
DSP	Defense Support Program
DSNET	Defense Secure Network
DTSS-D	Digital Topographic Support System-Deployable
DTSS-MSIP	Digital Topographic Support System - Multispectral Imagery Processor
DTSS	Document Exploitation (DOCEX) Transportable Support System
E-TRACKWOLF	Enhanced Trackwolf
Eagle Vision	COTS-Based Deployable Ground Station
ECHELON	Global Computer Network
EIS	Enhanced Imagery System
EKMS	Electronic Key Management System [NSA COMSEC]
EPDS	Electronic Processing & Dissemination System

ESS	Exploitation Support System
EWFAES	Electronic Warfare Flagging Analysis Expert System
EWIRDB	Electronic Warfare Integrated Reprogramming Database
FAISS	FORSCOM Automated Intelligence Support System
FAST-I	Forward Area SID and TRAP - Improved
FASTLANE	NSA ATM Cryptosystem
FCA	Future Communications Architecture
FDS	Fixed Distributed System
FIA	Future Imagery Architecture
FISTA	Flying Infrared Signature Technology Aircraft
FORMMS	Foreign Materiel Management System
FORTEZZA	NSA Crypto Component of MISSI [formerly Tessera]
GALE	Generic Area Limitation Environment
GBS	Global Broadcast Service
GCCS	Global Command and Control System
GCCS-I3	GCCS Integrated Imagery and Intelligence (I3),
GCCS GRIS	Global Reconnaissance Information System
GEODSS	Ground-Based Electro-Optical Deep Space Surveillance
GISTER	Evidential Reasoning System
GNAT-750	CIA Unmanned Air Vehicle
GRANDSLAM	NSA NRT Intelligence Initiative
GRCS	Guardrail Common Sensor
GSD	Graphical Situation Display
GUIDEPOST	Tools for Missile Analysis (Infrastructure Product)
HAARP	ELF/VLF Radio Detection of Underground Structures
HAE UAV Global Hawk	Global Hawk (Tier II+ High-Altitude, Long-Endurance UAV
HAE UAV Dark Star	DarkStar Tier III Minus
HARMONY	HARMONY
HAVE STAR	NAIC Missile Defense Threat Assessment

HEARTLEAF	Airborne Reconnaissance Ground SIGINT Systems (ARGSS)
HIGHTOP	NSA/Army INSCOM ELINT Program
HIMS	Human Information Management System
HMI	Host Message Interface
HOCNET	HUMINT Operational Communications Network
IAS	Intelligence Analysis System
IC4I	Integration for Command, Control, Communications, Computers and Intelligence
ICARIS	Intelligence Communications and Requirements Information System
IDHS	Intelligence Data Handling System
IDSF	Intelligence Defector Source File
IESS	Imagery Exploitation Support System
IEWCS	Intelligence Electronic Warfare Common Sensor
IFSARE	Interferometric Synthetic Aperture Radar - Elevation
IMACTS	Imagery Management and Communications Testbed System
IMETS	Integrated Meteorological System
IMOM	Improved Many on Many
IMP	Imagery Modernization Program (DIA)
IMPACTS	Information Warfare Mission Planning, Analysis and C2 Targeting System
INNET	Initial Network
IOSA	Integrated Overhead SIGINT Architecture
IPA	Image Product Archive
IPDS	Imagery Processing & Dissemination System
IPF	GUARDRAIL Integrated Processing Facility
IPL	Imagery Product Library
IREMBASS	Improved Remotely-Monitored Battlefield Sensor System
IRIS	Intelligence Resources Information System
IRON CLAD	EP-3B Special Projects Aircraft

ISFAR	Interferometric Synthetic Aperture Radar
ISMC	Intel Link Systems Management Center [NSA]
ISMS	Integrated Security Management System
ISP	Integrated Survey Program
IUBA	Image Understanding for Battlefield Awareness
JAMA	Joint Airborne MASINT Architecture
JASA	Joint Airborne SIGINT Architecture
JBS	Joint Broadcast Service
JDISS	Joint Deployable Intelligence Support System
JIRONET	Joint Intelligence Research Office Network
JIVA	Joint Intelligene Virtual Architecture
JMIOS	Joint Maritime Information Operations Strategy
JRICP	Joint Reserve Intelligence Connectivity Program
JSIPS-A	Joint Service Imagery Processing System - Augmentation
JSIPS-N	Joint Service Imagery Processing System
JSTARS-CGS	JSTARS Common Ground Station
JSTARS-GSM	JSTARS Ground Station Module
JWICS	Joint Worldwide Intelligence Communications System
KILTING	ELINT Database
LACROSSE	ONYX
LOCE	Linked Operations/Intelligence Centers Europe
Lofty View	GNAT-750 CIA Unmanned Air Vehicle
LONGROOT	Enhanced Automatic DF (EADF) HF/DF Processor Upgrade
LOOKING GLASS	SIGINT Analysis and Reporting Software
MAE UAV	Predator Medium Altitude Endurance Unmanned Aerial Vehicle
MAV	Micro-Air Vehicle
MDITDS	Migration Defense Intelligence Threat Data System
MERIT	Military Exploitation of Reconnaissance and Intelligence Technology

MEWSS	USMC Mobile Electronic Wafare Support System
MIDB	Modernized Integrated Data Base
MIES	Modernized Imagery Exploitation System
MIGS	Multi-source Intelligence Ground System
MIIDS	Military Intelligence Integrated Data System
MINS	Multisource Integrated Notification System
MIPE	Mobile Imagery Processing Element
MONTICELLO	FTSC Analyst Tools/Management System
MPAS	Measurement and Signature Intelligence Analysis
MPS	MC&G Production System
MRDBS	MASINT Requirements Data base
MSIIRS	Multispectral Imagery Interpretability Rating Scale
MSTS	Multi-Source Tactical System
MTN	Mission-22 (M-22) Tactical Network
MUSIC	Multi-User Special Intelligence Communications System [NAVSECGRU]
MVS	Mission Verification System
NAS	Network Access System
National Eagle	Radarsat/Landsat/SPOT Imagery Dowlink
NDS	NIMA Delivery Segment (NDS)
NEWSDEALER	NewsDealer
NES	NIMA/National Exploitation System
NEWSTAND	Newstand
NIEWS	Naval Imagery Exploition Work Station
NIEWS	NTCS-A Imagery Exploitation Workstation
NIMA softcopy	Softcopy exploitation
NIPRNET	Non-Classified Internet Protocol Router Network
NSAS	Noncommunications Signals Exploitation System
NSOC	National SIGINT Operations Center [NSA]

NTSDS	National Target/Threat Signature Data System
OASIS	Over-the-Horizon (OTH) Airborne Sensor Information System (OASIS)
OED	OSIS Baseline Upgrade (OBU) Evolutionary Development
OILSTOCK	NSA Geographic Information System
ONYX	LACROSSE
OV-1	Mohawk
PACER COIN	ANG C-130 IMINT
PARSEC	SIGINT Analysis and Reporting Software
Pathfinder	National Ground Intelligence Center Analyst Tool
PAVE MOVER	Forerunner to JOINT STARS
PC-I3	Personal Computer Integrated Imagery and Intelligence
PLATFORM	NSA CERCIS Program
PLATYPUS	National Migration System Secure Server Proof of Concept
PRAIRIE SCHOONER	Navy SIGINT Program
PRAIRIE WAGON	Navy SIGINT Program
PRCR MONITOR	Problem Report / Change Request Monitor
PRIVATEER	Naval Program
PSTS	Precision SIGINT Targeting System
Quickfix	Advanced Quickfix [AQF]
RAAP	Rapid Application of Air Power
Radiant Beryllium	Navy TENCAP Program
Radiant Frost	Navy TENCAP Program
Radiant Gold	Navy TENCAP Program
Radiant Ivory	National Systems Tactical Detection and Reporting (TACDAR)
Radiant Mercury	Radiant Mercury
Radiant Thunder	Navy TENCAP Program
Radiant White	Navy TENCAP Program
RAMROD	NSA/INSCOM/AIA ELINT Program [see RANGER]

RANGER	NSA/INSCOM/AIA SIGINT Program [see RAMROD]
RCSS	RC-135 Support Server
RF-4B/C	Unarmed photographic reconnaissance aircraft
RIVET AMBER	RC-135E ELINT Aircraft
RIVET BALL	RC-135S ELINT Aircraft
RIVET BRASS	RC-135 TELINT Aircraft
RIVET CARD	RC-135M SIGINT Aircraft
RIVET FIRE	EC-130H Compass Call Aircraft
RIVET QUICK	RC-135M SIGINT Aircraft
RMS	Requirements Management System
ROCKETEER	Crytptologic Support System
ROSTER	NSA/Army INSCOM SIGINT Program
RUWS	Remote Unmanned Work System
SAF	Source Acquisition File
SAIP	Semi-Automatic IMINT Processing Systems
SANDCRAB	AN/TLQ-17 TRAFFICJAM
SANDKEY	NSA Analysis and Reporting Software
SATRAN	Satellite Reconnaissance Advanced Notice
SB-WASS	Space Based Wide Area Surveillance
SDNS	Secure Data Network System [NSA]
SDS	Surveillance Direction System
SDS	SIGINT Data Server [ex SOMMS - SIGINT On-line Mission Management System]
SEABASS	Sea-Based Assets Security System
SENIOR GLASS	U-2 SIGINT Sensor Package
SENIOR MACE	SIGINT Exploitation System
SENIOR RUBY	U-2 ELINT Radar Emission Monitoring Sensor Package
SENIOR SPAN	Large Radome on U-2R
SENIOR SPEAR	U-2R COMINT System

SENIOR SPUR	Large Radome on U-2R
SENIOR YEAR	U-2 Reconnaissance Aircraft
Sentinel II	Computer Based Training (CBT) System
SHORTROOT	Automatic Digital Direction Finding
SIDS	Secondary Imagery Dissemination Systems
SIP	SIGINT and IMINT Processor
S&IPA	SIGINT & IMINT Pre-processing Architecture
SIPF	GUARDRAIL Surveillance Information Processing Facility
SIPRNET	Secret Internet Protocol Router Network
SMPAS	Space Mission Payload Assessment System
SOCRATES	Special Operations Command, Research, Analysis, and Threat Evaluation System
SOSUS	Sound Surveillance System
SOF-IV	Special Operations Forces - Intelligence Vehicle
SOMMS	SIGINT On-line Mission Management System [now SDS]
SPIRIT	System Parametric Information Relational Intelligence Tool
SR-UAV Pioneer	Pioneer Short Range Unmanned Aerial Vehicle
SR-UAV Hunter	Hunter Short Range Unmanned Aerial Vehicle
SI SSIXS	Special Intelligence Submarine Satellite Information Exchange Subsystem
SSEP	Submarine Surveillance Equipment Program
SSP-S	Single Source Processor - SIGINT
SSP-S (PI)	Single Source Processor - SIGINT (Product Improvement)
STICS	Scalable Transportable Intelligence Communications System
SUCCESS	Synthesized UHF Computer Controlled Equipment Subsystem
SUP	Segment Upgrade Program
SURTASS	Surveillance Towed-Array Sensor System
TACDAR	Radiant Ivory - National Systems Tactical Detection and Reporting
TACFIX	AN/TRQ-37

TADIXS	Tactical Data Information Exchange Subsystem
TACINTEL II+	AN/USQ-124 Tactical Intelligence Information Exchange Subsystem-Phase II
TAGBOARD	D-21 Ramjet-Powered Reconnaissance Drone
Talon COMMAND	Air Force TENCAP
Talon KNIGHT	Air Force TENCAP
Talon SHOOTER	Air Force TENCAP
Talon WARRIOR	Air Force TENCAP Direct Space Integration (DSI)
TAP	TPED Analysis Process
TAS	Timeline Analysis System
TASE	Threat Assessment Support Environment
TATERS	TROJAN Air Transportable Electronic Reconnaissance System
TCAC	AN/TSQ-130 Tactical Control and Analysis Center
TCAC PIP	Technical Control and Analysis Center Product Improvement Plan
TC XXI	Trojan Classic XXI
TDDS	Tactical Related Applications (TRAP) Data Dissemination System
TENCAP CSP	TENCAP Communication System Processor
TENCAP GUARD	Imagery Support Server Environment
TERPES	Tactical Electronic Reconnaissance Processing and Evaluation System
TES Light	Tactical Exploitation System - Light
TESSERA	NSA Crypto component of MISSI (see Fortezza)
TIBS	Tactical Information Broadcast System
TIDYTIPS-III	Collection System
TMWS	Target Material Work Station
Top Gable	AN/TSQ-163 SSP-S
TOPSCENE	Tactical Operational Scene
TPED	Tasking, Processing, Exploitation & Dissemination
TRAFFICJAM	AN/TLQ-17 SANDCRAB

TRAILBLAZER	AN/TSQ-138
TROJAN BARE	TROJAN Basic Architecture Receive Element
TROJAN LITE	TROJAN SPIRIT Lightweight Integrated Telecommunications Equipment (LITE)
TROJAN SPIRIT II	TROJAN/TROJAN SPIRIT II
TROJAN TATERS	TROJAN Air Transportable Electronic Reconnaissance System
TS-II	TROJAN SPIRIT II
T-UAV Outrider	Outrider Tactical Unmanned Aerial Vehicle
TUWVS	Tethered Unmanned Work Vehicle System
U-2	SENIOR YEAR / AQUATONE
U-2 DGS	Deployable Ground Station
U-125	PEACE KRYPTON
UAV-E	Unmanned Aerial Vehicle - Endurance
UAV-GCS	UAV Ground Control Station
UAV-TCS	Unmanned Aerial Vehicle - Tactical Control System
UNITARY DF	All-service DF Requirements
USAFE DIPS	USAFE Digital Imagery Processing System
USIGS	United States Imagery and Geospatial Information Systems Architecture
USIS	United States Imagery System Architecture
USSS	United States SIGINT System
VEGA	MASINT Spacecraft
VISTA	VISION/Very Intelligent Surveillance and Target Acquisition
Vortex-II	Advance Vortex
VTUAV	Vertical Take Off and Landing Tactical Unmanned Aerial Vehicle
WIN-T	Warfighter Information Network - Terrestrial
WRANGLER	WRANGLER
XIDB	Extended Integrated Data Base

REFERENCES

Albuquerque Public Schools, "Military Advancements During WWI", Available on site http://www.aps.edu/APS/EISENHOWER /Mercer/class/wars/ww1 /Matt.htm

Arbatov, A., "The National Idea and National Security", Mirovaya Ekonomika i Mezhdunarodnyye Otnosheniya, 5 May 1998,

Atay, M., "Stratejik Ulusal Güvenlik İstihbaratı", Strateji, Doğuş Matbaacılık Ltd.Şti., Ankara, No.1, 1996

Atkinson, R., "Crusade: The Untold Story of the Persian Gulf War" Houghton Mifflin Company, 1993, Available on site http://www.eskimo.com/%7Ektlange/MCOilFields.jpg

Barnet, T.B., "Life After DoDth: How The Evernet Changes Everything", Available on site http://www.geocities.com/ResearchTriangle/Thinktank/6926/LifeafterDoDth.htm

Bay, A., "Homeland Security: Disseminating the Information, No Easy Task", Aug 1, 2002 Available site on www.strategypage.com/inetpub\strategypageroot\onpoint\docs\2002.htm

Beaufre, A., "An Introduction to Strategy", Faber and Faber Publication, London, 1965

Berkowitz B.D. and Goodman, A.E., "Strategic Intelligence for American National Security", Princeton University Press, Princeton, 1989

Berkowitz, B.D. and Richelson, J., "The CIA Vindicated," National Interest 41, Fall 1995

Berkowitz, B.D., "Intelligence Reform, The Third Act", Orbis, Elsevier Science Publishing, Winter 2001, Vol. 45, Issue 1

Berkowitz, B.D., Goodman, A.E., "Why Spy--And How--In The 1990s?", Orbis, Elsevier Science Publishing, Spring 92, Vol. 36, Issue 2

Best, R. A., “Intelligence Issues for Congress”, Foreign Affairs and National Defense Division, June 4, 2001, Available on site http://www.fas.org/irp/crs/IB10012.html

Best, R.A., “Homeland Security: Intelligence Support”, CRS Report for Congress, Washington, August 7, 2002, Available on site http://www.usembassy.at/en/download/ pdf/homelandsec_intell.pdf

Best, R.A., “Reforming Defense Intelligence”, CRS Report for Congress, Rev. ed. Library of Congress, Washington, 22 Jan. 1992, 91-475F, June 11, 1991 Available on site http://www.chem.au.dk/~db/fusion/alpha_P

Bible,“The World English Bible (WEB)”, The Book Of Numbers, Available on site www.ebible.org/bible/web/ webrft.zip

Blair, D., “Associate Director Of Central Intelligence For Military Support”, 28 October 1995, Available on site http://www.janes.com/security/international_security/news/jiaa/jiaa 020704_1_n.shtml

Blum, H.R.(ed.), “Surveillance and Espionage in a Free Society” A report by the Planning Group on Intelligence and Security to the Policy Council of the Democratic National Committee, Praeger Publishing, New York,1972, Available on site http://intellit.muskingum.edu/genpostwar70s_folder/ postwar70sgen.html

Brian, F., and Wiersema, R., “Battlefield TECHINT: Support Of Operations Dessert Shields/Storm”, Military Intelligence Professional Bulletin, Apr-Jun 1992, Vol. 18, Issue 2

Builder, C.H., and Dewar, J.A., “A Time for Planning? If Not Now, When?” Parameters, Summer, 1994

Bundy, McG., ed. Smith, L.J., “Foreign Relations of The United States, 1961-1963”, Volume X, Cuba, 1961-1962, Department of State, Washington, 1997, Available on site http://www.state.gov/www/about_state/ history/frusX/index.html

Burrows, W., “Deep Black: Space Espionage and National Security”, Random House Publishing, New York, 1986

Cadena, L., "Rethinking the Missions and Priorities of the Intelligence Community", 1997, Available on site http://www.fas.org/irp/eprint/snyder/priorities.htm

Cameron, J., "Globalization and the Ecological State", Review of European Community & International Environmental Law, 1999, Vol.8, Issue 3

Canadian Security Intelligence Service, "1996 Public Report" Available on site http://www.csis-scrs.gc.ca/eng/publicrp/pub1996_e.html

Caşın, M.H., "Rus İmparatorluk Stratejisi", ASAM Yayınları, Ankara, 2002

Caşın, M.H., "Stratejik İstihbarat", Avrasya Dosyası (İstihbarat Özel), No: 2, Ankara, Summer 2002

Caşın, M.H., "Strategic Effects of World War I to International Security and Power Balances In The Middle East", The First World War: Middle Eastern Perspective, Israel-Turkish International Colloquy, Tel-Aviv, April 2000

Caşın, M.H., "Askeri İstihbaratın Politik ve Stratejik Yapısındaki Boyutsal Değişim", Strateji, Doğuş Matbaacılık Ltd.Şti., Ankara, No.1, 1996

Caşın, M.H., "Çağdaş Dünyada Uluslararası Güvenlik Stratejileri ve Silahsızlanma", SSM Yayınları, No. 17, Ankara, 1995

CIA, "A Consumer's Guide to Intelligence", September, 1993, (Undated) October 29, 1997 Available on site http://www.odci.gov/cia/publications.htm

CIA, "Global Trends 2015", Available on site http://www.odci.gov/cia/publications/globaltrends2015/index.htm

CIA, "Who We Are and What We Do", Available on site http://www.odci.gov/cia/ciakids/spyguy/index.html

CIA, "Analytical Products of the DI", Available on site http://www.odci.gov/cia/di/work/major.html

Clapper, J. R., “Challenging Joint Military Intelligence”, Joint Force Quarterly (JFQ), Spring 1994

Clausewitz, C., “On War” 1832, translated by Howard M.and Paret P., Princeton University Press, 1976/84, Compiled by Bassford, C., Bassford, 1998, Available on site www.clausewitz.com/CWZHOME/On_War/BK3ch01.htm.

Codevilla, A., “Informing Statecraft: Intelligence For a New Century”, Maxwell Macmillan, Canada, 1992

Cole, S. V., “How To Make War”, Available On Site http://www.strategypage.com/search.asp?target=d:\inetpub\strategypageroot\fyeo\howtomakewar\docs\archives\htint01.htm

Commission on National Security, “Road Map for National Security: Imperative for Change”, The Phase III Report, February 15, 2001, Available on site http://www.nssg.gov/PhaseIIIFR.pdf

Committee on Governmental Affairs, “A Lesson of the Gulf War: National Security Requires Computer Security”, Subcommittee on Government Information and Regulation, Washington, June 19, 1991, Available on site www.fas.org/irp/nsa/ioss/threat96/part02.htm

Conference on Security and Co-operation in Europe, “Treaty on Conventional Armed Forces In Europe”, Available on site http://www.osce.org/docs/english/1990-1999/cfe/cfetreate.htm

Cordesman, A.H., “The Changing Face of Terrorism and Technology, and the Challenge of Asymmetric Warfare”, Center for Strategic & International Studies, Available on site http://www.csis.org/hill/ts010327cordesman.htm

Davies, P.H.J., “Ideas of Intelligence: Divergent National Concepts And Institutions”, Hahvaro International Review, Fall, 2002

Davis, D., “The Challenge of Managing Uncertainty - Paul Wolfowitz on Intelligence Policy-Relations”, Available on site http://www.ci-ce-ct.com/article/showquestion.asp

Davis, J., “A Policymaker's Perspective On Intelligence Analysis”, Studies In Intelligence, 1995 edition, Vol.38, No. 5, Available on site www.cia.gov/csi/studies/95unclass

Dawson, A.K., “Turkish Brigade”, Military History Magazine, December 1997, Available on site http://europeanhistory.about.com/library/prm/blturkishbrigade1.htm

Davutoğlu, A., “Stratejik Derinlik”, Küre Yayınları, İstanbul, 2001, pp.17-29

Day, R.B., “Cold War Capitalism: The View from Moscow 1945-1975” Sharpe Publishing, New York, 1995

Dearth, D.H. and Godden, R.T. (eds), “Strategic Intelligence: Theory and Application”, (second edition), Defense Intelligence Agency, Washington, 1995

Defense Daily Network Report, “Open Source Intelligence: Private Sector Capabilities to Support DoD Policy, Acquisitions, and Operations,” 5 May 1998, Available on site http://www.fas.org/irp/eprint/oss980501.htm

Defense Intelligence Agency, “North Korea: The Foundations for Military Strength, Employing The Armed Forces”, October 1991, Chap. 6, Available on site http://www.fas.org/irp/dia/product /knfms/knfms_chp6.html

Department of Energy, “Acquisition Regulation, Classification, Security and Counterintelligence”, Rules and Regulations, Vol. 62, No. 192, 1997, Available on site http://www.fas.org/sgp/othergov/doecont.html

Department of National Defense, “Joint Doctrine For Canadian Forces Joint and Combined Operations”, B-GG-005-004/AF-000, Ottawa, Canada, 1995

Department of the Air Force, “Target Intelligence Handbook: Unclassified Targeting Principles”, 200-18, Washington, October 1, 1990

Department Of The Navy Office, “Naval Intelligence”, Naval Doctrine Publication (NDP) 2, Washington, 1993

Deutsch, H.C, "Commanding Generals and the Uses of Intelligence," Intelligence and National Security 3, No: 3, 1988

Domes, J. and Te-huai, P., "The Man and the Image" Stanford University Press, Stanford, 1985

Drake, R.J., "History of Intelligence, British Expeditionary Force, France, From January 1917 To April 1919", Available on site www.lib.byu.edu

Drew, D.M., and Snow, Dr. D.M., "Making Strategy: An Introduction to National Security Processes and Problems", Air University Press, 1988

Duncan, S.M., "Desert Shield/Desert Storm Employment or Reserve Component: Extracts of Lessons Learned", The United States Naval War College, Available on site www.fas.org/man/dod-101/ops/docs/p162.pdf

Dunnigan, J.F., "How To Make War", Quill Publishing, New York, 1983

Dziak.J.J., "Chekisky: A Story of the KGB", Heath&Co.,Lexington Books, Lexington, 1988

Eells, R.S., and Nehemkis, P.R., "Corporate Intelligence and Espionage: A Blueprint for Executive Decision Making" Macmillan, New York, 1984

Ersanel, N., "Siber İstihbarat", Jeopolitik-Strateji-Terör Dizisi, ASAM yayınları, Ankara, 2001

Feder, S.A., "Forecasting for Policy Making in the Post-Cold War Period." Annual Reviews: Political Science, 2002, Available on site http://polisci.annualreviews.org/cgi/content/full/5/1/111

Federal Standart 1037 C,"The Glossary of Telecommunication",1996, Available on site http://www.its.bldrdoc.gov/fs-1037/dir-033/_4879.htm

Feld, W. J. and Boyd, G., "Comparative Regional Systems", Pergamon Press, New York 1980

Fidan,H., "Intelligence and Foreign Policy: A Comprasion of British, American and Turkish Intelligence Systems" Unpublished Master Thesis, Bilkent University, Ankara,1999

Finley, J.P., "Nobody Likes to be Surprised: Intelligence Failures," In Military Intelligence, Vol 20, No. 1 (January-March), 1994

Fisher, J., "At Cold War's End: US Intelligence on the Soviet Union and Eastern Europe, 1989-1991", September 1999, Available on site www.odci.gov/csi/books/19335/art-1.html

FM 34-1 "Intelligence And Electronic Warfare Operations", Headquarters Department of the Army Washington, 27 September 1994, Available on site http://www.fas.org/irp/doddir/dod/index.html

FM 34-52, "Intelligence Interrogation", Headquarters Department of the Army, Washington, 8 May 1987, Available on site http://www.globalsecurity.org/intell/ library/policy/army/ fm/fm34-52/chapter7.htm

FM 43-54, "Battlefield Technical Intelligence", Headquarters Department of the Army, Washington, DC, 5 April 1990, Available on site http://www.fas.org/irp/doddir/army /fm34-54/Ch1.htm

Frederick C. W., " Troops to Equal Any" Available on site http://www.vwam.com/vets/ equal.html

Gaddis, J.L., " The Long Peace: Inquiries into the History of the Cold War" Oxford University Press, New York, 1987

Garst, R. D., "A Handbook of Intelligence Analysis", 2d ed., Defense Intelligence College, Washington, 1989

Gleijeses, P., "Ships in the Night: The CIA, the White House and the Bay of Pigs," Journal of Latin American Studies, 27 Feb. 1995

Government Printing Office, "IC21: The Intelligence Community in the 21st Century", Staff Study Permanent Select Committee on Intelligence, House of Representatives One Hundred Fourth Congress, Washington, 1996, Available on site http://www.access. gpo.gov/ congress/ house/intel/ic21/ic21_toc.html

Görgülü, İ., "Askeri Coğrafya", Harp Akademileri Basımevi, İstanbul, 1992

Gray, C. S., "Why Strategy Is Difficult", Joint Force Quarterly (JFQ), Summer 1999

Greenberg, M.R., and Haass, R.N. "Making Intelligence Smarter", Strategic Analysis, Monthly Journal of the IDSA, Vol. XXIV, No. 8, 2000, Available on site http://www.ciaonet.org/srchfrm.html,

Gries, D.D., "Intelligence in the 1990s," Studies in Intelligence 35, Spring 1991

GS-132, "Implementation of Army Occupational Guides (AOGs) for the Intelligence Specialist Series", Scientific and Technical Positions in Intelligence Production, 24 Apr 1991,

Nelson, H., "The U.S. Intelligence Budget in the 1990s," International Journal of Intelligence and Counterintelligence, Volume 6, 1993

Mackinder, H.J., "The Geographical Pivot of History," Geographical Journal, Vol. 23, 1904, Available on sitehttp://iserit.greennet.gl/jknuni/geopolit.htm

Haass, R.N., "Policymakers and the Intelligence Community in This Global Era," Remarks to CIA Strategic Assessments Group Annual Conference, Wilmington, 2001,Available on site http://www.state.gov/s/p/rem/6423.htm

Hadar, L.T., "Extricating America From Its Middle Eastern Entanglement, Policy Analysis No. 154, June 12, 1991, Available on site http://www.cato.org/pubs/pas/pa-154.html

Hastings, Max, ed., “Military Anecdotes”, Oxford University Press, New York, 1985

Held, D., “Globalization After September 11th”, Available on site http://www.polity.co.uk /global/ after_sept11.htm

Held, D., ed. al. “Global Transformations”, Executive Summary, March 1999, Available on site http://www.polity.co.uk/global/summary.htm

Heuer, R. J., “Psychology of Intelligence Analysis”, Central Intelligence Agency, Washington, 1999, Available on site http://www.cia.gov/csi/books/19104/index.html

Hiley, T., "Symposium on the Psychology of Intelligence Analysis," Center for the Study of Intelligence Bulletin 11, Summer, 2000, Available on site http://www.cia.gov/csi/ bulletin/ csi11.html

Hobsbawm, E., “The Age of Extremes: A History of the World, 1914-1991”, Pantheon Publishing, New York, 1994

Hopkirk, P., “On Secret Service East of Constantinople”, Oxford University Press, 1994

Hulnick, A.S., “Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century”, Praeger, Westport, 1999

Institute For National Strategic Studies “1997 Threat Assessment: Flash Points and Force Structure”, Chapter Nineteen, Available on site http://www.ndu.edu/inss/sa97/ sa97ch19.html

Intelligence Community Staff, “Glossary of Intelligence Terms and Definitions”, ICS, Washington, June 1989

Intelligence WEB Page “Counterintelligence” Available on site http://www.angelfire.com /ca7/Security/INTELLIGENCE.html

Interagency OPSEC Support Staff, “Compendium of OPSEC Terms”, Greenbelt, IOSS, April 1991, Available on site www.opsec.org/opsnews/Dec96/protected/InAName.html

Interview: DISA Center for Information System Security, November 3, 1993, Available on site www.fas.org/irp/nsa/ioss/threat96/part02.htm

Janes News, "Where does US intelligence go from here - and were they really to blame?", 27 September 2001, Available on site http://www.janes.com/security/international_ security/ news/jiaa/ jiaa020704_1_n.shtml

Joint Chiefs Of Staff, "Department of Defense Dictionary of Military and Associated Terms", Joint Pub 1-02, 23 March 1994, Washington, As Amended Through 7 December 1998, Available on site www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf

Joint Chiefs Of Staff, "Joint Doctrine Encyclopedia", U.S. Army Publishing, 16 July 1997, Available on site www.fas.org/man/dod-101/dod/

Joint Pub 2-0 "Intelligence Support to Operations", Joint Force Employment Briefing,, Joint Chiefs of Staff (CJCS), Available on site http://www.fas.org/irp/doddir/dod/jp2-0/index.html

Joint Pub 2-01, "Joint Intelligence Support to Military Operations", 20 November 1996, Available on site www.dtic.mil/doctrine/jel/new_pubs/jp2_01.pdf

Joint Staff of US Navy, "Chairman Of The Joint Chiefs Of Staff Instruction", J-5, 1 September 1997, Available on site www.dtic.mil/doctrine/jel/training_pubs/3150_05.pdf

Joint Staff, "Joint Doctrine for Intelligence Support to Joint Operations", Office of the Joint Chiefs of Staff, Washington, 05 May 1995

Jomini, A. H., The Art of War, Greenhill Books, London, 1992

Jones, R. V., "Some Lessons in Intelligence", Studies in intelligence, 1995, Vol. 38, No:5

Justino, P., "The Impact Of Globalisation And Trade Liberalisation On Household Poverty Dynamics", Poverty Research Unit Seminar on Globalisation University of Aarhus, 23 November, 2001, Available on site www.ulandslaere.au.dk/NOTICES/Events/ Oneday_seminar2001/ PatriciaJustino.htm

Kacowicz, A.M., "Nationalism: Convergent, Divergent or Overlapping?," Alternatives: Social Transformation & Humane Governance, 1999, Vol.24, Issue 4

Kahn, D., "The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet", Simon & Schuster Inc, 1997

Kanwal, G., "The New World Order: An Appraisal-II", Strategic Analysis:A Monthly Journal of the IDSA, Vol. XXIII, No. 4, July 1999, Available on site http://www.ciaonet.org/srchfrm.html

Katzenstein, P., (ed.),"Introduction: Alternative Perspectives on National Security" in The Culture of National Security, Colombia University Press, New York, 1996

Kent, S., "The Need for an Intelligence Literature" Central Intelligence Agency, Studies in Intelligence, 1955, Available on site http://www.cia.gov/csi/books/shermankent/2need.htm

Kirkpatrick, L.B., "The Real CIA", The Macmillan Company, New York, 1968, Chap. 8, Available on site http://www.rose-hulman.edu/~delacova/bay-of-pigs/kirkpatrick.htm

Korean War Home Page, "Turkey's Role in the Korean War", http://www.koreanwar. net/turkey.htm

Kramer, M., "Archival Research in Moscow: Progress and Pitfalls," Cold War International History Project Bulletin 3, Fall 1993,

Kym, A., "Globalization, WTO, and Asean," Asean Economic Bulletin, 2001, Vol.18, Issue 1

Laqueur, W., "A World of Secrets: The Uses and Limits of Intelligence" Basic Books Inc., New York, 1985

Laqueur, W., "The Future of Intelligence" Society, Jan/Feb 1998, Vol. 35, Issue 2

Liddell, H.B., "The Classical Book On Military Strategy", (2nd Edition), Meridian Publishing, New York, 1991

Mansfield, H.C., "Statesmanship and Party Government: A Study of Burke and Bolingbroke", University of Chicago Press, Chicago, 1965

Map Library, "Maps of Arab-Israili War" Depertment of History, Available on site http://www.dean. usma.edu/history/dhistorymaps/Arab-Israel%20Pages/aitoc.htm

Marcuse, P., "The Language of Globalization," Monthly Review: An Independent Socialist Magazine, Jul/Aug2000, Vol.52, Issue3

Maurer, A.C.,et. al., (eds.), "Intelligence Policy and Process", Westview Press, Boulder, 1985

McAuliffe, M.S. ed., "CIA Documents on the Cuban Missile Crisis", Central Intelligence Agency, 1962 Washington

McNamara, R. S. et al, "Argument Without End: In Search of Answers to the Vietnam Tragedy", Public Affairs, New York, 1999

MD 37-1C, "Stratejik İstihbarat Analizi", Silahlı Kuvvetler İstihbarat Okul Komutanlığı, Ankara, 2001

Medby, J., "IPB Considerations at the Strategic Level", Military Intelligence Professional Bulletin, Apr-Jun 2002, Vol. 28 Issue 2

Medina, C., "The Coming Revolution in Intelligence Analysis: What To Do When Traditional Models Fail," Studies in Intelligence, Vol. 46, No. 3

Meyer, H. E., "Real-World Intelligence", Weidenfeld & Nicolson, New York, 1987

Military Analysis Network, "Vietnam War", Available on site http://www.fas.org/man/ dod-101/ops/vietnam.htm

Mody, R., "The Enigma Machine", Available on site http://militaryhistory.about.com/ gi/dynamic/offsite.htm

Mooney, M., et. al., “2001 Technology Collection Trends in the U.S. Defense Industry”, Defense Research and Technology Horizontal Protection Publication

Moustafine, M., “Globalization and the Changing Role of Government,” Australian Journal of Public Administration, 1999, Vol.58, Issue 4

Murray, W. and Millett, A.R., (eds.), “Military Innovation in the Interwar Period”, Cambridge University Press, Cambridge, 1996

National Defense Panel, “Assessment of intelligence”, Quadrennial Defense Review, May 1997, Available on site http://www.defenselink.mil/topstory/ndp_assess.html

National Intelligence Course (NIC) Textbook, Joint Military Intelligence Training Center, November 1999

Nuechterlein, D. E., “America Overcommitted: United States National Interests in the 1980's”, 1985, Available on site http://dde.carlisle.army.mil/authors/RSA%20_Aid2001.pdf

O'Connell, K.M., “Intelligence in the Information Age: Spy Data for Sale”, Newsday, April 8, 2001, Available on site http://www.rand.org/hot/op-eds/040801ND.html

Office of the Auditor General of Canada, “The Canadian Intelligence Community”, Available on site http://www.oag-bvg.gc.ca/domino/reports.nsf

O'Leary, J., “ Surprise And Intelligence: Towards A Clearer Understanding”, Airpower Journal, Spring, 1994, Vol. 8, Issue 1

Olson, J.M., “A Never-Ending Necessity: The Ten Commandments of Counterintelligence”, Studies in Intelligence, Fall-Winter 2001, No. 11, Available on site http://www.cia.gov/csi/studies/fall_winter_2001/

On-Site Inspection Agency, "Fact Sheet: The Open Skies Treaty," May 1993, U.S. Arms Control and Disarmament Agency, Treaty on Open Skies (Official Text), April 10, 1992 Available on site http://www.usinfo.state.gov/topical/pol/arms/02081499.htm

OPSEC Support Staff, "Operations Security Intelligence Threat Handbook" The Interagency OPSEC Support Staff Publishing, April 1996, Available on site http://www.fas.org/irp/nsa/ioss/threat96/

OSS, "Ireland Police Found to Have Collaborated with IRA in Raid on Police Intelligence Files" Available on sitehttp://www.oss.net/extra/news/?module_instance=1&id=188

Overy, R., "War In History, Strategic Intelligence and the Outbreak of the Second World War", King's College Publising, London, 1998

Özdağ, Ü., "Stratejik İstihbarat", Avrasya Dosyası (İstihbarat Özel), No: 2, Ankara, Summer 2002

Papp, D., " The Impacts of Advanced Information and Communication Technologies on International Actors and the International System", in Strategic Environment, Air Command and Staff College Publishing, Alabama, 1996

Phillips,T.T., ed., "Roots Of Strategy, The Art of War", Stackpole Books Publishing, Pennysylvania, 1985

Pinchot, G., "Creating Organizations with Many Leaders", (ed.), Hesselbein, F., et.al., " The Leader of The Future" Drucker Foundation, New York, 1996

Poteat, G.H. "The Intelligence Gap: Hypotheses on the Process of Surprise," International Studies Notes, No. 3, 1976, Available on site www.ndu.edu/library/ic6/96-E-14.pdf

Renwick, R., "Economic Sanctions" Center for International Affairs, Harvard University, Cambridge, 1981

Report for Congress, "Critical Infrastructures: What Makes an Infrastructure Critical?", Library of Congress, Available on site http://www.fas.org/irp/crs/RL31556.pdf

Richelson, J.T., "The US Intelligence Community", Ballinger Publishing Company, Cambridge, 1985

Rose, P. K., “Two Strategic Intelligence Mistakes in Korea, 1950”, Fall-Winter 2001, No. 11, Unclassified Edition, Available on site http://www.cia.gov/csi/studies/fall_winter_2001 /article06.html

Rosen, S. P., “Winning the Next War: Innovation and Modern Militaries”, Cornell University Press, 1991

Rosenau, W.,"A Deafening Silence: U.S. Policy and the SIGINT Facility at Lourdes," Intelligence and National Security Publishing, October 1994

Sheehan, J.J., “Next Steps in Joint Force Integration”, Joint Force Quarterly(JFQ), Autumn 1996

Shu, G.Z., “Mao’s Military Romanticism: China and the Korean War, 1950-1953”, Kansas University Press, Kansas, 1995

Shulsky, A.N., “Silent Warfare: Understanding The World of Intelligence”, (2nd edition), Revised by Gary Schimitt, Brassey’s Publising, New York, 1993

Sibbet, D.B., "Commercial Remote-Sensing," American Intelligence Journal, Spring/Summer 1993

Simonds, L., “Magnetoelectronics Today and Tomorrow,“ Physics Today, April 1995, Available on site www.aip.org/pt/cont9504.html

Singh, J., “Time:The New Dimension in War”, JFQ, Winter 1995–96, Available on site www.dtic.mil/doctrine/jel/jfq_pubs/1510.pdf

Smith, D., “Intelligence and Sept. 11”, The Defense Monitor, Washington, Volume XXXI, Number 6, June–July 2002

Soviet Archives, “Cuban Missile Crisis”, Library of Congress's Documents from the Soviet Archives, Available on site http://www.ibiblio.org/pjones/russian/Cold_War__Cuban_ Missile_ Crisis.html

Steele, R.D., “Threats, Strategy, and Force Structure: An Alternative Paradigm for National Security in the 21st Century”, Available on site www.oss.net/Papers/white/ Strategy21.doc.

Steele, R.D., “Overview of Open Sources & Services”, Available on site http://isuisse.ifrance.com/emmaf2/96Vol1/ Chapter1.html

Steury, D.P., “Sherman Kent and the Board of National Estimates”, Collected Essays, Center for the Study of Intelligence, Available on site http://www.cia.gov/csi/books/ shermankent/toc.html

Stockwell, J., “In Search of Enemies, The Third World Traveller”, W.W. Norton, 1978, p. 250, Available on site http://www.thirdworldtraveler.com/Stockwell/In_Search_ Enemies.html

Summers, H. G., “The Korean War: A Fresh Perspective”, Military History Magazine, April 1996

Summy, R., "Politics of Globalization," Social Alternatives, 1996,Vol.15, Issue 1

Teke, M., “Priorities for the Possible Impacts of Information Warfare on The Future Battlefield”, Unpublished Master Thesis, Yeditepe University, Istanbul, 2002

Tetik, A., “Devletler Hukuku”, Harp Akademileri Basım Evi, İstanbul, 2001

The Cuba Missile Crisis Main Page “An Overview of The Cuba Crisis”, Available on site http://hyperion.advanced.org/11046/days/index.html

The White House, “The Cuban Missile Crisis”, Special National Intelligence Estimate, Washington, September 1962, Available on site http://www.gwu.edu/~nsarchiv/nsa/ publications/cmc/cmcdoc2.html

Toffler A. and H., “Savaş ve Savaş Karşıtı Mücadele”, translated by Harmancı, M., Sabah Kitapları, Temmuz 1994

Treml, V. G., “Censorship, Access, and Influence: Western Sovietology in the Soviet Union” The University of California Publishing, Berkeley, 1999

Treverton, G. F., “Reshaping National Intelligence for an Age of Information” Cambridge University Press, Cambridge, 2001

Trim, P.R., “The Company-Intelligence Interface and National Security”, International Journal of Intelligence, Vol 13, No: 2

U.S. Military WEB Page, “Glossary of Military Terms”, Available on site http://usmilitary.about.com/library/glossary/i/ bldef03160.htm

United States Congress, “Senate Report of the Joint Committee on the Investigation of the Pearl Harbor Attack”, US Government Press, Washington, 1946, Available on site http://www.ibiblio.org/pha/pha/congress/part_0.html

Upadhyay, G., “Will 1996 Be The Year of Internet?” Business World, January 24, 1996

US Army Home Page, “Biographic Intelligence” Available on site http://www.dl.army.mil/ portals/geopolitical/com/com205.htm

US Government Print Office,“Preparing for the 21st Century: An Appraisal of U.S. Intelligence”, March 1, 1996, Available on site http://www.access.gpo.gov/int/int023.html

Vector 21, “The Defense Intelligence Architecture”, A Strategic Plan for the Defense Intelligence Agency, Available on site http://www.fas.org/irp/dia/vector21/

Verton, D., “NSA Posts Declassified Intelligence From Korean War”, July 18, 2000, http://www.fcw.com/fcw/articles/2000/0717/web-nsa-07-18-00.asp

Waltz, K.N., “Man, the State and War: A Theoretical Analysis”, Columbia University Press, 1965, in Barnet, T.B.,“ Life after DoDth: How the evernet changes everything”, Available on site http://www.geocities.com/ResearchTriangle/Thinktank/6926/ LifeafterDoDth.htm

Warner, M., “The CIA's Internal Probe of the Bay of Pigs Affair”, Studies in Intelligence, Winter 1998-1999, Available on site www.cia.gov/csi/studies/winter98-99/art08.html

Warner, M., “Wanted: A Definition of Intelligence”, Studies in Intelligence, Vol. 46, No. 3, 2002, (Unclassified Edition), Available on site http://www.cia.gov/csi/studies/vol46no3/article02.html

Warren, P., "Technoterrorists: Growing Links Between Computer Technology and the Seedy Underworld of Terrorism, Organized Crime, and Spying." Computer Talk, 1989, Available on site www.fas.org/irp/nsa/ioss/threat96/part02.htm

Washington File “Congressional Report on North Korean Threat”, Available on site http://usembassy-australia.state.gov/hyper/WF991103/epf304.htm

Weekly Summary Excerpt, “ Soviet Expansionism in Korea”, 20 February 1948, Available on site http://www.cia.gov/csi/book/coldwaryrs/5563bod2.pdf

Weinberg, G. L., “A World at Arms”, Cambridge University Press, Cambridge, 1994

White, J., and Gordon, M., “After The Peace Dividend Its War As Usual: Understanding The Gulf Crisis” Available on site http://flag.blackened.net/revolt/awg/gulf_crisis3.html

Willing, R.,” Little changes in world of spying, experts say”, Available on site http://www.ci-ce-ct.com/article/showquestion.asp?faq=5&fldAuto=1260

Wilson, T.R., “Global Threats and Challenges Through 2015”, Statement for the Record, Senate Select Committee on Intelligence, 7 February 2001, Available on site http://www.dia.mil/Public/Press/statement01.html

Wohlstetter, R., “Pearl Harbor: Warning and Decision”, Stanford University Press, Stanford, 1965

Wood, S., ed al., “American Espionage, 1945-1989”, Defense Personnel Security Research and Education Center, Monterey, 1990

Yetiş, N., "Ulusal Güvenlik Sisteminin Geliştirilmesinde Stratejik Teknoloji İşbirlikleri", 2000'li Yıllarda Uzay, Havacılık ve Savunma Teknolojilerinin Öncelikleri Sempozyumu, Bildiriler, İstanbul, 29-30 Nisan 1999

Yılmaz,V., Siyasi Tarih, Harp Akademileri Basım Evi, İstanbul, 1998

Young, R., "Lessons Of Vietnam: A Conversation With Major H.R. McMaster", Available on site http://www.pbs.org/wgbh/pages/frontline/shows/military/etc/lessons.html

Zubok, V. M., "Espionage, KGB, CIA, 1960-1962", CWIHP Bulletin, Washington, Available on site http://cwihp.si.edu/cwihplib.nsf

ÖZGEÇMİŞ

Gökhan SARI

Kişisel Bilgiler :

Doğum Tarihi : 20.03.1970

Doğum Yeri : Balıkesir

Medeni Durumu : Evli

Eğitim :

Lise	1984-1998	Maltepe Askeri Lisesi / İzmir
Lisans	1988-1992	Kara Harp Okulu / Ankara
Yüksek Lisans	2001-2003	Yeditepe Üniversitesi Sosyal Bilimler Enstitüsü

Çalıştığı Birlikler:

1994-1995	Jandarma Komando Taburu Tim Komutanlığı / ELAZIĞ
1995-1997	Jandarma Özel Harekat Birlik Komutanlığı / ADIYAMAN
1997-2001	Jandarma Okullar Komutanlığı Öğretim Başkanlığı / ANKARA
2001	Güçlükonak İlçe Jandarma Komutanlığı / ŞIRNAK
2001-2003	Jandarma Bölge Komutanlığı / İSTANBUL