

Journal of Competitive Intelligence and Management

Special Issue *on Country-Specific Competitive Intelligence*

Introduction

- Australian CI Practices: A Comparison
with the U.S. Babette Bensoussan and Edward
Densham [p. 1-9](#)
- Competitive Intelligence in Korea.
Kwangsoo Kim and Seungjin Kim [p. 10-25](#)
- Competitive Intelligence in Russia.
Alexander A. Ignatov [p. 26-44](#)
- Competitive Intelligence in Spain: a Situational
Appraisal. Joaquín Tena Millán and Alessandro
Comai [p. 45-55](#)
- Evolution of Competitive Intelligence in Sweden.
Hans Hedin [p. 56-75](#)
-

Journal of Competitive Intelligence and Management

The Journal of Competitive Intelligence and Management (JCI) is a quarterly, international, blind refereed journal edited under the auspices of the Society of Competitive Intelligence Professionals (SCIP). JCI is the premier voice of the Competitive Intelligence (CI) profession and the main venue for scholarly material covering all aspects of the CI and management field. Its primary aim is to further the development and professionalization of CI and to encourage greater understanding of the management of competition by publishing original, high quality, scholarly material in an easily readable format with an eye toward practical applications.

Co-Editors in Chief

Craig S. Fleisher (fleisher@uwindsor.ca)
University of Windsor, Canada

John E. Prescott (prescott@katz.pitt.edu)
University of Pittsburgh, USA

Associate Editors

Europe - Sheila Wright,
De Montfort University, UK

Africa and the Middle East - Wilma Viviers,
North-West University, South Africa

Editorial Board

Ahmad Badr, *De Montfort University, UK*

David Blenkhorn, *Wilfrid Laurier University, Canada*

Patrick Bryant, *University of Missouri, Kansas City, USA*

Jonathan Calof, *University of Ottawa, Canada*

Alessandro Comai, *ESADE, Spain*

Blaise Cronin, *Indiana University, USA*

Paul Dishman, *Brigham Young University, USA*

Pat Gibbons, *University College-Dublin, Ireland*

Ben Gilad, *Academy of CI, USA/Israel*

Christopher Hall, *Macquarie University, Australia*

Don Hopkins, *Temple University, USA*

William Hutchinson, *Edith Cowan University, Australia*

Per Jenster, *Copenhagen Business School, Denmark*

Kwangsoo Kim, *Konkuk University, Korea*

Paul Kinsinger, *Thunderbird University, USA*

Qihao Miao, *Shanghai Library, China*

Jerry Miller, *Simmons College, USA*

Cynthia Miree, *Oakland University, USA*

Susan Myburgh, *University of South Australia, Australia*

Juro Nakagawa, *Tokyo-Keizai University, Japan*

Edna Reid, *Nanyang Technology University, Singapore*

Helen Rothberg, *Marist College, USA*

Luiz Felipe Serpa, *Universidade Catolica de Brasilia,
Brazil*

Kathy Shelfer, *Drexel University, USA*

Yoshio Sugawara, *Nihon University, Japan*

Tom Tao, *Lehigh University, USA*

Joaquin Tena, *University of Pompeu Fabra, Spain*

Jim Underwood, *Dallas Baptist University, USA*

Conor Vibert, *Acadia University, Canada*

Competitive Intelligence in Russia

Alexander A. Ignatov

Senior Partner & President, Ignatov & Company Group

Executive Summary

This article provides unique insights and a comprehensive treatment of competitive intelligence in Russia. The historical development of Russian CI is traced back to the military and government intelligence tradition left behind by the Soviet legacy. This is followed by a discussion of modern trends that are replacing the Soviet legacy with a professional, advanced, high-tech and ethical CI community. Next, an analysis of the structure of Russian CI is presented with special emphasis on structural organization, services specialization, branch distribution and territorial distribution. Several robust models of the CI market in Russia are developed with a focus on:

- 1) salient financial and operational characteristics of various service clusters of the CI market in Russia, and
- 2) categorization of Russian industries based on their level of transparency and their level of CI development

The various methods of CI that are used today in Russia are then explored including data collection, interviewing and information analysis. This is followed with an insightful perspective on the personnel backgrounds of current members of the Russian CI community including ex - MI/GI professionals and the new breed

of business school graduates. The major issues facing CI in Russia - secrecy, transparency, concentration - are then presented. The article concludes with a summary of expected changes that will define the future of the CI industry in Russia.

Key Words

competitive intelligence, Commonwealth of Independent States, espionage, ethics, government intelligence, market models, military intelligence, USSR, reforms, Russia, Soviet

About the Author

Alexander A. Ignatov is a Senior Partner and President of Ignatov & Company Group - a group of competitive intelligence and market research companies providing world-class service for international clients since 1998, with special emphasis on the Russian and CIS economy. Ignatov & Company Group is a Member of the Global Intelligence Alliance.

Introduction

The Russian and Commonwealth of Independent States (CIS) markets are very attractive and potentially very lucrative for world business - but, at the same

time, they can be perceived as very unstable and even unintelligible for global investors. In order to make sense of it all, it is very important to possess deep understanding as well as factual information about Russia and the CIS countries, specifically related to their resources, people, authorities, culture, regions, and economies. In addition, it is often necessary to acquire information on competitors or customers from Russia or the CIS countries.

The ancient Chinese military theorist, Sun Tzu, wrote: "Know the enemy and yourself, and your victory will never be in danger. Know the ground and the weather, and your victory is certain," (Tzu, 1963). In the business parlance of the 21st century, this means that every successful executive must possess maximum information on her/his own business as well as on her/his competitors' business. Sun Tzu's words - "ground" and "weather" - are analogous to their current counterparts - "environment" and "weather" - respectively. The (1) *environment* of a company (2) as well as the significant trends in modern development, or *weather* in which it operates, provide an accurate glimpse of the true situation.

Providing outsiders with the information they need, accurately and rapidly, is the task of the dynamically developing CI industry in Russia. Currently the industry is earning moderate revenues but it is enjoying faster growth rates than most other industries. It cannot yet boast high employment but the industry does, indeed, unite the most informed people in the Russian business community.

In 1998 - when our company was starting its operation in competitive intelligence - I asked myself a question on how to define the key sense of this kind of activity. The answer has come from an unexpected source, as is often the case. I was re-reading Frank Herbert's *Dune*¹ saga that is an excellent manual for any person charged with responsibility and accountability - from managers to state leaders (in my opinion, this book contains good description of the aftereffect of adequate and inadequate usage of power). To wit, in one of the passages in *Dune* there is a pearl of wisdom that is especially apropos for this article - the growth of any system is limited by the factors that are in minimum or, in other words, the least congenial feature defines the rate of growth. So it became clear for me why many global businesspeople have lost their investments in Russia. Seemingly, they possessed many of the requirements for a successful

global investment business plan - money, experience, and new technologies. Relevant information about the local business environment in Russia and the CIS, however, was sorely lacking. This type of information had become the least developed part of foreign investment business plans in Russia and was a significant factor in many failed or underperforming international business investments in this region. Therefore, the role of competitive intelligence (CI) could be specified as a method of making information the instrument for stable business development. Just as military intelligence /government intelligence (MI/GI) played a stabilizing role for the whole country's development, so too CI currently plays a similar stabilizing role in the Russian business sphere. CI is rapidly becoming one of the most significant components of the modern Russian business infrastructure, perhaps equal in importance even to the financial area or securities markets. CI delivers the most valuable resource - information - and so offers business decision-makers the ability to manipulate both the direction and the rate of business development. Moreover, CI has become a separate industry serving a variety of modern Russian businesses. This position allows CI in Russia to be described in a similar manner to that of any other industry in the modern Russian economy.

General Overview

CI in Russia is firmly rooted in the military intelligence (MI)/government intelligence (GI) infrastructure that flourished in late period of the USSR. Modern Russian CI still has many blurred boundaries given these foundations. In terms of Western CI practice, Russian CI is often perceived incorrectly as redolent of economical espionage. Reinforcing these perceptions is the fact that almost all Russian CI professionals come from a background in the military, intelligence, or police community. Additionally, the educational and training system for Russian CI is provided only by the methods taught in the correspondent state-owned military and intelligence academies.

In spite of these facts, Russian CI is trying to shake off its Soviet legacy. Since 2000-2001, new, non-espionage, approaches to competitive intelligence are being developed among local practicing companies. New people are trying to enter the CI industry - in the last 2-3 years, graduates of business and economics schools have

slightly forced out the traditional contingent (former MI/GI officers) in intelligence divisions of Russian corporations. The proprietors and top-managers of the largest Russian companies are beginning to understand that CI is no longer a method of commercial espionage but, rather, the working instrument for decision-making. Comprehension of the necessity of ethical standards is beginning to persuade the incumbent MI/GI mindset.

History Of Russian CI

During the late USSR regime, all companies in the region were state-owned so their interests (including those in the intelligence area) were considered as the interests of the state and vice versa. In such a situation of full convergence of business and the government, competitive intelligence was only the part of governmental intelligence activity. The main goal of such activity in the business sphere was to provide competitive advantages for Soviet manufacturers and exporters by getting an access to the most advanced Western know-how, technology, and solutions. Individual companies did not have the right to have their own intelligence divisions. The Soviet state was so afraid of any kind of possible internal opposition that any kind of 'uncontrolled' intelligence was perceived as a potential challenge to the state's authority. Only governmental agencies could carry out the intelligence tasks both inside and outside the country.

A comprehensive treatment of Russian intelligence activity in the military and political sphere is beyond the scope of this article. However, a brief discussion regarding how such activity was organized in the economic/business sector provides unique insights into the development of Russian CI.

The Soviet government established significant and highly effective intelligence systems in their state-controlled economy (Kolpakidi & Prokhorov, 1999). The primary customer of this intelligence was the so-called 'military-industrial complex' that united all enterprises working in weaponry development and production. Towards the end of the 1970s, it became clear to the Soviet government that the country's economy - especially in hi-tech industries - began to lag the Western economies. Therefore, the gathering of competitive information about technologies and research programs was declared the key task of intelligence. Additionally,

the Soviet economy strongly depended on the prices of oil and other natural resources that were the country's main sources of currency inflow. Hence, securing competitive information on events that could influence the global prices of energy resources became the second important goal for state intelligence agencies.

All work in economical intelligence was coordinated by the Military-Industrial Commission (after Mikhail Gorbachev became the Soviet leader in 1985 this Commission received the status of the Major Commission of the military-industrial complex). This commission managed all activity in economic and technological intelligence. Companies that needed intelligence transferred their orders to the correspondent state ministries. For example, all enterprises involved in electronics manufacturing informed the Ministry of the Radio-Electronic Industry of the USSR about their intelligence needs. After gathering such orders, the ministries transferred the unified requests to the Major Commission of the military-industrial complex. This Commission developed annual intelligence plans and brought them up to the state intelligence agencies.

In the late USSR, the infamous KGB (Andrew & Gordievsky, 1991) and GRU were involved in competitive intelligence but several other agencies were also involved - the State Committee on Science and Technics, the State Committee on Foreign Trade Relations, the special division of the Soviet Academy of Sciences, and a few departments of the Soviet Ministry for Foreign Trade. This system was effectively solving intelligence needs until the fall of the USSR and new independent states started establishing in the early 1990s.²

The history of the Russian CI can be divided into three main periods. The first period began in 1991 when Russia became an autonomous state. The cardinal reform of the former KGB led by Boris Eltsin (who was afraid of any opposition to the secret service) resulted in the termination of hundreds of officers from the secret service, many of whom were then forced to search for their place in the new post communist society. Most of them found positions in private security services and competitive intelligence. Because most companies remained state-owned, it was not a big problem for former KGB personnel to 'infiltrate' such enterprise as well as newly established private companies. The force of the Soviet period influenced intelligence activity in all aspects of Russian economy. This all-pervasive

impact of the state greatly diminished in the mid 1990s, however, when most non-defense enterprises in Russia were privatized.

The second period in the development of Russian CI started in 1994-1995 when owners of newly privatized companies began to establish their own intelligence systems independent from the state agencies. Despite having enough financial resources to establish private intelligence systems, these companies were still dependent on employing the 'old staff' - former Soviet intelligence and military officers - who brought the spirit and methods of the Soviet intelligence with them to these companies. As a result, the Soviet legacy stubbornly defined the face of the Russian CI at this stage of development. It was a period of corporate conflicts, murders, blackmailing, and racketeering. Corporate security divisions were strongly involved in these semi-criminal activities (Waller & Yasmann, 1995). Operations such as data gathering from open sources or in-depth CI analysis were not widespread because economic espionage was the main method of solving problems. To our common shame, many persons who currently consider themselves as 'CI professionals' were actively participating in those operations that labeled late 20th century Russia as 'wild capitalism country'.

Another development in this period was the split of CI into two segments. The first segment of Russian CI has continued to provide services to state-owned companies working in the defense industry (Conflict Studies Research Center, the Defense Academy of the United Kingdom, 2000). The second segment of Russian CI, however, has fully reoriented itself around the needs of private companies. The first segment is comprised of state intelligence agencies and the second segment is comprised of corporate security services and independent CI and market research agencies. This article will focus only on this second category of CI institutions in Russia.

The third period in the development of Russian CI - one that is continuing today - started in 1999-2000 when it became clear that Russia could very well become the derelict of the global business community because of its criminal methods of activity. Such comprehension has influenced a national reappraisal of the ethics of traditional Russian CI and, as a result, new trends have started to penetrate competitive intelligence in this nation (Alexandrova, 2001). Increasingly, there is

a diversity of influence defining modern CI in Russia - from the traditional constituency of former KGB officers (with their espionage methods) to new stakeholders such as modern, well-educated young people (with analytical approaches). This new stakeholder group is beginning to shape CI policy in Russia and will be a positive force for change in overcoming the negative aspects of the Soviet legacy as well as the shameful pages of the post communism chaos in the 1990s. The Russian CI community is well on its way to becoming a modern, hi-tech industry with strong ethical standards.

Modern Structure Of Russian CI

There are four main levels of organization that describe modern Russian CI:

1. Structural organization
2. Services specialization
3. Branch distribution
4. Territorial distribution

All these levels are closely connected, making CI one of the fastest developing industries in Russia.

Structural Organization

From the point of view of its structural organization, modern Russian CI is represented by corporate security services and independent CI agencies. The first corporate divisions responsible for CI activity were organized by the largest oil companies and banks in 1993-1995. Many former officers from KGB became the personnel of such divisions. Other officers preferred to establish their own 'consulting' agencies providing economic espionage to those who could afford their high priced services.

Most, if not all, large Russian companies have their internal security divisions. At least 12-15% of them have special CI sub-divisions inside security departments and only 4-5% have autonomous CI departments. Additionally, most large corporations have analytical departments whose personnel are involved in separate CI operations from time to time (Ignatov & Company, 2004a).³

Using a 6 level model (Ignatov & Company, 2004b) of CI maturity (absent, initial, regular, formalized, controlled and optimal levels), the largest Russian

corporations would be described as having a 'formalized' level of CI-development (*the author and the company at which he is working are using this 6-level model by analogy with the model of IT maturity provided by CobiT⁴*).

For mid-sized companies, the level of CI development strongly depends upon two factors - type of industry and region of location. In general, all mid-sized companies working in mining and metallurgy (i.e. in export-oriented branches of industry), as well as companies situated in Moscow (and another 12 cities with population more than 1 million people) have 'regular' or even 'formalized' levels of CI-development. Some mid-sized companies have reached only the 'initial' level of CI development. However, many of them are still at the 'absent' level of CI development with no CI capabilities in form or function. The same 'absent' level of business development also describes the level of maturity of CI in the small business sector.

CI in Russia is considered the key part of a more general kind of activity, the so-called 'economic security' that covers CI, corporate counterintelligence, and a few aspects of human resources management. For this reason, CI often becomes the responsibility of corporate departments responsible for 'economic security'. Only a few of the largest companies (closely connected with export trade) have separate CI divisions in their structure.

The federal law on private detective and security activity in Russia gives corporations the right to establish corporate 'security-detective divisions'. Accordingly, under clause 3 of this law, security divisions may "research markets, collect data for negotiations, reveal insolvent or unreliable business partners, and clarify biographical data of employees." It becomes almost immediately apparent to the CI savvy reader that the list of the allowed kinds of "data search" activity is not comprehensive. However, in spite of this fact, Russian CI professionals have learned to make a wider set of intelligence operations available by 'hiding' them under these legal definitions (Mirzoev, 2004).

Corporate security divisions are not allowed to provide CI services to external customers. This provides business opportunities for autonomous competitive intelligence agencies. Almost 2/3 of all autonomous CI companies prefer to work under the banner of a private detective or security agency (Interiors Ministry of Russia, 2003; 2004). Such status gives them possibility to use special

technical devices (teargas, rubber cudgels, etc.) as well as weapons. The federal law on private detective and security activity in Russia regulates such agencies' activity. Accordingly, under this law all agencies have to be licensed by the Ministry of Interiors; and all personnel of the agencies must have individual licenses. The Ministry of Interiors has established a difficult procedure of licensing that takes at least 6 months and costs few thousand USD per a licensed employee. Besides that, the Ministry of Interiors has official rights on continuous control over agencies' activity that includes possibility to enter the agencies' offices any time as well as to gain access to many of their documents.

Another 1/3 of CI professionals in Russia prefer to work under the legal status of CI or market research agencies. This status does not confer a right to use some technical devices but releases them from the importunate 'trusteeship' of the Ministry of Interiors. Currently, almost 100 companies in Russia declare that they are working in competitive intelligence and more than 1,500 companies name market researches as their key area of activity. Only 1/3 of these companies have a stable inflow of customers and the 50 largest agencies gain 75-80% of total revenues from CI activity (Interiors Ministry of Russia, 2003; 2004).

Services Specialization

All Russian participants of CI activity can be divided into classes according to their services specialization as follows:

- Corporate CI divisions and autonomous agencies that research domestic markets and companies
- Corporate CI divisions and autonomous agencies that research CIS markets and companies
- Corporate CI divisions and autonomous agencies that research non-CIS markets and companies
- Universal CI divisions and autonomous agencies that research both domestic and foreign markets and companies

The prevailing type of customers served provides another classification criterion:

- Corporate CI divisions that work only with their corporation
- Autonomous CI agencies that mainly work with domestic customers
- Autonomous CI agencies that mainly work with foreign customers

Accordingly, by using the two above classification criteria, several key clusters of CI activity that currently exist in Russia may be determined:

- *Corporate competitive intelligence* - activity of corporate CI divisions whose key goal is to provide correspondent corporations with primary data and analysis on their domestic and global competitors

- *Domestic markets for domestic customers* - CI services on research of Russian markets made by the Russian agencies for Russian customers
- *Foreign markets for domestic customers* - CI services on research of non-Russian markets made by the Russian agencies for Russian customers
- *Domestic markets for foreign customers* - CI services on research of Russian markets made by Russian agencies for the foreign customers

These CI clusters can be compared against a number of criteria such as number of operators, number of contracts, revenues, and rate of revenue growth as shown in Table 1. This article will present a preliminary model of the Russian CI market based on market research compiled in 2003 for a European provider of corporate knowledge management software and published in *The Evaluation of the Volume of the CI Market in Russia* (Ignatov & Company,

Table 1: Service Clusters in Modern Russian CI

CI Cluster:	Number of Operators:	Annual Number of Contracts for CI Services:	Annual Revenues:	Annual Rate of Growth:
Corporate CI	~3,000	~150,000	300 million USD	6-7% average; 10-12% in corporate TOP-100 segment
Domestic markets for domestic customers	~500	~25,000	50 million USD	6-7%
Foreign markets for domestic customers	<10	<100	2.5-3 million USD	34-37%
Domestic markets for foreign customers	~25	~1,000	4-4.5 million USD	Up to 100%

Source: Ignatov & Company, 2003

2003). Primary data was gathered by interviewing executives of corporate CI division and browsing the Russian segment of the World Wide Web.

Table 1 yields useful information for analysis of the current situation in the Russian CI community:

Russian corporations prefer to satisfy their CI requirements independently - via internal CI divisions (security or analytical departments). Such divisions investigate both domestic and global markets, gather primary data and analyze information, prepare reports and inform top-managers on various CI topics. The corporate CI cluster has to be considered as the largest segment that drives the entire CI market in Russia. All other clusters (except Domestic markets for foreign customers) can be defined as secondary and dependent on the corporate cluster. The future of this cluster is fully determined by the development of the correspondent corporations. It has the same rates of growth as that of the entire corporate sector.

Russian CI agencies earn their revenues mainly from contracts with domestic corporations. Sometimes Russian corporations hire independent CI agencies to do some work - mainly to research domestic markets or companies. The relative ratio of CI work made by corporate divisions and external agencies can be evaluated as 6:1. Foreign customers do not contribute significantly to Russian CI agencies' revenues. This market dynamic makes autonomous CI agencies highly dependent on the orders of Russian corporate customers. The growth rate of this cluster rivals that of the corporate cluster.

Russian corporations prefer to hire foreign CI consultants (especially global consulting companies) for non-CIS markets research. The market share of Russian CI agencies in the foreign market research sector is very low and can be ignored, but the cluster has a high rate of growth.

Few Russian agencies provide CI services and products to foreign customers. Currently this cluster holds a small share in the entire CI market but, due to the fact that this cluster enjoys the highest rates of growth, it has good possibilities to become the industry's key driver.

Other CI activities such as CI training centers or CI consulting for CI agencies are not currently offered in Russia.

Branch Distribution

The branch distribution of Russian CI companies has two main aspects. First, CI participants are represented irregularly in various branches of the economy. Corporations working in export-oriented industries have the highest level of CI development among all Russian companies. Stable revenues allow such corporations to establish and develop effective CI divisions. Russian oil companies as well as metallurgical holdings (Pechenkin, 2004) and major banks (Babkin, 2003) have strong CI divisions. These industries can be considered as the key drivers of the CI growth in Russia. By our estimation, oil and metallurgical corporations provide in total 65-70% of all CI activity. These corporations are the main customers of CI services both to their internal CI divisions and to external agencies.

Other export-oriented industries - such as timber-and-pulp, some sectors of machine-building and mining, as well as several domestic industries [telecom and fast moving consumer goods (FMCG)] stand in the middle of the list. Their CI divisions cannot be compared with the leaders by efficiency but, in any case, they have more resources at their disposal for CI than companies operating in other industries. The industries oriented towards the internal Russian market (light industry, machine-building, etc.) have the weakest level of CI development.

Another aspect of the branch distribution refers to the volume of industry-specific data available for collection and analysis by CI professionals. Such volume (as well as the data quality) directly depends on the level of the correspondent industry's transparency. It is easier to gather data referring to an industry (or companies working in such industry) that has a high level of transparency than to gather data in 'data-closed' sectors.

Currently, the following 'transparency' hierarchy exists in Russian industry (National Council on Corporate Governance, 2004b):

- *Industries with high level of transparency* - full availability of industry statistical data, participation of industry's companies in disclosure programs, relevant and full content in corporate websites. Currently, only the oil and gas industry can be included in this category, but since February, 2004 problems with state

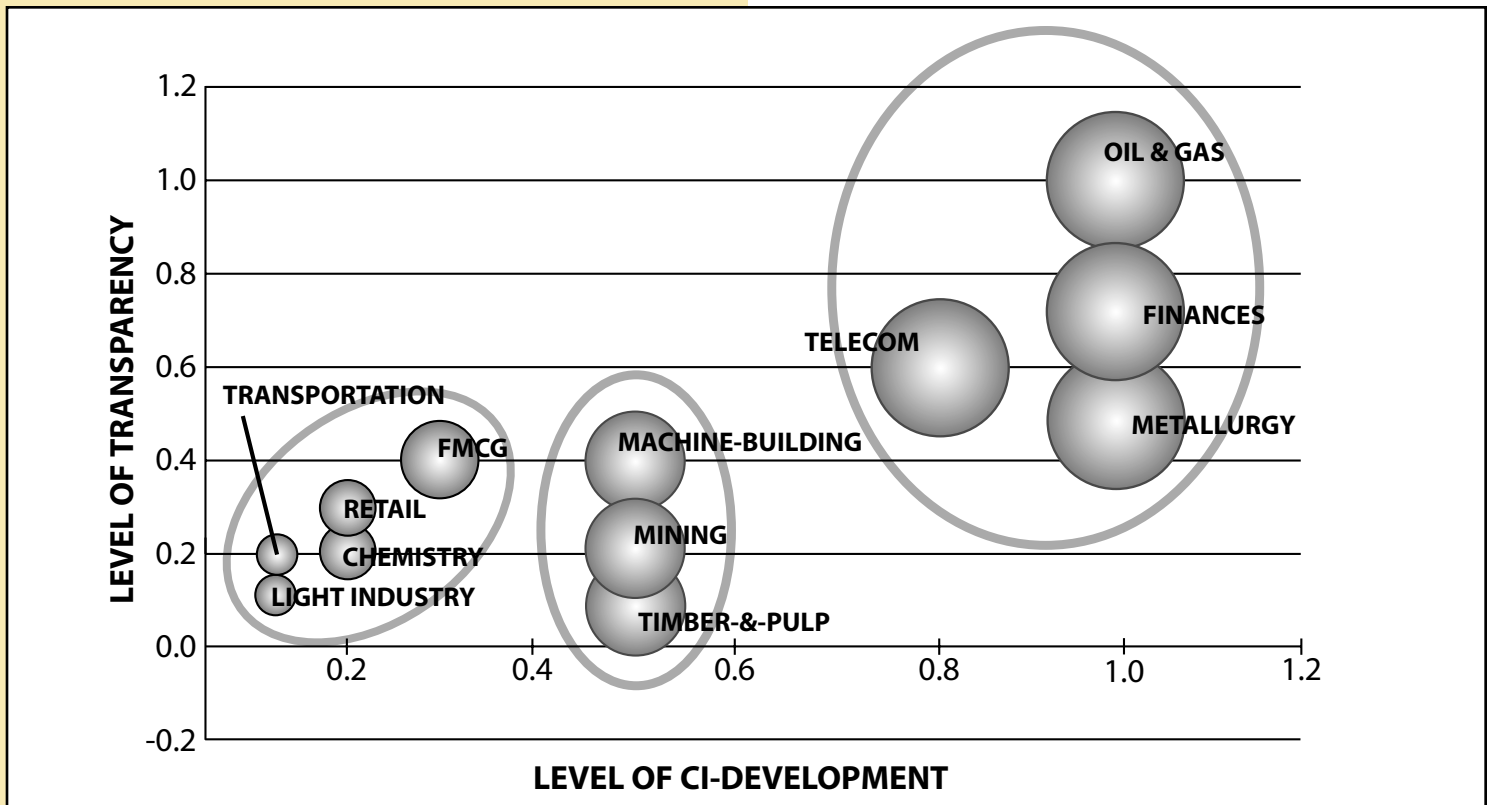


Figure 1: CI Branch Distribution

secrets exist in this industry as well, a topic that will be addressed later in this article.

- *Industries with moderate level of transparency* - partial availability of industry statistical data, only few companies participate in disclosure programs, corporate websites contain incomplete or partially irrelevant data. Ferrous and non-ferrous metallurgy (except noble metals segment), FMCG, financial sector (banking and insurance business), and the telecom industry can be included in this category.
- *Industries with low or absent transparency* - absent or irrelevant industry statistical data, industry's companies prefer not to disclose their corporate information, corporate websites are absent or contain only contact information. Currently, this category is the largest category of the Russian business - almost all companies working in mining, machine-building, timber-and-pulp, transportation, light industry, retail, chemistry, pharmaceuticals, and consumer-end services have the lowest level

of transparency.

Figure 1 provides a categorization of Russian industries based on their level of transparency and their level of CI development:

- Industries with a high level of CI development and high or moderate transparency (oil and gas, financial, metallurgy, telecom)
- Industries with a mid-level of CI development and moderate transparency (mining, timber-and-pulp, machine-building)
- Industries with a low level of CI-development and low transparency (chemistry, FMCG, light industry, transportation, retail)

The Figure 1 is the part of the market research compiled in *The Evaluation of the Volume of the CI Market in Russia* (Ignatov & Company, 2003). Primary data were gathered by interviewing executives of corporate CI division and browsing the Russian segment of the World Wide Web.

The level of transparency was determined according to classification of the National Council on Corporate Governance⁵.

Territorial Distribution

Almost 85% of all CI operators (both corporate divisions and autonomous agencies) are situated in Moscow (Interiors Ministry of Russia, 2004). This concentration of CI operators is determined by the fact that almost all of the largest Russian companies prefer to locate their headquarters in the Russian capital. For example, of the 11 largest oil companies only one company (Surgutneftegaz) has its headquarters outside Moscow. Even when a large company has official headquarters in some region of Russia, it owns a representative office in Moscow (and company's top-managers prefer to work here and not in regions).

Another 15% of CI operators are distributed by regions irregularly - at least 14.7% of them are situated in 12 largest cities with population more than 1 million people (Saint-Petersburg, Novosibirsk, Rostov-on-Don, Nizhniy Novgorod, Perm, Ekaterinburg, Kazan, etc.). Only 0.5% of the Russian CI industry is situated in other locations (Interiors Ministry of Russia, 2004).

CI Community in Russia

Currently, the CI community in Russia exists in a disconnected condition. Relations between CI professionals are of an incidental character and are based on personal contacts (especially if both parties had previously served in the same state agencies).

There are a few associations that act in the area of detective and security services but they refer mostly to the correspondent industries and do not take into account specific interests of CI. The main reason for such passivity is that modern Russian CI agencies and corporate divisions are self-sufficient. Their methods of work are based on the same experience required in their former occupations as MI/GI officers so they perceive a low need for any professional knowledge development or exchange. Given this current industry dynamic and the history behind it, it can be safely assumed that any CI associations will probably not be established earlier than 2005.

CI-related Sources in Russia

Currently, there are no nationwide (print) magazines or newspapers on the CI-related items in Russia. Few online sources exist that make it possible for the Russian CI professionals to discuss various problems of the industry, from which the most popular are the next:

- *Security and Safety Technologies*⁶ - the online forum on corporate security;
- *Business Intelligence and Information Management*⁷ - the online magazine on BI-related topics;
- *Oxpaha*⁸ - the online newspaper on corporate security

Methods of CI Work

The object of competitive intelligence activities is information. However, not just any kind of information can be integrated into competitive intelligence work. It is only information that can affect a company's plans, decisions, and operations that is the purview of competitive intelligence. We are inundated with information all around us. It is everywhere and sometimes it is difficult to assess the importance of the information with respect to corporate planning. This is one of the main goals of competitive intelligence - to separate useful information from informational garbage. However, at the same time, it is crucial not to lose some importance bits of knowledge in a mountain of useless data.

Data Collection

The primary goal of competitive intelligence is to gather information, but not any method of information gathering is useful in competitive intelligence. SCIP's definition of competitive intelligence stresses the word, 'ethical'. This means that, in contrast to espionage, competitive intelligence operates only on open sources of data/information. Open source is a military intelligence term referring to information in the public domain, such as news articles, corporate websites, and databases with unrestricted access.

Currently few primary intelligence sources are being used in the Russian CI community. Some of them can

be considered as legal and open sources, but others refer to semi-criminal or even criminal methods of data gathering (Chertoprud, 2003).

Online Open Sources

Based on experience with using various news/data sources in Russia and CIS, the following groups of online data sources are found to be the most useful and informative:

- Real-time news services (similar to Reuters)
- Multi-source and multi-format online databases (similar to LexisNexis)
- News digests prepared by analysts

Currently these three categories of sources are available in the Russian and CIS market, but there are some differences in their readiness for usage in daily CI operations.

Russia, Ukraine, Kazakhstan, and few other countries of the CIS and the Baltic region have national news agencies that provide local economic/political real-time news in native languages as well as in English. The most powerful agencies among them are the Russian ITAR-TASS⁹ (they consider themselves to be one of three leading world's news agencies), Interfax¹⁰ and RIAN ('Novosti' Agency)¹¹; they cover not only Russia, but also all of the other CIS countries and the Baltic region; they provide real-time news (via e-mail, websites, direct-push technologies) as well as an access to their news archives.

There are a few online databases that include text/graphics data from various online and offline sources. The main disadvantage of these systems is that most of the information is in Russian and/or a few other languages of the CIS countries and the online translation into English is absent or of low-quality. Currently, the most complete database (more than 5,000 sources from 12 countries with archived data from 1995-2004 related data) is the Russian database, Integrum Techno.¹²

A few agencies compile news digests on general or specific items. The digests can be done with or without translation into English. The main problems of these services - delays in delivery, low or middle-quality of translation, and irrelevant or preconceived sources of

primary data.

To summarize, the choice of correspondent online source depends on the customer's end use:

- Real-time but unprocessed news - subscription at news services is available
- Various text sources (via search strings) - subscription of databases services can be used
- Processed but not real-time news and analytics - subscription to news digests is the best method.

Databases

Various databases are among the main sources of primary data accessed by the Russian CI community but most of them offer illegal copies of official state databases. Currently, every interested person (who has enough money and knows where to look for suppliers) can purchase a wide set of databases containing:

- Registration data of Russian companies (currently various variants of registration databases are accessible - developed by Taxation Ministry, the State Committee on Statistics, etc.)
- Data on all export and import contracts with participation of the Russian companies (this database is developed by the State Custom Committee)
- Data on legal payrolls of Russian employees (this database is developed by the State Pension Fund; it also contains personal data of employees - like their home addresses, passport numbers, etc.)
- Data on personal and corporate phone numbers
- Data on cars' registration numbers and their owners
- Data on criminals and criminal activity (this database is developed by the Ministry of Interiors), etc.

All of these databases contain information that is considered to be confidential. In spite of the declared

measures on information protection, such databases are easily accessed by the public (CNews, 2003). Illegal trade in databases is not an uncommon type of criminal activity in Russia and its annual revenues exceed 5 million USD. The persons who are working in the correspondent state organizations represent the first link in this chain of criminal activity. Under the protection of some high-ranking officials, such employees (usually working in IT departments directly involved in database development) copy the entire databases from state-owned servers to some removable media. Then, such copies are transferred to wholesale intermediaries (usually they are partners of this criminal business along with the officials who patronize it). They copy databases onto CD-ROMs and sell them to the next level of participants - regional wholesalers. The retail traders who distribute CD-ROMs with databases to customers represent the final link at the end of this chain of criminal activity (Potresov, 2003).

So, it is possible now to get much confidential data from state databases - from home addresses of shareholders and top-managers to a list of their personal assets like realty or cars; from registration data of any company to information on its export contracts. A conservative estimate would assert that at least a half of all CI corporate divisions and almost 2/3 of all CI agencies use such illegal databases (Sharlot, 2002).

In spite of the fact that state authorities are developing databases, it is necessary to take into account the problem of their irrelevancy. The problem is not that correspondent state organizations are neglecting their responsibility for data gathering. Rather, the problem finds its roots in a recurring feature of business in Russia - almost 90% of all companies are registered by the home addresses and phones of their proprietors. However, many people register their businesses via addresses and phone numbers that were secured only for registration purposes. So, despite the fact that many of these addresses and phone numbers are legal, there is often no company located at listed addresses and/or phone numbers. In addition, many companies prefer to keep a low profile or even hide via unofficial transactions (not criminal, but without public reporting, etc.). By our calculations, almost 90% of the records in official databases do not refer the legitimate operating companies. As the result, it is necessary to undertake additional scrutiny to 'clean' the register of companies

to understand which companies are real, which ones are 'hidden', and which companies have been established for money laundering purposes.

There are a few CI agencies (and our company is among them) that prefer to use legal methods to secure access to state databases. The dearth of Russian laws in this area affords any person or company the right to purchase such information as the registration data of a specific company, etc. To accomplish this, it is necessary to fill out a special request form, to pay a legal fee to the correspondent state authority, and then search the desired information. For example, today everyone can retrieve the registration data of any Russian company for only 40 USD. It will take up to 5 days but if you want to accelerate the time delay to only one day, the fee doubles. For this extra fee one is able to retrieve not only registration data but also a copy of the company's Charter of Incorporation and similar documents.

Another possibility exists for large CI companies who can sign special legal agreements with the information distribution departments of state organizations. Such agreements allow CI agencies to secure access to several state databases (that have not been designated as secret or confidential). For this access, the agency has to transfer part of its income from data trade to the state organization. Of course, such legal methods of data access are not as profitable as purchasing illegal copies of state databases but they correspond to ethical standards as well as to legal rules. This method is the only worthy manner of making deals in CI data trade.

Interviewing

Most of our firm's partners outside of Russia make wide use of such methods as interviewing and surveying to gather useful primary data. Unfortunately, these methods will probably not become a key instrument for information gathering in Russia for several reasons (Starkova, 2001). Among all interviewing methods, the phone interviewing is the least useful for Russian market research. Most Russian and CIS-based companies prefer to answer questions by personal contacts or fax/e-mail and not by phone (especially if they are questioned on their companies' characteristics like employee numbers, production volumes, revenues, etc.). This tradition is determined by the fact that top-executives of large companies in Russia and the CIS prefer not to

take part in the interviews themselves but, rather, are apt to delegate this task. Hence, the delegate has to coordinate all his/her answers with the top-executives. This closed loop creates a situation in which answers to required questions will be given only after some period of 'thinking'. This situation is hardened by the fact that, in Russia and in the CIS, many companies were or are still working for the state and they need time to understand whether the questions and answers are consistent with the entrenched regime of secrecy. When elicitation methods are used too aggressively to coax answers, Russian interview respondents will respond with irrelevant or inaccurate answers.

The situation with small and medium-size companies is even more confusing. Small businesses are given preferential tax treatment in Russia. To keep this preferential treatment, they have to keep their staff at the same level. At the same time, almost 45% of small companies in total and almost 80% of small companies in manufacturing and construction have employee numbers that supercede the regulations for "small" business status (very often they exceed this number by a factor of 3-5 or more). The extra personnel are often citizens of the Central Asian republics, Moldova, Belarus, Ukraine and other CIS countries. They are mostly illegal immigrants. In addition - this is the main problem - these people are not being included to the official company employee numbers. To avoid problems both with tax authorities (because of their dubious status as a small business) and with the Ministry of the Interiors (because of the issue of hiring illegal immigrants), companies seldom reveal their employee numbers. They prefer to give the standard answer that they have 5, 9, or any other similar and officially acceptable number of people on their staff. Sometimes the Russian tax authorities and/or police departments use 'sociological' or 'marketing' surveys to secure legitimate data on employee numbers. They call by phone to the companies, say that they represent some Russian or even foreign company, and ask questions including those referring the quantity of the personnel. Small companies in Russia are well aware of such tricks of the authorities and prefer to release only official data to any interviewer.

The same problems plague available data on revenues (turnover). Even by official estimates, almost 3/4 of the revenues of Russian small businesses are hidden. In the interests of avoiding taxes, companies are hesitant

to release revenue information. Typically, companies will officially report only 15-20% of their revenues in financial statements. Because of the risk of conflicts with tax authorities, many companies are willing to discuss only official data about their revenues during the interview. Hence, the original assertion of this section that, in many cases, data gathered during interviewing (especially made by phone) is irrelevant in many cases (Tokarev, 2001).

Information Analysis

The second main goal of competitive intelligence is to analyze information. Raw data and information are particularly helpful in supporting everyday business decisions. Before information can be used for decision-making, it must be processed or analyzed.

There are many methods of data and info analysis that are being used in the Russian CI community. Russia has many strong scientific schools in mathematics, statistics, data-analysis, cybernetics, etc. The country's IT professionals are well-known all over the world for their high skill in 'brainware' as well as for their ability to find non-traditional methods to solve problems. As a result, Russian analysts prefer to use complex methods like scenario planning and analysis, simulation and modeling, content analysis, text analysis, knowledge discovery in databases, case based reasoning (CBR), decision trees, neural networks, genetic algorithms, evolutionary programming, etc. (Doronin, 2000).

Due to the former MI/GI experience of the Russian CI professionals, such special methods of analysis (used usually in governmental intelligence agencies) as rumor scanning and filtering, war-gaming, environmental scanning, etc. are being used.

Some analytical methods widely used by the American and European CI companies - like SWOT analysis, gap analysis, benchmarking and few others - are not widely spread among those Russian professionals who came from MI/GI backgrounds. However, the new generation of CI specialists - those who have graduated from business schools - often incorporate these methods in their CI analysis.

To summarize, analysis has long been the strongest suit of the Russian intelligence tradition - a strength which continues today in the Russian CI community as well.

Personnel Backgrounds in Russian CI

Currently, two main human resource models exist in the Russian CI community. The first was born in the early 1990s and until 1999-2000 it was the dominant model. This model implies that only former military, intelligence, or police officers can work in CI. The second model appeared in the Russian CI in 1999-2000 and it refers to cooperation of former MI/GI officers with non-intelligence analysts who have a civil education (Chertoprud, 2002).

MI/GI Professionals

This group of professionals occupies approximately 4/5 of all positions in the modern Russian CI community. This disproportionate share is a manifestation of the history of CI's development in Russia. Currently, few military and intelligence academies educate intelligence professionals expressly for MI/GI. Many graduates become CI specialists after some period of work in the state agencies. Few young graduates of these academies prefer to go to business immediately after graduation. The main reason for transfer of the MI/GI professionals to CI area is financial, that is private companies pay up to 5-15 times more than state agencies (Linder, 2001).

Several state agencies of the former KGB such as FSB (Federal Security Service), SVR (External Intelligence Service), FSO (Federal Guards Service) and a few others - are the main suppliers of personnel for CI divisions of Russian corporations. Former KGB officers hold up to 2/3 of all positions in the country's CI infrastructure. Former officers of the military intelligence (GRU, or the Major Intelligence Department of the General Staff of the Armed Forces of Russia) occupy approximately 15-20% of Russian CI employment. Former police officers (especially those who served in special economic crimes departments) occupy the remaining share of positions in the Russian CI industry. This distribution of employment is reflective of the various specializations of correspondent state agencies - the KGB has always been oriented at political and economical intelligence while Russian military intelligence has a more applied character (Kochetkov, 2002).

This category of professionals always brings the spirit of government intelligence to CI activity. This means that espionage is considered to be the main method of gathering information while open sources are not widely used. So, the main principle of this human

resources model can be expressed as 'spies but not analysts'. Moreover, it is necessary to mention that this motto has numerous supporters among proprietors and top-managers of Russian companies. They consider espionage to be an effective *and* acceptable method of gathering competitive data (Chertoprud, 2003).

Analysts

By 1999-2000, the first human resources model - a remnant of the wide usage of former MI/GI officers - had been marginalized by a number of factors. First, numerous scandals with corporate espionage increased the demise of the old model. Further accelerating this decline were additional scandals swarming around the policy of state agencies that attempted to prevent competition by private enterprise in the intelligence area. This dual impact has forced Russian CI to begin its transformation.

The principle 'spies but not analysts' was changed to 'spies and analysts' and later to 'analysts but not spies'. The new policy in CI methods had been started among the largest corporations with new policies necessitating the need for new personnel with different attitudes, ethical values, and skill sets. As a result, three main tendencies can be observed.

First, structural changes are being observed among former MI/GI professionals working in CI. As recently as 5 years ago, almost all former officers who were working in CI represented the espionage level of correspondent state agencies. Currently, more and more representatives of the analytical divisions of correspondent state agencies are beginning to enter CI. In spite of the fact that they are former intelligence officers, they can be considered more as 'analysts' than as 'spies'.

Secondly, and on the other hand, many former MI/GI officers are seeking additional, non-intelligence education. Many are successfully pursuing "second" academic careers at business and law schools. Very often, this education has a great influence on their manner of thinking; so much so that after graduation they often embrace the analytical methods of CI and turn away from the old ways of rough espionage.

The third tendency is that young people with civil educations are beginning to occupy positions in the Russian CI community. Most of them are graduates of business/economics schools and with this education

comes knowledge of modern economics and global business - training that helps them to become very good analysts in corporate CI divisions (Zabello, 2002).

Key Problems and Issues

Secrecy

The problem of secrecy plays a significant role in the Russian CI community. Since the times of the USSR, Russian governmental agencies have been obsessed with the protection of state secrets. Many facets of business activity are heavily impacted by this so-called 'state secrets regime'. Recent events revolving around secrecy underscore how this phenomenon severely complicates CI activity in Russia (Vus & Federova, 2003).

The federal law regarding state secrets protection was adopted in 1993 and it has absorbed the worst features of the Soviet system of secrecy. It is necessary to remember that, in the USSR, almost all business information was considered to be secret. Obviously, data on military affairs or information relating to the defense industry was considered state secret. Perhaps less obvious was the fact information on natural resources extraction and non-defense manufacturing were also declared to be state secrets. This was yet another control tactic designed by the KGB to tighten its iron grip over the entire nation. Only this agency could allow any person to get access to state secrets. In many ways, the KGB determined the fates of all people employed in the Soviet economy. The KGB could deprive any person the right to work with secret information by making it impossible for certain people to work in the defense industry or in state service. Given that employment in these areas were widely regarded as the most prestigious and profitable, it becomes clear how the KGB could regulate the behavior of many well-educated people.

After the fall of the USSR, individuals comprising the KGB became the authors of the new law on state secret protection. In an attempt to retain the reins of power, they aggressively strived to implement the same model - to declare as many things as possible to be state secrets and to set up a procedure of licensing of those people who would work in such areas. The KGB's main successor - the Federal Security Service - is still responsible for protection of state secrets and it still regulates the behavior of those who work at the state

service and in defense industries.

This line of succession had and still has a direct impact on CI activity in Russia. Because many areas of business activity are under the regime of state secrets protection, any person who gathers information in such areas risks being accused of secrecy violation. CI professionals are particularly vulnerable to these accusations. In spite of the fact that the law contains the closed list of problems that can be declared as state secrets, all Russian state bodies prefer to set up their own requirements in this area. These state actions function surreptitiously as a good method to hide any important information and to distribute it only to affiliated persons and companies. Therefore, if one even knows that the law does not consider some specific information as secret, one cannot be sure that some Russian state organization has not declared it to be a state secret. Moreover, Russian authorities like to set up the secret lists of data that have to be considered as secret. This means that CI practitioners cannot always know for sure that some information is secret because it was declared as secret by secret document.

In the last year the situation has worsened. Until 2003, it was widely agreed that only people who had an official access to state secrets could be accused in secrecy violation. It was a logical practice - some person could disclose the state secrets only if he/she knew such secrets. But, in 2003, several Russian courts have decided that all citizens could be accused in state secrecy violation - even those people who have no access to such secrets. Moreover, these courts decided that open sources could contain state secrets. In reality, this development means that every person in Russia who works with open sources can be accused of secrecy violation with a risk of 10-15 years of imprisonment. Determination of secrecy violation is unilaterally determined by one state agency - the Federal Security Service - that has exclusive rights to investigate all cases of secrecy violation. In 2003 / 2004 at least two people were sentenced by the Russian courts to long prison terms based on such denunciations¹³.

Yet other examples of this untenable situation abound. The Russian oil industry provides another case in point. The Russian oil industry is widely considered as the key driver of the national economy. Foreign investments in this industry were declared to be an issue of national priority. The Russian President stood behind top-executives of TNK (Tyumen Oil Company) when they were signing

an agreement on joining with BP in 2003. Enthusiastic comments on the potential of global investment for the Russian oil industry had been overflowing in the Russian and foreign mass-media. However, joyful representatives of BP as well as other foreign players did not know that Russian authorities had secretly adopted some changes to the law on state secrets. These changes had been enacted in February, 2004 and already in May, 2004 the foreign managers of newly established BP-TNK have met with their after effect. The officers of the Federal Security Service had gone to the BP-TNK office in Moscow and had withdrawn some documents regarding the company's activity. According to the changes in the law, all data on the Russian oil reserves have been declared as state secret since February 11, 2004. The foreign managers of BP-TNK were accused with having access to secret information without licenses issued by the Federal Security Service. At the same time, according to the law, foreign citizens cannot be licensed to have access to state secrets. A special decision of the Russian Government has to be adopted for each foreign person's access to such information. Such a procedure may be applied only to the citizens of those countries that have special secrecy protection agreements with Russia. This means that foreign managers cannot get access to data on oil reserves of their own companies. All this occurred during a period in which the Russian oil industry had a good chance to become the global leader in oil reserves (a lost opportunity amplified even more by simultaneous scandals with overestimated reserves in several other global oil companies). Once again, the personal interests of the Russian state officials had crushed the interests of the entire nation.

The only good event that occurred in this area during the past few years was the removal of secrecy from the data on noble metals and gems reserves and extraction. However, even here, those who are interested in protection of their privileges make every possible attempt to slow down the process of declassification of this information. The secrecy law on this data was abolished in 2003 but Russian authorities continue to protect secrecy in this area choosing to rationalize their delay tactics as "necessary to change some instructive documents". Moreover, given the local situation, we can expect that the data on diamonds or gold reserves will finally become accessible via open sources in perhaps 2 years but not earlier. In the interim, some state officials (supported by unfair businessmen) will do all they can to stall this process.

These developments underscore the significant legal challenges that impede the development and practice of CI in Russia. However, as powerful political connections and historical/cultural values continue to be challenged by the majority of Russian citizens who are fair-minded, this situation will steadily improve.

Transparency

The problem of transparency directly influences CI activity in Russia. The main idea of CI is to collect data from open sources. It implies that such sources have to contain relevant data referring to various aspects of business activity. However, it is very difficult to gather data in sources where there is no any data.

As reflected in a previous sub-section, many remnants of the Russian state prefer to hide various pieces of information by declaring them to be state secrets. The same situation exists in the corporate sphere - many Russian companies prefer not to publish data on their activity (National Council on Corporate Governance, 2003; 2004a). By our opinion, only 10-15% of the Russian companies comply with the modern requirements of information disclosure. The remaining 85-90% don't comply even under the requirements of the federal law on joint stock companies that directly requires all public joint stock companies to publish their quarterly and annual statements. Some companies have been re-registered by their owners from joint stock companies to limited liability companies - a classification category that requires no legal duty to publish information. Other corporations that continue to act as joint stock companies publish their statements with large delays (often in 1-1.5 years) by which time the information is out-of-date and irrelevant.

The only factor that stands a high probability of influencing the level of corporate transparency in Russia is a desire to enter global financial markets. Only those companies that want to undergo a successful IPO process or to issue ADR or Eurobonds have published their statements in full volume. They know that if they are unable or unwilling to openly publish relevant data, they will be summarily excluded from participating in global financial markets. Therefore, the positive incentive of global financial markets serves to induce many Russian corporations to become more transparent. However, this effect will only impact a small percentage

of the largest corporations that are large enough to enter world markets. Most of the companies in Russia are still too small to be realistically impacted by this promising incentive.

This lack of corporate transparency continues to plague the Russian economy. Many CI professionals still refer to illegal data sources (like copies of state databases) to secure useful information because they cannot find it in open sources. The problem of espionage in Russian CI still exists today and will continue to exist until there is a dramatic improvement in corporate transparency.

Concentration

Concentration can also be considered as one of the main tendencies of the Russian CI market. The first aspect of this process refers to integration of CI agencies and the second aspect refers to ongoing consolidation..

During the first developmental stage of the Russian CI market, small companies (with 2-3 employees) dominated the landscape. It was simply very easy to register a company and name it as a competitive intelligence firm. The main goal of such companies was to find some large corporate customer and become its exclusive CI supplier. In many cases, this objective could be achieved with a payoff or bribe to the corporation's executives who became 'partners' in the CI firm. The arithmetic of the process was clear. Imagine, for example, some CI agency that wanted to earn 50 thousand USD for its services. In such a scenario, the total price of the contract between CI agency and its corporate customer would be 150 thousand USD, from which 50 thousand went to CI agency, 25 thousand USD - to the head of the corporative security department and 75 thousand USD - to the top-executive of the corporation who had signed the contract. This system was wide-spreaded in Russia and by our observations, almost 4/5 of all large corporations have had such pocket CI 'consultants'.

However, when large corporations began to actively enter the global market, their CI needs had changed a lot. Small CI agencies could not satisfy new requirements in real intelligence data. As a result, a new formation of CI consultants began to grow in Russia. The main advantage of these new CI consultants was the higher level of professionalism achieved by sharing the labor between staff members. The 'minimum efficient scale'

so to speak of a CI agency of medium size had to have at least 10-12 employees in its staff of which 7-8 persons have to be CI professionals (data builders, analysts, etc.). The agencies that pretend to become the Russian market leaders had to increase their personnel up to 30-50 employees and more. These developments resulted in many small companies choosing or being forced to exit the market.

The same tendency can also be seen in corporate CI. A few years ago, the average CI department of a large corporation (with a few thousands employees) could conceivably contain 3-4 professionals. Today, Russian business giants try to hire at least 15-20 employees to realize CI programs.

If this consolidation trend continues, we can expect that the total number of Russian CI agencies will decrease to 50-60 in the next 2-3 years. At the same time, these agencies will grow both by revenues and employee numbers. It is the earnest wish of top tier firms in the industry that the Russian CI market will be occupied by large responsible companies, possessing high-class professional personnel that are able to realize a wide range of complex CI programs.

Conclusion

Given that the fundamental purpose of CI is to provide forward-looking and future-oriented information, this article will conclude with a brief list of future developments that can be expected in the Russian CI sphere:

- The Russian economy will continue to expand and become more integrated in the global economy thus creating an strong demand for Russian CI by both the domestic Russian and international business community.
- The incidence of corporate espionage will decrease dramatically in the next 5 years as the new breed of business school CI professionals displaces the MI/GI generation and begins applying more of an analytical mindset. Espionage will also decline as both internal corporate CI departments and CI agencies realize that highly ethical conduct and a sterling reputation are extremely valuable marketing tools both in domestic and international markets.

- The CI community in Russia will begin coalescing around a regional industry trade associations.
- Positive steps will be taken against database piracy in alignment with the global movement to protect intellectual property.
- Private company intelligence in Russia will continue to pose challenges.
- The Russian CI community will continue to develop a core competency in strategic intelligence by leveraging its inherent skills in higher order analysis and complex methods.
- The high economic cost of lost foreign investment as a direct result of untenable secrecy laws will provide strong incentives for Russia to legislate more equitable secrecy laws. This development will increase the availability of open source information and will further reduce the perceived need for espionage and will increase the demand for legitimate primary and secondary CI.
- Membership by Russia in supranational organizations such as NATO, G8, WTO, EU, OECD etc will also provide strong incentives for global harmonization and the attendant increases in transparency. This development will increase the availability of open source information and will further reduce the perceived need for espionage and increase the demand for legitimate primary and secondary CI.
- Consolidation will improve the overall quality of Russian CI practice. A top tier of professional full service CI firms will emerge to lead the industry's best practices in intelligence gathering, analysis, ethics and skills development.
- Russian CI agencies will broaden their portfolio of products and services to include process consulting, CI technology, benchmarking, ethics, and strategic intelligence.

Notes

1. The *Dune* saga consists of a series of 12 novels in the fantasy genre.
2. More details on the Soviet and Russian GI/MI practices are available at *Agentura* - Russian-language source on the Russian and the world's secret services available online at <http://www.agentura.ru>.
3. Research of the corporate structure of the Russian TOP-100 companies was made by Ignatov and Company Group in February, 2004 as the basis of investigation of corporate annual statements published at Interfax's corporate disclosure website <http://disclosure.interfax.ru>
4. CobiT (Control Objectives for Information and related Technology) issued by the IT Governance Institute and now in its third edition, has been developed as a generally applicable and accepted standard for good Information Technology (IT) security and control practices that provides a reference framework for management, users, and IS audit, control and security practitioners. Description of the project, its standards, case studies, articles and other related items can be found at website of ISACA (Information Systems Audit and Control Association), available online at <http://www.isaca.org>
5. The classification used to determine the various levels of transparency were determined accordingly to criteria developed by the National Council on Corporate Governance. The specific criteria are available online at the website of the National Council on Corporate Governance <http://www.nccg.ru>
6. More information regarding the publication, *Security and Safety Technologies*, is available online at <http://www.tbforum.ru>
7. The publication, *Business Intelligence and Information Management* is available online at <http://www.ris.ru> <http://www.ris.ru>

8. More information regarding the online newspaper on corporate security, *Oxpaha*, is available online at <http://www.oxpaha.ru>
 9. More information regarding the ITAR-TASS News Agency is available online at <http://www.tass.ru/eng>
 10. More information regarding the Interfax International Information Group is available online at <http://www.interfax.com>
 11. More information regarding the RIAN ('Novosti' Information & News Agency) news agency is available online at <http://www.en.rian.ru>
 12. More information regarding the Integrum Techno agency is available online at <http://www.integrum.com>
 13. As an example of cases involving secrecy violations, see the Sutyagin case website with materials on Igor Sutyagin who was sentenced to 15 years of prison for "espionage". <http://www.sutyagin.ru>
- References**
- Alexandrova, A. (2001). "Hear, Comrade!" *Career Magazine*, 10 (October 2001): 46-49
- Andrew, . and O. Gordievsky. (1991). *KGB: The Inside Story of Its Foreign Operations from Lenin to Gorbachev*. New York, NY: HarperCollins.
- Babkin, V. (2003). *Bank Business Intelligence*. <http://www.it2b.ru/it2b2.view3.page106.html>.
- Chertoprud, S. (2002). "Competitive Intelligence in Russia: Personnel is the Critical Factor," *World of Security Magazine*, 4(101)
- Chertoprud, S. (2003). "Competitive Intelligence and Economical Espionage: Ethics of Methods," <http://profi.gateway.kg/chertoprud>.
- CNews (2003). *It's Possible to Purchase the Phone Subscribers Database only for 600 Rubles*. www.cnews.ru. March 6.
- Conflict Studies Research Center, the Defense Academy of the United Kingdom (2000). *The Federal Security Service of the Russian Federation*. March.
- Doronin, A. (2000). *Analytical Work in Non-governmental Security Services*. <http://www.bre.ru/security/14987.html>
- Ignatov & Company Group. (2003). *Evaluation of the Volume of the CI Market in Russia*. Bespoke Report. (available by request).
- Ignatov & Company Group. (2004a). *Corporate Structure of the Russian TOP-100 Companies*. Bespoke Report. (available by request).
- Ignatov & Company Group. (2004b). *6 Level Model of CI Maturity for CIS-based Companies*. Available by request.
- Interiors Ministry of Russia, General Editorial Board. (2003). "Annual Statistics: Data on Registration and Control over Activity of the Private Detective and Guard Agencies in Russia for 2002."
- Interiors Ministry of Russia, General Editorial Board. (2004). "Annual Statistics: Data on Registration and Control over Activity of the Private Detective and Guard Agencies in Russia for 2003."
- Kochetkov, V. (2002). "The Technology of the Start: Former KGB Officer or Former Police Officer?" *Vedomosti Newspaper*, 126(689)
- Kolpakidi, A.I. and D.P. Prokhorov. (1999). *Empire of the GRU*. Moscow, Russia: Olma-Press Publishing House.
- Linder, J. (2001). "The Soldiers of the Invisible Fronts," Interview published at <http://www.rabota.ru/library/article311.html>

- Mirzoev, S. (2004). "About Sad: the Russian Corporate Security Services Live According to the Laws Adopted by Themselves."
http://advokaty.org/vslux4_04.php
- National Council on Corporate Governance (2003). *It's Better to be Rich and Transparent*. Bulletin 1(1): 11-12
- National Council on Corporate Governance (2004a). *National Corporate Governance: Overviewing Specifics*. Bulletin 2(2): 2-6
- National Council on Corporate Governance (2004b). *Rating Russian Companies*. 2(2): 17-20
- Pechenkin, I.A. (2004). *CI in Metallurgy*. Report at conference, *Information in Metallurgy*, Moscow, January 15-16, 2004.
- Potresov, S. (2003). *The Database at Your Shelf*.
<http://www.izvestia.ru/tech/article29061>
- Sharlot, V. (2002). *The Russian Database in Informational-Analytical Work*.
<http://compintel.narod.ru>
- Starkova, J. (2001). *Marketing in the Regions of Russia: Problems and Perspectives*. Abercade Consulting.
- Tokarev, B.E. (2001). *Methods of Collection of Marketing Information in Russia*. Jurist Publishers.
- Tzu, Sun. (1963). *The Art of War*. Translated by S.B. Griffith. Oxford, UK: Clever Press.
- Vus M.A. and A.V. Federova. (2003). *State Secrets and Their Protection in Russia*. Juridical Center Press Publishers.
- Waller J. M. and V.J. Yasmann. (1995). "Russia's Great Criminal Revolution: The Role of the Security Services," *The Journal of Contemporary Criminal Justice* 11(4) December, 1995.
- Zabello, J.Y. (2002). *CI Professionals Training: Problems and Perspectives*.
http://profi.gateway.kg/kadry_ci