NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

OPEN-SOURCE INTELLIGENCE IN THE CZECH MILITARY: KNOWLEDGE SYSTEM AND PROCESS DESIGN

by

Roman Krejci

June 2002

Thesis Advisor:	Mark E. Nissen
Second Reader:	Kenneth R. Dombroski

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2002	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Open-Source Intelligence in the Czech Military: Knowledge System and Process Design			**5. FUNDING NUMBERS**
6. AUTHOR(S) Roman Krejci			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT

Owing to the recent transitions in the Czech Republic, the Czech military must satisfy a large set of new requirements. One way the military intelligence can become more effective and can conserve resources is by increasing the efficiency of open-source intelligence (OSINT), which plays an important part in intelligence gathering in the age of information. When using OSINT effectively, the military intelligence can elevate its responsiveness to different types of crises and can also properly allocate its limited resources into areas, in which covert collection is unavoidable.

This thesis combines modern knowledge-management theory with current issues in military intelligence, creating a base for designing a future OSINT system in the Czech military. First, the thesis introduces recent US research in knowledge management and examines the current intelligence issues. Then the thesis examines the Czech military intelligence environment in the framework of the national security and defense policy and also analyzes the actual use of OSINT in the Military Intelligence Service, following the four stages of the knowledge system and process design. Finally, the thesis outlines the main aspects of the future OSINT knowledge-management system and recommends further research and development.

14. SUBJECT TERMS Knowledge Management, Intelligence, Open-Source Intelligence, Czech Military			**15. NUMBER OF PAGES** 133
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

THIS PAGE INTENTIONALLY LEFT BLANK

OPEN-SOURCE INTELLIGENCE IN THE CZECH MILITARY: KNOWLEDGE SYSTEM AND PROCESS DESIGN

Roman Krejci
Lieutenant Colonel, Army of the Czech Republic
ing., Military College Vyskov, CZ, 1985

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
June 2002

Author: Roman Krejci

Approved by: Dr. Mark E. Nissen
Thesis Advisor

Kenneth R. Dombroski
Second Reader

Douglas A. Brook, Ph.D.
Dean, Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Owing to the recent transitions in the Czech Republic, the Czech military must satisfy a large set of new requirements. One way the military intelligence can become more effective and can conserve resources is by increasing the efficiency of open-source intelligence (OSINT), which plays an important part in intelligence gathering in the age of information. When using OSINT effectively, the military intelligence can elevate its responsiveness to different types of crises and can also properly allocate its limited resources into areas, in which covert collection is unavoidable.

This thesis combines modern knowledge-management theory with current issues in military intelligence, creating a base for designing a future OSINT system in the Czech military. First, the thesis introduces recent US research in knowledge management and examines the current intelligence issues. Then the thesis examines the Czech military intelligence environment in the framework of the national security and defense policy and also analyzes the actual use of OSINT in the Military Intelligence Service, following the four stages of the knowledge system and process design. Finally, the thesis outlines the main aspects of the future OSINT knowledge-management system and recommends further research and development.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES AND GRAPHS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ABBREVIATIONS

ACE	Allied Command in Europe
ACR	Army of the Czech Republic
AJP	Allied Joint Publication
ARCTSC	Analysis of Required Capabilities, Target Structure and Composition
BBC	British Broadcasting Corporation
BIS	Bezpečnostní informační služba (Security Information Service)
C4I	Command, Control, Communication, Computers, and Intelligence
CBW	Chemical and Biological Weapons
CCIRM	Collection Coordination and Information Requirements Management
CD	Compact Disc
CD-ROM	Compact Disc—Read Only Medium
CEDSP	Common European Security and Defense Policy
CIA	Central Intelligence Agency
CIMIC	Civil-Military Cooperation
CIO	Chief Information Officer
CKO	Chief Knowledge Officer
CNN	Cable News Network
COMINT	Communication Intelligence
COTS	Commercial Off-the-Shelf
CSFs	Critical Success Factors
DBMS	Database Management System
DBK	Dominant Battlespace Knowledge
DVD	Digital Video Disc
DW/DM	Data Warehouse/Data Mining
DoD	Department of Defense
ELINT	Electronic Intelligence
EU	European Union
ES	Expert Systems
FAS	Federation of American Scientists
FBIS	Foreign Broadcast Service
HUMINT	Human Intelligence
ICBM	Inter-Continental Ballistic Missiles
IMINT	Imagery Intelligence
INFOSEC	Information Security
INTs	Intelligence Disciplines
IT	Information Technology
KBS	Knowledge-Based System
KMLC	Knowledge Management Life Cycle
MASINT	Measurement and Signature Intelligence
NATO	North Atlantic Treaty Organization
NIPRNET	National Internet Protocol Routing Network
NMS	National Military Strategy

NOSINTH	NATO Open-Source Intelligence Handbook
NSS	National Security Strategy
OSINT	Open-Source Intelligence
OSINTH	Open-Source Intelligence Handbook
OSIS	Open-Source Information Network
PCR	Police of the Czech Republic
PEO	Peace Enforcement Operations
PfP	Partnership for Peace
PKO	Peace Keeping Operations
R&D	Research and Development
SIGINT	Signal Intelligence
SSL	Secure Sockets Layers
StB	Státní bezpečnost (State Security)
UN	United Nations
ÚZSI	Úřad pro zahraniční styky a informace (Bureau for Foreign Contacts and Information)
V-OSINT	Validated Open-Source Intelligence
VOZ	Vojenské obranné zpravodajství (Military Defensive Intelligence)
VPN	Virtual Private Network
VZ	Vojenské zpravodajství (Military Intelligence)
VZS	Vojenská zpravodajská služba (Military Intelligence Service)
WMD	Weapons of Mass Destruction
ZZS	Zákon o zpravodajských službách (Intelligence Services Act)

ACKNOWLEDGMENTS

The work I accomplished could be hardly possible without the help and support of many people.

I would like to thank my supervisor and my colleagues for all the support and goodwill that allowed me to study at the Naval Postgraduate School. Also, I want to acknowledge my professors and lecturers, who led me through the studies—particularly Prof. John Arguilla for his excellent insight into the military matters and astounding clear-headedness of an exceptional thinker. Many thanks to my thesis advisor, Dr. Mark Nissen, and to my second reader, Kenneth Dombroski, for their candid approach and unstrained facilitation of my research and thesis work. Furthermore, I want to thank my thesis editor, Ronald Russell, for his excellent, highly professional editorial work, and also for his friendship. Finally, my greatest appreciation goes to my wife Věra, my daughter Jana, and my son Víťa for their patience and support while I completed this work.

THIS PAGE INTENTIONALLY LEFT BLANK

I. THESIS SUBJECT, OBJECTIVES, AND RESEARCH APPROACH

Chapter one discusses the purpose and objectives of this thesis. It presents brief background information and the research questions. The chapter also provides an overview of the research approach and describes its scope, limits, and assumptions.

A. BACKGROUND

The Czech military intelligence needs to evolve into a different type of service—for several reasons. Recent political, economical, and social transitions have imposed different security threats on the Czech Republic. Moreover, accession to NATO has brought a large set of requirements that military intelligence must meet. In addition, the information revolution presents permanent challenges for intelligence collection and processing.

Indeed, much has already changed since the peaceful revolution in 1989. However, many of the military intelligence procedures and assets remain frozen in an old-fashioned mindset. The economical and political disposition of the Czech government during the mid-1990's left the top military management with many unanswered questions. Furthermore, frequent ad hoc adjustments in both organizational and procedural arrangements have not significantly helped the military intelligence to move ahead.

It is obvious that the Czech Republic does not have, and will unlikely ever have, the collection and processing capabilities of the major powers, such as the USA, Canada, and the UK. The Armed Forces of the Czech Republic, limited by budget constraints and by the sociopolitical situation inside the country, cannot simply make a huge leap toward state-of-the-art military technologies. However, if the top management of military intelligence really wants to improve the service, a systematic and scientific approach is necessary in order to achieve positive results.

One way to increase intelligence effectiveness and conserve resources is to employ *open-source intelligence* (OSINT) efficiently. Military intelligence should fully embrace all the advantages of OSINT, which plays an important part in intelligence gathering in the age of information. When using OSINT effectively, the military intelligence can elevate its responsiveness to different types of current crises and can also allow the proper allocation of its limited resources into other areas, in which covert collection is unavoidable.

Although the Czech military intelligence currently uses open sources for gaining different kinds of information, a systematic approach to this domain has been missing and the use of OSINT is far from an ideal solution. However, by building upon the framework of knowledge management theory, a basic design of modern OSINT in the Czech military intelligence can be created. Such an arrangement can then be considered as a base for further research and development in this area.

B. OBJECTIVES

On one side, knowledge management theory and its implications represent a new arena for the Czech military, an arena that has not been explored yet. On the other side, using open sources for intelligence purposes was significant even in the pre-revolution information gathering. But OSINT was practically abandoned in the early 1990's and has not been systematically modernized since then.

This thesis seeks to meet the following objectives:

- To introduce recent US research in knowledge management to the Czech military environment.
- To indicate contemporary problems in intelligence and to examine current knowledge about OSINT.
- To inquire the military intelligence environment in the framework of the Czech security and defense policy, and to analyze actual use of OSINT in the intelligence.
- To create a theoretical base for future design of OSINT systems and processes in the Czech military intelligence.

- To make a set of recommendations for further research and development.

C. RESEARCH QUESTION

This research is focused on answering a primary question "How can the Czech military intelligence design its open-source intelligence?" To help answer the question, these subsequent secondary questions will be addressed:

- What is knowledge, and how is it used in military intelligence processes?
- What is open-source intelligence (OSINT), and how does it contribute to military intelligence?
- What is the current status of OSINT in the Czech military intelligence?
- How can the basic steps of knowledge system and process design be used to model the improved OSINT in the Czech military intelligence?
- What recommendations can be made for the Czech military intelligence management?

D. SCOPE, LIMITATIONS, AND ASSUMPTIONS

The scope of this thesis includes an overview of knowledge management theory. Also, the thesis provides a current view of intelligence in general, and further concentrates on the currently most auspicious discipline, open-source intelligence (OSINT). The author builds on the extant security and defense policy of the Czech Republic and examines the present approach to using OSINT in the Czech military intelligence. Most of the attention is paid to the strategic level, represented by the Military Intelligence Service (VZS). However, other levels are included whenever possible in order to provide for wider context in OSINT knowledge management process and system design.

The author does not look for particular information technology (IT) solutions in terms of hardware and software procurement. Moreover, purely IT oriented solution are always interim and provide only temporary competitive advantage. Neither does the author want to create a complete organizational model. For such a goal, specialized teams and whole sets of introductory steps would be needed. So, the thesis stresses valid principles, taken from both the knowledge management theory and the current literature about intelligence, and establishes a base, upon which the further development of OSINT in the Czech military intelligence can be made.

Also, the thesis does not strive to serve as an account of available open sources. A complete account is not possible owing to the volume and dynamics of OSINT. Even for one single area of interest, an extract of available open sources will be intensely discriminative. So the references to open sources used in this thesis will serve only for explanatory purposes and as examples.

E. OVERVIEW OF THE RESEARCH APPROACH

The research techniques used for this thesis include a review of topical literature related both to knowledge management and intelligence. Also, a review of current Czech military doctrines and policies is performed. Subsequently, a deductive and inductive approach is applied to conduct an analysis of the author's own observations related to OSINT in the Czech military intelligence. This analysis is also accompanied by the results of semi-structured interviews with Czech intelligence staff members. Finally, a knowledge management framework is used to create an introductory design of the OSINT system and processes in the Czech military intelligence.

II. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

This chapter outlines the basic aspects of knowledge management. It also looks at intelligence in general and open-source intelligence (OSINT) in particular in order to create sufficient theoretical background for further use.

The first part of the chapter briefly introduces the current understanding of knowledge, knowledge management, and the knowledge process and system design. The next section examines the body of knowledge about intelligence in general. The last part concentrates on open-source intelligence in more details.

A. KNOWLEDGE MANAGEMENT

Knowledge is power. This expression has not changed much over time. But the importance of such power has changed, owing to the evolution of technological tools that can be used to manage knowledge. The recent widespread advances in computer and communication technologies are usually labeled as the *information revolution*. While the new technology has reached every possible corner of the business world, the military with its highly hierarchical structure struggles to achieve interconnectivity and information superiority in the future battlespace.

Owens (2000) and others argue that the information revolution and advances in computer technology have brought unfailing possibilities for future combat. Such optimistic exponents believe that the advances in computing and communication are truly revolutionary and will change the very nature of the military. According to them, widespread knowledge about potential and existing adversaries—enabled by computer networks, advanced overhead surveillance, and real-time communication—will allow armies to wage better wars. In such an environment of *Dominant Battlespace Knowledge* (DBK), the military will be smaller yet stronger and more mobile, able to react on a short notice. Through the use of advanced information technology, the friendly forces should be better protected and employed more wisely while the enemy forces will be shattered—mostly thanks to the ability to find and track all important enemy assets promptly.

Opposing Owens' views, O'Hanlon (2000) and others see certain disparities in the military assets evolution and argue that while there has been very significant progress in computing and communication systems, there are many other areas where the limits are still severe and evolution slow. Constraints will still remain significant in infantry and urban warfare; optical and radar penetrability of forests and buildings will probably not be improved radically; acoustic and other types of sensors are unlikely to increase their reach dramatically; and detection of chemical and biological materials will likely remain severely limited unless the agents are released out of their carriers.

Many lessons can be learned from the recent developments in the intelligence community. Indeed, the Czech military intelligence should not be built on purely technical premises. On the other hand, proper application and systematic use of technological tools will help to manage knowledge effectively.

1. Data, Information, and Knowledge

In order to understand knowledge and knowledge management principles better, one must clearly distinguish *knowledge* from *information* and *data*. People commonly use "data" and "information" as synonyms while "knowledge" is more clearly viewed as the data or information that people retain in their minds. As the three terms are sometimes used interchangeably, they must be defined at the onset.

Data: Data are most frequently perceived as being related to computer and communication technology. Few authors even bother to define the term, assuming that its meaning is so obvious that it does not require classification. Many misunderstandings can arise from failing to consider the meaning of such a basic concept.

On the academic basis, Clarke (2001/1) provides one useful and simple definition: "Data are any symbol, sign or measure in a form that can be directly captured by a person or a machine." On the military side, the US Department of Defense (DoD), for example, uses this definition of data: [Data represent facts, concepts, or instructions, such as characters or analog quantities, to which meaning is or might be assigned. Data exist in a formalized manner, suitable for communication, interpretation, or processing by humans or by automatic means.] (JP-1.02. 1994)

So data are understood as a set of discrete facts and events, such as text, numbers, signs, and so on. By itself, data have no meaning until placed in an appropriate context and transferred into information.

Information: The term "information" also requires a proper definition. Dictionaries are usually too vague and different researchers often bring inconsistent definitions. Clarke (2001/1), for example, provides for a definition by encapsulating these elements: "Information is data that has value. Informational value depends upon context. Until it is placed in an appropriate context, data are not information, and once it ceases to be in that context it ceases to be information." A definition invoked in the NATO military intelligence only states that "Information is unprocessed data of every description that may be used in the production of intelligence." (AJP-2.0. 2001) One can see that these definitions do not agree—while the former accentuates information value that is built upon data, the latter merely states information serves as base for an intelligence product.

Information should be understood as a message that possesses meaning; that is what distinguishes it from data, which have no significance on its own. The meaning need not to be the same in the minds of both the sender and receiver. Actually, it is the receiver's cognition what makes the data become information (Davenport and Prusak 1998).

Knowledge: The term "knowledge" is often used to refer to "a body of facts and principles accumulated by mankind in the course of time" (Clarke 2001/2). This is just one of many definitions, but it precisely expresses the necessity of human ability to build knowledge and also the dependence of knowledge on time. This definition also shows that knowledge is based upon previously gained information.

As to the forms in which knowledge can exist, theory distinguishes two main categories—*explicit* knowledge and *inferred* knowledge.

Explicit knowledge is formal, structured, and readily accessible. It can be found in books, manuals, instructions, on the Web, in groupware, and databases (Nonaka 1994, Nissen 2001). Explicit knowledge is easier to manage and is better supported by existing IT tools. Optimally, an organization should aspire to capture and to use as much knowledge as possible in this form.

Tacit, or *inferred*, *knowledge* is informal, unstructured, and can be accessed only via eduction and observation of behavior (Liebowitz 1999). Tacit knowledge refers to expertise contained within the minds of people (Nonaka 1994, Nissen 2001). It is hard, if not impossible, to transfer it to an explicit form; inferred knowledge is difficult to manage.

In relation to these two categories, one should see that transfer of knowledge can occur either through *structured media* (such as documents and books) in the case of explicit knowledge, or by *interpersonal contacts* (such as conversation, training, apprenticeship, and so on) in the latter instance.

Nissen et al. (2000) summarized work of scholars concerning the distinction between data, information, and knowledge according to their *abundance* and *actionability* [applicability, or practicability], or knowledge hierarchy is exhibited in *Figure 1*.

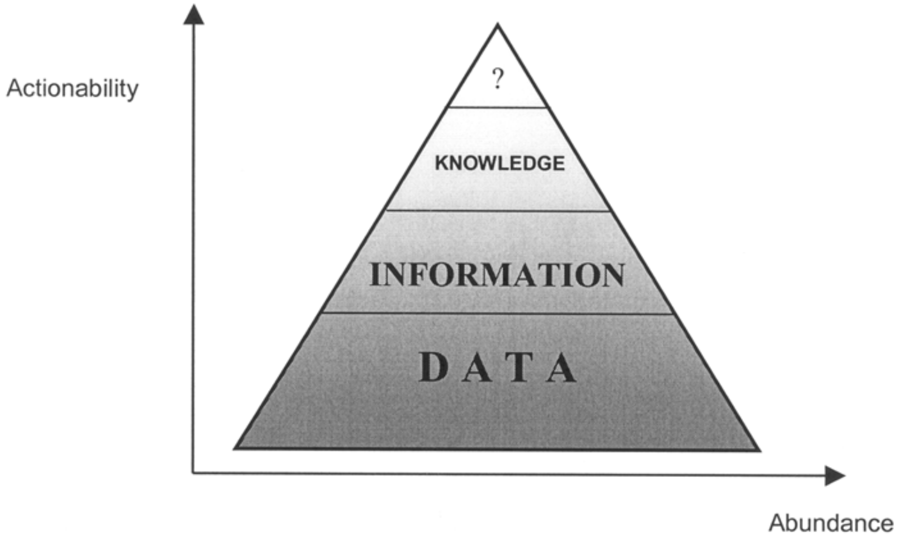


Figure 1. Knowledge Hierarchy

The correlation of the three layers, data, information, and knowledge is as follows: Data become information when the receiver adds meaning to it. Information becomes knowledge when it is applied, or when an action, based upon information, occurs.

Knowledge lies in the "hierarchical pyramid" above information and data. However, most information technology (IT) employed in order to manage knowledge appears to target data and information rather than knowledge itself (e.g. Ruggles 1997). Moreover, existing IT is oriented primarily at database management systems (DBMS), data warehouses, data mining (DW/DM), Internet/intranets and groupware (O'Leary 1998). Extant IT provides, at a maximum of its ability, only common, machine-dependent means for the management and distribution of information, not knowledge.

For example, one can see that data mining applications are mostly associated with sophisticated data pattern matching. Databases and indexing help structure data and information. Groupware and search engines are mostly related to distribution of information. However, the actual ability to build knowledge upon such data and information still remains highly individualized.

2. Knowledge Management and Knowledge Flow

The power of knowledge has been acknowledged for hundreds of years. However, today it is recognized more at the enterprise level rather than at the level of successful individuals. Studies of prominent technology firms showed that knowledge has become the key economic resource and dominant source of comparative advantage in the market competition (Drucker 1995, and others). Such "corporate" knowledge is denoted as *knowledge management* (Davenport and Prusak 1998). Although the definitions of knowledge management vary (see for example Leibowitz's summary 1999), they share similar key points—knowledge must be systematically built and applied to fulfill organization objectives, enhance collaboration, support innovation, and magnify performance. Commonly, knowledge management means "to get the right knowledge to the right people at the right time to allow the right decisions."

Knowledge can generate innovation, and an organization can obtain a competitive edge through such innovation (Davenport and Prusak 1998). But, to posses the competitive advantage, knowledge must be not only created but also transferred and used throughout the whole organization. Such movement is called *knowledge flow*. It is obvious, for the military, that knowledge flow is imperative. However, the phenomenon of knowledge flow is not properly understood, and the benefits of theory of knowledge management and its application are not fully employed.

The mechanics of knowledge flow between two *nodes*, or *agents*, in the organizational structure—no matter whether the nodes are people or machines—is quite similar to inter-computer data flow through several layers of hardware and software. The flow starts at the knowledge level and descends through information to data in one agent. The data are then transmitted via certain media (e.g. a computer network) and flow to the other agent. Then the flow ascends in the reverse order through information to knowledge (Nissen 2001).

This notion of *layered processing for knowledge flow* has brought some very important insights:

- In this concept, machines, such as computers, expert systems, and intelligent agents, and people, as individuals, in groups, or in organizations, exchange knowledge via layers of information and data in a similar fashion.
- Direct transfer of knowledge or information is not possible because the exchange always occurs at the data level. Implicitly, if knowledge is to be transferred between different agents, the agents must be able to send and to receive data, upon which the knowledge is based.
- To comprehend knowledge flow, one must understand the processing used by various agents (again, human or machine) to transform data and information into actionable knowledge, and vice versa.
- The abstract and "intangible" concept of knowledge can be turned into an observable and measurable action—thus allow differentiating the knowledge of various agents based on their relative performance.

The primary objective of knowledge flow is "to enable the transfer of capability and expertise from where it resides to where it is needed—across space, time, and organizations as necessary." (Nissen 2001, p. 1) Studying knowledge management and knowledge flow in its complexity, researchers Nissen, Kamel, and Sengupta described the cyclical flow of knowledge in its complexity by developing the *Knowledge Management Life Cycle* (KMLC).

3. Knowledge Management Life Cycle

Knowledge management has been investigated for many years. Different authors were describing knowledge and knowledge management, mostly concentrating on how knowledge is captured and shared. A comprehensive view was missing until Nissen et al. (2000) presented a life cycle associated with knowledge management. Their amalgamated model of KMLC is depicted in *Figure 2*.

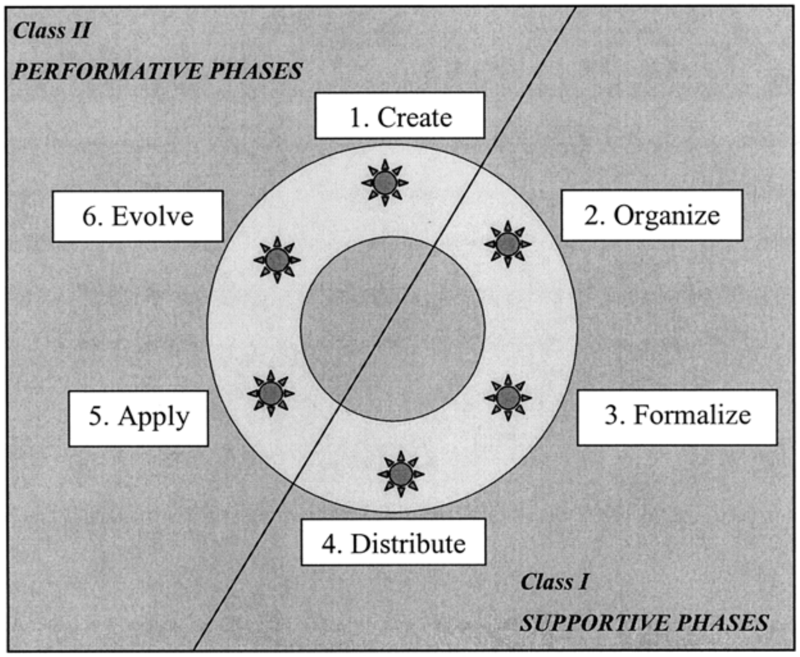


Figure 2. Knowledge Management Life Cycle

As exhibited in the figure, the KMLC is divided into six phases and two classes: *Creation* of knowledge occurs primarily in the minds of individuals. This creation encompasses the discovery and the development of new knowledge (Gartner Group 1998). Such knowledge is tacit, unstructured and external to the organization (Nonaka 1994). In the second phase, which definitely pertains to the organization, knowledge is *organized*. It is mapped, or bundled, so that the organization can recognize it. Then, in the phase of *formalization*, such knowledge is to be transposed from its tacit to its explicit form. Now, knowledge is structured and internal to the organization. Once formalized, knowledge is *distributed* throughout the organization in order to be shared among its members. This phase, heavily supported by existing IT tools, is currently the most emphasized phase. Knowledge, after that, can be *applied,* or used for problem solving or for decision-making processes. Finally, knowledge can further *evolve*, meaning that it can be refined and continually developed. Moreover, the evolution of knowledge can lead to the creation of new knowledge, thus to the generation of a new KMLC.

When comparing the six phases of the KMLC, Nissen et al. noted that extant systems and practices support the process of knowledge management unevenly. Especially at the organizational level, they mostly support knowledge organization, formalization, and distribution, i.e. the phases grouped in *Class I*. This class is inherently *supportive* to people in the organization because it supports people in the enterprise, whom in turn apply, evolve and create knowledge in the organization. Class I systems are known as *localized management systems*, represented by tools such as knowledge maps, "yellow pages," distributed lessons learned, and others. Obversely, the phases from *Class II* are not well supported by existing IT. They are innately *performative* in nature because they perform knowledge-management activities, either in combination with or instead of people in the organization.

Researchers (e.g. Nissen et al 2000) have shown that the knowledge flow has not been fully explored yet, especially in terms of integrating the knowledge *process design* with the knowledge *system design*. Yet they concluded that the current set of methodologies used in reengineering, expert systems, and information systems provide capabilities to design and develop IT, which is necessary for knowledge management systems and processes. Furthermore, the researchers stressed that no single methodology is sufficient to develop all knowledge management systems and processes; a multiple developmental approach is essential. Such approach is represented by the *knowledge system and process design*.

4. Knowledge System and Process Design

As IT has become more and more present in our daily lives many enterprises and governmental organizations view it as a magic tool that could improve performance dramatically. Indeed, computer networks can create an infrastructure requisite for knowledge exchange, but reality proved many times that a simple insertion of IT into existing processes does not provide a warranty for the desired improvement. As noted by Weber (1993), IT provides only a temporary competitive advantage; it is just "self-canceling technological advantage." Contrary to material assets knowledge can grant sustainable advantage because it generates increasing returns—knowledge assets increase with use (Davenport and Prusak 1998).

Nissen and other researchers have revealed that information technology must be integrated with the design of the process it supports—including the organization, people, procedures, organizational culture, and so on. They identified two *contextual factors* that define and limit knowledge management systems design: the *organization*, and the *nature of knowledge underlying the task* (Nissen et al. 2000).

When considering the first contextual factor, an organization, attention should be paid to these aspects:

- *Not everything that occurs is recorded*: An organization has memory systems that maintain the lessons learned from experience (Levitt and March 1988). The knowledge resident in an organization’s memory establishes a mechanism for conserving its history, routines and the lessons learned over time. As outlined, these memory elements can be recorded in many ways, formally as well as informally. However, no organization can currently record all of the existing memory elements.

- *Essential aspects of knowledge reside in the informal state*: Knowledge captured via informal mechanisms is often richer and more important than what is stored formally. So the key to building useful knowledge management systems lies in solutions that can capture the essence of informal knowledge in a shape that can be preserved. Such knowledge, once lost, cannot be re-created easily (Hutchins 1991). When, for example, a member separates from the organization, the potential for loss of knowledge is ample, especially in cases when locating existing knowledge in time and transferring it to where it is essential is troublesome.
- *The structure of the organization significantly influences the practice of knowledge creation, storage, and dissemination*: Conventional organization structures rely more on informal networks and communities, and have well-developed channels and norms for communication. Modified organizational forms enabled by information technology, such as virtual and networked organizations, are typically ad hoc in nature and must form such channels first. Moreover, maintaining continuity is difficult, and the history of relevant organizational knowledge is not easily available.
- *Retention and updating of knowledge is mostly an upstream activity while the benefits from its dissemination and use go downstream*: (Davenport and Prusak 1998, Grudin 1996) This contraposition creates specific problems. The decision is often made on the basis of managerial factors, such as cost and schedule. Because capture of knowledge can add to the cost and cause time delays, high proportions of projects are terminated before they are completed. Also, the benefits of the knowledge are usually accrued in the latest stages of the project and many times by different people. Thus focusing only to technical aspects of knowledge management applications is insufficient. Such systems can only prosper if appropriate incentives for the retention and updating of knowledge are provided.

The nature of knowledge underlying the task, the second contextual factor, defines and limits knowledge management systems design in the following ways:

- *Hierarchical practices, such as manuals and job descriptions, frequently used to organize the processes are usually inadequate for complex problems*: That is because the effort involved in acquiring knowledge required to perform a complex task effectively is not negligible (Lave 1988, Lave and Wenger 1990), and because the knowledge acquired and represented in the canonical methods can become obsolete with changes in the task-related technology (Suchman 1987).
- *The actual approach to complex problems solving often departs from the prescriptive methods*: Individuals performing complex tasks may improvise, resorting for non-orthodox practices to overcome shortages of hierarchical approaches. (Zuboff 1988) These non-formulary practices can serve as extensions of canonical methods, compensating for the omissions and inadequacies of prescriptive knowledge. Such practices can also modify the hierarchical methods, once they seem obsolete or less effective than the corresponding methods used in practice.

When studying the knowledge management, researchers Nissen, Kamel, and Sengupta focused on knowledge management from three integrating angles: reengineering process innovation, expert systems knowledge acquisition and representation, and information systems analysis and design. They coordinated these three perspectives into one complex design approach, which starts with the analysis and design of the organizational interest, continues with the knowledge capture and formalization, and ends with the system design and implementation. Their design process is referred to as the *knowledge system and process design.*

According to the researchers' study, the knowledge system and process design should follow four stages (Nissen et al. 2000, Nissen 2001):

(1) *Process Analysis*: The first stage requires understanding the objectives and strategies of an organization. Without understanding the process (including different variations) and required knowledge, there is no use to begin

designing the system. The aim here is to define the knowledge ensuring effective performance of each process of interest. Canonical practices might be of help but a "hands-on" approach is also needed.

(2) *Knowledge Analysis*: This analysis results from the previous analysis and concentrates on identifying and analyzing the knowledge within an organization. Central to this step is identification and analysis of *critical success factors* (CSFs)—activities that must be performed effectively in order for the mission to be successful. CSFs are useful to identify what knowledge is crucial to process performance in a particular organizational setting and context.

(3) *Contextual Analysis*: In this phase, knowledge itself should be captured, particularly the tacit knowledge used by specialists. Databases, intranet applications, and search and retrieval systems can be used to organize, to formalize, and to distribute the captured knowledge. "Yellow pages" and knowledge maps, when available, can help identify who possesses what kind of knowledge. Understanding the organization and the nature of knowledge is essential in this assessment.

(4) *Systems Analysis and Integration*: In this final stage, the organization's current procedures and information systems are analyzed. Also, any methodologies, techniques, and tools that are available and are understood can be employed to develop a knowledge management system. Information systems required to automate and support knowledge work can then be effectively designed.

Knowledge itself seems to be difficult to manage and is resistant to reengineering and process innovation (Davenport 1995). The key point is that all three "facets"—*process*, *knowledge*, and *information*—should be considered together when designing knowledge systems and processes (Nissen et al 2000). Abrupt implementations of "IT solutions" into existing processes and organizations without having considered all key factors helps little.

As expressed before, knowledge management is essential for an organization striving for a competitive advantage. Certainly knowledge management represents a significant challenge in such a complicated and large "enterprise" as a military. Yet, effective knowledge management is vital for the military domain that is solely based upon knowledge—military intelligence.

B. INTELLIGENCE AND MILITARY INTELLIGENCE

Since the end of the Cold War, many nations, including the Czech Republic, have found their security less threatened. Thus the focus of national security has changed, but the mission of the military intelligence community remains the same: to provide timely assessed intelligence for military commanders and to support military operations.

Initially this section presents some basic information related to intelligence, as a foundation for further analysis. As military intelligence is just a more specific subset of intelligence, most of the general facts about intelligence also apply to military intelligence.

1. Intelligence Functions and Intelligence Disciplines

As the term "intelligence" is used in numerous ways, defining the term is essential. In terms of national security, intelligence, as it is more or less unanimously defined, can be seen as:

- A *process* during which required information is collected, processed, analyzed, and disseminated to the customers of final intelligence. In other words, intelligence is a process that converts raw data into a solid product, which satisfies the needs of those to whom it is concerned.
- A *product* representing the result of the intelligence process.
- An *organization* or an *agency*, which actually conducts some or all of the intelligence functions.

Many people assume that the main task of an intelligence service is to describe the truth about something in reality. As Lowenthal (2000) explains, intelligence is not about truth. If something were known to be true, states would not need intelligence services to collect or to analyze the information about these facts. The requirement to always discover the truth would set a standard that no intelligence agency could achieve. Thinking of intelligence as a matter of describing approximate reality is more accurate. Intelligence tries to understand what is occurring in any given issue and tries to produce reliable, unbiased, and honest (i.e. objective and non-politicized) intelligence.

So, why do we have intelligence agencies? Intelligence should exist solely to support decision-makers. To allow better decisions, intelligence agencies must provide decision-makers with accurate, timely, and tailored intelligence. This is true for every intelligence service—be it a national foreign intelligence service, a military intelligence agency at the strategic level, or a military intelligence unit on the battlefield. Any motive other than supporting decision-makers would be wasteful or even illegal. According to Lowenthal (2000) intelligence services exist for at least four reasons:

(1) *To Avoid Strategic Surprise*: The leading goal of any intelligence service must be to monitor threats, troops, and events that can potentially jeopardize the nation's existence.

(2) *To Provide Long-term Expertise*: As policy makers come and go, being versed in all the national security issues with which they deal is impossible. They need intelligence personnel with extensive expertise and knowledge on many subjects. The intelligence community has a relatively stable analytical staff, and it tends to have fewer political appointees than other elements of the state bureaucracy.

(3) *To Support the Policy Process*: Policy makers constantly need tailored and timely intelligence that will provide background information and warnings. Intelligence agencies can prepare such information and assess the risks and benefits of the steps the policy makers intend to take.

(4) *To Maintain the Secrecy of Information, Needs, and Methods*: Since adversaries and competitors withhold information, and since we also want to keep specific information secret, each nation must possess effective intelligence services. With such services, a nation has the means for collecting

and processing information about other potentially hostile nations while guarding its own sensitive information against the adversary nations.

The complexity of all the functions listed above, coupled with the development of the technical means for collecting information, has led to a specialization in intelligence gathering. Hence separate, yet interconnected, *intelligence disciplines* have been created. Realistically, no single individual or organization can efficiently and accurately collect and process all the available information, and this fact has generated a need for intelligence specialization. Furthermore, considering the impact of IT on today's society, further specialization will likely occur.

Over the past four decades, NATO intelligence disciplines have evolved and have been categorized into five main categories:

- *Human Intelligence* (HUMINT);
- *Signal Intelligence* (SIGINT), which has two subcategories:
  - *Communication Intelligence* (COMINT), and
  - *Electronic Intelligence* (ELINT);
- *Measurement and Signature Intelligence* (MASINT);[1]
- *Imagery Intelligence* (IMINT);
- *Open-Source Intelligence* (OSINT).

Obviously, HUMINT represents human, non-technical discipline while SIGINT, IMINT, and MASINT are mostly technical. OSINT comprises both human and technical approaches.

2. Intelligence Process and Intelligence Cycle

This section concentrates on intelligence as a process. According to current definitions,[2] intelligence as a process involves requests for the collection and analysis of

[1] This discipline is recognized only by the US intelligence. Other nations do not use this category as a separate intelligence discipline. Also, this category is not included in NATO allied doctrines, such as AJP-2.0. (2001)

specific types of information, and then provides the finished intelligence to decision-makers. In these terms, the intelligence process should be understood as a set of interrelated steps, transforming raw information into a finished intelligence product. To describe the entire process, the intelligence community uses a model called the intelligence cycle.

Most publications (e.g. AJP-2.0. 2001, FAS 1996) describe the intelligence cycle as both separated, and yet inter-connected, components of direction, collection, processing, analysis and production, and dissemination. To this, Lowenthal (2000, pp. 50-51) presents his more explicit model, which also contains consumption and feedback. To better describe the complexity of the intelligence process graphically, the author created an amended model of the intelligence cycle. The model is depicted in *Figure 3*.

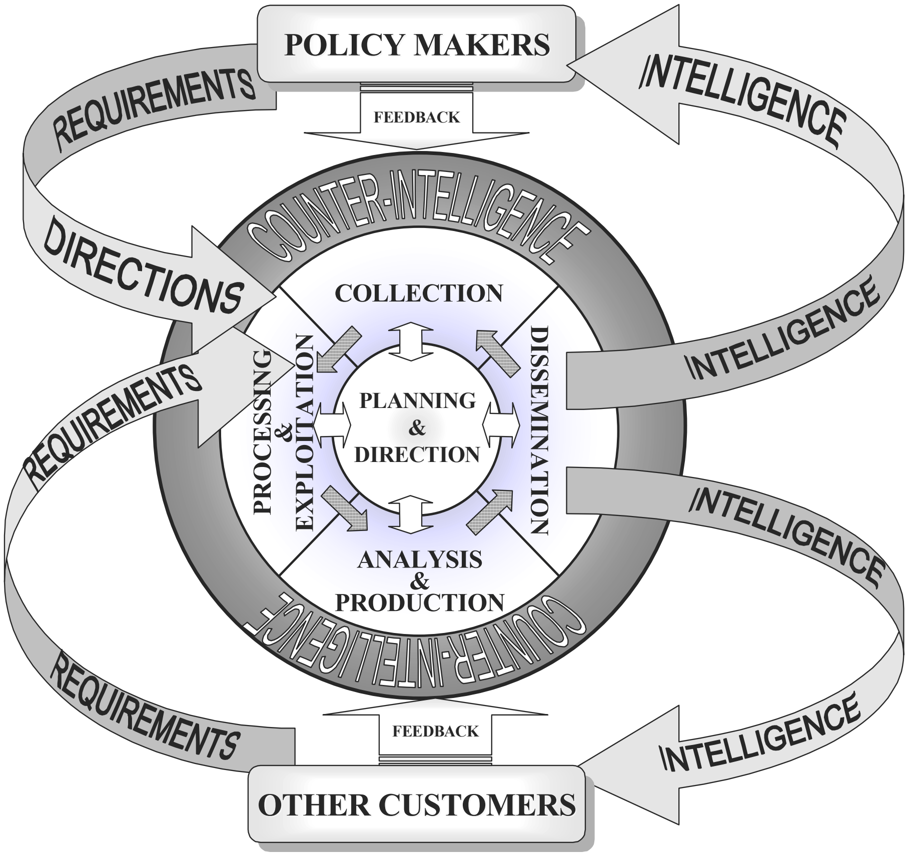


Figure 3. Amended Model of the Intelligence Cycle

[2] See for example: AJP-2.0. 2001, p. 1-2-3 or Lowenthal 2000, p. 8.

The intelligence process, by nature, is rather continuous. The intelligence cycle has no specific or definite beginning or ending. Intelligence operates in an environment with erratic information, changing requirements, and unending analyses. However, the following separable components of the intelligence process have been determined:

Planning and Direction: In the amended model presented in Figure 3, planning and direction are in the center as the core elements of the intelligence process. Intelligence organizations are predominatingly bureaucratic in nature, so planning and direction is vital to keep them effective. Moreover, as the intelligence budgets and manpower decrease and possible threats become more scattered, intelligence must be oriented toward the stated or implied needs of its customers.

Planning and direction emanates outside the intelligence agency, but is also necessary inside the organization itself. As decision-makers pose their tasks and questions, an intelligence agency further specifies, analyzes, and refines the requirements to ensure that:

- The intelligence organization comprehends the requirements;
- The tasking authority understands the capability of the agency;
- The available collection assets will be properly tasked in accordance with the intelligence requirements.

Rather than seeing planning and direction as only the first phase of the intelligence cycle, one should understand it as a core element that receives tasks, sends commands and collects feedback almost continuously.

Collection: Collection is the actual gathering of information needed to produce the finished intelligence. Intelligence assets collect information using different sources and methods, generally referred to as "intelligence disciplines." The five collection disciplines, HUMINT, SIGINT, MASINT, IMINT, and OSINT, were already introduced in the previous section.

Collection assets gather information, in accordance with plans and procedures, to fill the gap between what is already known and what must be known in order to answer the consumers' questions and to fulfill the tasks assigned to the intelligence agency.

Processing and Exploitation: This phase fulfills a dual function in that the collected data and information are usually processed and then exploited for further analysis. This is especially common for the technical intelligence disciplines where data does not arrive in ready-to-use form. *Processing* converts the collected signals into images or other forms. In *exploitation*, analysts transfer the data and information into a more usable form through decryption, language translation, data reduction, and so on.

Analysis and Production: Information is seldom usable in its raw form. Therefore, it must be analyzed. Furthermore, information can often be fragmentary and even contradictory. During the analysis, new value is added through *collation*, *evaluation*, *analysis* and *integration*, and *interpretation*. An analyst constructs a coherent picture of the evaluated information and produces the finished intelligence product that assesses events, judges possible implications and estimates further development.

Dissemination: If the finished intelligence is not delivered to its intended recipients, it has zero value regardless of its quality. Thus dissemination is an equally important part of the intelligence cycle. The finished intelligence must be distributed in an accurate, complete, yet concise and timely fashion, and it must satisfy the customers' needs.

Counter-intelligence: The amended model sees counter-intelligence as an envelope protecting the entire intelligence process. Moreover, counter-intelligence should also protect the distinct parts of the intelligence cycle separately. However, one should consider that the counter-intelligence process moves through the same cycle as depicted in Figure 3.

Consumption: Lowenthal includes "consumption" among the intelligence cycle steps. This thesis considers consumption as an interaction with intelligence, rather than as one particular step in the intelligence cycle itself. As mentioned before, intelligence products are intended to help decision-makers take an action. But, as Lowenthal points out, “policy makers are free to reject or to ignore the intelligence they are offered.” (Lowenthal 2000, p. 8) An intelligence organization cannot compel its customers to use its product—it can only do the best to meet the customers’ needs.

Feedback: Feedback is rarely seen in the intelligence community. This is reflected in many different models (e.g. AJP-2.0. 2001, FAS 1996), in which feedback is not even mentioned. As Lowenthal (2000) stressed, ideally the community would receive information about whether its product has been useful or not, about which areas of interest require increased attention, and so on. But in reality such feedback is rarely received. This lowers the effectiveness of the intelligence process.

However, feedback can be considered as information flowing in an opposite direction throughout the intelligence cycle—as a tool beneficial to the community rather than as a separate component of the cycle itself.

3. Common Problems and Challenges in Intelligence

Now, before entering the specifics of OSINT, some of the problems and challenges prevalent in intelligence will be discussed. Understanding the nature and causes of such challenges will establish a firm basis for the analyses in later chapters.

Intelligence as a very old and frequently used tool of statecraft faces many difficulties. Some of the intelligence requirements have significantly changed over time while others remain almost constant. Here is an overview of main issues in contemporary intelligence:

Intelligence Requirements: The current international situation is in many ways more complex and more difficult than the relatively "stable" bipolar Cold War. The absence of one or a few overwhelming intelligence requirements has been replaced by many new requirements, none of which has the same lasting importance. Unlike twelve years ago, nowadays intelligence issues are of the highest priority for rather short periods of time. At the same time, the human and budget resources available to the intelligence community continue to decline in many countries.

The U.S. Ambassador Robert Kimmitt, former Under Secretary of State for Political Affairs, once stated that the intelligence community “will have to be an inch deep and a mile wide, with the ability to go a mile deep on any given issue." No longer is there just one enemy creating one global nuclear threat—nowadays, there are many "newcomers" at play. Not only military personnel, installations or units, but also paramilitary and civilian organizations and individuals have gained the attention of the military intelligence. Rogue non-state actors, such as terrorists, ethnic extremists, and religious fanatics—all potential users of proliferation of weapons of mass destruction (WMD)—rapidly increase the demand for intelligence supporting efforts (Tenet 2000).

Today's electronic environment complicates the situation even more, allowing possible adversaries to act more effectively than before because interconnectivity has become global.

Value and Vulnerability of Information: The information revolution has not been an easy transition from a person-to-person type of society to a global-information-network society. Yet, today's information is equivalent to the information gathered a few centuries ago in terms of its importance. The propagation of satellites, massive databases, cellular phones, fax machines, and computer networks created a new dimension in the intelligence environment.

In the electronically interconnected world, information moves at the speed of light, is nonmaterial, and is of enormous value—hence information itself has become a vital strategic resource (Schwartau 1996). On one side, information is now considerably more vulnerable; on the other side, it can be used with surprising effectiveness. Information that leads to correct decisions and wins the battle is a weapon in itself.

Secrecy versus Openness: A vast amount of information is available from open sources. But we still need to gain information that our potential adversaries conceal while sufficiently protecting our own intelligence. Of course, existing and rising democracies seek as much openness and freedom of information as possible.

Knowledge often equates to power, so there will always be a tendency to keep at least some knowledge confidential. And some people will always want to acquire knowledge for their own use—for reasons that could be selfish, unethical, or even criminal. We are unable to change this situation today. As long as information can be kept secret or can be misused, such a situation prevails.

However, it should be understood that intelligence need not be only about secrets. Definitely, intelligence collection has two facets—*open* and *covert*. Each side has its own importance and should be effectively employed and managed. But in practice, many segments of the intelligence community undervalue open-source intelligence.

Intelligence "Stovepipes": Two characteristics related to intelligence disciplines are frequently denoted as intelligence "stovepipes." The first characteristic is that all disciplines but OSINT have end-to-end processes, from collection to dissemination. The second characteristic is that the intelligence disciplines are practically separated from one another, being competitors for various reasons. Thus intelligence disciplines are often visualized as distinct "pipelines" or "stovepipes"—complete, yet completely individual and separate processes.

The five intelligence disciplines, HUMINT, SIGINT, MASINT, IMINT, and OSINT, have not developed evenly throughout NATO, and as a result, intelligence agencies do not manage them in similar manners. Each discipline has particular strengths and weaknesses, one working better or worse than the other in specific intelligence tasks. This situation stems from the Cold War when intelligence was more linear and oriented in one direction. Today, a number of individual organizations perform distinct missions and yet support an overlapping set of customers. Furthermore, these organizations have become competitors for resources. All of this regularly complicates the decisions about overall collection needs and resources.

Physical Capabilities and Limitations of an Intelligence Analyst: Especially in the technical categories of intelligence, not all of the collected data are exploited and processed. The future development of sensors and advanced communication will increase that amount of unprocessed information, thus contributing to the all-source analysts' workload. Today, intelligence is becoming based on real-time demands, and intelligence consumers sometimes expect immediate answers while the intelligence analysts can offer only tentative analytical estimates.

Information Overload: Widespread information technology and electronic communication has also created very specific problems in the intelligence community. On one hand, a vast amount of information is readily available and can be collected by all sorts of reconnaissance and intelligence assets. On the other hand, this availability creates an enormously high demand for analyses, processing, and dissemination of intelligence.

Although the technical collection disciplines radically improved in terms of gaining information, this improved ability also inundates agencies with too much information. As the power of computers doubles every 18 to 24 months (Moore's law), working with information and building knowledge has become the key for gaining the competitive advantage. How do we decide what information we need? Can we make rational, well-informed decisions about which information is truly valuable or which piece of information is even reliable?

Today, the emphasis is still placed more on processing masses of information rather than on identifying and structuring information according to its likely utility. Unstructured information of all kinds is widely dispersed not only throughout the intelligence agencies, but also throughout different non-military organizations. For example, shortly after the terrorist attack on September 11, 2001, many journalists quickly obtained information that had been available prior to that terrifying date. But different elements of the data were spread throughout different agencies, and no person, organization or momentum was able to connect the whole puzzle that would prompt the requisite countermeasures.

Information management is definitely an extraordinarily demanding task, but knowledge management is an even more crucial element to explore.

Knowledge Management and Intelligence: In the corporate world, the growing importance of professional knowledge work has been reflected in the rapidly increased employment of computer and communication technologies. This has also been reflected in the newly created managerial posts—such as "Chief Information Officer" (CIO) or "Chief Knowledge Officer" (CKO). The military services have also recognized the emerging importance of knowledge management. Not unlike the civilian sector, knowledge management has become a fad to many—and a nightmare to others. No wonder that in many cases, the design or reengineering of information systems did not follow the four-step procedure of the knowledge system and process design described before. Many systems, experimenting with software applications without a scientific basis, have been built by trial and error.

Certainly, managing knowledge in such large and complex organizations as in the case of the military is quite difficult. With intelligence, the situation is even more problematic because all the services have developed their intelligence elements at different command and control levels. Furthermore, intelligence disciplines have not developed consistently throughout the intelligence community.

Today, a more dynamic military environment creates more changes in the presence of military personnel in the battlefield. Examples from operations in Persian Gulf, Bosnia, and Kosovo showed that the rotation of personnel, for example, causes obvious losses of knowledge that were previously gained. Understanding various actions and events in the operational theater requires considerable time, and such knowledge has been hard to capture and to formalize for further use.

C. OPEN-SOURCE INTELLIGENCE (OSINT)

This section briefly examines some aspects of open-source intelligence (OSINT). After open sources and OSINT are defined and categorized, the basic principles and current problems and challenges of OSINT are presented.

1. Definitions and Categories

Open sources are unclassified sources of information in the public domain or available from commercial services (Denning 1999, Lowenthal 2000). They can be gained in various forms:

- *Printed Publications*, such as newspapers, magazines, journals, books, reports, conference proceedings, and manuals;
- *Broadcast Services*, such as radio and television;
- *Electronic Resources*, such as off-line and on-line information databases, the Internet, and multimedia CDs;
- *Public Demonstrations*, such as speeches, hearings, press conferences, symposia, and trade shows;
- *Conversation* with scholars, experts, and event participants.

Categories of Open Sources: Open sources are categorized according to their media, on-line or off-line accessibility, costs, and so on. This thesis classifies open sources as follows (NOSINTH 2001, OSINTH 1997, and others):

- *Traditional Media Sources*: This category encompasses domestic and foreign print and broadcast media, radio and TV, as well as electronically available products. Media sources still remain the core of OSINT. The US Foreign Broadcast Service (FBIS) and the British Broadcasting Corporation (BBC) Monitoring Service are considered excellent examples of media sources.
- *Internet*: The Internet is mostly used for Web browsing and e-mail, but it provides an array of other services—electronic conferences, news groups, and also provides direct access to a growing number of specialized databases. In fact, the Internet has become the communication backbone of the commercial world.
- *Commercial Online Premium Sources*: These sources are usually civilian commercial organizations charging a subscription fee or a usage fee for online access to their information. Many of these sources represent years of work on specific subjects, offering validated information, indexes, abstracts, and so on. Such services can also be obtained through information brokers or professional librarians. Frequently cited examples of commercial online premium services are LEXIS-NEXIS, FACTIVA, and DIALOG.
- *Other Commercial Sources*: This category includes professional services available through direct subscription, both on the Internet and in the form of

hardcopy or CD-ROM publications. Many of the services are directly oriented to areas of military interest. For example, The British Library monitors international publications and conferences about many general topics, including military matters, and produces excellent proceedings; Orders of Battle, Inc. offers complete orders of battle of 188 countries.[3]

- *Gray Literature*: Gray literature refers to public non-proprietary documents that are available in very limited numbers and are mostly accessible only inside the country of publication. This category encapsulates working papers, technical reports and blueprints, pre-prints, and so on. Gray literature, positioned between online information and human expertise, contains an important collection of knowledge.
- *Commercial Imagery*: Overhead imagery is no longer solely a military domain. In recent years, commercial industry gained significant capabilities, such as high-resolution electro-optical imagery, useful especially for multi-national joint combined military operations. For example, SPOT Image offers various products ranging from digital geospatial data, to overhead imagery, radar imagery, natural hazard assessment, evaluated image maps and 3-D terrain mapping.
- *Overt Human Experts and Observers*: For many topics finding exactly what is needed is hard. Moreover, both electronic and printed public information is scarce for many countries. In all cases, an expert or an observer with direct experience represents the ultimate open source. First, internal subject-matter experts who are scattered across various elements of the organizational structure can be found within the military organization. Second, based on their accomplishments and publications, outside experts can be located. Finally, "local knowledge" experts, such as frequent travelers, local residents, and event participants, can frequently provide deep insights into specific conditions.

[3] Actual numbers may vary. See http://www.orbat.com.

The above categories are not intended as strict divisions and may overlap to some degree. They are mentioned here merely to provide a sketch of open sources.

Open-Source Services: Aside from the information provided, many commercial sites also offer extended services associated with open sources. Such services vary, but they generally fall onto the following three categories (NOSINTH 2001):

- *Collection Services*: Collection services include online data collections by specialized researchers, off-line acquisition of documents or gray literature, different forms of surveys and polling, private investigations, aerial surveillance, and so on. Many essential documents can be gained through private-sector organizations that are established worldwide.
- *Processing Services*: This category embodies data conversion, indexing and abstracting, interpretation of imagery or signals, translations from foreign languages, database creation, and other similar services.
- *Analysis and Production Services*: Individual experts and commercial and academic organizations can be hired to analyze and produce various services, especially when the topic requires high expertise or the topic is out of reach of one's organization. Outsourcing may deliver excellent results if real experts are employed.

OSINT: Similarly to the other intelligence disciplines, OSINT involves much more than just collection; it goes through all the phases as described in the intelligence cycle. So, processing and analyzing the collected open-source information adds value. Open-source intelligence, like any other discipline, requires humans—to exploit the information, to sort the important from the unimportant, to retrieve relevant knowledge, and to judge the reliability of the source.

The NATO Allied Joint Intelligence, Counter-Intelligence and Security Doctrine (AJP-2.0. 2001) defines OSINT as "Intelligence derived from a wide range of open sources such as radio, television, newspapers, and books to which the public has access." The NATO Open-Source Intelligence Handbook (NOSINTH 2001) further divides intelligence emanating from open sources into two distinct categories:

- *Open-Source Intelligence* (OSINT): OSINT applies the proven model of the intelligence cycle to the broad diversity of open-source information and creates intelligence products;
- *Validated Open-Source Intelligence* (V-OSINT): V-OSINT possesses a very high degree of certainty. It can be produced by all-source professionals with access to classified information, or it can originate from trusted open sources whose validity is without question.

2. Problems and Challenges in Open-Source Intelligence

OSINT, as one of the intelligence disciplines, bears some of the general problems of intelligence "business"; OSINT also carries some specific problems not seen in other disciplines. In this section, some of the prevailing problems and challenges in OSINT will be discussed.

Use of Open Sources: During the Cold War, at least 20% of the information contained in intelligence reports came from the public domain. Today, in light of the greater openness of governments around the world, that figure can be as high as 95% (Johnson 2000). Although the percentage varies with the originator—starting as low as 40% (CIA), OSINT clearly plays an important role in intelligence.[4]

Certainly, open sources could replace pure field intelligence in many areas, or at least could compete sufficiently.[5] Keenan (1997) projected that up to 95% of what the US government needs to know could be acquired through a careful and competent study of open-source information that exists within the country. Indeed, in this area the United States has attained a high level of success. But many other countries, including the Czech

[4] Here is a true story: When NATO decided to bomb targets in Kosovo, many European countries had their intelligence agencies on stand-by alert. One nameless intelligence team, tasked to report when the mission would start, received this advice from the supervisor: “Switch-on the TV and watch CNN!”

[5] See, for example: A story about British intelligence using mainly open sources during the Falklands War (Adams 2000, p. 225). Another example is a "contest" between Robert Steele and CIA to obtain a complete intelligence report on the African nation of Burundi over a three-day period (Denning 1999, p. 80).

Republic, can also gain a significant portion of their needed information from their open sources and from sources abroad.

However, OSINT should not be the only intelligence collection discipline used to provide accurate intelligence. OSINT can serve as the first resource for any intelligence analysis—but cannot replace the other disciplines in full. Clandestine collection and information operations cannot be omitted; in some cases they can "make the difference between life and death on the battlefield or between an aborted and a tragic terrorist incident." (Denning 1999, p. 81) For this reason, there should be no competition between OSINT and other disciplines. Instead, OSINT should serve as a broad base for the other intelligence disciplines in which intelligence must be collected by other than overt means.

OSINT is vital to the all-source intelligence analysts because "it provides the historical background information, the political, economic, social, demographic, technical, natural, and geographic context for operations, critical personality information, and access to a wide variety of tactically useful information about infrastructure, terrain and indigenous matters." (NOSINTH 2001) For most cases, OSINT can really serve as a foundation for constructing the whole intelligence picture—principally when the military must understand its involvement in non-traditional tasks, such as ethnic and religious conflicts, clashes for scarce natural resources, mass migrations, natural and technical disasters, international organized crime, and so on.

OSINT can contribute to classified collection methods in the following areas:

- *Tip-offs*: Electronic media, the Internet in particular, provide vast opportunities for information exchange. As a result, the number of areas with denied access to information has diminished since the end of the Cold War. Today, many services provide non-traditional news alerts, witnesses post their messages on the Internet newsgroups, and so on. Hence, there are many situations where OSINT can provide the first indication of an event—even before it is covered by the media such as CNN.
- *Targeting*: Both OSINT and classified sources can be optimized for a particular intelligence problem. This allows intelligence personnel to concentrate on issues that can only be discovered covertly and also to validate the OSINT products via the classified collection. Thus, OSINT optimized with

collection from other sources allows all-source analysts to work more effectively.

- *Validation*: Classified reports are often narrowly focused and represent separate pieces of intelligence. To counter the preoccupation with only one direction, one can place such reports into a wider context, supplementing necessary background information from the OSINT environment. Cross checking such intelligence through multiple open sources can assure its validity.
- *Cover*: In some instances, open sources can serve as a plausible cover for the sanitation of classified reporting. If one understands the information available in unclassified systems, the ability to use a plausible alternate open source as a cover is facilitated. Thus, open sources can serve as a shield that can conceal the real source of the information.

Misconceptions: Theoretically, the greater availability of open sources should ease the task of the intelligence. However, intelligence services were created to collect secrets—and using open-source information seems not congruent to the task at hand. That is probably why intelligence agencies have difficulties assimilating open sources into their processes. Intelligence services often do not want to confess that much of their work is based on open sources. Many intelligence agencies will not admit that they rely on OSINT heavily because they fear that their budgets will be severely cut, that they will lose professional respect, or even that their departments will be eliminated. They assume that most taxpayers might ask, "Why do I have to pay for an intelligence agency that reads the newspaper?" Some people mistakenly equate the value of intelligence with the degree of difficulty involved in obtaining it and with the classification level assigned to it.

Another common misconception about OSINT is that it can be obtained without cost. But one can easily understand that gaining information from open sources is subject to direct and indirect costs. Direct costs include the cost of printed materials, the fees for subscription to electronic resources, the expense for experts from outside the organization, and so on. Indirect costs include, for example, expenditures for supporting

IT tools, paying analysts inside the organization, and opportunity costs. However while open-source information is not free, the associated costs are often far less than those of collecting and processing classified information.

Another misunderstanding is that the Internet is the primary origin of most OSINT. Indeed, the Internet has about 500 million users and is increasingly used as a means of open-source collection that holds about one billion documents, many of which are linked. Expert forums, including private teams with their own newsletters and e-mail information alerts, represent important parts of the Internet exploitation. Yet this represents only about 30% of the total open sources. Moreover, unlike printed publications, anyone can post anything on the Internet—which increases the probability of obtaining fictitious or erroneous information if one relies on the Internet exclusively. This is commonly known as the "garbage in, garbage out" effect. Information relevance and correctness has certainly become an extremely sensitive issue. Furthermore, extant active Web agents called "intelligent agents," "network robots" or simply "bots" searching the Internet for specific information cover only about 15% of the visible Web, overlooking complex sites with many subsequent levels known as the "deep Web." On the other hand, bots can inundate one with vast quantities of data in response to simple queries. So Internet search engines might return thousands of links for certain queries while important information may be omitted if the usual keywords are missing. This degrades the practicability and usefulness of bots in some cases. Clearly, one must approach the Internet as just one of the open sources and be aware of its strengths and weaknesses. The Internet, despite its rapid growth, is more of a vehicle for open cooperation and collaboration than a reservoir of flawless and reliable knowledge.

Advantages and Disadvantages: The major advantage of OSINT is its accessibility. It is readily obtainable although it requires collection. Open sources are available extensively and that also makes OSINT less susceptible to manipulation and deception. Moreover, unlike covert operations, OSINT is not hazardous for the collectors. Furthermore, unlike any other intelligence category, OSINT products can be shared with virtually anybody, without requesting security clearances.

All of this makes OSINT extremely valuable for cooperation with civilian coalition partners and for intelligence dissemination in the multi-national non-Article-V operations.[6] As the role of the military shifts from collective defense to collective security, many non-traditional non-military cases require intelligence sharing with non-governmental and humanitarian organizations. OSINT appears to be a primary platform for such challenges.

In the case of NATO multi-national coalition operations, the involved nations tend to protect their national intelligence resources and their intelligence services do not cooperate well with each other. Yet, the same nations will be willing to use an open-source environment for both information gathering and intelligence sharing. So, in such a case, the combined joint command should initially use the OSINT process instead of turning to classified national intelligence collection. Moreover, NATO has usually no tasking authority over national intelligence assets while it can use open networks to propagate its intelligence needs without severe limitations.

The main disadvantage of OSINT is its abundance. Computer technology's ability to produce, to manipulate, and to store information increased exponentially, creating an information explosion. So, sifting through the information field to collect information that is relevant, correct, and needed has become more and more difficult. This is often called the "wheat and chaff" problem. As previously stated, single analysts and analyst cells cannot process all the available information. The intelligence community must find ways to create and to maintain virtual nets of information sources, OSINT collectors, and analysts.

Furthermore, military intelligence must use all the presently available options to disseminate OSINT products. Classified networks have the principal disadvantage for OSINT dissemination in that they must separate the products from the sources. Systems based on the Virtual Private Network (VPN) arrangement can provide ready access to the original materials with the advantages of security safeguards. The US system NIPRNET,

[6] Article V of the North Atlantic Treaty states that NATO members must consider coming to the aid of an ally under attack. However, it does not guarantee assistance. Article V is the Treaty's key provision. It states, in part, "…an armed attack against one or more allies shall be considered an attack against them all." Since the early 1990s, NATO has begun to adopt new missions, such as crisis management and peacekeeping, sometimes referred to as "non-Article V operations."

used by different US military services to share unclassified information, and the US Open-Source Information System (OSIS), which is a confederation of information systems serving the intelligence community with open-source intelligence, are examples of an OSINT sharing environment.

Naturally, OSINT is not an exclusive part of intelligence agencies—in practice, that is impossible. Open-source exploitation is relevant not only to the intelligence professionals, but also to all military personnel who may need open-source information. Indeed, intelligence professionals must support commanders and other decision-makers. But if adequate answers are readily available from open sources, engaging an intelligence agency is just pure inefficiency. Therefore, intelligence professionals should encourage their superiors and customers to manage their own open-source collections. If a robust OSINT system exists, it can save much time and reduce unnecessary requests for information. Once all staff elements have direct access to open sources, the intelligence staff can help facilitate the OSINT knowledge flow while evaluating sources and providing professional guidance.

All of the intelligence disciplines but OSINT have their dedicated collectors, processors and exploiters. In the case of OSINT, analysts are often expected to act as their own collectors. This situation would be considered preposterous if it happened in any other intelligence discipline. This flawed perception represents one of the major challenges OSINT faces.

Obviously, intelligence agencies under the pressure of cutbacks, reduction of personnel, and increasing intelligence requirements can hardly compete with CNN's worldwide coverage. So, military intelligence does not need to conceal its reliance on open sources or, even worse, to conceal that it collects open-source information by classifying it. Instead, it must develop its OSINT branch to be a state-of-the-art information collector and establish proper procedures to manage the vast amount of information that is available from open sources. Open sources should also be the first choice in the collection process because OSINT conserves resources by reducing the unnecessary use of costly covert means. And finally, OSINT represents a usable platform for disseminating vast amounts of information and the unclassified finished intelligence products among national and international organizations.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CZECH MILITARY, INTELLIGENCE, AND OSINT

This chapter examines the status of the Czech military, intelligence services, and use of OSINT. The first section traces the current security environment of the Czech Republic focusing on the main security concerns of the state. Also, the principal tasks of the military are surveyed and categorized. The second section of this chapter introduces the Czech intelligence services, particularly, the military intelligence. Moreover, current intelligence requirements are listed as a base for further analysis of possible applications of OSINT. The last section follows the four stages of the knowledge system and process design to analyze OSINT in the Czech military intelligence.

A. CZECH SECURITY ENVIRONMENT AND THE MILITARY

The Czech Republic was established on January 1, 1993 and was grounded on the Czechoslovakian democratic tradition created before WWII. The Czech leadership had to consider the geopolitical definition and the external security environment that Czechoslovakia had faced since its creation in 1918. During this period, adverse powers militarily occupied the country twice—in 1939 and 1968. These interventions and the nation's subsequent loss of independence, accompanied with economic, cultural, and moral devastation weakened the nation's resolve to defend and nurture democratic values. This weakening even included the military defense of the state. These experiences also negatively distorted the public's image of the armed forces and the nation's international conduct.

1. New Security Environment

The Czech Republic, formerly Czechoslovakia, was a part of the Warsaw Pact for four decades. After the so-called Velvet Revolution in November 1989, the Czech Republic began developing a democracy. Dynamic changes in the political, economical, and social situation in Central and Eastern Europe during the 1990's, as well as increased globalization and international exchange, raised many national security questions. Now being part of NATO, the Armed Forces of the Czech Republic have developed new defense concepts and doctrines as a result of such influences.

After removing the old communist regime in the 1990, the newly sovereign federation had to create a new security policy. Three years later, the Czech security had to be reconsidered again when the Czech Republic and Slovakia divided. From 1997 to 1999, the Czech security and military strategies had to be changed once again—this time moving away from a purely national posture toward a collective defense organization within the NATO structure.

Nowadays, although the Cold War is long over, the Czech Republic sees NATO as the key security organization in Europe. On 12 March 1999, the Czech Republic joined NATO, thus acquiring the security guarantees of a collective defense in accordance with Article 5 of the North Atlantic Treaty. NATO membership obligated the Czech Republic to reinforce its own defense capacity and to share in the defense of its allies. Participating in NATO involves assuming full responsibility for decisions and being prepared to share in their implementation. The new Strategic Concept, approved by the NATO summit in Washington in April 1999, expands NATO's fundamental tasks to include a share in crisis management throughout the Euro-Atlantic region, to develop a partnership and to cooperate with other states in the area.

Indeed, NATO is being transformed from an essentially military organization to a more political one. The likely accession of new member states from the Baltic in the fall of 2002 will further accelerate the metamorphosis of the Alliance from an instrument for delivering collective defense to an organization for managing collective security. The Alliance with less US military presence and with more involvement from its European members will certainly be different from the body "reinvented" in April 1999. Many European countries want to more actively ensure the security of the Euro-Asian region. The Czech Republic wants to assist actively in the important role played by the EU security bodies. The Czech political leadership sees a partnership in the Common European Security and Defense Policy (CESDP) as a way to further increase the responsibility and participation in the European collective security.

The current Czech defense policy is based on the hypothesis of the indivisibility of security and on the universality of basic human rights and freedoms. The Czech Republic is therefore by no means indifferent to the fate of other nations and regions. It identifies its own security with the global security situation and is prepared to work actively with the international community to solve these problems. The Czech Republic makes it a priority to solve crises peacefully, but it may decide to use force in accordance with constitutional law if necessary (NSS 2001).

2. Current Threats and Risks to Czech National Security

As already mentioned, the Czech Republic judges threats to its security in the wider Euro-Asian context. The international community is trying to maintain or to restore peace, to protect human rights and freedoms, to condemn and punish war crimes, to create democratic institutions, and to foster economic recovery and regional development. However, inconsistently applied political and economic reforms have generated a number of new problems, including lowered standards of living and booming organized crime and corruption.

The regions in the southeast and east of Central Europe pose the most serious global threats to European security and to Czech security in particular. The Balkan crisis has not been fully solved yet; religious and ethnic tensions have been rising in the Trans-Caucasus region and Central Asia; and a critical situation has also evolved in some regions of Russia. Economical and social instability in those areas, the spread of individual or group violence, and negative demographic trends are substantial, even though indirect, risks to Czech security.

Widespread political and economic migration results from regional conflicts and differences in the standard of living. Migration is a sensitive issue in the European cultural and historical environment. Insularity of some population groups condemns immigrants to the margin of society where they can be lured into individual and organized crime. In turn, the native citizens reject further immigration.

The end of the Cold War substantially relaxed many tensions and significantly lowered the risk of worldwide confrontation. After the Iron Curtain fell, the national threats for states on both sides of the curtain changed radically both in positive and negative ways. Now, new threats are surfacing while some long-term problems persist. In the case of the Czech Republic, the National Security Strategy, first established in 1998 and amended in 2000, lists nine possible threats (listed below). Only two of them are directly linked with military threats or attacks. The other seven deal with economical, political, terrorist, and drug proliferation issues. The potential security threats and risks are defined in terms of their probability as follows (NSS 2001):

(1) *Natural Disasters, Industrial and Environmental Accidents, Emergence and Spreading of Epidemics*: These risks, permanently present and highly topical, can emerge within a few hours or days, and their nature and extent are difficult to predict.

(2) *Disturbance or Abuse of Standard International Economic Relations*: Disruptions of flows of strategic commodities and raw materials, as well as attacks on computer networks or threats to security of information databases, represent significant danger to the internal economic affairs of the Czech Republic.

(3) *Individual Acts of Terrorism and Organized Activities of International Crime of an Extraordinary Extent*: Attacks against citizens and economic, infrastructural, or administrative facilities may inflict severe casualties. Although the Czech Republic is not considered a potential terrorist target, it cannot disregard such threats.

(4) *Massive Waves of Migration*: The vast number of immigrants to the country could become violent, both inside and outside the state's borders.

(5) *Violence by Alien Powers*: Foreign countries may conduct violence against persons or property in the Czech Republic because the country has participated in international peace-support operations or humanitarian missions.

(6) *Threats to Essential Principles of Democracy and Civil Liberties in Other Countries*: Internal political violence and low intensity conflicts outside the Czech territory could seriously endanger international security.

(7) Extensive Subversive Actions: Adverse forces can execute subversive actions to render the Czech Republic's defense assets useless and to disrupt the country's transition to the state of war.

(8) Direct Threat of Aggression. An attack against an allied nation is a direct threat to the Czech Republic.

(9) Direct Military Attack against the Czech Republic.

The risks listed in paragraphs two to six above are highly relevant. They can be initiated in combinations and can therefore produce threats that are difficult to predict. Such risks can be activated in a few days to several years. The military will only assist in eliminating such risks and its deployment will involve a limited use of combat assets.

The risks specified in paragraphs seven to nine above obviously pertain to the military. Their current probability is low, and they are easier to predict. Such risks can be activated in months to years, and they would inflict major destruction. To eliminate such risks, the Armed Forces would be engaged in progressively escalating combat.

3. Czech Military

The Czech military has marched along a crooked and rough road—from the highly politicized and anti-Western service of the 1980's to the NATO-allied army at the end of the twentieth century. Today, the Army of the Czech Republic (ACR)[7] is certainly different from that of twelve years ago. The early 1990's realigned the structure, the personnel, and the orientation of the Armed Forces owing to the end of the Cold War and the fall of the communist regime. The disinterest of top policy-makers in security and defense matters in the mid-1990's negatively imprinted the Czech military, leaving it

[7] The name "Army" does not have the same meaning in the Czech Republic as it does in the USA, for example. In the Czech Republic the word encompasses all three military services—the Ground Forces, the Air Force, and the Territorial Defense Forces. See the organizational structure of the ACR, described later in this chapter.

without any nation-level defense policy and allowing unsystematic decisions. And NATO membership brought a large set of new requirements during the late 1990's.

Indeed, the Czech military's doctrines, structure, and tasks have changed significantly since 1990. During the 1990's, the Czech Republic suffered drastic declines in the size of the military structure and personnel. Also, the cutbacks in the military budgets significantly eroded the combat capabilities, simply because the extent of equipment and personnel reduction did not match the decreases in funding. Moreover, until the succession to NATO, the Czech political leadership paid only limited attention to security and defense issues, which worsened some of the problems. Unfavorable public opinion, limited expertise of the top military leadership, controversial decisions about procurements and modernization, as well as shortages in the readiness and training accompanied the Czech Republic's integration into NATO.

Despite the Czech Republic's small size, the contribution to NATO's missions, although severely limited militarily, has become highly valuable politically. Recent participation in many UN-based or NATO-based operations, such as in the Persian Gulf or in the former Yugoslavia, has proved that the Czech Republic desires a useful role in alliance operations. As to the current comparisons with other countries of similar size and military capabilities, such as Portugal, the Czech Republic is not perceived as a "free rider" but rather is seen as an average or a below-average NATO member in terms of contribution.

Like other NATO members, the Armed Forces of the Czech Republic have earmarked most of their forces for the Alliance—78%. However, having all the units achieve the NATO standard capabilities, as set in the Force Goals is proving difficult. Given the current state of build-up, training, and logistic support of the forces, even high-priority units would have difficulties in terms of the required readiness, level of training, compatibility of weapons and equipment, command and control systems, transportability and mobility, firepower, efficient engagement, and force sustainability, if they were evaluated in accordance with the *Force Standards for the Rapid and Immediate Reaction*

Forces.[8] NATO standards and the interoperability requirements certainly represent the main NATO-related concern of the ACR. (ARCTSC 2001)

Now, let's focus on the principal tasks, the organizational structure, and the reform of the ACR. This will encompass the current and the future environments of the Czech military, thus providing a sufficient base for the knowledge system and process design.

Tasks: According to the National Military Strategy (NMS 1999), the ACR has four principal tasks:

(1) *To Defend the Czech Republic against an Outside Attack*: To defend the country's territory once an outside adversary has attacked it, the ACR will conduct operations either independently or together with NATO forces. The Armed Forces will assign and prepare one to two tactical groupings of peacetime strength units for rapid deployment to eliminate local destructive operations of forces organized along military or paramilitary lines. In the case of an extensive threat to national security, the ACR will continue to reinforce peacetime strength units as necessary. Also, it will prepare territorial defense elements to protect important facilities and assets in cooperation with other regular forces. To be able to defend its country, the ACR continuously prepares a build-up of troops to wartime strength and their deployment in a mobile, flexible, deep operational formation in order to conduct operations along one threatened axis, either independently or together with the allied forces. Moreover, the ACR builds and prepares the infrastructure to support operations of their own troops and to allow Alliance forces to be received and deployed in the country's territory. And finally, the Czech military provides for and conducts training of the professionals, conscripts, and reservists and participates in the education and training of Czech citizens for the defense.

[8] These standards have been established by the Allied Command in Europe (ACE) for the force performance evaluations at the tactical and operational levels (TACEVAL, or OPEVAL, respectively).

(2) *To Take Part in Defending the Alliance*: The Czech Republic, as a full member of NATO, partakes in protecting freedom, security, and other vital interests of all the Alliance members. To fulfill its obligations in accordance with the North-Atlantic Treaty, the Czech Republic established its NATO-command forces, NATO-assigned forces, and NATO-earmarked forces. These forces are built and trained as professional combined-arms formations and units, which are ready for airlift by allied air assets and can conduct operations outside the Czech territory as a part of the NATO task forces. As its top priority, the ACR develops and provides for compatibility and interoperability with the armed forces of the Alliance, paying particular attention to command and control systems, information and intelligence systems, and technical surveillance systems.

(3) *To Participate in Peace-Support Operations, Rescue-and-Relief Operations, and Humanitarian Operations*: The ACR takes an active part in peace-support operations and also participates in rescue, relief, and humanitarian operations abroad. It assigns forces up to a mechanized battalion plus a special company, the combined number of which is up to 1,000 people. The ACR builds and prepares military rescue units and other available peacetime forces capable of saving civilian population from dangers threatening their lives, health, or property. Depending on the tasks at hand, the military selectively reinforces and deploys specialized units to provide assistance in the event of a natural disaster or industrial accidents abroad.

(4) *To Participate in the Elimination of Non-military Threats*: The military can confront non-military threats to national security and can protect internal security and maintain public order within the country. To be able to participate in such tasks, the ACR selectively prepares a part of the ground, air, and territorial defense forces to act as reinforcements of the Police of the Czech Republic (PCR).

Organization: The current organizational structure of the Army of the Czech Republic is depicted in *Figure 4*.[9]

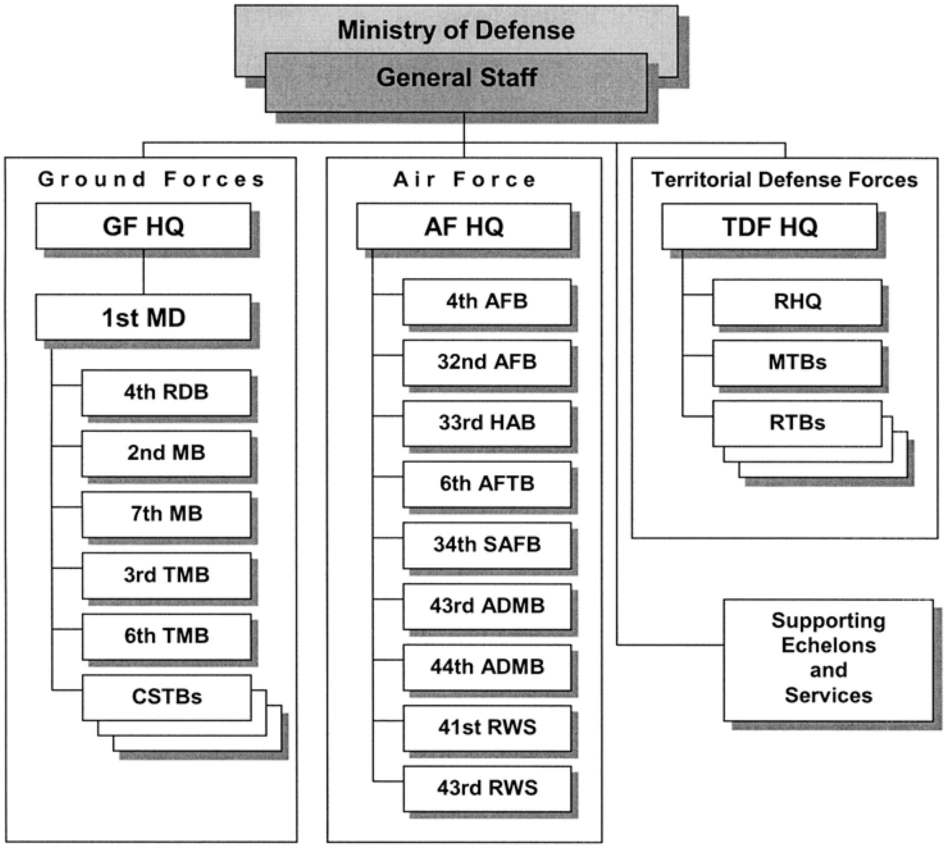


Figure 4. Organizational Structure of the ACR

[9] The figure depicts only main combat and support formations down to the brigade/base level. Legend: HQ = Headquarters; MD = Mechanized Division; RDB = Rapid Deployment Brigade; MB = Mechanized Brigade; TMB = Training and Mobilization Base; CSTBs = Combat Support Training Bases (one per each combat support element, i.e. reconnaissance and electronic warfare, signal, artillery, engineer, and chemical XXX); AFB = Air Force Base; HAB = Helicopter Air Base; AFTB = Air Force Transportation Base; SAFB = Special Air Force Base; ADMB = Anti-Defense Missile Brigade; RWS = Surveillance and Warning Sector; RHQ = Regional Headquarters; MTBs = Mobilization and Training Bases; RTBs = Rescue and Training Bases.

Reform of the military: The Czech military still has to overcome many negative preconceptions. Although some of the biases stem from the traditional Czech anti-military proclivities, low regard for the military should not be treated as something deterministic. Second, other more realistic problems, such as insufficient and ineffective planning and budgeting, lack of modern weaponry, incompatible command and communication systems, and unsuited proportion of personnel still exist.

The ACR has been continuously restructuring since its official formation in 1993. During the process, the ACR has attempted to adapt internally to the external environment. Much progress has been made, especially in preparing for membership in and accession to the Alliance. The invitation to the Czech Republic to join NATO and the fulfillment of the minimum military requirements as of the accession day is undoubtedly a great success. Yet, none of the restructuring processes undertaken so far has brought about a qualitative change in the ACR's capabilities. Also, many disputable decisions have been based upon political and personal interests, not always in line with the worldwide military trends. The purchase of the L-159 light attack aircraft and upgrading of the T-72 main battle tank, for example, have consumed substantial funds from the defense budget. (ARCTSC 2001)

The last reform of the ACR, started in August 2001, is designed to improve the position of the ACR in a democratic society and to allow the ACR to cope better with the present security risks and challenges while using the allocated funds most efficiently. The new military leadership, especially the Minister of Defense Jaroslav Tvrdík, clearly expressed the needs for more transparent management, high economic efficiency, and increased force effectiveness. For the ACR to fulfill the vital and strategic interests of the Czech Republic adequately, it must also have the required capabilities. Along with other alterations, reforming the Armed Forces will cause the following changes (Reform 2001):

- The Czech Republic will gradually shift to fully professional armed forces and cancel the conscript service. By 2003, the ACR will prepare the groundwork for necessary legislative changes toward all-voluntary forces; by 2005, all NATO-earmarked forces should be fully professionalized; by 2007, the Armed Forces will be all-volunteer personnel.

- The ACR will be divided into *Deployable Forces* and *In-Place Forces*. Furthermore, they will be sub-divided into *High Readiness Forces*, *Forces of Lower Readiness*, and *Long-Term Build-Up Forces*.
- Well-equipped, well-trained, and well-supported deployable forces will be the priority.
- The ACR will focus on developing passive surveillance systems and protection against weapons of mass destruction (WMD), particularly detecting and identifying chemical and biological substances.
- The ACR will improve its capabilities in psychological operations, deceptive operations and civil-military cooperation (CIMIC).
- By 2007, the Armed Forces will not exceed 34,000 to 36,000 active soldiers plus up to 10,000 civilian employees.[10] The maximum wartime numbers will not exceed 1.8 times their peacetime counterparts. [11]

The ACR's definite role remains the same—to guarantee the defense of the Czech Republic. Possible military involvement has these three alternatives:

- All Czech Republic's armed forces will participate in one major Article-V operation;
- The Czech Republic will send a brigade-size contingent (up to 5,000 persons without replacement) to participate in one operation for up to six months;
- The Czech Republic will participate in one long-term operation with a battalion-size contingent (up to 1,000 persons without replacement) and, concurrently, in another operation with a smaller contingent (up to 250 persons).

Aside from that, the ACR must be able to provide forces and assets for the Czech integrated rescue-and-relieve system inside the country.

[10] As of January 1, 2001, the Armed Forces totaled 69,296 persons; 23,184 of them were professional soldiers, 24,955 conscripts, and 21,157 civilian employees. See for example http://www.army.cz/reforma/english/docs/p07.htm.

[11] To better understand the insufficiencies of the ACR, as well as to apprehend the amount of work accomplished so far, one should see the analyses provided by the *Center for Preparation of the Armed Forces Reform*, posted at http://www.army.cz/reforma/index.htm.

Figure 5 illustrates the future organizational structure, as proposed by the conception.[12]

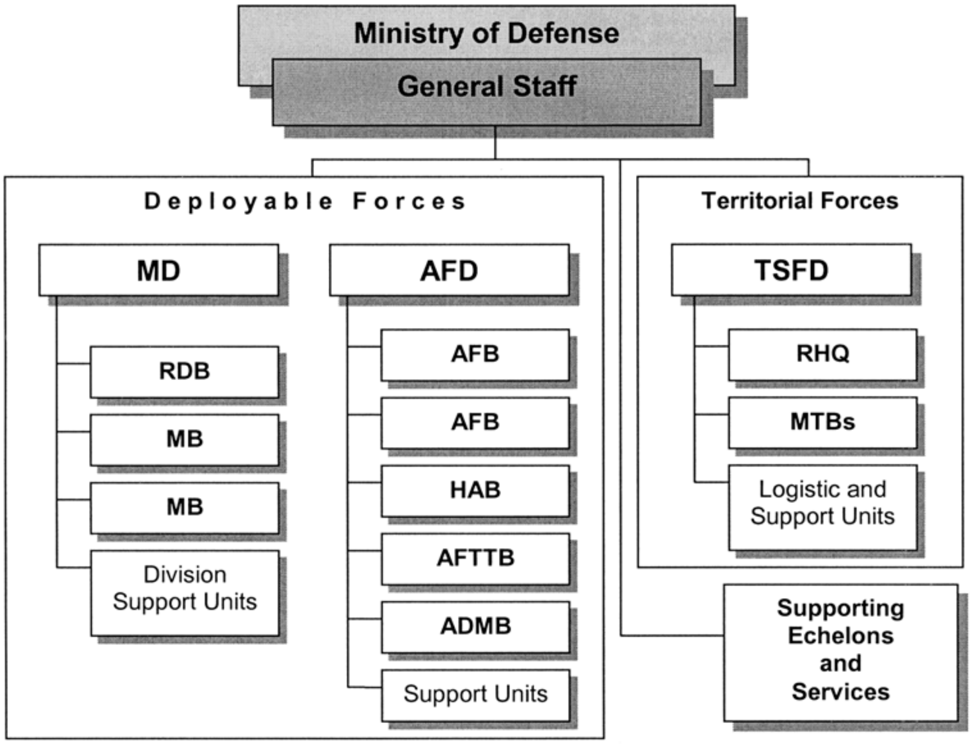


Figure 5. Organizational Structure of the ACR by 2007

Regarding the military intelligence, the reform concept stresses the importance of analytical outputs for the defense planning and preparation. Yet, the military intelligence will probably be included in the whole reformative package covering all Czech intelligence and counter-intelligence services. The intention to reduce the overall number of services has existed since the early 1990's, accompanied by various inter-agency "turf wars;" so it is likely that the military intelligence will face some reform in the near future.

[12] The figure depicts only main combat formations down to the brigade/base level. Legend: HQ = Headquarters; RDB = Rapid Deployment Brigade; MB = Mechanized Brigade; AFB = Air Force Base; HAB = Helicopter Air Base; AFTTB = Air Force Transportation and Training Base; ADMB = Anti-Defense Missile Brigade; RHQ = Regional Headquarters; MTB = Mobilization and Training Base.

As of April 2002, the *Conception of the Professional Build-up of the ACR* has been prepared and submitted for approval. The government acquainted with the document; however, with the upcoming elections in June 2002, the administration postponed the document's approval, leaving further reform-related decisions to its successor.

B. CZECH INTELLIGENCE AND COUNTER-INTELLIGENCE SERVICES

"I don't need intelligence services. CNN is enough for me." This comment, credited to Prime Minister Václav Klaus in 1994 (Hořejší 1997), summarizes the general attitude of both politicians and the public. This attitude has not changed much since 1990. The Czech intelligence services, including the military intelligence, underwent many reorganizations and management changes. During the mid-1990's the power over the intelligence agencies shifted from the President and Parliament to the government and Prime Minister, but they had little interest in exercising it. Only in the late 1990's did the government and the Parliament formulate basic policies, amend obsolete laws and create new ones, and constitute clearer oversight over the intelligence services.

After the split with Slovakia and the end of the federation in the 1993, the Czech Republic established four intelligence agencies, based on their federative predecessors:

- The *Bureau for Foreign Contacts and Information* (Úřad pro zahraniční styky a informace–ÚZSI), a civilian agency responsible for foreign intelligence;
- The *Security Information Service* (Bezpečnostní informační služba–BIS), a civilian counter-intelligence agency;
- The *Military Defensive Intelligence* (Vojenské obranné zpravodajství–VOZ), a military counter-intelligence agency;
- The *Military Intelligence Service* (Vojenská zpravodajská služba–VZS), the intelligence agency of the ACR.

Organization structures and tasks of the above listed services have changed slightly since then. Their core responsibilities are summarized in the following section.

1. Services, Tasks, Cooperation, and Oversight

The organizations and tasks of the Czech intelligence and counter-intelligence services are somewhat different from those in the USA, for example. Yet, the basic functions remain similar throughout the world—what usually differs is the actual numbers, subordination, flow of information, and oversight. In order to provide for a broader frame into which to fit OSINT later on, one should first understand the organization and main tasks of the Czech intelligence and counter-intelligence services.

Military Intelligence (VZ): In 1994 the Military Defense Intelligence (VOZ) and the Military Intelligence Service (VZS) were formally amalgamated into the *Military Intelligence* (Vojenské zpravodajství–VZ) through Law No. 153, or "intelligence bill" (ZZS 1994). But the two segments of the VZ practically work independently, even though a certain level of cooperation has been attained. While the former reports directly to the Minister of Defense, the latter is subordinated to the Chief of the General Staff. The subordination is illustrated in *Figure 6*.

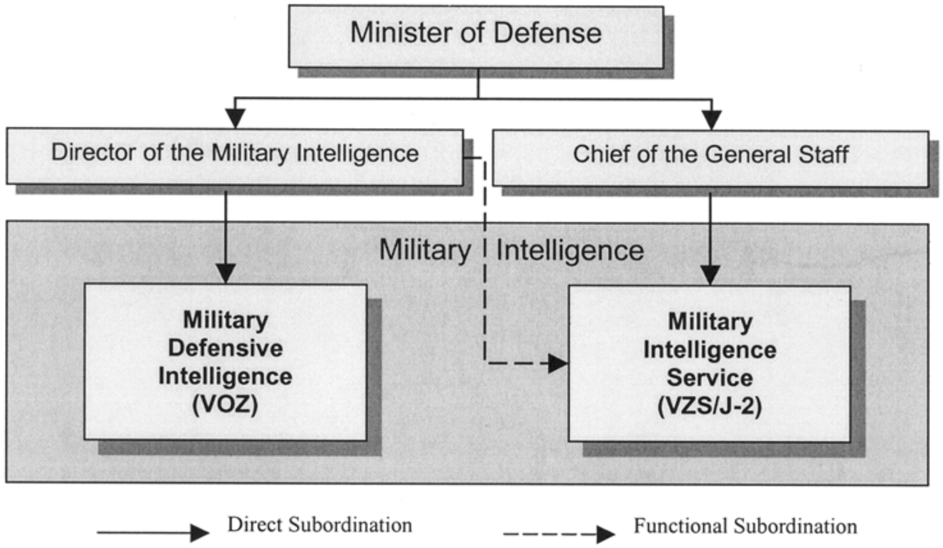

Minister of Defense
Director of the Military Intelligence
Chief of the General Staff
Military Intelligence
Military Defensive Intelligence (VOZ)
Military Intelligence Service (VZS/J-2)
Direct Subordination
Functional Subordination

Figure 6. Subordination of the Military Intelligence Services

In accordance with law, "the Military Intelligence (VZ) provides the following information:

(1) Information about intentions and activities that represent military threats to the Czech Republic.

(2) Information about foreign military intelligence services.

(3) Information about intentions and activities directed against the assurance of the defense of the Czech Republic.

(4) Information about activities endangering state and service secrets related to the defense of the Czech Republic." (ZZS 1994)

The VZS has full responsibility for the first item in the above list. The other three items are mainly under the jurisdiction of the VOZ; however, the VZS participates in those tasks when gaining relevant information abroad. Moreover, the VZS not only fulfills the tasks of the military intelligence but also functions as the J-2 branch, being responsible for the military reconnaissance and electronic warfare at the strategic level.

Security Information Service (BIS): The Security Information Service (BIS) has probably been the most "torn and twisted" service since it represents a domestic intelligence bureau. As such, considering the very negative reputation the former totalitarian state secret police (State Security, or StB) earned, the BIS leadership has been under severe pressure from both the politicians and the public. Notwithstanding accusations of being politicized, the BIS is also known for numerous cases of misconduct among its members. Yet, one should be aware that the BIS lacks sufficient human and material resources while having to tackle a wide variety of tasks.

According to law, the BIS provides information:

- About intentions and activities, such as political extremism and subversive actions, aimed against the democratic institutions, sovereignty, and territorial integrity of the Czech Republic;
- About foreign intelligence services;
- About activities compromising state and service secrets;

- About activities endangering the security or important economic interests of the Czech Republic, such as corruption, money laundering, WMD and arms proliferation, and so on;
- About organized crime and terrorism.

Although successful and publicly praised in some cases, the BIS is often cited for its insufficient coverage of foreign espionage and organized crime. An enormous turnover in personnel is probably the most serious cause of such problems.

Bureau for Foreign Contacts and Information (ÚZSI): According to its vague mandate, the Bureau for Foreign Contacts and Information (ÚZSI) provides for "information originating abroad important for the security and protection of the foreign-policy and economic interests of the Czech Republic." (ZZS 1994) The ÚZSI studies global risks, such as terrorism, extremism, proliferation, drugs and arms dealing. The activities of the ÚZSI and its intelligence productivity remain close to the public. Yet, it is known that, owing to the shutdown of espionage after 1989, the ÚZSI has continued to work largely from open sources and via liaison officers abroad.

Interagency Cooperation: Cooperation among the services is based upon inter-agency agreements that the government must approve. Moreover, each agency can exchange information with its foreign counterparts and other services if approved by the government. Statistics, related to the amount of cooperation among different services, if any exist at all, are not publicized. Probably the largest amount of information is exchanged between the BIS and the police, owing to the fact that both services cooperate closely in combating corruption, organized crime, and terrorism. As for the Military Intelligence (VZ), its two parts, the VZS and the VOZ, have connected with tens of intelligence and security agencies and also integrated into the intelligence system of the NATO Allied Command in Europe (ACE).

Direction, Reporting, and Oversight: The President and the government task intelligence services in accordance to their respective functional areas. The Czech government coordinates all the services via its permanent *Intelligence Committee* and bears the responsibility for the services' activities. Practically, all the services except for the BIS are subordinated to a ministry. The director of the ÚZSI reports to the Minister of Interior and the director of the VZ is subordinated to the Minister of Defense. The director of the BIS, however, answers to the entire government. The subordination of the ÚZSI and BIS are not what one would normally expect but rather a result of the mistrust of domestic intelligence.

All the services prepare and submit their annual reports to the President, the government, and their respective ministers.

As to the parliamentary oversight, the Parliament exercises direct oversight only over the two counter-intelligence agencies—BIS and VOZ. However, the Intelligence Committee advises the Parliament of the activities of all the intelligence services on a regular basis.

2. Current Military Intelligence Requirements

Since the Czech Republic gained its independence, both politicians and the public have perceived the defense planning and especially the role of military intelligence as entirely theoretical. Unlike Poland or Hungary, where instability in the former USSR states or the Balkan crisis continues to shape the states' defense policies, the geographical location of the Czech Republic, its succession to NATO, and the absence of a direct threat make the country highly unlikely to be threatened militarily. The hypothetical threats from Germany and Russia would endanger the Czech Republic's sovereignty, but such threats are very unlikely to occur. More likely, the Czech Republic can be involved in regional, border, or internal conflicts that will not affect the country so radically. Fortunately, the Czech Republic security establishment sees the NATO and European security and economic institutions as sufficient tools to deal with such conflicts effectively. Finally, a conflict with Slovakia also seems to be extremely unlikely, for no serious border or minority problems have occurred since the split in 1993.

Although the probability of a direct military attack against the Czech Republic has been significantly reduced and is unlikely in the near future, military attacks cannot be ruled out completely. Indeed, the most probable threats in the foreseeable future are organized crime, terrorism, and waves of refugees; such problems may cause internal instability and unrest. Especially terrorism or international crime may infiltrate the Czech Republic—and being endangered by a force of such a magnitude the country may need the military to eliminate the threat.

In practice, the shift to non-military and semi-military threats and risks has changed the intelligence requirements. The VZS, although still tasked to assess traditional military targets, is becoming more and more involved in providing intelligence about other non-military topics as well. The following briefly covers the areas that deserve the attention of the military intelligence.

Weapons of Mass Destruction: The threat of nuclear weapons and other weapons of mass destruction (WMD) has not been totally eliminated. The expanding group of entities with these weapons or attempting to acquire them is particularly disturbing. These entities are often states with non-democratic and unstable regimes. It is especially dangerous when individuals or non-state entities control weapons of mass destruction, whatever the quantity, however few. Intelligence predicts a significant risk of such an encounter within the next few years.

Traditional actors may also pose significant danger to the global security. The chance of war between India and Pakistan is now greater then ever in the last three decades. Although both states are publicly downgrading the risk of nuclear conflict, a conventional war could escalate into a nuclear confrontation. Iraq's regime continues to restore its military force and to fund its pursuit of WMD, despite its own positive diplomatic efforts toward the UN and neighboring states. Furthermore, NATO states can face threats from the inter-continental ballistic missiles (ICBM) that exist or that are being developed in North Korea, Iran and Iraq.

When developing advanced weapons, WMD proliferators build upon the experience of others and take advantage of the dual-use nature of WMD-related technologies. For example, networks of fictive companies and organizations help conceal the transfer of radioactive materials, coming to the Czech Republic mostly from the former Soviet Union. Many chemical and biological weapon (CBW) facilities are hidden in plants that are very hard to distinguish from genuine commercial sites. Unlike nuclear or chemical weapons, bacteriological weapons can be constructed in very small laboratories within a few days. That is why all WMD transfers, including delivery means, special components, and production technology are one of the main concerns of the intelligence services in all democratic countries.

Terrorism: Count de Marenches, former head of the French intelligence services, insisted that the Cold War was really World War III, and that World War IV is now under way, full of new enemies. He predicted in 1992: “The Fourth World War will be a terrorist war.” (Marenches and Andelman 1992) Unfortunately, he seems to be right and the recent tragic events of September 11, 2001 have confirmed his prediction.

Domestic unrest and political, religious, or ethnic conflicts in weak states are factors conductive to terrorism. The problems terrorists exploit—poverty, alienation, and ethnic tensions—are estimated to increase over this decade. The world's poorest and most politically unstable regions in Asia and Africa will have the largest youth population in the near future, expanding the recruiting potential for extremist groups.

Intelligence services generally fear that not only conventional explosives but also nuclear, chemical, or biological weapons could be used as a means of blackmailing the government or international organizations. Terrorist groups have ready access to information on WMD via open sources, especially the Internet.

So far, the Czech Republic has not been a terrorist target. Although over two hundred explosions have been recorded since 1990, all the cases were labeled as the work of amateurs without detectable political motives. Yet, adversarial groups or individuals may use the Czech Republic as a base for attacks in other states, or they can attack Czech-based institutions, such as embassies or the Radio Free Europe/Radio Liberty in Prague. In general, terrorists can target high-profile government facilities, famous landmarks, and infrastructure nodes, such as airports, bridges, and dams. To stop or prevent such attacks is enormously difficult, and the intelligence services play an exclusive role when collecting and analyzing information on the intentions and movements of terrorist groups and individuals.

In a number of regions, Islamic fundamental terrorism in particular is already a frequent and dangerous phenomenon. The region closest to the Czech Republic that is important to the military intelligence is the Balkan Peninsula. Furthermore, worldwide organizations, such as Al-Qa'ida, Hamas, Hizballah, and others that have already planned and successfully accomplished various strikes against allied targets in Europe and must be monitored attentively.

Information Warfare:[13] High performance electronic information systems have created global network cyberspace. Not only were corporate businesses and governments able to attain high technology, but also tens of millions of individuals suddenly within less than a decade gained tools and capabilities, which had been previously limited to a selected few. Today, many state and local governmental organizations are establishing a presence on the Internet. Also, thousands of private agencies are reachable via online information services. That has radically complicated what intelligence agencies had to face in the past into something very complex now, and which will be even more troublesome in the future.

The Czech military often depends on civilian information networks. Most of the peacetime military communications, for example, travel over the same phone networks used to fax a contract or to talk with a friend. Also, the national electric power grid powers military and police bases. Purchases for military organizations are paid via the commercial banking network. People from national security organizations are transported under the guidance of civilian rail and air traffic control systems. Each of these information or transportation nodes creates a substantial vulnerability for the military in a crisis.

Today, one who controls information controls people. Relying on information systems presents an attractive but two-sided opportunity—intelligence can use information systems effectively to gain, store, and retrieve information but adversaries can also attack such systems. Such development has created the *information war*. An

[13] Although some authors see information warfare (IW) more as a combat arm, it definitely represents a highly topical issue for the military intelligence. However, the extent of IW is so wide that it exceeds the scope of this thesis. To better understand IW and its relation to terrorism and organized crime, see the works of Arquilla, Denning, Ronfeldt, and Schwartau.

information war has no front line. The potential battlefields are anywhere networked systems allow access. Information warfare is a low-budget, high-tech vehicle for mass destruction. (Schwartau 1996) Indeed, cyber terrorists attack information networks relatively cheaply already.

Organized Crime: Offenses such as arms proliferation, smuggling, computer crime, drug trafficking and other crimes directly impact the Czech Republic citizens and economy, regardless of their origin. The democratic development and still primitive tools for maintaining security in the Czech Republic are attractive targets for criminal activities. Transnational organized crime is currently the greatest imperilment. The Czech Republic is attractive both as a market and a transit route due to the weaknesses in its legal, policing and judicial structures. The political, social, and economic changes occurring in Eastern Europe and in the former USSR have provided significant, unintended opportunities for organized crime and criminal enterprises. Illegal syndicates set up their underground networks for illegal migration, drug trafficking, and arms proliferation.

Criminal organizations operating in the Czech Republic come mainly from the countries of the former Soviet Union, former Yugoslavia, and Bulgaria, together with those from Italy and Southeast Asia. For example, Asian criminals, especially Vietnamese, have been involved in organizing illegal migration and smuggling goods. Arabian, Yugoslav and Albanian groups concentrate on drugs and deal in arms. Well-organized criminals from Russia, Ukraine, Chechnya, and the former Yugoslavia are becoming more aggressive and are typically involved in criminal violence. The groups from the former USSR are now the most active, merging with various illegal groups that operate internationally.

As to the illegal migration, refugees crossing Czech borders in recent years decreased because of improvements in Kosovo. Yet, the number of fugitives from other parts of Europe and Asia increased. Some foreigners do not legalize their residence in the Czech Republic and participate in various criminal activities. Their arrival and residence is mostly planned and conducted by internationally organized groups.[14] Indeed, illegal migration is moving mostly from the East and Southeast to Germany. Statistical data confirm that the Czech Republic remains a transit country for fugitives on route to Western Europe (Zpráva 2000).

Narcotics and drug proliferation is another threat that spreads across borders. The narcotics have become a global problem that is likely to rise dramatically in the Czech Republic in the next few years. Statistics on illicit drug consumption in the Czech Republic[15] indicate that drug use and drug trafficking is on the rise. The Czech military has not participated in any particular anti-drug operation so far; however, the ACR should not exclude the possibility of being involved in a larger anti-narcotic operation.

Illegal trade in arms and explosives has remained almost constant recently. Criminal groups illegally sell and purchase explosives, weapons, and ammunition with no identification marks, frequently offered on the black market.

Economy: We traditionally tend to think in either military or economic terms, instead of recognizing the synergy of the two and treating them as a single concept. The collection strategies of adversaries and allies alike will not only focus on defense-related information but will also focus on scientific, technological, political, and economic information. Misinformation, blackmailing, destruction, or other means of economic disruption must be anticipated. From a military perspective, economic vulnerability of well-developed countries as well as the economy of potential adversaries should be

[14] In 2000, 32,720 persons were apprehended while illegally crossing the national borders; 94% of them—30,761 persons—were foreigners. Most were from Romania, Afghanistan, Moldavia, Sri Lanka, India, Ukraine, and Bulgaria (Zpráva 2000).

[15] Estimated numbers of consumers (based on the demand side) for the year 2000 were as follows:

- Marijuana and hashish: 250,000 consumers
- Pervitin (a Czech-made, ephedrine-based synthetic drug): 22,500 consumers
- Heroin: 15,000 consumers
- LSD: 6,540 consumers
- Ecstasy: 5,820 consumers.

Illicit drug consumption totaled 0.8% of the GDP. *Note*: According to researchers, the numbers are probably underestimated due to very insufficient data collection, particularly in the case of Ecstasy (SANANIM 2002) .

considered when providing intelligence to commanders and policymakers because economy plays a very important part in a country's development.

C. OSINT IN THE CZECH MILITARY INTELLIGENCE SERVICE

In the age of information, intelligence is less a matter of penetrating secrets, and more a matter of extracting useful information from the flood of open information that is legally and cheaply available. The single most significant step an intelligence organization can take to increase the value of the information it acquires is to increase the speed with which the information is acquired and acted upon (Steele 1993). Yet, this would not be enough. As explained in the previous chapter, information is just a middle part of the pyramid—even if information is timely and accurate, it has no value unless it is used to create, distribute and use knowledge in decision-making processes.

The Czech military intelligence must react to the enormous impact open sources and information systems have on all aspect of intelligence dealings. The VZS can differentiate itself not solely by what collection assets it has at its disposal or how much or how little money it spends, but rather on the basis of what its people know. The author believes that OSINT, built on the knowledge management principles is a useful concept that can meet the consumers' needs. Some older practitioners may consider the concept revolutionary—but it is actually rather an incremental step that should be taken to manage open sources properly, using the advantages of modern information technology.

Indeed, the thesis will not provide a full analysis and a complex solution for OSINT knowledge management in the military intelligence—this is not a task for one person and a few months of research. However, by focusing on the challenges that should be considered, the four stages of the knowledge system and process design used in this section will help explain the role of OSINT in the Czech military intelligence. The section identifies target knowledge that can be acquired via OSINT, analyzes current OSINT procedures, and also identifies processes that must be addressed in future OSINT development. The section targets the Military Intelligence Service (VZS) in particular;

however, when appropriate, generalizations are made to express the broader applicability of the knowledge system and process design.

1. Process Analysis

In this first stage of the knowledge system and process design, attention is paid to objectives and strategies of the ACR in order to identify the knowledge that OSINT can attain and the VZS can manage. The OSINT system must not be built without understanding the tasks of the VZS; for each process, the knowledge that can ensure an effective performance must be defined.

First of all, the VZS serves as a decision-making tool for the strategic military commander, namely the Chief of the General Staff. Although some daily practices may suggest otherwise, the VZS is an organization that must provide military related intelligence—its first and foremost role. This role implies that the VZS builds its knowledge base upon the objectives and strategies of the ACR.

The objectives and strategies of the ACR have already been introduced in the previous sections. Now, combining the potential security threats and risks with the principal tasks of the ACR, the use of the Armed Forces is summarized into two main categories, each of which comprises a subset of probable tasks:

a) *Inside the Territory of the Czech Republic*: The ACR can be employed in the case of a threat or a risk that may have a direct impact inside the Czech Republic. The ACR may be particularly engaged to counter:

- Acts of the international organized crime of larger extent, such as proliferation of arms or weapons of mass destruction (WMD), drug trafficking, and extended communication and computer network attacks;
- Terrorist activities, either intended or realized;
- Immigration waves of a large magnitude;
- Natural disasters or technological accidents.

b) *Outside the Territory of the Czech Republic*: The ACR can be involved in military and non-military activities to prevent or to counter possible threats that may have both direct and indirect impact on Czech or European security. Most likely, Czech troops will not act outside their territory on their own but rather under the umbrella of the UN or NATO operations, or as a part of the CESDP rapid reaction forces. The ACR may be employed in:

- NATO operations, either under the Article 5 or in non-Article-5 operations;
- UN-lead peace-support operations;
- UN/EU humanitarian missions of various nature;
- Actions realized under bilateral and multilateral military cooperation, such as the Partnership for Peace (PfP) program, military exercises, on-demand expertise, and so on.

One can easily see that most of the above mentioned tasks are of a non-combat or semi-military nature, although the military engages its combat assets during those missions and the possibility of direct combat cannot be excluded. Operations may not necessarily be waged against single and easily recognizable foes.

The ACR will likely participate in the missions abroad more frequently than engage inside the country. Intelligence needs for such missions seem to be relatively straightforward, considering the contemporary dynamic mode of operations. At the strategic level, there will generally be less need to discover the intention of an aggression, as in such cases the adverse activities will already be occurring. But the VZS will certainly need to gain and to use knowledge related to the local political situation, culture, demographics, terrain, weather, infrastructure, and composition and deployment of hostile and friendly forces. In some cases, such as WMD industry issues or technological disasters, very specific knowledge and expertise may be required.

U.S Ambassador Kimmit's requirement of the intelligence "an inch deep and a mile wide, with the ability to go a mile deep on any given issue" is certainly valid for the VZS as well. Yet, there is probably no intelligence organization in the world that is able to manage such a requirement solely on its own. That applies to the VZS in particular, knowing the limitations and circumstances under which the organization operates.

2. Knowledge Analysis

This second stage of the knowledge system and process design results from the previous analysis. In this part, the analysis concentrates on identifying the knowledge that is needed within the VZS.

When asked, the top VZS management confirmed that the service is now more involved in non-military topics than in traditional military subjects. As foreshadowed in the second chapter, the VZS simply cannot use only its own secret collection and analytical assets to cover the customers' needs—and neither can it acquire the required knowledge through OSINT itself. In all issues, OSINT must function as the first instance, as a broad knowledge base and as a knowledge gap filler.

Let's now have a brief look at the knowledge that can be build via OSINT and what purpose it may serve.

Warning: Military commanders and defense policy-makers will always be concerned about strategic warning. OSINT can provide a sufficient base for monitoring events that can potentially endanger the nation's existence, focusing on three main issues—nuclear attack, conventional attack, and unconventional developments.

As already mentioned, the nature of nuclear attack has changed. Arms reduction and the close monitoring of traditional nuclear powers, such as Russia or Kazakhstan, have been effective. On the other hand, the growing list of other nuclear-capable states consists of many unstable regimes whose interests and policies are contentious to those of the Czech Republic and its allies.

Conventional attack warning will probably remain an everlasting concern for the military intelligence, maybe even more so when the nuclear threat has diminished. Possible forward force deployments and military engagements in crisis regions is the reason for a continuous "intelligence watch."

Insurgencies, terrorist incidents, humanitarian crisis, and so on represent unconventional developments. The ACR and its allies will likely be encountering such developments more frequently. The Balkan situation, for example, represents an area of uncertain Czech policy interests but definitely continues to have the potential for humanitarian crisis or other disasters. Instability in Central Asia threatens gradually to involve many regional powers, such as Russia, Turkey, China, Iran, India, and Pakistan. These developments, however, can be sufficiently monitored using open source news alerts and similar expert services. Also, non-state actors that use terrorism as "cheap warfare" frequently come from revolutionary, sectarian, and extremist religious groups, knowledge of which can frequently be through OSINT. Similarly, the VZS will mostly turn to open sources when seeking for knowledge related to international crime.

Peace Keeping/Peace Enforcement Operations (PKO/PEO): Kuwait, former Yugoslavia, Afghanistan—what will be next? For many years, Czech military units and individuals participated in peacekeeping operations; yet the military intelligence supporting those in the peacekeeping missions remains far from ideal. The intelligence support must not be aimed only at the top political-military command, i.e. the Ministry of Defense and the General Staff, but also at the troops in the field. Indeed, as both the VZS and the military units gained experience with the PKO/PEO, the situation has improved since the Persian Gulf War. However, the national intelligence support to the troops in the field is not systematic yet. OSINT can provide far more than narrow secure intelligence channels because it has the advantage of unlimited distribution and sharing. The military intelligence elements detached to support the peacekeeping forces also need—besides the traditional intelligence on orders of battle or weapons and equipment—detailed information about ethnic and religious groups, belligerent leaders, political parties and factions, military and civilian infrastructure, social structure, humanitarian needs, and so on. Obviously, not only military intelligence personnel but also every soldier on the field has a part in OSINT for the PKO/PEO.

Technology Proliferation and Arms Control: The issue of technology proliferation relates to both military and non-military technology and has become very complex. Military proliferation includes WMD, conventional systems, as well as support systems, such as command-control-communication-computer-intelligence systems (C4I), and associated technologies. The Military Intelligence Service (VZS) will have to keep up with the expanding transnational flow of subject-related knowledge. Fortunately, much of what is needed is available from the open academic and industrial sources; yet preserving and upgrading relevant knowledge will be very challenging, should the VZS continue to track the flow of technologies and knowledge. The interchangeability of technological application between military and commercial sectors and the transnational nature of technology proliferation further complicate this issue.

Other Transnational Issues: Natural disasters, population dislocations, epidemics, environmental pollution, and similar uncontrolled large-scale problems can exacerbate regional instability; so the military intelligence will be tasked to focus on such issues should it become the concern of political leaders and military commanders.

Large numbers of people have become displaced economically or as a result of ethnic and religious conflicts in the former Soviet republics, the Balkans, Eastern Europe, and other places. These people move to the political and economical refuges of Western Europe and North America where the receiving countries experience pressures in terms of social services, housing, and increased ethnic dissension. The Czech Republic is embroiled in this pressure as it frequently serves as a transit country.

Significant health problems result from mass starvation and epidemics of diseases such as AIDS. Also, older forms of diseases, such as tuberculosis are reemerging owing to the recent conflicts in the Balkans, Chechnya, and other places and to uncontrolled migration.

Environmental concerns, such as hazardous waste disposal and the safety of nuclear power plants have also become important, being exemplified by the Chernobyl disaster or by the gradual destruction of most of the drinking water supply in Russia.

Photographic intelligence assets or other parts of the military intelligence may be tasked to contribute when a nation tackles the above-listed problems. Indeed, if it were tasked to provide intelligence on these issues, the VZS could not manage required knowledge without a connection to the outside open-source world.

Central to this part of the knowledge system and process design is identifying and analyzing *critical success factors* (CSFs)—activities that must be performed effectively in order for the mission to succeed. The CSFs must be in harmony with the organization's core competency, namely providing intelligence for military commanders and other intelligence customers. The VZS may need a detailed study of its own tasks and capabilities to identify what knowledge is crucial to assess performance in the VZS' organizational setting and context. After the study is conducted, each of the factors should be separately evaluated as a single-target process. Using pre-defined configuration measurements, an existing configuration must be diagnosed in terms of process pathologies to determine how well does the existing process meet the desired goal. The diagnosis then helps eliminate the pathologies from the process.

3. Context Analysis

In this phase of the knowledge system and process design, knowledge—particularly the tacit knowledge possessed by specialists—stemming from OSINT should be captured. Once captured, the VZS can use information systems and other software applications to organize, to formalize, and to distribute the knowledge.

Organizational knowledge starts with individuals. The VZ must first recognize the knowledge its members possess, capture it, share it throughout the organization, and reuse it. In this way, the members amplify the knowledge and internalize it as a part of the organization's knowledge base. The management must be aware that intellectual capital is the most valuable asset. Collection tools and modern IT can acquire, process, and share information—but the knowledge of employees, experts outside the VZ, and the consumers of intelligence is what must be fostered and leveraged most. Managing knowledge is much more than merely storing and manipulating data—managing knowledge also recognizes the human assets that can be accessed and used by those who make decisions.

Without understanding the nature and organization of knowledge, the military intelligence personnel can hardly be effective in OSINT. An intelligence analyst, for example, may be both the seeker and provider of open-source knowledge in some cases. When solving a problem, the analyst can reach a point when further knowledge is required. The same analyst then can identify, capture, and organize the knowledge needed. In other situations, analysts will outsource this knowledge work when they lack the time, propensity, or ability to do it by themselves. Then, the analyst will just use knowledge delivered by the provider. And this example is valid virtually for all knowledge workers, whether they solve intelligence requirements or daily routine work.

The VZS should develop knowledge maps to identify who possesses what kind of knowledge, both inside and outside the organizational structure. In order to build a foundation of open-source knowledge, the VZS must create "yellow pages" and knowledge maps of military and civilian experts and analysts. To accomplish this, first the organization's internal documents, the Intranet, databases, and directories must be carefully studied to identify and capture the OSINT knowledge already existing inside the VZS. Then, virtual network organizations, research and development (R&D) centers, librarians, annual reports and conference proceedings, association directories, and many more sources can and should be mapped to create maps of knowledge existing outside the VZS' organizational structure and to identify how this knowledge can be reached.

This whole procedure will certainly take much effort and time. Yet, it is probably the only systematic way to identify existing open-source knowledge and capture it. It will also help to find if any overlaps or inefficiencies exist in the extant or generated OSINT system and process design.

4. Systems Analysis

In this final stage of the knowledge system and process design, the organization's current procedures and information systems are briefly analyzed. First, the organizational design is surveyed. Then, controlling strategies and the information-flow configurations are summarized. Finally, the analysis basically follows the six phases of the knowledge management life cycle (KMLC), describing each particular phase in terms of extant procedures and practices within the VZS. Personal conversation and a written questionnaire[16] were used to expand the author's personal experience with the VZS.

[16] The sample consisted of ten VZS employees. Five of them were analysts; the other five were supervisors.

More detailed process and systems analysis is certainly desired, should the future knowledge design for OSINT be developed. However, the following paragraphs convey basic ideas about the VZS' organization, procedures and practices.

Organizational Design: A contingency model (Jansen et al 2000) is used to determine the current organization type of the VZS. The model explains the reason a specific form of knowledge management may or may not work in the OSINT. Here, the model is used to identify the whole organization; however, it will be useful to apply it to multiple VZS levels.

The contingency model uses four general strategies for knowledge management that differ from one another as to complexity and variability of the organizational environment. The model and the position of the VZS are depicted in *Figure 7*.

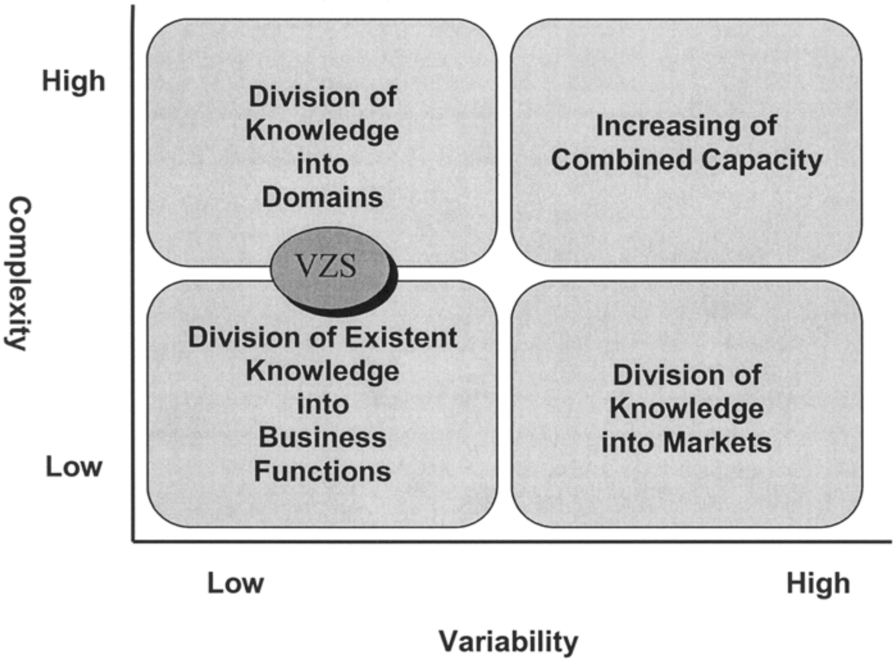

High
Division of Knowledge into Domains
Increasing of Combined Capacity
Complexity
VZS
Division of Existent Knowledge into Business Functions
Division of Knowledge into Markets
Low
Low
High
Variability

Figure 7. Four Strategies for Knowledge Management and the VZS

The current organizational design of the VZS and its information and communication technology does not exactly fit any of the four illustrated types. While the organization's structure evidently has some elements of the division into business functions, in some parts the VZS reveals existing domains of expertise. *Table 1* summarizes the main characteristics of the extant organizational design and IT.

Organizational Type	Organizational Design	IT and Communication
Division into Business Functions	• Centralization • Staff Organs • Rules and Procedures • Separate Departments	• Formal, Central Information System Focused on Compilation and Retrieval • Intranet
Division into Domains	• Separate Knowledge Domains • Individual Knowledge Levels • Group Knowledge Levels	• Generally Accessible Information System • Newsgroups and Bulletin Boards within Some of the Knowledge Domains

Table 1. Characteristics of the Extant Organizational Design and IT in the VZS

Dividing existent knowledge into business functions is mostly used in situations that are neither complex nor dynamic, and the organization does not actually create knowledge but frequently uses and refines it. Although this is not the case, the organization of the VZS is divided into separate functional departments and sections. The knowledge is also concentrated in the minds of individuals and very small, enclosed information entities. This is definitely a concept of the past when the required knowledge was clearly defined and this functional form was effective. However, this approach is still valid when existent knowledge must become explicit and when individuals want to use the knowledge.

Dividing knowledge into domains or areas of expertise is characteristic by dividing activities into different professional domains. Specialists for limited areas of expertise have the appropriate knowledge at their disposal; and the VZS management often uses these specialists to solve complex problems by creating ad hoc teams or cross-functional projects. The knowledge is used; the focus stays more on the application of implicit knowledge that the experts possess, rather than on knowledge content or knowledge creation.

It is no wonder that, in practice, the VZS has to adapt its organizational character and alter the strategy of knowledge work. The dynamics of information environment and variable requirements do not fit the military hierarchy well. Today, the adaptations are merely a passive reaction to the disordered outside environment. But the VZS should actively decide to choose a different path and should become an organization that creates knowledge, making it a more virtual, project-oriented enterprise. OSINT is the foremost arena where such a shift is possible.

Controlling Strategies and Information Flow: The existing organizational structure of the VZS, with its vertically oriented control, fully reflects the traditional military hierarchy. A simplified version of controlling and collaborating is illustrated in *Figure 8*. The structure of the VZS is formally built to let knowledge flow up while controlling its distribution down. However, the incoherent changes in the outer dynamic environment often force the organization's elements to collaborate in the horizontal directions, both formally and informally. The two functions of the VZS, i.e. the function of the defense intelligence agency and the function of the strategic directorate for reconnaissance and collection have created organizational difficulties, supporting stovepipes of the information flow.

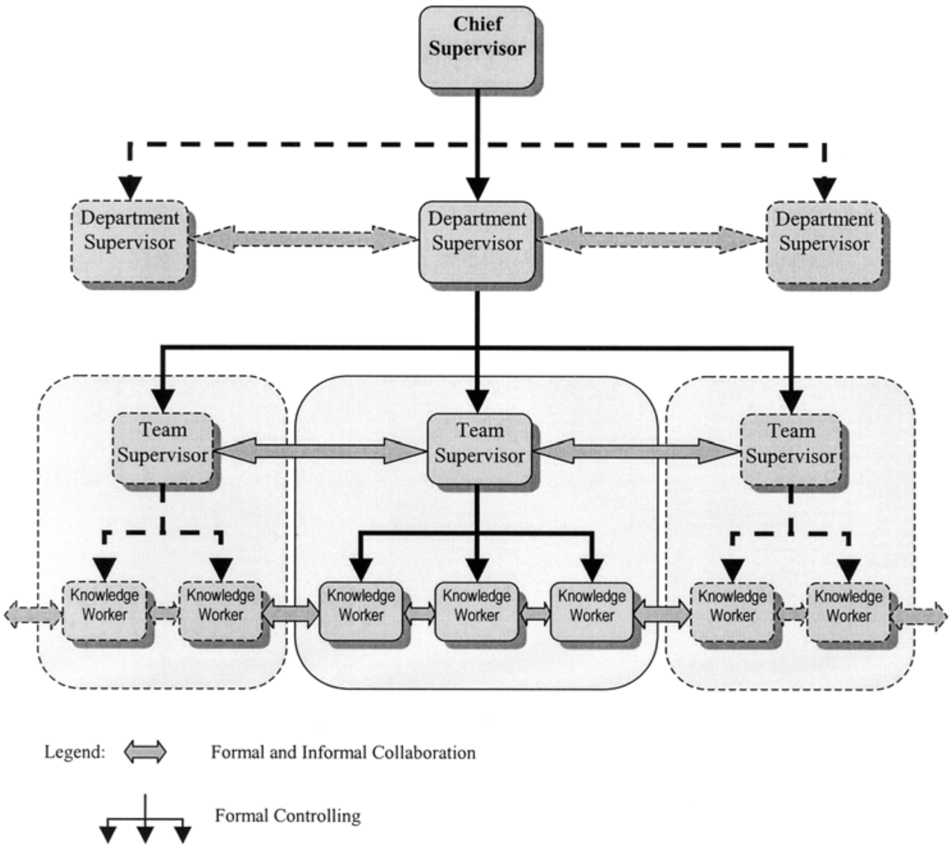


Figure 8. Controlling and Collaboration in the VZS

After the succession to NATO, the Czech military adopted a formal model of the NATO intelligence cycle in order to meet standardization requirements; however, the organizational structure and intelligence procedures have not fully reflected the standardized collection coordination and information requirements management (CCIRM) model. To amalgamate the existing structure and standardized intelligence procedures, the VZS uses the following CCIRM system, illustrated in *Figure 9*.

Extant Procedures and Practices: Using Nonaka's interaction modes between tacit and explicit knowledge, one can begin to study how every organization creates, organizes, and formalizes its organizational knowledge. The possible interaction modes are illustrated in *Figure 10*.

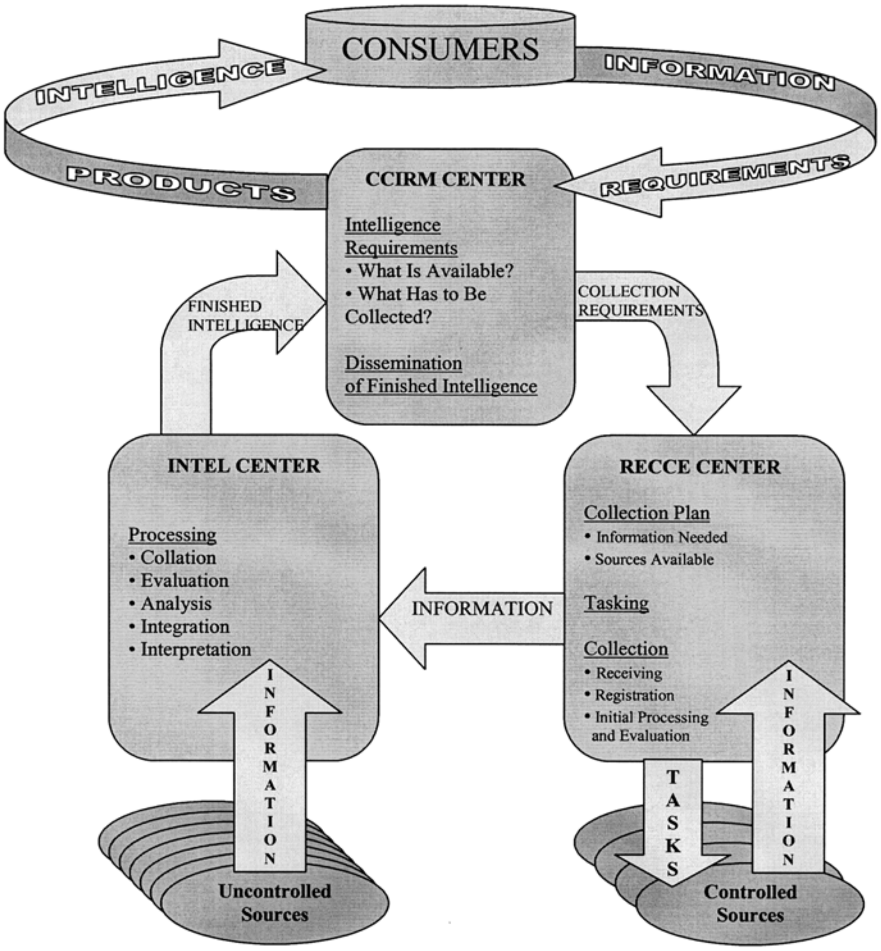


Figure 9. Collection Coordination and Information Requirements Management in the VZS

Although tacit knowledge held by individuals is the core of the knowledge creating process, full benefits can be obtained only when dynamic interaction occur through all possible modes—tacit to tacit, tacit to explicit, explicit to tacit, and explicit to explicit. As to the military intelligence, the actual intensity of the possible interaction modes is expressed by the thickness of the arrows. Most interactions are realized through the explicit channels, such as written orders and requirements, intelligence working papers, manuals, database exchange, or electronic communication. Then interaction also occurs between the tacit and explicit nodes, probably more in the direction from the explicit form to the human recipients. And the smallest portion of knowledge is actually

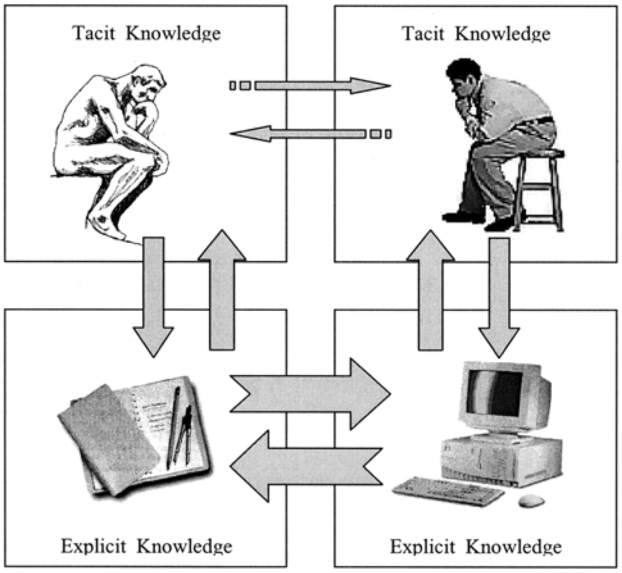


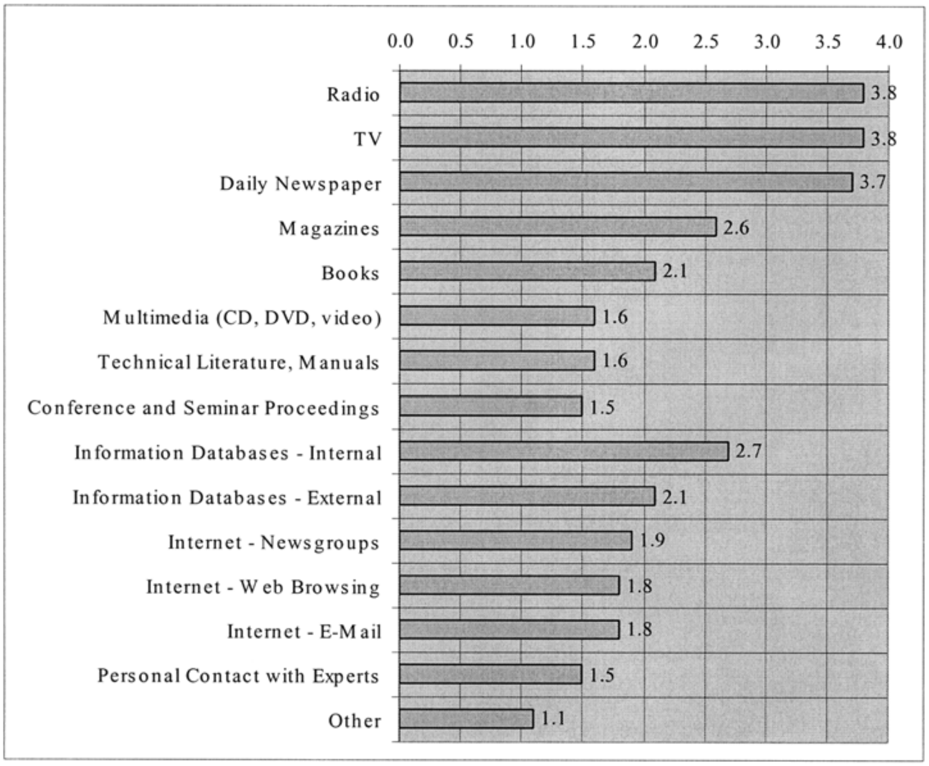
Figure 10. Military Intelligence and Knowledge Interaction Modes

exchanged through human-to-human communication, despite the fact that the tacit knowledge is probably the most important part of the organizational knowledge base, as already stressed.

To further quantify how often the VZS personnel uses each of the four modes of knowledge interaction, the representative sample of the VZS employees has been questioned. The following graphs express how often they interact with different forms of open sources.[17] *Graph 1* represents domestic sources; *Graph 2* illustrates the situation with sources abroad.

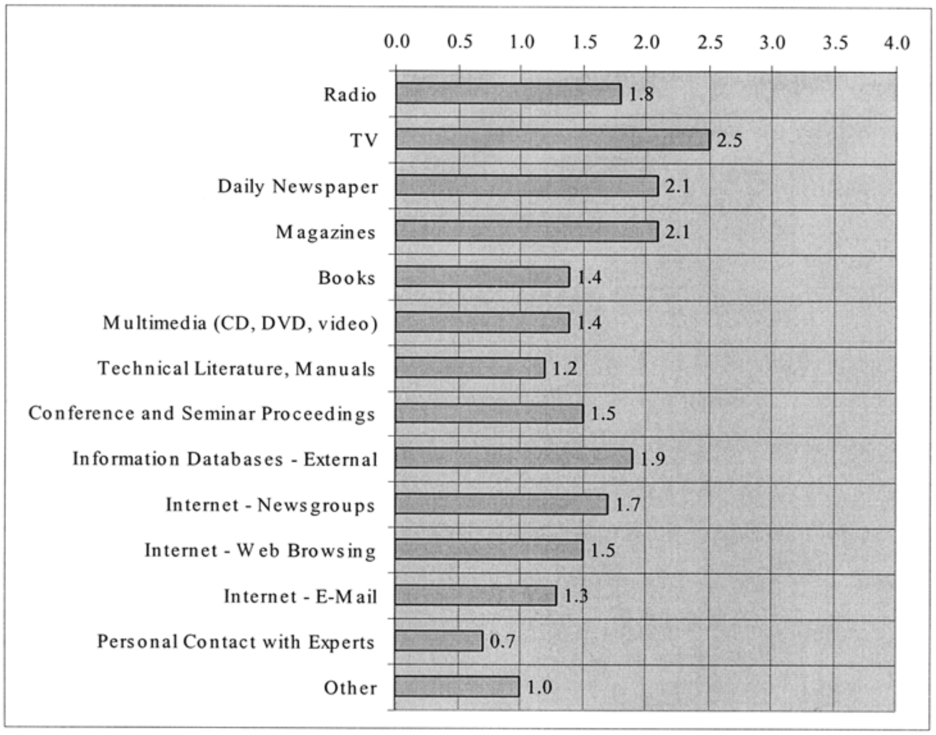
The knowledge created or captured in the OSINT seems to be based more on media and databases than on person-to-person contacts. This may be a result of many factors, such as source availability, language barriers, or budgetary restrictions. Further study will be definitely advantageous to future knowledge managers in the VZS.

[17] The frequency of use was graded as follows: 0—Never; 1—Seldom (at least once a year); 2—Occassionally (at least once a month); 3—Frequently (every week); 4—The most often (daily).



Graph 1. Frequency of the Use of Domestic Open Sources

As to the phase of knowledge formalization, the formalization of the knowledge does not occur systematically and regularly throughout the VZS. As the collected open-source data and information allow for creating new knowledge, this knowledge is frequently directly used during the intelligence process. To the author's best knowledge, the VZS has not yet employed any knowledge-based system (KBS) that could serve as a means to formalize open-source knowledge inside the organization. Existing information system is oriented toward information storage and exchange and can hardly serve to knowledge formalization. This is mainly because knowledge formalization requires that the knowledge management system be designed *after* the nature of knowledge itself is analyzed—not *before* or *without* such analysis. Unfortunately, intelligence managers and IT people often believe that a computer network can store human intelligence and experience.



Graph 2. Frequency of the Use of Foreign Open Sources

The formalization of knowledge also bears one negative aspect when it comes to the final fusion and production of the all-source intelligence. During the all-source analysis, the job of selecting and using appropriate knowledge is done twice—first, for open-source information, and then again with classified information. Current security apparatus is very restrictive as to channeling both classified and unclassified data into the same workstation. An extant information system does not allow automated merging of these two, owing to inadequate security measures. Data storage for classified data has evolved in a closed internal system, which is connected only to external systems of the same classification. This is certainly positive in terms of intrusion and computer attacks; however, it creates many "roadblocks" to all-source intelligence production.[18]

[18] Most interviewees estimated that the VZS uses 30-50% of open sources for all-source intelligence.

Distribution of knowledge both inside and outside the VZS is problematic, too. Knowledge based on classified information has its own specific distribution problems, as already foreshadowed. Knowledge based on open sources can be distributed freely; yet it seems as though *all* the information distributed and *all* the knowledge shared is tainted with the principle "need to know"—even unclassified information had to be registered until two years ago.

Estimated 75% to 80% of information is distributed on paper. As the existing electronic system does not provide for sufficient knowledge formalization, it cannot allow for knowledge sharing either. Printed lessons learned, handbooks, and intelligence manuals do exist; but they do not count for a significant part of the existing organizational knowledge.

It has been already stressed that knowledge should help individuals and organizations make decisions. In the VZS, the knowledge is applied mostly within the minds of individuals based upon the information set that is available at the moment. The knowledge base, which would help form one's decisions, does not exist. The OSINT center of the VZS has been redesigned recently, however, it seems to be established upon the traditional assumption—that OSINT is merely a counterpart, rather than a base, for secret collection. It is assumed that compiling data and information in a central repository can ensure that everyone with an access to the repository is capable of and willing to use it. This assumption is not valid. Most managers—the VZS not excluding—make decisions based on their interaction with others who they account knowledgeable about the issues. That does not signify that those accounted for the knowledge by managers are really the most knowledgeable persons. Without proper knowledge management, it is likely that managers will judge one's knowledge merely on one's glibness rather than on one's actual contribution to the organizational knowledge.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ADAPTING KNOWLEDGE MANAGEMENT THEORY TO THE CZECH MILITARY INTELLIGENCE

Knowledge work is the core business of the military intelligence. As stressed beforehand, knowledge work is not limited to the VZS; virtually all organizations across all the governmental and private sectors are becoming knowledge intensive (Drucker 1994). The Czech military cannot avoid this development; the Czech military must rather adapt to it. Today, the massive flow of open-source information overwhelms the traditional collection and analysis system that the military intelligence uses. Information is lost or wasted and even critically important information, when acquired, is not always turned into "corporate" knowledge. To achieve a working synthesis of IT and different knowledge domains, OSINT requires multi-disciplinary expertise, collaboration, and mutual learning. New models, leadership commitment, and new ways of thinking are needed.

This chapter outlines the main aspects of the OSINT knowledge system and process design for the Czech military. The first section presents the major steps to building knowledge management, focusing on the main areas to which the Czech military, particularly the VZS, should pay attention when designing its future OSINT. Then the second section of the chapter discusses the objectives and limitations of the OSINT process and system design. Finally, the last section encapsulates the OSINT process and system design and presents the general alternatives to the OSINT knowledge-management system.

A. MAJOR STEPS TO BUILDING OSINT KNOWLEDGE-MANAGEMENT SYSTEM

Introducing knowledge management into the existing OSINT environment of the VZS is a long-term task that should be built in incremental steps. Karl Wiig (1999) introduced sixteen building blocks that should be considered for introducing a new knowledge management practice. Based on his work, the following section describes seven basic steps in their approximate order of implementation that the VZS should take when designing its OSINT knowledge-management system.

Management Commitment: Management commitment is essential for all the knowledge management efforts. Knowledge management champions among the top VZS leaders are needed to help create a shared vision of how the OSINT will be managed. Furthermore, both the leaders and the knowledge workers must develop a mutual conviction that knowledge management is the proper way to conduct OSINT. They must believe that it is worth their effort. To do so, well-founded, specific, relevant and realistic examples must be created to present the new knowledge-management opportunities to both the management and knowledge workers. That does not necessarily mean that the VZS must create such examples by itself first; many good examples of efficient open-source knowledge management can certainly be found in the business world and in academia, too.

Knowledge Mapping: Knowledge maps and similar surveys must first and foremost provide the understanding of the OSINT knowledge state. Such maps will describe major OSINT-related knowledge assets, activities, and practices, and will compare them to existing assets outside the VZS. Existing knowledge assets must be carefully mapped and collated with the directions and tasks assigned to the military intelligence. The VZS management needs OSINT knowledge mapping to establish the groundwork for a knowledge strategy and to identify specific needs and opportunities.

Owing to limited budgets and other restrictions, the VZS may not want to hire an external survey team to map the knowledge inside the organization. So, the VZS should build one or a few dedicated teams by itself to survey quickly and economically the existing open-source knowledge and to create OSINT knowledge maps. These maps will help propose actions the VZS management and knowledge workers must take, and the maps will also help define key OSINT requirements.

Knowledge Strategy: The VZS is an organization large enough to need a formally formulated OSINT strategy. A knowledge strategy is needed to determine how OSINT will support the overall knowledge management, to set knowledge management priorities, and to determine key knowledge requirements, i.e. critical success factors (CSFs). The purpose of the strategy is to outline OSINT objectives by reflecting the knowledge management vision in a consistent framework. An explicit strategy will help OSINT managers and knowledge workers create and select specific solutions fitted to current and future conditions inside and outside the VZS. The strategy can improve decision-making by establishing a consensus around long-term goals, and by creating a vision for the OSINT knowledge workers. A strategic plan for OSINT should comprise at least the following elements:

- OSINT vision;
- List of the goals with regards to OSINT;
- Forecast of developments in the external environment to which the VZS must respond;
- Statement about how the VZS will extend its current OSINT system in the future;
- Actions and milestones regarding decisions and projects, including milestones and financial projections.

Key Knowledge Acquisition: Key knowledge must be acquired to fulfill the requirements of the CSFs. Here the focus is to obtain and to characterize the detailed open-source knowledge that will meet the CSFs demands. This can be done by gaining information from various open sources that will describe the actual knowledge in sufficient details for communication to other people and knowledge repositories. Using previously generated knowledge maps, knowledge workers can acquire the desired knowledge from individuals inside the VZS. Especially when employees are promoted or when they leave the organization, others should capture their valuable knowledge for reuse. Lessons learned, training, apprenticeship, and many other knowledge engineering methods are available to elicit extant knowledge. Furthermore, when sources of knowledge are outside the VZS—which, considering the nature of OSINT, will be the most frequent case—that knowledge must be gained for incorporation to the VZS knowledge assets.

Knowledge Transfer: Once the key knowledge has been obtained, it must be transferred to its users. Information technology (IT) itself does not manage knowledge, but it can greatly help the knowledge management process. It is important that the military management does not perceive knowledge management as just another database or a software program. These are just tools that support knowledge content. No system does it all; hundreds of products have different supporting functions, such as information search and retrieval, categorization, knowledge formalization, and distribution. The IT support personnel do not choose or create knowledge and its content. But they have the difficult task to select carefully commercial off-the-shelf (COTS) products that will support knowledge management well. The VZS must build a comprehensive knowledge transfer system by creating an expert OSINT network, consisting of experts online, expert software systems, intelligent software agents, and so on. Usually, the extant knowledge transfer systems follow traditional paths and are uncoordinated. Also, some parts of the expert network may be missing in the existing organizational structure and procedures, owing to limited budgets and deficient incentives. It is likely that such inefficiencies will be discovered during the process of knowledge mapping; so in this stage, the builders of the expert OSINT network must address them. Detail studies of commercially available IT tools will be necessary prior to selecting COTS hardware and software, as well as training programs for those who will use them. Following this, the expert OSINT network will serve its purpose—to make the knowledge possessed by individuals available for distribution to the VZS employees and customers.

Incentive Programs: VZS managers should motivate OSINT personnel to act intelligently—to be innovative, to capture new knowledge, to share their knowledge, and so on. Soon after the VZS management decides on a vision for OSINT, and after knowledge mapping indicates any needs for incentives or for removal of disincentives, the OSINT leaders can construct incentive programs in order to make OSINT knowledge workers personally responsible for knowledge mindfulness. The VZS management should know which factors influence behavior of OSINT personnel both positively and negatively and discuss these factors personally throughout the organization. Such factors may be associated with insufficient time or manpower, with people's self esteem, values and emotions, with job security and social support, and so on. Because of the complexity and importance of such factors, the incentive programs must be continuous and flexible.

Knowledge Assets Facilitation: Knowledge assets, both tacit and explicit, must be carefully managed through all six phases of the knowledge management life cycle, using extant IT tools. A proper distinction between knowledge assets that are owned by the VZS and those existing outside the organization, together with balanced investments for these two asset categories, can help build and exploit knowledge assets, provide essential support, and steer the desired OSINT activities. When building or improving the expert OSINT network, all the important knowledge "pathways" must be addressed. Ideally, the OSINT system will provide functions for all the KMLC phases—not only for knowledge organization, formalization, and distribution, but also for knowledge creation, application, and evolution. Moreover, the network must allow consistent knowledge asset management at every level of the VZS.

B. OBJECTIVES AND LIMITATIONS TO BUILDING OSINT KNOWLEDGE-MANAGEMENT SYSTEM

This section synthesizes the objectives of the OSINT knowledge management process and system design and the major limitations that are likely to occur during the design process. After presenting the core issues of the knowledge management process, the key points of the organizational design are compiled. In addition to that, the section also pinpoints three challenges specific to the Czech military intelligence.

1. OSINT Knowledge Management Process

Understanding the objectives and limitations of the knowledge management life cycle in the Czech military is a necessary condition for designing a future OSINT knowledge-management system. The core issues of knowledge creation, sharing, and distribution are as follows:

Knowledge Creation: Creating new knowledge does not come automatically. It is typically an act of establishing a meaningful relationship between concepts or objects that have not previously been related. It could happen by a fortunate accident, or it could be a result of an appropriate organizational environment that fosters creativity. Creativity also requires certain personal qualities, such as curiosity, imagination, assertiveness, self-confidence, risk acceptance, and so on. The VZS certainly does not need castle-builders, but it may need visionaries and creative people. Intelligence personnel need to recognize when intelligence analysis may be no more sophisticated that existing "conventional wisdom" on a given issue, but they also need to recognize when "common sense" does not work properly and a non-conventional approach may help.

Motivating creativity in OSINT is certainly challenging. The most important aspects are developing communication networks and also a culture with freedom of thought and enjoyment in the performance. These aspects have certain organizational implications for OSINT that are summarized as follows:

- Organizational structure is flat, without hierarchical control, with task-oriented teams;
- Intelligence processes are directed toward generation, selection, and use of knowledge, with flexible planning and loose control;
- Reward system allows autonomy of individuals and recognition of their abilities;
- Knowledge workers elaborately combine technical knowledge with creative personal characteristics while managers act as sponsors and facilitators. (Galbraith and Kazanijan 1986)

Some of the implication listed above, especially those going against traditional hierarchy, are hard to imagine and extremely difficult to promote in the military. Yet, these are desperately needed, if the Czech OSINT should reach its fully creative stage. Although it is unlikely that the military intelligence will reach ideal conditions for creativity, the VZS can certainly adopt some of the above-mentioned aspects to its structure and processes.

Knowledge Sharing: No matter how good the OSINT system is, unless it is directly tied to visible organizational benefits, the implementation of a knowledge-management system can result in negative attitudes, low returns on investments, and resistant behaviors of those who are supposed to use it. Many organizations started building IT systems for knowledge management before building the cultural and collaborative base for such systems. But the issues of collaboration are important. For example, when tasked to contribute with their knowledge, people often see the request as:

- Extra work (they are not paid for it);
- No benefit for them (they do not need to share);
- No benefit for the organization (they are not sure who will use the shared knowledge);
- Benefit for others but little value to them.

It is no wonder that with such attitudes and beliefs people do not want to share, and therefore to give away what they know and what they have learned, sometimes at great expenses. In reality, one does not lose anything by sharing knowledge; personnel still retain what they know. But practically, knowledge sharing depends on how much people believe in and value themselves and the others. (Coleman 1999)

Knowledge sharing must be encouraged by certain rewards. The VZS management should not be surprised that it will want to implement a new information system, and it may end up solving the compensation issues. Obviously, that purely financial motivation to share knowledge is severely limited under the extant fixed disbursement system of the Czech military; however, economic incentives are not impossible. Moreover, people also respond to motives other than financial, such as to high cultural and professional values shared throughout the organization. The assistance of human resource professionals may be useful in building knowledge infrastructure and IT support when the VZS managers want to overcome traditional procedures and believes, which often judge an individual's value only in terms of what and whom that person knows. The military intelligence will need to establish trust within its OSINT network, both inside and outside the organization, to be able to share knowledge. Such trust is tough to build—especially within and among the intelligence services, where secrecy, suspicions, and distrust have strong roots. However, OSINT is an arena where one does not need to hide one's existence and interests; on the contrary, extended contacts and mutual trust are critical to knowledge sharing in OSINT. For these reasons, the OSINT leaders must build mutual trust, find common context, establish reasons for knowledge sharing, and provide the space to think and share.

Knowledge Distribution: One should clearly distinguish between the dissemination of information and the dissemination of knowledge. Many technologies currently used by the VZS and other Czech military organizations only provide access to data or information alone. This would work assuming that the users could understand the presented data or information so well that they could easily convert it to knowledge or assuming that the users already had the knowledge to understand and use the data directly. But such assumptions are usually not valid, as probably no one can be knowledgeable in all subjects and also, intelligence personnel do not have the time to learn about a new subject in detail when they are usually tasked to answer specific questions. So, consultants and expert systems are frequently needed if the intelligence questions are to be answered correctly.

One way to answer questions out of one's expertise is to locate an appropriate specialist, simply by selecting someone from a list of experts or by finding people who posses the expertise. Another way is to use an expert system—often complex computer software, usually interconnected with other expert systems, containing the experts' decision-making knowledge and allowing the knowledge to be effectively distributed to users. The reader may know of medical, legal, and other expert systems being successfully implemented in the business world. Indeed, expert systems are not remedies for all the OSINT needs. Sometimes immature, expert systems are just as good as the people who created them, yet they are still behind any human specialist in terms of the ability to create, to share, and to use knowledge. However, expert systems can be an excellent solution for both intelligence analysts and intelligence consumers in many cases.

2. Organizational Design

Many managers in the Czech military believe that redesigning a system is creating new organizational charts and regenerating the tables of personnel and materiel. Yet, defining the future OSINT structure is definitely more complex than that. Here are the key points of the organizational design that must be considered during the OSINT design process:

Hierarchy in the Organizational Design: Complex organizations, such as the military, traditionally approach their needs for specialization, coordination, and cooperation by creating hierarchical structures. As Max Weber (1968) described decades ago, bureaucracies with their hierarchical structures, with coordination and control through rules and standard operating procedures, and with separation of jobs and people eliminate most of the natural human behavior—cooperation, innovation, personality, variation, and emotion. Contrary to these structures, often called *mechanistic* structures, an organization can adopt an *organic* form of its structure—a form that has less narrowly defined tasks, all-directional communication, widely dispersed knowledge, and people loyal to the organization and its goals, rather than to their immediate supervisor.

In the military, seemingly, no alternatives to hierarchy exist. As long as there are benefits from division of labor and specialization, hierarchy is inevitable. But the important issue is how the hierarchy should be structured and how the different parts of it should be related to one another. As shown in the previous chapter, the VZS is currently identified with an administrative hierarchy, in which the members are organized along superior-subordinate lines. Problems occur when the bureaucratic system with its standard procedures and high level of specialization has to produce various outputs from various inputs, using poorly implemented IT in a changing environment. The intelligence process can be jeopardized when the flow of information up the hierarchy and the flow of decisions down the hierarchy are too slow. So, the VZS should reorganize its OSINT structure to increase responsiveness to external changes. Although different branches and sections of the VZS can reach open sources with certain degree of independence from other subsystems, loose bonds of OSINT elements, equipped with more sufficient means for communication and coordination will certainly increase the effectiveness for the whole VZ. Several factors urge the OSINT to move "beyond bureaucracy":

- The centralized, structured organization cannot readily adapt to change; to be responsive to external change, OSINT needs to be decentralized, with less specialization, and looser control.
- The information revolution changed the conditions for efficiency. Administrative bureaucracy and information systems to control people, as well as highly specialized manual labor, are less needed. Now, computer-integrated knowledge work and job flexibility are priorities.
- Decision-making power is needed at the operational level and should be accompanied by curtailing top-level staffs.
- To improve cross-functional cooperation, teamwork must be emphasized as the basis for organizing separate intelligence activities.

Designing OSINT Elements: If the OSINT system requires some form of hierarchy of its subsystems and elements, it is important to decide how the individuals are to be formed into teams and units within the VZS. For example, the OSINT elements can be organized on the basis of common task where the employees and assets are grouped according to their principal roles—information collectors, intelligence processors, communication specialists, and so on. The VZS might also develop its OSINT structure along the OSINT process itself, having separate elements for OSINT planning and direction, collection, processing, and dissemination. Or the VZS can organize its OSINT personnel according to their final products, such as OSINT daily monitoring awareness summary, all-source daily intelligence briefing, or monthly intelligence summary. Finally, OSINT elements can be grouped along their actual geographical location—or along the geographical location they pay attention to, such as the Balkans, the Middle East, or Russia. To decide properly, the military intelligence leaders must first understand the benefits and disadvantages of organizing the OSINT elements on one basis compared to an alternative basis, and then, when possible, combine the best of all the systems to design the organizational structure and management system of the future OSINT.

A critical design issue is the optimal degree of job specialization. Increased specialization certainly increases efficiency, but it also increases the need for coordination.

For example, the VZS can organize its OSINT knowledge workers into small cells—OSINT units. These units can consist of one or a few people according to the desired specialization, geographical location, and so on. Instead of a highly top-down controlling structure, the OSINT units can be organized rather loosely. Knowledge workers can then cooperate more easily both inside the OSINT unit and with other units through information networks and other IT tools. A rather loose organization structure of OSINT units is expressed in *Figure 11*.

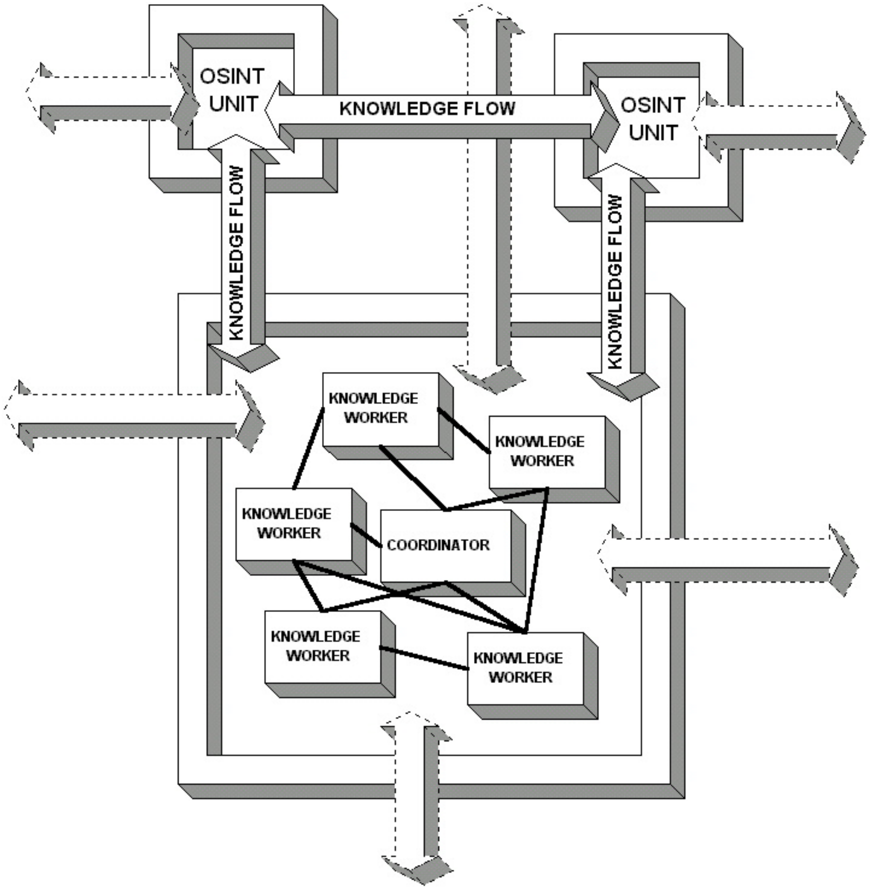


Figure 11. Loose Organization of OSINT Units

Coordination and Control: Coordination is vital to the organization's performance. The VZ specialists may be the best in the world—but unless they can coordinate their effort, their output is less than useful. Coordination in the VZ is not a technical issue; it is an issue of cooperation among different members of the organization who have different goals. Technology can just link those individuals and empower them to perform their tasks more efficiently. Coordination is mainly about establishing the knowledge-management system and procedures than can permit OSINT specialists, i.e. knowledge workers, to relate to one another and to adjust their individual actions. Three different mechanisms are basically available for achieving goal alignment within the VZ: *control mechanism*, *reward incentives*, and *shared values*.

Control Mechanisms typically consist of a manager supervising a group of subordinates. The manager monitors the subordinates' behavior and performance, and the subordinates are required to ask for approval when their actions are outside their reference. The incentives to comply with the existing hierarchy are both positive—promotion up the hierarchical ladder, and negative—no promotion or dismissal. Control mechanisms are demanding in terms of several layers of supervisors that are needed to conduct the functions of monitoring and coercion. This mechanism would probably be efficient in situations where the knowledge workers would systematically use extant knowledge to produce standard output—similarly to workers in a production line. It is doubtful that such a situation would be the usual knowledge work in the VZS.

Reward Incentives involve rewarding one’s actual performance. Such incentives directly link rewards to output, which is highly desired. Moreover, this mechanism significantly reduces the need for a costly management structure. However, this may be challenging in terms of performance measurements. Military intelligence specialists should not be rewarded according to the number of pages they produce on intelligence; they also should not be rewarded for how many hours they spent at work. The VZS employees do not work on machines producing nuts and bolts; they are supposed to create and use knowledge. Regular, even real-time adjustments and feedback to knowledge workers would help them take full responsibility for their work, without the necessity for supervisors. The key to promoting effective cooperation is to have more sophisticated incentives than just the threat of dismissal or of losing a promotion. Obviously, establishing accurate performance measurements—so that a person can be rewarded for his or her actual knowledge performance— requires profound studies by experts.

Shared Values can be rewarding by themselves when the organization's goals are conflict free. Then, the VZ can achieve high levels of cooperation without extensive control mechanisms and without performance-related rewards. Unfortunately, the organization's goals are generally not conflict free, and such a mechanism is effective only in small teams that consist of highly devoted members of the intelligence community. Yet, this type of mechanism should not be forgotten because individuals who are driven more by their moral and ethical values than by their pay do exist and are often superior employees. Professional intelligence culture, comprising of positive beliefs, values, and behavioral norms can certainly influence how the VZ employees think and behave. Indeed, organizational culture takes a long time to develop and cannot be changed easily. However, open-source environment does not need to be wrapped up in mysteries and secret intelligence games, thus the organizational culture can serve as a unifying factor for cross-functional OSINT teams.

One way or another, the future OSINT structure in the Czech military should provide for both a team-based and a project-based network of open-source experts, who will be available both inside and outside the VZ. Such a network can be flexible and responsive to various OSINT tasks, if the VZ focuses on coordination rather than on control. The OSINT knowledge-management system must permit knowledge to flow both vertically and horizontally. A well-balanced combination of the possibilities mentioned above is needed if the knowledge assets in OSINT are to be employed effectively.

3. Challenges Specific to the Czech Military Intelligence

Common challenges for knowledge management and OSINT have already been mentioned throughout the thesis. But the Czech governmental intelligence services, such as the VZ, also have to face other specific challenges.

First, the VZ must strictly obey the laws and regulations related to vetting of its personnel and to handling classified documents. In author's opinion the Czech Republic's laws and regulations in this area exceed any practical needs while often creating serious problems for individuals and organizations that must meet these formal requirements. Also, the "secrecy games" often limit, if not prevent, sharing of information and knowledge and additionally narrow the amount of people who can participate in the organizational knowledge sharing and decision-making processes. In scientific work, secrecy hinders the advancements of knowledge; in military strategy and tactics, secrecy can prevent careful planning and implementation of projects. Secrecy also obstructs reasoning, limits the perception of the problem, and limits alternatives to solving the problem, thus restricting choices and decisions (Bok 1983). Fortunately, OSINT need not be encumbered with such restrictions. The military personnel dealing with OSINT may certainly be the same people who deal with secrets. It just takes a specific mindset, as well as training and practice, to distinguish properly between unclassified and classified information when necessary and to amalgamate the two when needed.

Second, information attained by the intelligence service is usually stored for a long period of time in order to provide for long-term analysis. However, the amount of information accessible from the open sources largely exceeds the amount collected covertly. Moreover, the dynamic nature of open sources does not support simple storage of data or information gained via OSINT, as they could easily become obsolete. So, rather than store everything in the OSINT cycle, OSINT collectors, analysts, and managers will have to carefully consider the relevancy of information and intelligence products and use the IT tools at their disposal cleverly.

Third, many documents must exist on paper. Although automated document processing is not a new concept, the VZ and other military organizations still require documents on paper, mostly signed by the top commanders and directors. (The higher, the better.) A secure electronic document exchange would speed routine daily work tremendously. Unfortunately, most military personnel still trust paper more than computers, although the paper is usually not a qualitatively higher form of information storage and bears many limitations that electronic systems do not have. Currently, with increasing concerns about information security (INFOSEC),[19] the Czech military tends to be quite cautious about using computers and information networks. However, the Czech military can ensure necessary data integrity and availability through the smart use of modern technology for INFOSEC, such as the virtual private network (VPN), the Secure Sockets Layer (SSL), and many other techniques.[20] Indeed, collaborative computing may have its strict limitations in classified matters; but with OSINT, the military need not be so concerned.

C. OSINT KNOWLEDGE MANAGEMENT PROCESS AND SYSTEM DESIGN

This section presents an alternative model of the future OSINT knowledge-management system of the Czech military. First, the section discusses the use of IT in general, and four main IT tools that should be employed in the Czech military OSINT—intelligent agents, knowledge repositories, groupware, and expert systems. Then, a general model of the OSINT knowledge-management system is designed.

[19] Generally, INFOSEC covers everything that is related to information systems security—personnel security, physical security, operations security (OPSEC), communication security (COMSEC), computer security (COMPUSEC), emissions security, and so on. INFOSEC issues for OSINT represent a field for a separate specialized study.

[20] Data secrecy, data integrity, and data availability are three objectives of information security (INFOSEC). Data secrecy is of no concern in OSINT. However, data integrity, i.e. prevention of unauthorized modification and assurance of data accuracy, as well as data availability, i.e. timely response of the system, are important parts of the OSINT knowledge management system design.

1. Facilitating Knowledge Flow

Military intelligence analysts, as well as decision-makers, can frequently answer their own questions using open sources. To do this effectively, they need IT tools that will allow them to find the desired knowledge, as well as to store and to share the knowledge they already posses. As stressed before, the Czech military must adapt to changes and requirements of the outside environment, partially by improving IT. Today's information technology allows one to capture and to store OSINT knowledge and to disseminate it throughout the organization. The Czech military must take advantage of extant IT to codify tacit knowledge, store it, and make it accessible to others.

The future IT infrastructure of the VZS should provide as much functionality as possible. Here are just a few examples of what the IT infrastructure can provide to support the OSINT knowledge-management system (Wiig 1999, Nissen et al 2000):

- Information gathering and information exchange through E-mail, intranet, Internet/WWW;
- Internet/intranet data/information gathering through intelligent agents ("bots");
- Collaboration through groupware;
- Knowledge maps and knowledge "yellow pages" on intranets;
- Access to knowledge base systems/expert systems;
- Automatic pattern matching and inference from databases;
- Knowledge creation tools for discovery in databases;
- Knowledge organization and formalization tools;
- Global knowledge distribution and sharing;
- Office automation and management functions;
- Distance learning.

In the following, four main IT tools that should be incorporated in the future OSINT system in the Czech military are discussed.

Intelligent Agents: Intelligent agents are computer programs that can autonomously perform some human-like tasks and act on behalf of their users. These agents mostly integrate, analyze, evaluate, and interpret collected raw data; so they do not perform any knowledge-management functions, but they are certainly useful by automating the data processing and exploitation. Most readers have probably already used intelligence agents, in one form or another, when searching for information on the Web. Obviously, intelligent agents can be employed in various areas of the military intelligence functions. For example, they can be used to interact with an OSINT knowledge base, to determine how the given task can be fulfilled effectively, and to perform the necessary actions to reach the desired goal. Intelligent agents, connected with sensors on reconnaissance assets and performing automated tasks, can serve as other examples. Either way, the possible employment of intelligent agents should be carefully studied in order to decide about their applicability to the Czech military OSINT.

Knowledge Repositories: Knowledge repositories can capture and formalize knowledge in its explicit form for further use throughout the VZS. Two basic types of knowledge repositories are

External knowledge, which refers to knowledge about entities outside the VZS;

Internal knowledge, which could be either structured, in a form of intelligence summaries, intelligence manuals, and so on, or informal, e.g. discussion forums, lessons learned, and so on. (Davenport et al 1998)

As explained in the previous chapter, the military intelligence deals with all forms of knowledge—tacit and explicit, external and internal. So, knowledge repositories can certainly be used in the future OSINT system in order to provide basic platform for transferring the tacit open-source knowledge from individuals into a knowledge repository. The VZS should employ a nation-wide electronic discussion system as a part of its knowledge repository, through which it will be able to access experts outside the organization. The VZS should also build electronic OSINT knowledge repositories to perfect the knowledge transfer and knowledge internalization processes. The OSINT knowledge repositories must be made available through electronic networks to the military units, especially when they are deployed in the military operation during a crisis or in humanitarian relief.

Groupware: Groupware techniques allow individuals to communicate and collaborate with high efficiency by providing rich content and interactivity through real-time presentations, electronic boards, discussion forums, and video conferencing. This overcomes problems with dispersion of the military personnel in time and space and also avoids some of the negative aspects related to turnover of personnel and lack of face-to-face communication. Groupware can significantly help OSINT personnel participate remotely in the intelligence cycle processes. Moreover, groupware helps orient newcomers, familiarize them with procedures within and outside the intelligence community, and supports transitions of the organizational practices from one person to another (Davenport et al 1998). While such knowledge is relatively easy to capture and store, it will be difficult to find and to use without proper indexing and searching tools (Oxendine and Nissen 2001). The VZS should utilize COTS groupware, such as Lotus Notes, to facilitate the capture and the exchange of tacit knowledge. Moreover, the use of groupware must be accompanied with proper incentives for the VZS employees, as well as for the people outside the organization to contribute and to share OSINT knowledge.

Expert Systems: Expert systems (ES) are computer programs that help non-experts make decisions similar to those of experts through an emulated interaction with a specific expert domain, such as finance, history, electronics, law, medicine, and so on. When communicating with the ES, users usually have no or limited knowledge about the subject but the ES supplies a part of an expert's decision-making knowledge through knowledge capture, storage, and dissemination. An expert system basically consists of a knowledge base and a capability to inference, which is provided by "interactive" communication between a user and the ES. By asking questions, making recommendations, following the Yes/No decision trees, and so on, the ES can play an important role in the OSINT knowledge-management system.

The Czech military should use outside expert systems intensively, as well as create a military intelligence expert system on its own. Especially in the times of crisis, or when the troops are deployed far from the direct intelligence support of the VZ, finding a specialist and communicating face-to-face can be hard to arrange. ES can assist commanders and staffs in the field to evaluate and interpret open-source information, help them recognize threats and trends, and support commanders' decisions.

Indeed, creating an OSINT expert system is not a trivial task. First, the VZS must capture and formalize the necessary OSINT knowledge to create a knowledge base. This part is many times the Achilles' heel, for the ES developers must choose a proper set of knowledge-engineering tools and techniques and also knowledge workers must carefully fill the knowledge base with data—which is difficult and time consuming. Then, when the knowledge base is ready and the expert system is operational, future refinements are likely as the ES further develops. The expert system can serve, in the long-term, as an overlay interacting with the knowledge repositories that will be created in the short-term, looking for the relevant knowledge, and using it as a part of the ES decision support process (Oxendine 2000).

Figure 12 illustrates the incorporation of IT tools, and the way the IT infrastructure can help facilitate knowledge flow in the OSINT system. One should not perceive the four IT means outlined above as "either-or" options. All the means are applicable to the OSINT knowledge-management system in the Czech military—but the means differ in their sophistication and complexity, budgetary demands, and implementation time.

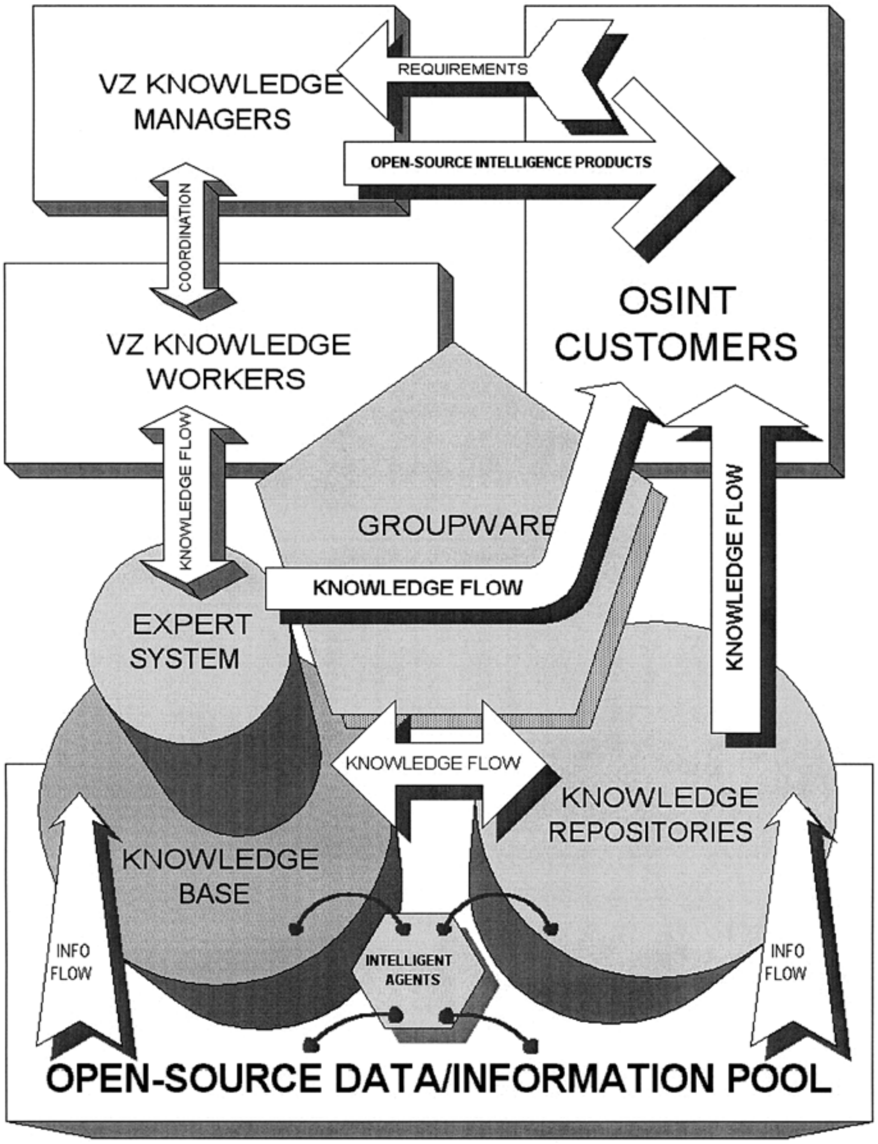


Figure 12. OSINT Knowledge Flow and IT infrastructure

2. Organization of the OSINT Knowledge-Management System

Jansen's contingency model, introduced in Chapter III, helped define the current organizational design of the VZS as a mixture of two types—division into business functions, and division into domains. The extant organizational design and IT does not reflect the characteristics of the modern open-source environment, which is perceived as highly complex and highly variable. In such an environment, the knowledge of each element of the organization is no longer sufficient to manage this knowledge. In order to manage this knowledge, the VZS should organize its OSINT structure to allow interpreting implicit knowledge, as well as to link old knowledge with new knowledge, thus creating new knowledge again. This is called *combined capacity* (Jansen et al 2000). The VZS should build mechanisms, such as knowledge repositories and groupware, to bond the compiled knowledge and to provide for its distribution and reuse.

Building upon the Jansen's contingency model, one can see that the VZS organizational design should migrate toward creation knowledge through increased combined capacity of OSINT units, as depicted in *Figure 13*.

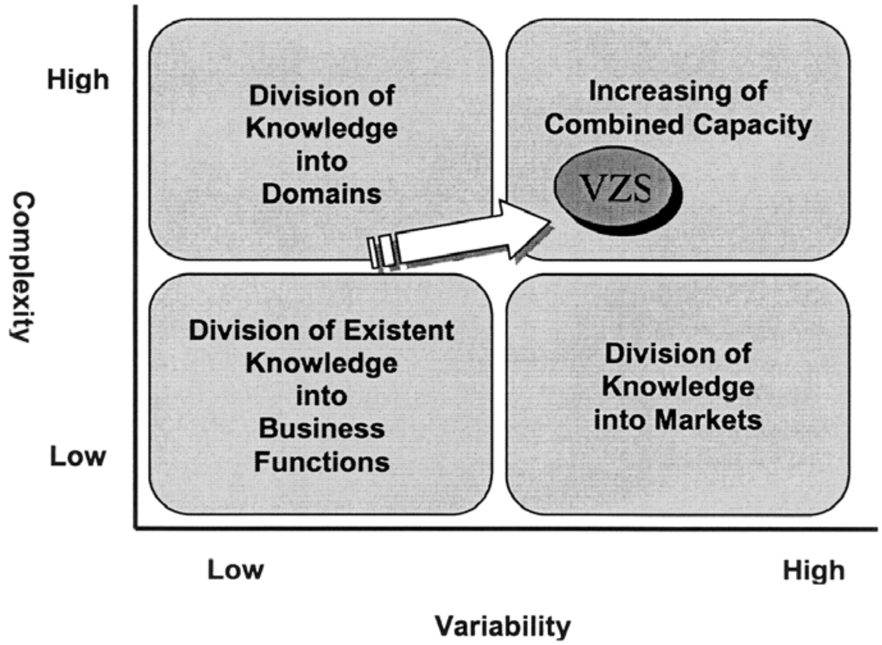

High
Low
Complexity
Division of Knowledge into Domains
Increasing of Combined Capacity
VZS
Division of Existent Knowledge into Business Functions
Division of Knowledge into Markets
Low
High
Variability

Figure 13. Four Strategies for Knowledge Management and the Future VZS

The increase of combined capacity is the only way to create new knowledge out of existent knowledge (Jansen et al 2000). If the military intelligence wants to maximize the combined capacity in OSINT, it must explore new forms of work, minimize rules and procedures for OSINT, and allow the highest possible degree of freedom for OSINT knowledge workers.

The new organizational design of the VZS and its information and communication technology should reflect the characteristics summarized in *Table 2*.

Organizational Type	Organizational Design	IT and Communication
Increase of Combined Capacity	• Organizing in Projects • Little Control, Much Freedom • Virtual Organizational Structure	• Informal System Focused on Knowledge Creation • Intranet/Internet, Intelligent Agents/Search Engines, Groupware, Expert Systems

Table 2. Characteristics of the Future Organizational Design and IT in the VZS

The new OSINT knowledge management system does not need to dispose of old practices—as long as the practices sustain continuous reexamination and prove to be the best practices. Similarly, not everything that is newly created represents a better alternative to the knowledge already existing. Hence the VZS should build its OSINT knowledge-management system to balances efficiency—by propagating and disseminating extant knowledge—and flexibility— by creating and renewing knowledge.

Virtual OSINT Organization: As mentioned in the previous chapter, the current organizational structure resembles a traditional vertically oriented control with accentuated bottom-up knowledge flow while the daily life requires the VZS personnel to collaborate in the horizontal direction. OSINT—in comparison with other "INTs"—is much less limited than typical secret intelligence activities; OSINT managers can certainly be pioneers in exploring new controlling strategies and in creating a modern OSINT structure.

One way to "organize" OSINT is not to organize it at all—at least in the traditional meaning. A concept of a virtual OSINT organization is very broad and is probably more limited by the people's will to accept such a notion than by extant IT means. A virtual OSINT organization can be a network of independent elements—OSINT units in the VZS, individuals and groups inside the Czech military, experts in academia, and so on—linked by IT to create, share, and distribute OSINT knowledge, as well as to share costs that are related to it. IT plays a central role in developing such virtual organization (Byrne 1993). A knowledge base in a virtual organization is widely distributed and this wide knowledge spread can enormously benefit all members of the virtual organization. The virtual model probably represents the highest flexibility in terms of timelines, responsiveness, and exploiting knowledge. Unlike the fixed organizational structure, such a broad virtual organization can easily modify its structure once the specific opportunity has been exploited or once the given task has been solved. Ideally, each element of the virtual OSINT "corporation" will cooperate in accordance with its core competencies. The partnership among the different elements will last as long as it is beneficial for the cooperating partners (Dees et al 1995). The whole structure will concurrently work on various issues through computer networks in real time.

Figure 14 illustrates a simplified vision of the virtual nation-wide OSINT organization. The main emphasis of the virtual organization is to complement and share resources in order to increase effectiveness and to lower costs. For small organizations or for organizations with severely limited resources—such as the Czech military—the virtual concept enables OSINT knowledge workers to join other organizations and to work on a much larger scale. In its maximal variant, the military, the police, academic researchers, intelligence services, other governmental bodies, and so on can create a nation-wide OSINT corporation that will be highly competitive internationally. The VZS does not need to be a dominant element of such nation-wide OSINT network—but it can certainly be the leader and the core of the OSINT network in the Czech military.

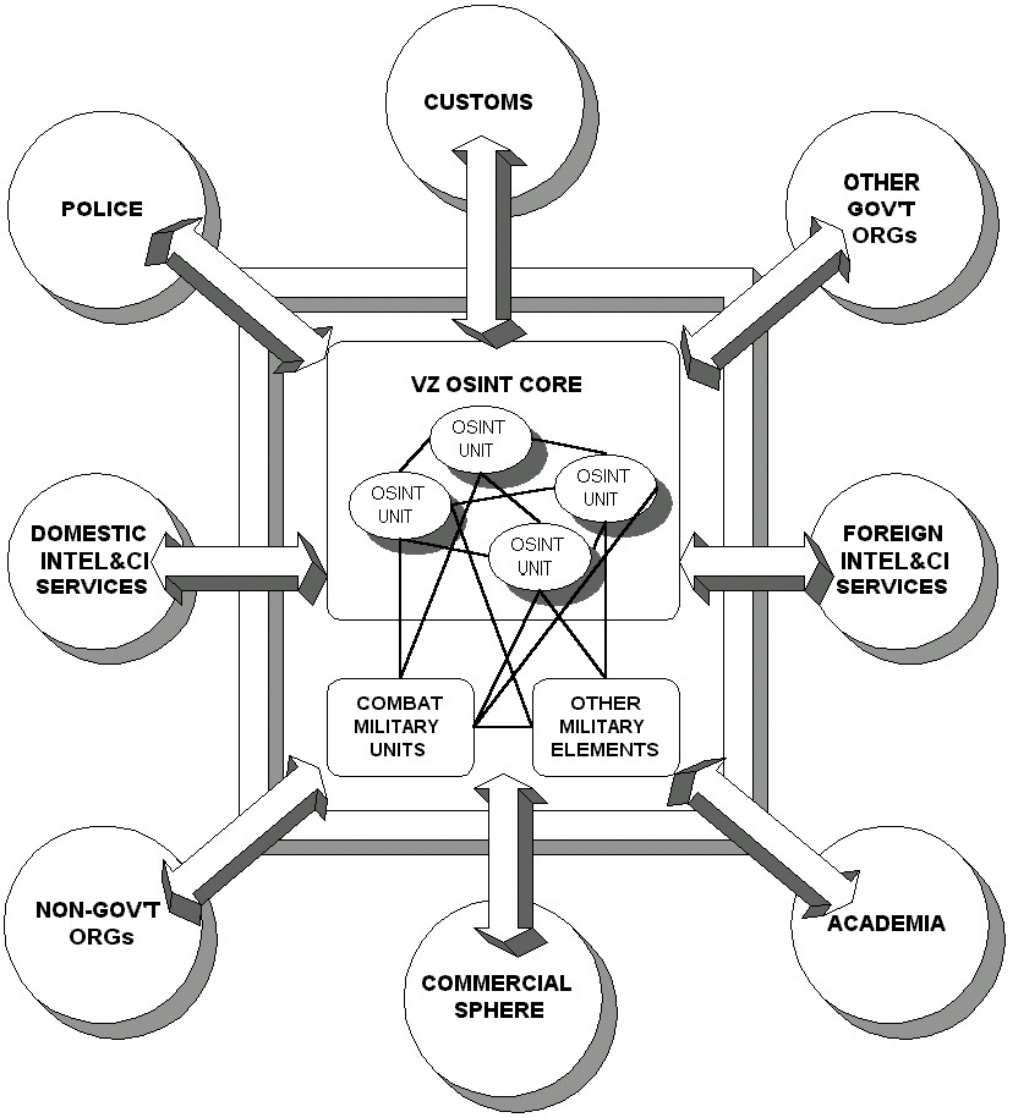


Figure 14. Virtual OSINT Organization

V. CONCLUSIONS AND RECOMMENDATIONS

This chapter summarizes the main points of the previous chapters. The first section of this chapter stresses the significance of system approach and summarizes the main steps that the VZS management should take. The second section underlines the multifunctional and cross-organizational nature of OSINT and the importance of a virtual OSINT network. The last section offers possible directions for further research and development.

A. SIGNIFICANCE OF SYSTEM APPROACH

Intelligence agencies are traditionally very conservative organizations. The Military Intelligence Service (VZS) management, as well as some of the knowledge workers may perceive changes to OSINT as a threat to the VZS and/or to themselves. Yet, improvements in the OSINT gathering and processing are not a threat to intelligence— reforms can ensure that a modern future for the Czech military intelligence exists. The Czech military intelligence should welcome all the advantages of modern open-source environment, which plays a highly important role in today's intelligence.

Today, as many individual organizations perform distinct intelligence tasks supporting an overlapping set of customers, deciding what an intelligence agency needs to collect is becoming more complicated. This is particularly true with OSINT, which is also influenced by the fact that Czech intelligence services now compete for resources. When using OSINT effectively, the military intelligence can respond to diverse crises efficiently and can also better allocate its severely limited resources into other areas of intelligence collection, when expensive covert means are unavoidable.

If the VZS wants to improve its OSINT, a systematic approach to the open-source domain is needed. As shown in this thesis, the VZS can design a modern OSINT for the Czech military by adopting knowledge management theory. The key point is that those who will devise the future OSINT knowledge-management system should systematically follow the four stages of the knowledge system and process design—process analysis, knowledge analysis, contextual analysis, and systems analysis and integration. Systematically applying the knowledge system and process design will help achieve the objectives and strategies of the VZS, and pinpoint the knowledge required so that the organization can reach its objectives.

One must realize that the knowledge management system must be designed *after* the nature of knowledge itself is analyzed. Then, the knowledge within the VZS can be identified, captured, organized, formalized, and distributed throughout the organization. The VZS must develop knowledge maps to identify who possesses what kind of knowledge, both inside and outside its organizational structure. Moreover, the VZS must carefully survey its organizational design, focusing on controlling strategies and the information-flow configurations. Finally, the OSINT knowledge management designers must study each of the six phases of the knowledge management life cycle (KMLC) in terms of extant procedures and practices within the organization.

The VZS should gradually build a comprehensive knowledge management system by creating a virtual OSINT network, consisting of experts online, expert software systems, intelligent software agents, and so on, to make open-source knowledge available to the VZS employees and customers. Future OSINT network must support creativity, content-rich communication, and effective knowledge sharing.

A systematic approach will certainly require much effort and time, but the VZS will not be able to manage OSINT knowledge properly without this effort and without a long-term commitment. The systematic approach will identify existing open-source knowledge and capture it. It will also help find possible overlaps or inefficiencies in the existing or future OSINT knowledge-management system. This approach presupposes not only comprehensive knowledge about an adversary but also the ability to update this knowledge continually so that the military intelligence can react quickly to a changing situation. We have to move toward "situational awareness," which will depend on advanced information processing technologies, such as artificial intelligence, in order to fuse large quantities of open-source information into an accurate, real-time intelligence. Hence, OSINT must serve as a wide base for the other intelligence disciplines.

It must not be forgotten that the entire knowledge management effort will just be rhetoric without a management commitment. Knowledge management champions among the top leaders must envision how the OSINT will be managed, pursue the vision, and share it with others. OSINT managers and knowledge workers must believe that a modern knowledge-management system is the proper way to conduct OSINT, and that it is worth their effort. Such conviction is not implied—people must create it.

B. ORGANIZATIONAL ISSUES

Every intelligence organization should serve not only the highest levels of government but also the subordinate levels, where actions are taken on a day-to-day basis. Several intelligence studies, made by research organizations and governmental bodies (e.g. Gannon 2000/1, IC21 2000, Nissen 2001), showed that a major key to improving the intelligence community in the information age is the concept of "corporateness." That means, the VZS should function and behave as a part of a more closely integrated entity working toward a highly defined goal: the delivery of timely intelligence to various military and civilian decision makers.

The Czech intelligence community needs to manage knowledge smarter, finding new ways to do more with less. Rapid technological advances in knowledge management may offer new possibilities and advantages. The intelligence community should not ignore these advances—just as terrorists, proliferators, smugglers, information warriors, and other potential adversaries capitalize on such advances.

Owing to the information explosion, single analysts and analyst cells are not able to process all the available open-source information anymore. A robust OSINT knowledge-management system can save much time and resources, reducing unnecessary intelligence requests. The VZS must find ways to create and to maintain a virtual network of information sources, collectors, exploiters, analysts and customers, as appropriate, and maximize the productivity and responsiveness of individual analysts. The future OSINT organization should effectively and economically share resources.

OSINT is an intelligence discipline that allows the VZS to become a virtual, project-oriented enterprise. The VZS can adopt an organic, as opposed to a mechanistic structure—a form that does not have closely defined tasks. A rather loose organizational structure that emphasizes teamwork, all-directional communication, and widely dispersed knowledge can provide a desired environment for the future OSINT knowledge workers.

The VZS should not struggle to divide the OSINT elements into strategic and tactic levels, trying to follow the traditional military hierarchy. Once the OSINT elements are connected through electronic networks, all organizational levels de facto disappear, and the OSINT units work as parts of one large virtual corporation.

IT infrastructure will play an important part in the future OSINT system. The future IT structure should guarantee automated electronic document storage, retrieval, and exchange. Internal knowledge must be stored in the electronic knowledge repositories, and these repositories must be available through electronic networks. Groupware technology must facilitate the capture and the exchange of knowledge. Intelligent agents should be used to interact with open-source databases. A nation-wide electronic discussion system should provide access to experts outside the military. In the long term, the VZS should create a military intelligence expert system, which will be available to the military units, especially when they are deployed during a crisis or in humanitarian relief.

C. RECOMMENDATIONS FOR FURTHER RESEARCH AND DEVELOPMENT

This thesis establishes a base for the Czech military to employ modern knowledge-management theory and to build a future OSINT system. Further research and internal analyses are necessary to design the OSINT knowledge-management system. Moreover, as the knowledge process and system design is applicable to other intelligence disciplines as well, the VZS may want to analyze the other "INTs" in similar manner as the OSINT system.

First, the VZS may need a comprehensive study of its own tasks and capabilities to identify what knowledge is vital in order to assess performance in the VZS. After the study, each of the critical success factors (CSFs) should be evaluated as a single-target process. Then, the existing OSINT system must be evaluated in terms of process pathologies to determine how well the existing process meets the desired goals. Such a diagnosis will help eliminate the pathologies from the process. Also, the VZS should study how its employees utilize different methods of communication; here the assistance of human-resource professionals may be particularly useful.

Once the designers analyze each process in the extant OSINT system and design the future knowledge-management process, the VZS must reconsider its IT infrastructure. IT specialists must conduct thorough studies of commercially available IT tools and then select appropriate COTS hardware and software. The VZS should consider using intelligent agents and determine their applicability to the Czech military OSINT. All of this is certainly a complex task—random and rushed implementations of "IT solutions" into existing processes cannot work in both the civilian and military organizations.

Finally, the VZS must determine the future organizational structure of OSINT elements—yes, this is the last step, not the first one. The OSINT system designers must recognize the benefits and disadvantages of different bases, and then combine the best of all the alternatives to create the future organizational structure of the OSINT knowledge-management system.

Closing Thought: People, not machines, are the key element of the intelligence community. All of the collection capabilities would be meaningless without dedicated and well-educated people who know how to manage knowledge and how to use modern IT tools. The knowledge of many experts in the intelligence community who claim to know something about computers, software, and technology in general is still low. Few military employees have the insight to recognize adequate and inadequate computer technology. Although many employees have become more “tech-savvy” during the last ten years, continuous education and training is needed to move ahead, toward the world of open sources.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES AND WORKS CITED

Adams, J. (1998): *The Next World War*. Simon&Schuster, New York, 1998.

Allied Joint Publication No. 2.0 [AJP-2.0.] (2001): *Allied Joint Intelligence, Counterintelligence and Security Doctrine*. 2nd ratification draft. Military Agency for Standardization, Intelligence Working Group (MAS/INTWG), NATO HQ, Brussels, 2001.

Analysis of Required Capabilities, Target Structure and Composition of the Armed Forces of the Czech Republic (2001). Center for Preparation of the Armed Forces Reform, Prague, CZ, 2001. (Online) http://www.army.cz/reforma/english/dokument.htm.

Arquilla, J. and Ronfeldt, D. (eds., 2001): *Network and Netwars*: *The Future of Terror, Crime, and Militancy*. Santa Monica, CA, 2001.

Bok, S. (1983): *Military Secrets*. in: Derth, D.G. and Gooden, R.T. (eds., 1995): *Strategic Intelligence*: *Theory and Application*. DIA/JMITC, Washington, D.C. Second edition, 1995.

Buchanan, B.G. (2001): *Creativity at the Metalevel*. AAAI-2000 Presidential Address. AI Magazine, Fall 2001.

Burns, T. and Stalker, G.M. (1961): *The Management of Innovation*. Tavistock Institute, London, 1961.

Butler, R. (1991): *Designing Organizations*: *A Decision-Making Perspective*. Routledge, London, 1991.

Byrne, J.A. (1993): *The Virtual Corporation*. Business Week. February 8, 1993.

Clarke, R. (2001/1): *Fundamentals of Information Systems*. (Online) http://www.anu.edu.au/people/Roger.Clarke/SOS/ISFundas.html.

Clarke, R. (2001/2): *Knowledge*. (Online) http://www.anu.edu.au/people/Roger.Clarke/SOS/Know.html.

Coleman, D. (1999): *Groupware: Collaboration and Knowledge Sharing*. in: Liebowitz, J. (ed., 1999): *Knowledge Management Handbook*. CRC Press, Washington, D.C., 1999.

Cooper, J.R. (1997): *The Emerging Infosphere*. McLean: Science Applications International Co., Virginia, 1997.

CRS Report for Congress (2001): *Terrorism*: *Near Eastern Groups and State Sponsors, 2001*. Congressional Research Service, The Library of Congress, USA, 2001.

Davenport, T.H. (1995): *Business Process Reengineering*: *Where It's Been, Where It's Going,* in Grover, V. and Kettinger, W.: *Business Process Change*: *Reengineering Concepts, Methods, Technologies.* Idea Group Publishing, Hershey, PA, 1995.

Davenport, T.H., DeLong D.W., and Beers, M.C. (1998): *Successful Knowledge Management Projects*. Sloan Management Review, Winter 1998, in: Oxendine, E. and Nissen, M.E. (2001): *Knowledge Process and System Design for the Carrier Battle Group*. Knowledge and Innovation: Journal of the Knowledge Management Consortium International. Vol. 1, No. 3, April 15, 2001.

Davenport, T.H. and Prusak, L. (1998): *Working Knowledge: How Organizations Manage What They Know.* Harvard Business School Press, Boston, MA, 1998.

Dees, G.G., Rasheed, A.M.A., McLaughlin, K.J., Priem, R.L. (1995): *The New Corporate Architecture*. The Academy of Management Executive. Vol. 9, 1995.

Defense Science Board – DSB (1996): *Improved Application of Intelligence to the Battlefield.* A DSB Study, May-July 1996. (Online) http://www.fas.org/irp/program/dsb_battlefield_rep.htm.

Denning, D.E. (1999): *Information Warfare and Security*. ACM Press, New York, NY, 1999.

Drucker, P.F. (1995): *Managing in a Time of Great Change*. Truman Talley, New York, 1995.

Federation of American Scientists [FAS] (1996): *The Intelligence Cycle*. 1996. (Online) http://www.fas.org/irp/cia/product/factell/intelcycle.htm.

Federation of American Scientists [FAS] (2002): *Nuclear Forces Guide*. (Online) http://www.fas.org/nuke/guide/index.html.

Galbraith, J.R. and Kazanijan, R.K. (1986): *Strategy Implementation*: *Structure, Systems and Processes*. 2nd ed., West, St. Paul, MN, 1986.

Gannon, J.C. (2000/1): *Analytical Uses of Collaboration*. 2000. (Online) http://www.cryptome.org./cia_auc.htm.

Gannon, J.C. (2000/2): *Intelligence Challenges Trough 2015.* (Online) http://www.odci.gov/cia/public_affairs/speeches/gannon_speech_05022000.html.

Gartner Group (1998): *Knowledge Management Scenario*. Conference presentation, 1998.

Grant, R.M. (2002): *Contemporary Strategy Analysis*. 4th ed., Blackwell, Malden, MA, 2002

Grossman, M. (2002): *Seven Themes that Shape our World*. U.S. Department of State, International Information Programs, March 1, 2002. (Online) http://usinfo.state.gov/topical/pol/nato/02032705.htm.

Grudin, J. (1996): *Evaluating Opportunities for Design Capture*. in: T. P. Moran and J. M. Carroll (Eds.): *Design Rationale: Concepts, Techniques and Use*. Lawrence Erlbaum Associates, Mahwah, NJ, 1996.

Hořejší, T. (1997): *Bezpečnost státu*: *Pozdní procitnutí*. (State Security: Late Awakening) Týden (Week), No. 50, December 8, 1997. in: Williams, K., Deletant, D. (2001): *Security Intelligence Services in New Democracies. The Czech Republic, Slovakia and Romania,* p. 83. Palgrave, New York, N.Y., 2001.

Hutchins, E. (1991): *Organizing Work by Adaptation*. Organization Science 2(1), 1991.

IC21: *The Intelligence Community in the 21st Century*. (2000) Permanent Select Committee On Intelligence, House of Representatives. Staff study. U.S. Government Printing Office, 2000. (Online) http://frwebgate5.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=667669372

Jane's Intelligence Review (2000): *Managing Information Overload*. March, 2000. (Online) http://jir.janes.com.

Jansen, W., Steenbakkers, G.C.A., and Jägers, H.P.M. (2000): *Knowledge Management and Organization Design*. in: Malhotra, Y. (ed., 2000): *Knowledge Management and Virtual Organizations*. Idea Group Publishing, Hershey, PA, 2000.

Johnson, S.E. and Libicki, M. C. (1996): *Dominant Battlespace Knowledge.* National Defense University Press, Washington D.C., 1996.

Joint Staff Publication No. 1-02 [JP-1.02.] (1994): *Department of Defense Dictionary of Military and Associated Terms*. in: US Federal Standard 1037-C: *Telecommunications: Glossary of Telecommunication Terms*. 2000 (Online) http://www.its.bldrdoc.gov/fs-1037/dir-010/_1401.htm.

Lave, J. (1988): *Cognition in Practice: Mind, Mathematics, and Culture in Everyday Life*. Cambridge University Press, 1988.

Lave, J. and Wenger, E. (1990): *Situated Learning: Legitimate Peripheral Participation*. Cambridge University Press, 1990.

Lefebvre, S. (1995): *The Army of the Czech Republic: A Status Report.* Journal of Slavic Military Studies, Vol. 8, Is. 4., December 1995.

Levitt, B. and March, J. (1988). *Organizational Learning*. Annual Review of Sociology, pp. 319-340, Vol. 14, 1988.

Liebowitz, J. (ed., 1999): *Knowledge Management Handbook*. CRC Press, Washington, D.C., 1999.

Lowenthal, M.M. (2000): *Intelligence*. *From Secrets to Policy.* CQ Press, Washington, D.C., 2000.

Malhotra, Y. (2000): K*nowledge Management and New Organizational Forms*: *A Framework for Business Model Innovation*. in: Malhotra, Y. (ed., 2000): *Knowledge Management and Virtual Organizations*. Idea Group Publishing, Hershey, PA, 2000.

Marenches, A. and Andelman, D.A.(1992): *The Fourth World War: Diplomacy and Espionage in the Age of Terrorism*. New York: William Morrow, 1992

Martin, F.T. (1998): *Top Secret Intranet*. Prentice Hall, Upper Saddle River, NJ, 1998.

Michta, A.A. (ed., 1999): *America's New Allies. Poland, Hungary, and the Czech Republic in NATO*. University of Washington Press, Seattle and London, 1999.

Miller, J.H. (1995): *Information Warfare: Issues and Perspectives.* March, 1995. (Online) http://www.inss.com
Lefebvre, S.: *The Army of the Czech Republic: A Status Report.* Journal of Slavic Military Studies, Vol. 8, Is. 4., December 1995.

Nastoupil, R. (1999): *Current Czech Defense Policy.* Journal of Slavic Military Studies, Vol. 12, Is. 2., Jun 1999.

National Security Strategy (2001). (Online)
http://www.vlada.cz/1250/vrk/rady/brs/dokumbrs/strategie2001.pdf.

National Military Strategy (1999). (Online)
http://www.vlada.cz/1250/vrk/rady/brs/dokumbrs/rok99/vojenstr.il2.htm.

NATO Open Source Intelligence Handbook [NOSINTH] (2001). U.S Army, 2001.

Nissen, M.E., Kamel, M., Sengupta, K. (2000): *Integrated Analysis and Design of Knowledge Systems and Processes*. Information Resources Management Journal, January-March 2000.

Nissen, M. (2001): *Facilitating Naval Knowledge Flow*. Naval Postgraduate School, NPS-GSBPP-01-004, 2001.

Nonaka, I. (1994): *A Dynamic Theory of Organizational Knowledge Creation*. Organizational Science Magazine, May 1994.

O'Hanlon, M.E. (2000): *Technological Change and the Future of Warfare.* The Brookings Institution, Washington D.C., 2000.

O'Leary, D.E. (1998): *Enterprise Knowledge Management*. Computer Magazine, March 1998.

Open Source Intelligence Handbook [OSINTH] (1997). Proceedings of the 6th International Conference *Global Security and Global Competitiveness: Open Source Solutions*. Open Source Solutions Inc., 1997.

Owens, W.A. (2000): *Lifting the Fog of War*. Farrar, Straus and Giroux, New York, 2000.

Oxendine, E. (2000): *Knowledge Management Support to Network-Centric Warfare (NCW)*. Master Thesis, Naval Postgraduate School, September 2000.

Oxendine, E. and Nissen, M.E. (2001): *Knowledge Process and System Design for the Carrier Battle Group*. Knowledge and Innovation: Journal of the Knowledge Management Consortium International. Vol. 1, No. 3, April 15, 2001.

Reform of the Armed Forces of the Czech Republic: *Objectives and Principles* (2001). Center for Preparation of the Armed Forces Reform, Prague. (Online) http://www.army.cz/reforma/english/dokument.htm.

Ruggles, R. (1997): *Knowledge Management Tools*. Butterworth-Heinemann, Boston, MA, 1997.

SANANIM—Drug Information Server. 2002 (Online) http://www.sananim.cz/dis/index.htm.

Schwartau, W. (1996): *Information Warfare*. 2nd ed. Thunder's Mouth Press, New York, 1996.

Steele, R.D. (1993): *Theory and Practice of Intelligence in the Age of Information*. Open Source Solutions, Inc., 1993. (Online) http://www.oss.net.

Suchman, L. (1987): *Plans and Situated Actions: the Problem of Human-Machine Communication*. Cambridge University Press, 1987.

Tenet, G.J. (2000): *The Worldwide Threat in 2000*. Washington, D.C., 2000. (Online) http://www.cia.gov/cia/public_affairs/dci_speech_020200.html.

Ulrych, M.P. (1999): *Democratizing Communist Militaries: The Cases of the Czech Republic and Russian Armed Forces.* Ann Arbor: University of Michigan Press, 1999.

Wagner, J.A., Hollenbeck, J.R. (1998): *Organizational Behavior*. 3rd ed. Prentice Hall, Upper Saddle River, NJ, 1998

Weber, M. (1968): *Economy and Society*: *An Outline of Interpretive Sociology*. University of California Press, Berkeley, 1968.

Wiig, K.M. (1999): *Introducing Knowledge Management into the Enterprise*. in: Liebowitz, J. (ed., 1999): *Knowledge Management Handbook*. CRC Press, Washington, D.C., 1999.

Williams, K., Deletant, D. (2001): *Security Intelligence Services in New Democracies. The Czech Republic, Slovakia and Romania.* Palgrave, New York, N.Y., 2001.

Zákon o zpravodajských službách č. 153/1994Sb. (Intelligence Services Act No. 153, 1994)

Zpráva o situaci v oblasti veřejného pořádku a vnitřní bezpečnosti na území České Republiky v roce 2000. (Report on the internal security in the Czech Republic in 2000) Ministry of Interior, 2001. (Online) http://www.mvcr.cz/dokumenty/bezp_si00/2_11krim.html.

Zuboff, S. (1988): *In the Age of the Smart Machine*. Basic Books, 1988.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dr. Mark E. Nissen
   Naval Postgraduate School
   Monterey, California

4. Kenneth R. Dombroski
   Naval Postgraduate School
   Monterey, California

5. Ministry of Defense
   General Staff
   J-2, Chief
   Kafkova 19 P.O.B 238
   160 41 Prague, Czech Republic