

Need for Economic Intelligence*

Jan Leijonhielm

FOA, Stockholm, Sweden

1. Intelligence estimates of changes in Europe at the end of the 20th century

National Intelligence services largely failed to foresee the great changes in Europe in the '80s and '90s, at least in the sense that they conveyed them to partners and/or convinced their governments to act upon them. In some cases, as in the matter of the Baltic states' independence struggle, the KGB was accurate in its warnings, but failed to convince the leadership to act upon this Intelligence.

Do these Intelligence failures exhibit similar characteristics over an extended time period? To a large extent, I believe they do. My arguments for this hypothesis are:

Systematic errors

- Intelligence systems tend to pay attention to signals that support current expectations regarding the behavior of other nations or actors. This often leads to "group think". It is also a fact that defensive is more common than offensive irrationality.
- There is usually adequate documentation, even in the case of unexpected developments, in the materials gathered by Intelligence services. The fault is generally not in the collection of Intelligence, but in the analysis, and incorrect analysis leads to inaccurate targeting of new Intelligence areas.

* Reflections on the topics addressed at the Round table "Intelligence and National Security at the Beginning of the 21st Century", Dubrovnik, October 27-28, 2000.

- Intelligence organizations are seldom equipped with "devil's advocates", who are free to say: "But what if..."
- Cognitive rigidity, plus anxiety over deviating analyses in the Intelligence services, create an obstacle to pluralism.
- Analyses prepared by both academics and professional Intelligence officers has proved to be the best system, but this mix rarely exists in reality.

Human-related factors

- The main reason that serious misinterpretations of events occur is due to the aura of secretiveness and mystery in the Intelligence world. Secrets - for example the operational capacity of a military body, new weapons, or military R&D progress - can be obtained. But what is in the human mind, what a dictator's ultimate intention is, or how he will react, is almost impossible to gauge unless one is able to utilize human Intelligence (HUMINT) at a very close range to the leader in question. Even so, there is always room for uncertainty. It was impossible, for instance, for anyone to have claimed knowledge about Saddam Hussein's attack on Kuwait, or Yeltsin's move to dissolve the Soviet Union in Belovezha in 1991. Even the acting Belorussian president Shushkevitch, by his own admission, had not been informed of the ultimate purpose of the meeting.
- The greater his influence, the more difficult it is to predict a sovereign's actions.
- Another cause of Intelligence failures due to human-related factors is the relationship between Intelligence services and politicians.² Politicians are often unwilling to make costly decisions which could accelerate an ongoing conflict or harm the politician. The personal chemistry between the messenger and the politician has therefore played an important role. Generally, decisionmakers' inability to react is more common than the Intelligence services' inability to warn.

2. The role of Intelligence in conflict resolution.³

The political and military elements involved in peacekeeping require Intelligence in order to ensure the safety and success of the operation. UN peacekeeping forces have often lacked that capacity. The UN's own Intelligence, termed "information" for psychological reasons, must often be substituted by the participants' national Intelligence. Intelligence requirements vary, from data on possible attacks in peace enforcement operations, to HUMINT-

related Intelligence regarding the state of mind in a specific, small area, which could indicate an outbreak of violence in low-level conflicts. A whole range of specific Intelligence requirements is therefore needed. These more complex type of requirements have emerged in the post Cold-war era. At the same time, more attention must be paid to political consequences at home, to the media, and to the organization in question.

The Intelligence service of a peacekeeping operation is usually more fragmentary than ordinary Intelligence, which makes it difficult to obtain a clear picture. The connection between strategic and tactical levels is very strong. When processing Intelligence from a peacekeeping operation, it is seldom possible to use traditional criteria utilized in "ordinary" wars. The multinational elements place new demands on the Intelligence process as well. Ways to promote effectiveness and resolve these difficulties are:

- Whenever possible, cooperate on strategy, terminology, etc., in advance of an operation conducted under UN auspices.
- Use national Intelligence sources in the field to ensure a common approach, and move gradually to joint efforts.
- During an operation, create two to three scenarios, based on the political-strategic situation, but adapted to tactical levels. New tactical Intelligence can be used to better evaluate the strategic situation.

3. Subjects and methods of Intelligence agencies at the beginning of the 21st century: possibilities and limits.

Intelligence has been increasingly privatized during the past decade. The number of large and medium-sized corporations, banks, financial institutes, political and economic, academic and non-academic think tanks dealing in Intelligence, has grown at an astonishing speed. The need for and volume of economic Intelligence has grown at the same pace. According to the CIA, 40 per cent of its collection and analysis in the mid 1990s concerned economic matters⁴. Since the Primakov era, its Russian counterpart has also placed a high priority on economic Intelligence, and the same trend is evident in most Intelligence agencies, especially in Germany, Japan and France. Large companies often invest more capital and human effort in Intelligence than small nations.

The reasons for this development are obvious: most nations, especially small ones, are vulnerable to external pressure and rapid changes in the world. Economic sanctions, financial instability, flow of raw materials, speculation on the local currency, and various types of dependence, however necessary, present poten-

tial dangers. Even unintentional economic misconduct by a large neighbouring nation, resulting, for example, in lost market shares, could become a serious danger. By the same token, companies and other economic factors are under pressure to interpret and evaluate their environment.

The link between economy and security has therefore become stronger. This can be exemplified in several ways: prosperous nations today are more inclined to be peaceful, since prosperity is tied to economic interdependence, and is too valuable to risk. A good economic performance thus creates stability, and enhances the survival of democracies, the most obvious example being North and South Korea.

Economy will continue to influence security policy in the future. It will be much safer and more effective for developed nations to use economic instruments to achieve security policy goals, and this will also place more demands on economic Intelligence.

Economic security has not often been addressed in the western media, though the debate has been quite strong in Russia. There are several reasons for this. The most important is that economic security can be interpreted differently depending on the level of society: in terms of personal security, which was severely damaged during the transition period, security of supplies and provisions, which is often in danger in some parts of Russia, the nation's security and economic survival, and, finally, its role on the world.

Economic Intelligence will become more internationalized and transparent in the future. The necessity for speedy reaction will increase as economic threats and situations which require a quick response appear without warning. As a result of this, national, traditional Intelligence may become less useful and effective, except in military matters. These new, rapidly changing threat dimensions do not allow as much time as before for thorough analysis and decision-making. As Francesco Cossiga⁵ has pointed out, the mix of private and governmental actors, and the question of offensive and defensive Intelligence, present another problem. In the future, not only the threats, but also the actors, will become more indefinable. Economic, political, or military targets in an information warfare attack will be more indistinguishable, easier to disguise, and harder to oppose. The Russian threat, as expressed in its 1993 Military Doctrine, to use any kind of retaliation, including nuclear arms, in response to a massive IW attack demonstrates the potential future dangers. A clever hacker with sufficient computer power could quickly close down a small country economically, and severely damage sectors of society in a larger one. A Swedish hacker recently succeeded in paralyzing a major part of Florida's rescue service.

We cannot escape new and increasing threats to society, and we are bound to become more dependent on high-tech solutions. What we can do is use Intelligence to better understand the nature of these threats, and build scenarios to predict them and to prevent hasty and unpremeditated counteraction.

NOTES

1 See e.g. Betts. "Analysis, War and Decisions" *World Politics*, Oct 1978

2 Herman. "Intelligence in Peace and War", Cambridge University Press 1996

3 This part largely relates to conclusions in the FOA study: "Intelligence in Peace Support Operations" by Eriksson, Rekkedal and Strømmen

4 Colby: "Reorganizing Western Intelligence", from *Intelligence and the New World Order*, Potsdam 1996.

5 Cossiga: "The Economic Intelligence Services", *National Security and the Future*, vol 1, spring 2000.