Strategic Dossier 162 B
Economic intelligence in a global world

Spanish Institute for Strategic Studies

ieee.es

MINISTRY OF DEFENCE

Strategic Dossier 162 B
Economic intelligence in a global world

Spanish Institute for Strategic Studies

ieee.es
Instituto Español de Estudios Estratégicos

MINISTRY OF DEFENCE

SPANISH OFFICIAL PUBLICATIONS CATALOGUE
http://publicacionesoficiales.boe.es/

Publishes:

MINISTERIO DE DEFENSA

SECRETARÍA GENERAL TÉCNICA

http://publicaciones.defensa.gob.es/

Publication date: february 2014

NIPO: 083-13-250-1 (e-book edition)
ISBN: 978-84-9781-896-4 (e-book edition)

ÍNDICE

Strategic intelligence and economic security

Eduardo Olier Arenas

Introduction

In 1992, one of the authors of this report published a book entitled "*La máquina de Guerra económica*"[1]. In the first pages the author warned about the importance of economy in international relations, from the end of the Second World War to the early stages of globalization, and its exchanges that were changing the notion of conflict itself. The author also warned about the repercussions of the economic war which, unlike traditional war, implies actions that are frequently invisible and decisive.

When the Cold War was over, Harbulot focused on the end of global polarization and on the increasing American hegemony. After the collapse of the Soviet Union, there was only one player left. A fact that worried Jean-Jacques Servan-Schreiber[2], who many years before, in 1968, categorically stated: "We are neither witnessing a classical political imperialism nor a wish to conquer, but a power that surpasses all limits because of the difference of "pressure" between North America and the rest of the world, including Europe". In another passage of the book he said, "Acting, how? Against whom?...General Motors is not Wehrmacht, the Bull case is

[1] Harbulot, Christian. La machine de guerre économique. Etats-Unis, Japon, Europe. Ed. Economica.

[2] Servan-Schreiber, Jean-Jacques. *El desafío americano* (The American Challenge). Plaza y Janés. 1968.

not Munchen and the Concorde is not Sedan. We are witnessing the first great war without weapons or fortifications".

The French were not the only ones to be aware of this problem. The Japanese also became aware of the importance of economy as a new niche of dominance. Almost since the end of the Second World War, with their armed forces destroyed and without any capability to rebuild them, they started their way to industrial reconstruction to become one of the world economic powers. Therefore, as time went by, in the early nineties, they started their third industrial revolution with the powerful MITI conducting offensive and defensive economic operations. Along with Japan, other nations also developed strategies to expand their economic, technological or commercial power to other places. This expansion proved to be defensive in some cases, especially in smaller countries such as Sweden.

Shortly before the publication of the above-mentioned book by Harbulot, the Romanian US-based Edward Luttwak, an expert on geopolitics, launched a new concept in The National Interest[3] magazine. The term geo-economy emerged for the first time. For Luttwak, "geo-economy is maintaining old rivalry among nations using economic means instead of military ones". He expanded on it in his book *The Endangered American Dream*[4] by saying "geo-economy measures progress considering the performance of a product in the market instead of focusing on the advance of a military force on the map". And thus a connection emerged between economy and geopolitics. Economic wars become an integral part of the economic fact. Economics and politics joined in new war scenarios far from traditional military conflicts.

As new scenarios, they become more and more complex. These new wars become increasingly sophisticated. A fact ratified by another geo-economy theorist, Pascal Lorot, in the early nineties.

Lorot, founder and editor of the French magazine *Géoéconomie,* defined geo-economy in 1990 as "the analysis of economic strategies – especially commercial ones – designed by the States within the context of those policies aimed at safeguarding national economies and some of the elements inherent to them, mastering certain key technologies and/or conquering certain sectors of world market regarding the production or marketing of a sensitive product or set of products which provides its holders (State or domestic company) with some power or international projection and contributes to reinforcing their socioeconomic power". A power that would be exerted according to the "soft power" concept developed by Joseph S. Nye[5].

[3] Luttwak, Edward. "From Geopolitics to Geoeconomics: Logic of Conflict, Grammar of Commerce". *The National Interest,* Summer 1990, pp.17-23.

[4] Luttwak, Edward. *The Endangered American Dream*. Simon & Shuster, 1994.

[5] Nye, Joseph. Soft Power. *The Means to Success in World Politics,* Public Affairs, 2004.

The soft power strategy needed new techniques. One of them, old as the war arts, was the use of intelligence services. In order to anticipate the enemy, it was necessary to know its strategy and movements in advance. Therefore, it was necessary to find new methods in line with the new times. Economic intelligence strongly emerged as the use of intelligence services in the economic sector. The States needed to know what to do in the new global world that was approaching.

Intelligence activities took a new turn with the emergence of the concept "economic intelligence" as a set of coordinated actions for investigating, processing and distributing information in order to make economic decisions in the field of economy. These actions focus both on the domestic economy and on the business sector since the market globalization challenges companies. The defense of economic interests, on the one hand, and the need to achieve economic advantages against competitors – at state or business level – have been a decisive driving force for the development of powerful economic intelligence tools at the service of national interests and powerful transnational companies which nowadays control the global economic scene.

The Institute of Strategic Studies' report falls within this frame of reference since the defense of national interests must also include economic aspects which are essential in the current world. A fact that Spain has ignored for a long time and is now dealing with: the importance of economic intelligence services beyond the protection of people or critical premises.

Economic globalization and geo-economy

We have briefly mentioned geo-economy above. Let's go back to this concept.

While Edward Luttwak and Pascal Lorot did not expressly affirm it, they insinuated that something had changed in the world scene to have economy as a determining element. Perhaps the authors, both experts in geo-politics, were not able to notice the economic globalization movements which were, in fact, the focal point of these changes because, since the end of the Second World War, especially with the Bretton Woods Agreements, a new world economic order was emerging. This new world order was controlled by the US and this fact worried Servan-Schreiber.

The ongoing economic globalization is a movement, perhaps spontaneous, by which nations have become increasingly interdependent. In fact, similar situations took place many years ago. For example, the Phoenicians traded throughout the Mediterranean and the Romans expanded their dominions by building impressive stone roads to move their troops and extend their economy far away from their borders, from Egypt to England. Egypt, for example, was the Empire's granary for decades. Also

Spain, the United Kingdom and Holland extended their dominions almost throughout the entire world. But we should underline that, as far as economy is concerned, trade transactions and financial movements were quite limited. To such an extent that economic crises have been always limited to certain areas and have not expanded all over the world. A fact that still remains nowadays since globalization only makes sense within the financial world. As far as trade is concerned, the world moves towards globalization and basic commercial activities are carried out among bordering countries or specific regions.

However, we should underline that globalization is not limited to the commercial and financial sectors but also includes cultural, social and political aspects which give rise to a new order characterized by four main features[6]:

- Important transfers of people from one country to another;
- Large capital flows across borders;
- Increasing international trade; and, especially
- Strong technological innovation.

Since 1945 we can identify six stages[7] towards globalization. The last one has entered a new phase after the financial crisis which started in the US in 2008 and we do not know how it will evolve.

1945-1960. The great industrial machinery. After the Second World War, the USSR, the United States and some European countries had powerful industries emerge during the conflict: automobiles, railroads, aviation, electronic industries, etc. In parallel, there was a real estate boom coupled with a huge demographic growth: the so-called baby boom. GDP doubled in all industrialized countries, as did purchasing power and consumption of the middle class.

1960-1973. Geopolitical turmoil. It was a period of economic prosperity and tensions caused by the Cold War. The period ended with the OPEC oil embargo (Organization of Petroleum Exporting Countries). It was a decade of intense decolonization in a large part of Africa where more than 30 new countries emerged. It was a period of great changes that witnessed the landing of the first man on the moon, the revolutions in South America, the assassination of Kennedy, the Vietnam War, and a series of developments that ended in the French events in May 1968. The Palestinian Liberation Organization (PLO) was also set up in this timeframe and the Six Days War broke out in 1967 leading to the Israeli occupation of the Palestinian territories of Gaza and the West Bank and of the Golan Heights in Syria.

[6] Olier, Eduardo. *Geoeconomía: las claves de la economía global.* Pearson-FT-Prentice Hall. 2011.

[7] Olier, Eduardo. Ibíd.

1973-1982. Energy stanflation. Economic stagnation plus heavy inflation is called stanflation. The OPEC oil embargo provoked a 70% increase of oil prices which caused high inflation, economic stagnation and unemployment. Post-war wealth came to an end. Many public companies were privatized, especially in the USA. In this period, the Iranian revolution and subsequently the Iran-Iraq war broke out.

1982-1989. Economic liberalism and market economy prevail. US President Ronald Reagan formed his government in 1981. The supply-side economics started. It was an economic strategy aimed at encouraging the production of goods and services based on the idea that supply generates its own demand, according to Say's Law, one of the economists from the Classical School. This was followed by economic liberalization and tax cuts. The US government's revenues increased almost automatically due to the rise in productivity and the boost of savings which led to a higher rate of employment and sharp economic growth. Decreasing inflation increased consumption and reactivated bank credits. In England, Margaret Thatcher, appointed prime minister in 1979, followed the same line of action. A liberal wave spread all over the Western countries. Post-Second World War Keynesian policy was no longer valid. The Berlin Wall collapsed in 1989 and the two superpowers' polarization came to an end. A period, however, that witnessed one of the most serious financial crises of the century, the so-called debt crisis of many Latin American countries that declared themselves unable to pay off their debts owed to international bodies, especially the FMI (International Monetary Fund).

1989-2000. The interconnected society. On the night of 9-10 of November, 1989, the *Berlin Wall* fell down. It did not take too long until consequences were noticed; on 25 of December, 1991, Mikhail Gorbachov, known as the *Father of Perestroika*, resigned. The Soviet Union and the "system of blocs" collapsed as well. This phenomenon led to the opening of world borders, the intensive use of information technologies and telecommunications, the emergence of the Internet and the definite starting of economic globalization. The world trade quickly flourished and there were great technological achievements in every field, particularly as a result of the development of electronic microprocessors that revolutionized industry, particularly medicine. The world economy began to grow leading to the globalization of the financial markets. The world witnessed a soaring economic growth which was halted by the so-called *dot-com crisis,* technological companies that prompted a serious although controlled capital crisis.

2000-2010. A globalized world amid a global financial crisis. Japan, the second largest economy in the world behind the United States, showed signs of exhaustion in the early nineties, when the Japanese banks were not able to withstand the loss of value of the real estate assets they had several years before. Then, the *subprime* crisis emerged and the 2007

global financial crisis began to spill over from the United States into the Western world in 2008. Economic wars became evident and the world economic center of gravity shifted to the East. The Asian economy, which accounted almost for 20% of global economy in 1970, exceeded 28% in 2007, the European community's economy fell from 34% to 25% during the same period, and the US economy remained at 33%. The 11-S bombings also changed power relations. The bipolar world preceding the fall of the Berlin Wall led to a multi-polar world including regional actors such as Brazil, China, India, Russia (BRIC countries), Turkey and Iran. Islamic pressure as a very influential religious and cultural movement should not be forgotten.

The post-crisis world will be different from the previous one; however it is still too soon to forecast how it will evolve. In the economic field, the situation will be quite different. Geo-economy has become evident. The current situation is marked by the convergence of political interests and dominance of markets. Previous military actions led to more sophisticated efforts; strategic capital investments, manufacture and technological innovations of interest for the state, a leading position in the markets instead of invading territories, custom duties, regulatory measures, devaluation of foreign currencies and other similar actions mark current strategies.

In this new context, the previous elements have become obsolete and the value of information no longer provides a competitive advantage. At present, knowledge is necessary to anticipate the moves of countries and businesses. Currently, intelligence is one of the keys, i.e. structured knowledge for decision-making. Hence, economic intelligence is essential for businesses and institutions in the geoeconomic context and should allow us:

- To describe the competitive environment, i.e. to identify its factors and elements. Competitors, products, regulatory requirements, etc.; price structures and technologies included in this environment that may provide an alternative.
- To forecast the evolution of those competitive factors, including disruptive technologies, new competitors, etc.
- To verify if the foundations of this strategy prove solid, if they have been laid properly in accordance with the present environment and the foreseeable one.
- Intelligence should respond to those aspects questioning the strategy. In this context, proper assessment and monitoring technologies will be needed to collect the necessary information.
- To thoroughly identify threats and weaknesses, as well as strengths and prospects according to the classic DAFO chart.
- To identify if the agreed strategy is no longer sustainable. This decision should be dynamic in order to be consistent with further actions.

Strategic and economic intelligence

The term intelligence usually leads to mistakes, to confusion. And confusion increases as adjectives are added. Each expert or group in this field understands intelligence in a different way. We have identified four categories.

Apart from the intelligence services, which are well-known and identifiable bodies, there are other fields and concepts that interrelate with each other. In the field of intelligence, we have identified five categories according to their technological nature (see Figure 1):

- Artificial Intelligence
- Knowledge Management
- Economic Intelligence
- Competitive Intelligence, and
- Strategic Intelligence

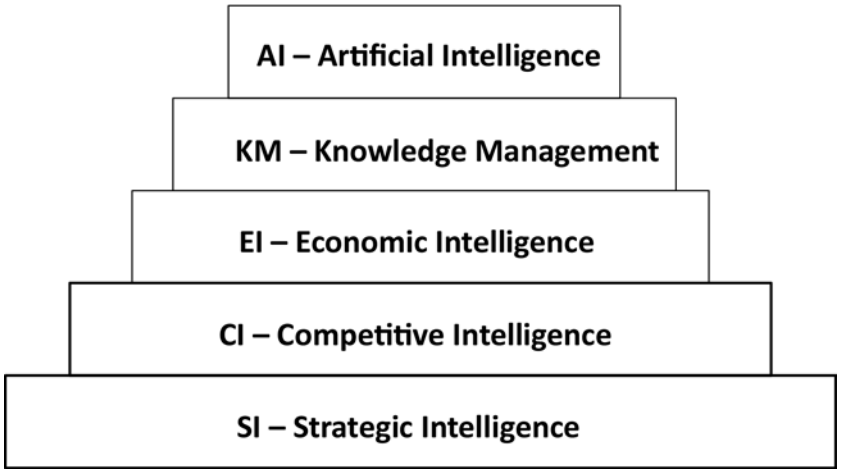

Figure 1.- Hierarchy of Intelligence Systems

The first two categories are highly reliant on commonly used technologies. Artificial intelligence has been developing since the fifties and is mainly aimed at understanding how human beings think, learn and reason in order to develop techniques and computer programs that try to emulate human behavior. This was the origin of robotics, expert systems and systems to help decision-making. All of these systems rely on technologies capable to learn.

Knowledge management systems, mainly related to expert systems, were a breakthrough. These systems gave rise to a branch of engineering currently known as Knowledge Engineering that uses techniques fo-

cused on several elements, including acquisition of knowledge, coding of knowledge, assessment and tests of the coded system and implementation of the system. Coding is usually based on rules that, as they become more complex due to multiple chains, they can turn into *neuronal networks*. This is another way of emulating how the human brain works and the starting point for implementing other functions, including language comprehension systems, computerized vision, etc. These techniques do not represent what is understood as Economic, Competitive or Strategic Intelligence but help to develop them.

There is a myriad of ways to define Economic Intelligence, and its applications will be different depending on the country and on who interprets it. In the United States and other Anglo-Saxon countries, the term business intelligence refers to the activities related to knowledge management, particularly the methods and models designed to find "hidden" information in databases for decision making. These include marketing intelligence, which deals with the trade and marketing aspects of businesses within their competitive environment. The behavior of current and potential clients is "standardized" that way in order to increase sales or just to prevent those clients from looking to rival companies.

The French define[8] economic intelligence – *intelligence économique* – as a series of coordinated actions aimed at investigating, processing and disseminating useful information for the economic actors to be able to exploit it. According to the authors, this definition includes two aspects. On the one hand, scientific intelligence aimed not at "coming up with the greatest possible invention" but at investigating accessible scientific sources in order to find new scientific fields which may provide further economic advantages. On the other hand, competitive intelligence aimed at tracking the activities of laboratories or plants of rival countries or businesses in order to become aware of their breakthroughs and improve one's own competitiveness; for instance, pharmaceutical laboratories of other countries.

Other non-Anglo-Saxon countries understand economic intelligence as the state's activities designed to defend its economic interests at international level. Therefore, these activities are run by intelligence services, as is the case in Spain.

Competitive intelligence, as the term suggests, is aimed at improving the competitive position of countries or enterprises in the markets. However, competitive intelligence has further developed within enterprises, where it focuses on increasing their knowledge in order to improve their position. While knowledge provides an added value, intelligence provides

[8] Martre, Henri. *Intelligence Économique et Stratégie des Entreprises.* La Documentation Française. February 1994.

power, as Helen Rothberg and Scott Erickson state[9]. In other words, competitive intelligence looks for what is needed based on what is known. Nevertheless, those authors do not consider other circumstances which, in our opinion, should be included as essentials of competitive or even strategic intelligence. The four essentials of the rhombus of intelligence shown in Figure 2 should be established for efficient decision making: determining assumptions (what we know that we know); latent knowledge (what we don't know that we know); information vacuum (what we know that we don't know), and the blind points (what we don't know that we don't know). We can conclude that intelligence activities, regardless of how they are labelled, must provide knowledge in every vertex of what we define as rhombus of intelligence. These aspects of intelligence are interrelated. We must point out that if we link the vertical points, i.e. "the things that we know", we will be within the strategic environment of an organization; if we link the horizontal points, i.e. "the things that we don't know", we will be in the axis of intelligence. "Working" in both directions, we would be able to provide intelligence with its strategic nature, which is what makes the competitive difference.

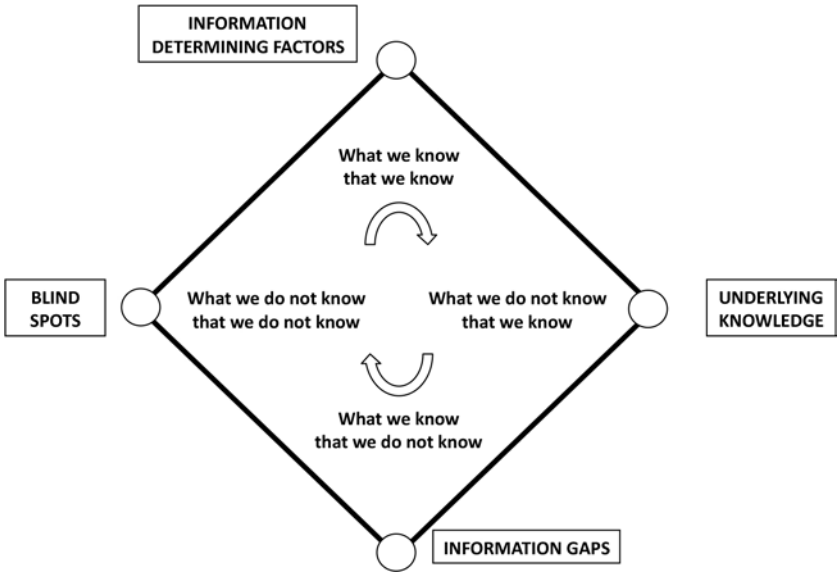

Figure 2.- Intelligence Diamond

Strategic intelligence will therefore encompass the above-mentioned, with the aim of providing information and knowledge in order to help decision-making processes of a strategic nature. It should be born in mind

[9] Rothberg, H. and Erickso, S. *From Knowledge to Intelligence: Creating Competitive Advantage in the Next Economy.* Butterworth-Heinemann/Elsevier. 2005.

that some pieces of information may lead to non-desired rumours or confusion, as shown in Figure 3[10], instead of knowledge.

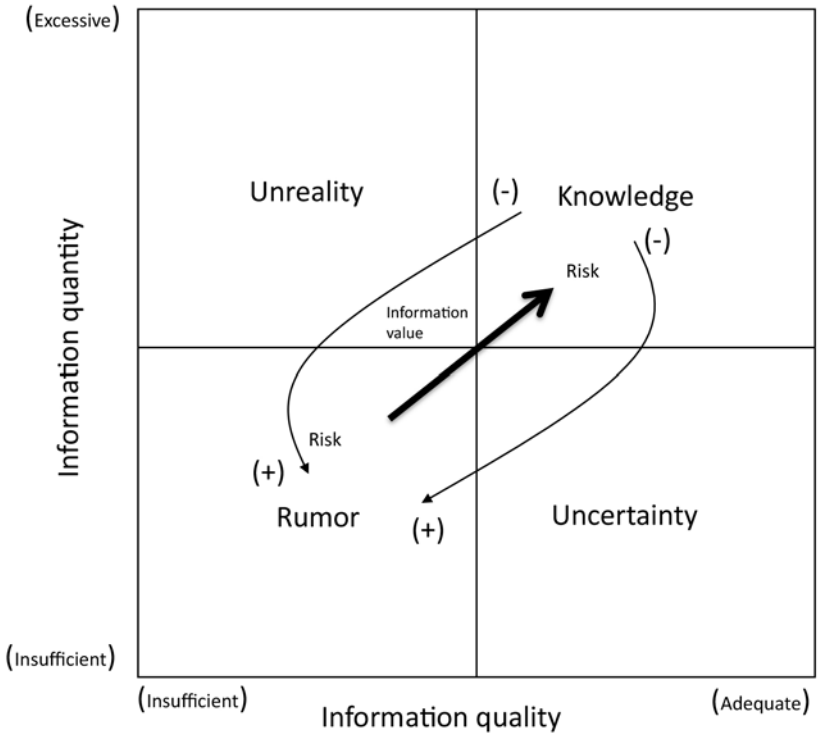

Figure 3.- Information, Rumor and Knowledge

Models of economic intelligence

the concept of economic intelligence and strategic intelligence will be used from now on without distinction, but assimilated to the French concept, i.e. to the *intelligence strategies for decision making in defence of the State or companies' economic interests.* It is in this context that we can make a foray into the situation of some of our neighbouring countries.

The situation in those countries could be assessed according to their potential positioning – Figure 4, which shows the different intelligence levels according to the objectives to be reached and their strategic level. Strategic intelligence appears in those areas where this view is fostered. Nevertheless, a summary description of the different systems will be

[10] Olier, E. La inteligencia estratégica al servicio de la competitividad. Global Security Magazine. Choiseul Institute, Spain. Summer of 2011.

made, taking into consideration the most developed countries: the U.S., Japan, Sweden, Germany, France and China.

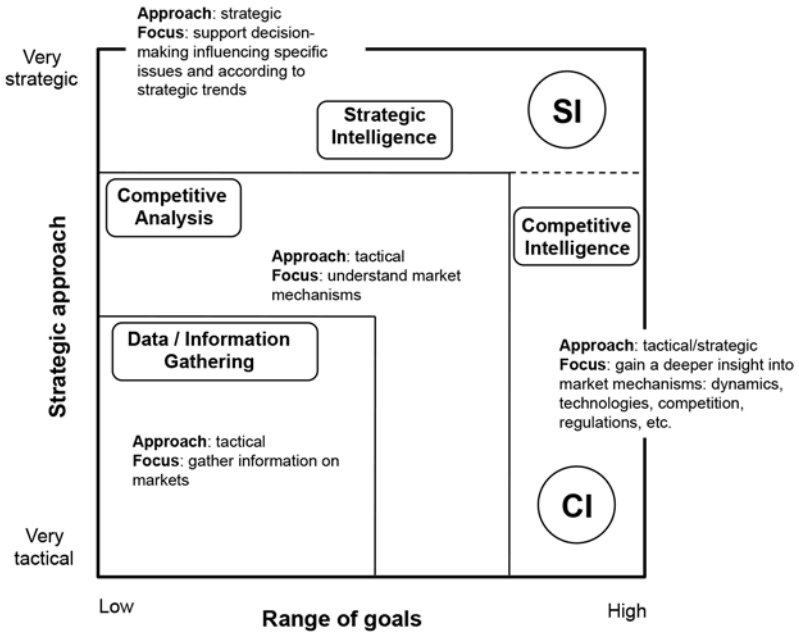

Figure 4.- Strategy vs Economic Intelligence Goals

In its global economic expansion, the U.S. developed a strategy of domination based on four pillars: military, technology, economy and culture, with the first two and the last two somehow interconnected. Its financial domination has been essentially based on currency. With the disappearance of the pound as a currency of reference at the dawn of the Second World War, the dollar decisively imposed itself on the markets. Firstly, because of its reference with gold: the price of gold as against the dollar is $35 per ounce. Secondly, for US preponderance in Bretton Woods Agreements and, especially, in the newly-born International Monetary Fund. With regard to its cultural domination, the Hollywood film industry, and even rock music, have been strong soft power tools capitalized on by Americans. All that encompassed by a perfect economy intelligence network linking the Pentagon with other multiple actors: federal agencies that involved, apart from traditional ones, the National Science Foundation or the Naval Research Office; powerful think tanks and even prestigious universities such as the MIT; security and intelligence companies such as Kroll or SRI International; transnational companies and even legal offices and lobbies. All under the formula that "national security" equals "financial security".

The Japanese, for their part, as previously mentioned, developed their economic intelligence strategy around the Ministry of International Trade and Industry (MITI). It is a "glocalization" concept that implies the need to protect its domestic market while fostering the expansion of international trade. The Japanese market has been traditionally very difficult for foreigners, and the large Japanese companies dominated the electronic or car international markets. It was a system of economic intelligence developed in seven strategic lines perfectly coordinated from "top to bottom", which involved companies and government services:

- Global and local approach to markets.
- Commercial penetration tailored to the economic context and each country's way of life.
- Very selective information policy, also with the participation of companies, on a daily reporting system basis.
- Long-term economic strategy.
- Integrated approach and coordination between large industrial conglomerates.
- Selective release of information according to levels.
- Training programmes in companies for young professionals, on a country-by-county-specialization basis, even mastering foreign languages and understanding local cultural events.

Sweden is a small European country that, however, understood the need to develop an economic protection system to boost the creation of large multinational corporations, while developing an international educational system based upon knowledge of at least three languages per student; a means to compensate their geoeconomic difficulties. In 2010, Sweden already had 30 companies in the Forbes 2000 ranking list: AstraZeneca in biotechnology, Telia Sonera in telecommunications, Ericsson in technology, Ikea in furniture and other household accessories, ABB in energy and capital goods, and so on. This would not have been achieved if it had lacked a policy and economic intelligence systems able to overcome many difficulties. A "bottom to top" plan opposed to the Japanese one, since the State is not the one to boost the system or the criteria to be applied, but companies and their information systems, which aim at improving their competitiveness.

The German system meets the characteristics of the German State: it has a federal structure, and there is intertwined three-level coordination: administrations, financial institutions and industries, a scheme that has given rise to natural alliances between industries and financial institutions, where trade unions take part as active agents in the march of economic progress. Agents that participate and do not protest, since their power lies not in the former postulates of class

struggles, but on becoming elected delegates in the definition of economic policies. Thus, it is possible to establish government alliances between parties competing from social democratic or Christian democratic positions, and also alliances between very different trade unions and businessmen, as well as with federal governments, where consultancy firms and political or cultural foundations also participate. A plan that leads to:

- A permanent coordination among the different economic communities: banks, industrial groups, etc.
- Flexibility and a coordinated approach to different markets.
- A coordinated use of German immigrants abroad.
- A search for German common interests beyond disagreements, which boosts intelligence activities.

In France, economic intelligence is a State issue. The well-known Carayon Report, presented in 2004 by the deputy M Bernard Carayon before the Finance Commission of the National Assembly, under the title "Strategy of National Economic Security", is a clear sign of the importance that these techniques and services have for French political forces. .

It was not the first time that the French State took the implementation of a national economic intelligence system very seriously. Nevertheless, deputy Carayon's report included some differences. In its introduction, it already mentioned a new situation:

"11-March attacks in Madrid – it said – *have painfully reminded it to us: Europe is a privileged target for terrorists. If the bombs represent an essential threat in our collective subconscious, the reach of the threats to our societies is even greater. After twenty years, our country – without being fully aware – has entered the age of information society. The production of national wealth currently lies, apart from in the quality of the people, in the bulk of legal, financial, commercial, scientific, technical, economic or industrial information. The threats against our productive structure have also evolved. Now, these are vaguer".*

He proceeded:

"The exacerbation of international competence transforms the strategic information of companies into a real "economic war".

The French system, for many years now, is perfectly designed and tailored to the new circumstances and needs. Apart from state agencies, leading companies on strategic intelligence, and a whole network of Chambers of Commerce that try to defend French interests inside and outside the country, participate in this system. It is a "top to bottom" structure, simpler than the Japanese one. It is an intelligence structure well interwoven in a context of very powerful and well-developed soft power all around French-speaking countries; a context of 58 Member States, along with

another 20 observer states. A clear commercial power supported by the hard power that comes from French military capabilities.

I will finish this review with a comment on China – a new and significant player. However, this country is always involved in international conflicts, and the US and England have systematically charged it with illegal practice before the WTO.

Moreover, China has a powerful and sophisticated economic intelligence, which integrates the following aspects:

- It is focused on the search of intangible properties: copyright, patent rights, etc.
- It includes networks of executives from Chinese multinational companies who work with big corporations selling them technology and services.
- It has a group of officials highly trained in cyber security (both for defense and attack) which works in close cooperation with universities.
- A decentralized system, with well-defined control commands and a vague division among intelligence services, companies and military defense structures.
- It has services to specifically protect strategic industries.

Strategic intelligence and economic security

Intelligence systems — particularly those of strategic intelligence — are essential in today's complex world. However, these systems and the organizations responsible for them usually focus on security. Thus, most of them focus on defensive espionage or on protection of facilities or services very valuable for the State, companies or other organizations. To this aim, they follow the intelligence cycle and underscore analysis as a means of specifying information and knowledge in order to make decisions. The scheme in Figure 5 is applied, taking the available data as a base to reach the knowledge that will make decisions easier, if made according to the intelligence cycle (Figure 6).

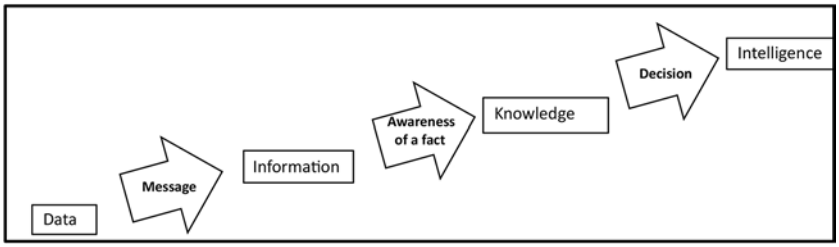

Figure 5.- Data to Knowledge Process

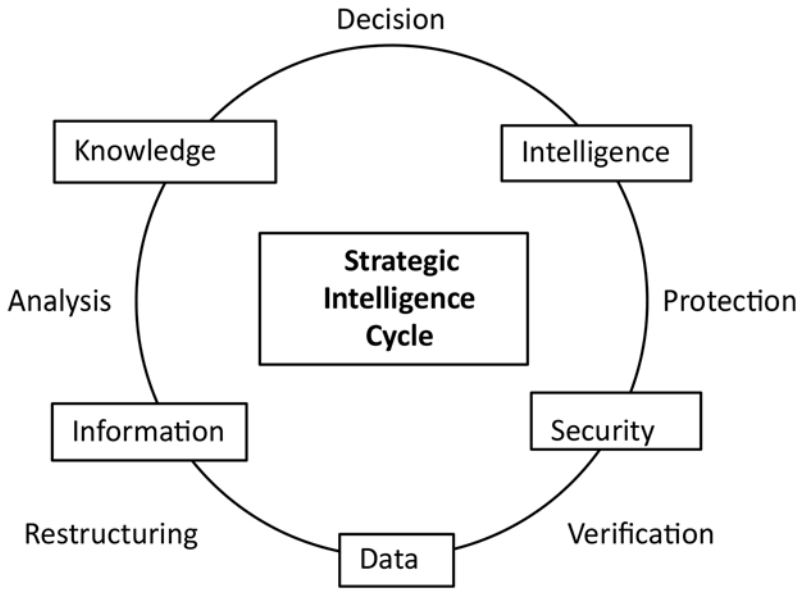

Figure 6.- Intelligence Cycle

However, a question which is obviated most of the time is that intelligence results from a strategic process; a model of economic intelligence cannot be implemented without strategy. If intelligence is *the capability of understanding and interacting with the milieu in order to act to obtain competitive advantages,* it could not be tackled without a defined and flexible strategy to adapt to the variations in the milieu. This process should take into account, at least, the following aspects:

- To define the strategy, including the approach and the task of the organization.
- To have the capability for abstract reasoning and understanding of the multiple interactions existing in complex environments, including a capability of judgment and knowledge development.
- To have the capability to detect substitute products or disruptive technology and to understand cultural or demographic changes.
- To develop the capability to be ahead of changes in regulatory or economic conditions of market dealers in order to launch offensive or defensive actions.

Intelligence must be firstly strategic and then economic. Then, it will be competitive or solely reduced to the analysis previous to knowledge acquisition through the appropriate techniques and technologies. These state level techniques will be different depending on the terminology: SIGINT, signals intelligence — the process of tapping electronic communications transmitted through radars, radio, or weapon-control-systems;

HUMINT, human intelligence that obtains information through persons; MASINT, that is to say, the use of intelligence to make reports on the targets; GEOINT, images acquisition including those coming from satellites; OSINT, intelligence from open sources, especially from mass media and the Internet and IMINT, or image creation through electronic systems such as radars or electronic optics-based systems, etc.

The strategic intelligence, then, will focus on the established strategic interests and on defining the goals to be achieved. These goals, in a geoeconomic context will be aimed at[11]:

- Making analyses of economic forecasts in complex competitive situations and understanding the political and geostrategic circumstances involved.
- Knowing the legal and regulatory aspects in detail and assessing foreign policy interests and international relations that could condition them.
- Developing strategic programs and monitoring the achievement of goals.
- Making a detailed analysis on economic and commercial forecasts in times of market changes or new political situations.
- Making assessments on threats and risks, and establishing timely criteria and security systems, both real ones and those coming from the Network.

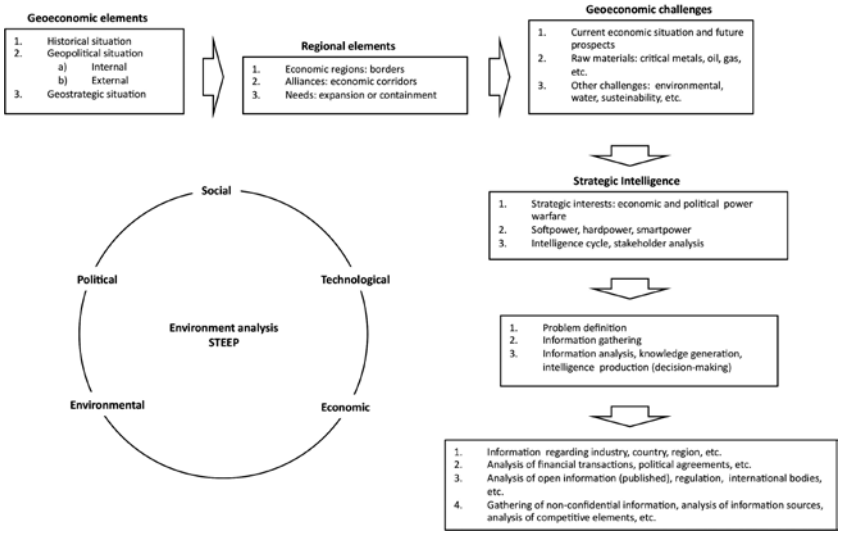

Figure 7.- Strategic Intelligence Methodology

[11] Olier, Eduardo. *Geoeconomía: las claves de la economía global.* Pearson-FT-Prentice Hall. 2011.

This scheme cannot be isolated from the analysis of the milieu, and should make a STEEP analysis considering all the elements: political and geostrategic factors, regional circumstances, strategic challenges, etc., as shown in figure 7.[12]

Here is where intelligence activities connect to security — economic in this case —. This would be the Swedish case. A small country, though leader in strategic and competitive intelligence, since it does not consider economic intelligence as a military category but as a means to ensure peace and economic prosperity. Therefore, Swedish multinational companies, banks and the government (and diplomatic missions abroad) share information and establish strategies to improve the country's competitiveness. Also universities, like Lund University, develop doctorate programs on these issues. Moreover, other small and middle-sized companies develop disruptive technologies while sharing information as an economic security and competitiveness strategy. This methodology shows the success of combining intelligence and economic security.

Influence as an essential element in economic intelligence

However, all the above-mentioned facts are not enough to develop an effective program on economic or strategic intelligence. Currently, the powerful countries and the most important companies stake their influence capabilities that go beyond what is commonly understood by lobby. In this sense, influence included within the context of strategic intelligence has three components that should not be implemented separately.

Therefore, strategic intelligence, regardless of its goals, is based on defining a strategy and is achieved by implementing coordinated actions in line with a program based on goal-achievement. If these goals are complex, they should not be considered a series of short-term actions, since strategy is not only that. Thus, the difference between lobby, corporative diplomacy and strategic influence can be expressed this way:

- Lobby, characterized by punctual, very short-term actions and that should never be used.
- Corporative diplomacy, characterized by actions carried out to develop a concrete influence program and uses of lobbies and biased information with the intention of misinforming.
- Strategic influence, characterized by a long term strategic program and carried out through lobbying coordinated actions (if necessary), social learning (actions in the socio-cultural field), advocacy (actions of public political influence), development of influence

[12] Olier, Eduardo. Ibíd.

networks, alliances, communication policies (and counter-communication or counterintelligence), and the large-scale use of social networks (under a defined strategy).

Thus, influence should be understood as the combination of performances — either direct or indirect, open or closed — regarding persons, groups, organizations and/or States with the aim of obtaining more credit or influence, and channeling decisions towards the desired direction[13].

Influence is, therefore, a power strategy that takes advantage of diverse tools, with communication strategy being of paramount importance, since communication helps to pass on messages based on arguments, far away from merely "transmitting news". Influence is, above all, a question of content: in order to be able to influence there must be a message, especially a coherent message.

And here is where different techniques and procedures come into play. Influence is part of the intelligence strategy. It is not an out-of-the-method activity. So, tools like economic diplomacy will have to be used. That is to say, a series of activities aimed at achieving favorable positions in the international economic field, including complex investment structures, markets, institutions, protection and economic security, and the whole global economic framework. This framework cannot be improvised; on the contrary, it requires structured and constant activity and medium to long term actions.

Likewise, social learning techniques are essential; they are aimed at achieving a socio-cultural influence and developing a soft power program that can be implemented in the field of Universities, NGOs and social networks. Social learning has not been designed only for states. Large companies like Microsoft, Google, Twitter, etc., use it profusely, especially in market-oriented techniques; this has resulted in the new concept of social marketing and in the appearance of network communicators: the community managers.

We are talking about a *strategy of power*. That is, a capability to "dominate" others through the capability to exert influence on their conducts and feelings. This has resulted, in the economic intelligence field, in a "soft" way of imposing a strategy aimed at achieving some commercial or economic control goals. And it has also resulted in a way of defending oneself earlier from the "attacks" of other competitors. All in all, this is a sophisticated implementation of the *soft power*, and considering the case, of the *smart power* or the *hard power*, according to Joseph Nye[14], who connects leadership with power under the three following meanings.

[13] Revel, Claude. *France, a country under influence?* Vuiver. 2012.

[14] http://www.hks.harvard.edu/netgov/files/talks/docs/11_06_06_seminar_Nye_HP_SP_Leadership.pdf.

- Leadership based on *soft power*, which transmits values on three levels:
- Political view: attractive for the followers and effective concerning ideals and capabilities.
- Communication: persuasive, both for close and distant people, through symbols and messages.
- Emotional: from the personal point of view: self-confidence and self-control and with regard to others by managing relations with charisma.
- Leadership based on *hard power*, which is directed toward a transactional leadership with:
- Organization capability: managing rewards, information systems and external and internal influence circles, both bureaucratic and institutional.
- Political skills: intimidation, pacts, purchase and competence.
- Leadership based on *smart power*, which will be a combination of the two above-mentioned. Deeply based on emotional intelligence to understand the development of the environment (which will require wide political capability) and make the most of the situation by anticipating the likely trends and, at the same time, adapting the style to the context and the needs of the followers.

Economic intelligence and cyber security

The current economic world cannot be understood without Internet technologies and developments. It is the environment where a real and true economic – or better said, financial – globalization occurs. It is where movements of capitals or financial operations are made in real time, moving foreign currencies and all kinds of financial operations from one place to another on the planet.

However, the *Net* is not just the virtual environment of economic affairs. It is also the virtual environment of the criminal affairs. Where attacks can be launched against critical infrastructures or where patents can be stolen or just where one can steal from unprotected or scarcely protected bank accounts.

As a reference, we can mention that one study carried out in 2011 about the situation in the United Kingdom[15] showed that the economic losses caused by the *cybercrime* reached as much as £27 billion the

[15] *The Cost of Cybercrime. A Detica Report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office*. February 2011. http://www.detica.com/uploads/press_releases/THE_COST_OF_CYBER_CRIME_SUMMARY_FINAL_14_February_2011.pdf

previous year. The cases ranged from industrial espionage to patent stealing, commercial bids stealing in international tenders, operations to acquire or sell companies, industrial design stealing, marketing campaigns, and a long list of information valuable in the business world. According to this study, the computer services companies were the most attacked, with losses reaching up to £2.5 billion, followed by financial services, with £2.3 billion and electronic companies, with £1.7 billion.

Actually, the exact economic cost of losses caused by the espionage from the *Net* is unknown. A former study prepared for the US Congress in 2003[16] raised the figure to US$226 billion all over the world; and added that losses due to attacks from the Net of highly valued companies could reach 5% of their value in the days following the intrusion. All this deployment materializes in different practices, all of them punishable, such as:

- Cyber-attacks on sensitive information of countries. This was the case of the "virus" *Stuxnet* that prevented the Iranian nuclear plant from coming into service.
- Information stealing by employees. The case of soldier Bradley Manning and the leakage of data to the page *Wikileaks*.
- Attacks on browsers as a means to access users' systems.
- File and database stealing, including bank *phishing*, *carding* or *skimming* systems and other similar techniques.
- Security in the cloud. All the systems placed in the Cloud Computing services add to the concern on the security of the "traditional" cyber space.
- Risks for smart telephones and tablets.
- Attacks on corporate networks.

More recently, in January 2012, the prestigious magazine *Wired*[17] published an amazing piece of news concerning the dimension of what they called *cyber-crime*. The piece of news referred to a lecture given in July 2011 in the American Enterprise Institute, Washington, by General Keith Alexander, director of the National Security Agency and International Security and the U.S. Cyber Command, in charge of protecting the country from cyber-attacks. The General warned about cyber-attacks that caused "the greatest transfer of wealth in history", and mentioned figures of statistics of computer safety companies as Symantec Corp. that insisted that stealing copyright in US companies caused an economic loss of US$250 billion yearly. He estimated that, at a global lev-

[16] Cashell, B., Jackson, W. D., Jickling, M. and Webel, B. *The economic impact of cyber-attacks. CRS Report for Congress.* Government and Finance Division, April 2004. http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.

[17] http://www.wired.com/threatlevel/2012/08/cybercrime-trillion/all/.

el, such a cost could reach a trillion dollars, nearly the amount of the Spanish GDP; urging the US Congress to develop an active strategy with enough means to ensure a cyber-defense program in the United States. Another report by the digital security firm McAfee Inc.[18] was also mentioned. This report shows the dangers of criminal activities in the Net for the economy.

Once again, China was mentioned as one of the most feared origins of these cyber-attacks; talking even about a *digital Pearl Harbor* that could paralyze the entire country. And the Bloomberg agency was told that a group of Chinese hackers, known as *Byzantine Candor*, had allegedly stolen classified information from about twenty organizations, including the renowned company Halliburton Inc.

This situation recently prompted the Spanish Ministry of Defense to establish, on the Minister's initiative, the *Mando Conjunto de Ciberdefensa de las Fuerzas Armadas* (MCCD), the Armed Forces' Joint Command for Cyber Defense. Other less developed countries, such as Colombia, have long been sensitive to these threats that are a reality today. Thus, it was there where the Minister of Defense was entrusted with the leadership of all the activities related to the defense of cyber space, creating under its command the colCERT (*Equipo de Respuesta a Emergencias Informáticas de Colombia*) in 2009[19].

This whole scenario affects the economic interests of any country or even company and has to be taken into account whenever a consistent strategy of economic intelligence is to be developed.

Goal of this strategic dossier

For the first time, the *Instituto Español de Estudios Estratégicos* tackles the problem of economic intelligence. Besides, the title of this Dossier leaves little room for doubt about its purpose: *The economic intelligence in a globalized world*. The globalization and the geoeconomic problems demand special attention to be drawn on this issue. Furthermore, this issue is also related to the needs of the national defense of any State. Economic intelligence is not only an issue of intelligence or diplomatic services posted abroad, it is an issue that, as we mentioned at the beginning of this article, is linked to any country's geoeconomic strategy and, therefore, establishes a new scenario of conflicts where the economy is set as the scenario of confrontation.

[18] *Unsecured economies: Protecting vital information.* http://www.mcafee.com/us/resources/reports/rp-unsecured-economies-report.pdf.

[19] http://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estudios%20sectoriales/Notas%20de%20Investigacion/Ciberseguridad%20y%20ciberdefensa.pdf.

However, although the issue of economic intelligence is wide, in this first Dossier, all problems are presented; the reader can find highly qualified authors on the subject we are dealing with.

Therefore, this Dossier starts with a general overview of the problem, focusing on the most complex element, which is strategic intelligence. Professor Díaz Fernández presents the historical evolution of strategic intelligence, moving deeper into the current situation, particularly in the new context aroused after the 11S attacks on the *Twin Towers* in New York.

Professor Harbulot, already mentioned in these pages, director of *l'École de Guerre Économique,* and acknowledged international expert on economic intelligence, widely certified economic conflicts, their causes and their context. In a chapter entitled *Estudio de la guerra económica y las problemáticas relacionadas* (Study of the economic war and related problems) he masterly clarifies this relation. Not only does he refer to the economic space, but he also frames it within the ideological field – a key geoeconomic aspect – since cultural and ideological factors are essential pieces in the movements of command and influence. It is a deep and very detailed study of all the context of economic war that gives authorized justification for the Armed Forces to take seriously this new dimension of non-armed but determining conflicts that occur in globalization.

Under this situation of economic intelligence, we will now deal with three essential aspects. The first one, mainly forgotten on many occasions, refers to the role that the Law has to play in these new scenarios. It is essential that, as in armed conflicts, economic war has its rules. Professor González Cussac stresses the "value" of the Law within the context of economic intelligence. This implies – according to his words – *developing self-protection and cooperation rules, apart from a regulation capable of offering a greater capability to compete on equal terms with the other countries*. In accordance with what González Cussac defines as a fourth-generation war. An interesting and new concept to be taken into account.

With this outlook, more focused on the legal aspect, the problems of competitive intelligence are dealt with. *La Inteligencia para Competir, nuevo paradigma en la dirección estratégica de las organizaciones en un mundo globalizado* (*The Intelligence to Compete, a new model of strategic management of the organizations in a globalized world*) is the title of Professor Fernando Palop's chapter. Once Professor Palop reviews the state of the art, its meaning and what is made in other environments, he also tackles the issue of influence, above-mentioned in this introduction as an essential tool in the practice of economic intelligence. This influence is connected to security, given that, as Professor Palop states, exerting influence is not only an activity of offensive nature, but essentially a defensive attitude on many occasions.

This Dossier ends with the contribution of Ambassador Henning Wegener. His knowledge of the problems occurred in the *fourth space* puts cyber security and the new concept of *cyber peace* into context.

We believe that the reader has this issue at sight, although being a first step in the way to better understand the context of economic intelligence achieves the goals set: providing a global perspective on such an important problem like this one in the current world.

Chapter I

The role of strategic intelligence in the modern world

Antonio M. Díaz Fernández
University of Cádiz

Abstract

The aim of this chapter is to explore what is meant by strategic intelligence in the early twenty-first century. Created during the Cold War, decision-makers' intelligence needs were faced by intelligence structures focused on avoiding strategic surprises. Generating real knowledge of the global scenario and even trying to modify it is a task that is now required by the intelligence agencies. Monitoring the environment without falling into the fallacy that technology can work by itself without the assistance of the policy maker, who must tell them where and what to look at, would be a fundamental error in the construction of a new model of intelligence. This new model will have economic intelligence as one of its key elements and will represent the struggle between nations and global corporations at the beginning of this century.

Key words

Intelligence, strategy, planning, strategic surprise.

Introduction

I hope that the reader who begins reading this section of the Strategy Dossier comes previously equipped with their own definition of strategic intelligence. If intelligence is based on prior warnings I honestly believe this should be the first of them. As Heidenrich states[1], although we all use the term 'strategic intelligence' extensively we would be no better off if we had to give a more or less refined definition of it. Probably, after a brief thought, we would say that it has something to do with decision making and strategy, in order to go on to define it by its opposite, that is, it is not the intelligence that is aimed at solving today's problems, it is not tactical intelligence, but it is that which goes further, that which is focused on giving support to a country's national strategy.

I also hope the reader will permit me not to enter into the usual accumulative relationship of definitions of the word intelligence that other authors in the past have already done so well[2], because the challenge of this chapter is two-fold: on the one hand, to define what strategic intelligence is in order to subsequently reflect on what its future will be, and on the other hand, in this regard, what place economic intelligence should occupy. Therefore, as a starting point, we can basically assume that information is equivalent to data and that intelligence is a prepared product that enables decision making with the least possible uncertainty. This reflection on strategic intelligence begins from here.

However, I do believe it necessary to begin with some prior reflection on what strategy, planning and management are. States are complex organisations that manage innumerable resources with a purpose and a use, the most basic of them all being to guarantee security and a food supply for its citizens. But even to guarantee these basic functions a strategy is needed, given that resources are limited and there will be other organisations (States or not) in continuous competition for them.

Paraphrasing the disappearing Cheshire cat in its dialogue with Alice, if we do not know where our organisation is going it makes no difference which path (strategy) we take. That is why I understand that strategy has to reflect the thoughts and actions of an organisation regarding its environment. That said, an organisation or a country can plan its future without necessarily having to commit to a formal plan; even though plans are made they do not have to be activated and turned into the path to be followed.

---

[1] Heidenrich, John G., *The State of Strategic Intelligence. The Intelligence Community's Neglect of Strategic Intelligence*, 2007 https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol51no2/the-state-of-strategic-intelligence.html

[2] Richelson, Jeffrey, *A century of spies*. Oxford, Oxford University Press, 1997; Lowenthal, Mark *Intelligence: From secrets to policy*, Washington DC: CQ Press, 2006.

But after a strategy is accepted its management – which is what a State does – would not have to be any more than putting the organisation at the service of the strategy; therefore the management itself does not constitute a strategy. Lesourne[3] maintained that "a strategic decision is either one that creates an irreversible situation for the entire organisation or one that anticipates an environmental change apt to provoke such an irreversible situation", although I do not believe that this assimilation is immediate, as the Theory of Organisations covers, it is certain that the variety of options available after choosing is successively limited. Hence the idea that "strategic management" is almost a pleonasm and that "prospective strategy", if not an oxymoron, is at least a contradictory although compatible term, since some prospects are strategic and others not. I am not speaking about strategic decisions, but about decisions taken considering that we have "strategic" intelligence, because without intelligence, strategy is merely an abstract game with blue and red teams on a board without defined limits.

We are so eager to label a concept or phenomenon with a new name – as if finding it a name would make all the qualities for understanding it stick – that we do not pay the necessary attention to its definition, interaction and functioning. That is why I consider the use of the term "strategic" inappropriate as an adjective to classify any concept, idea, process, relationship or product that is relatively important. Although this is almost impossible to get around, what we can do is prevent its immediate association with irreversible decisions that an organisation adopts. Behind this suspicion there lies a certain mistrust motivated by the difficulty that I have qualifying the word "intelligence" with complements that are already typical, which are inherent to it; because if it is not proactive, what is it if not intelligence? The problem with "strategic", as Heidenrich states[4], is that it is difficult to abandon decades of routine during the Cold War of abusing the use of the strategic concept and, what to say about its direct assimilation in the "long term".

The always helpful official documents do not throw any light on what strategic intelligence is. From the few official definitions that we can find, that of the Pentagon tells us that it is "the intelligence that is needed for the formulation of strategy, policy, plans and military operations at a national level and on the battlefield"[5]. However, this definition stands alone in the American government outlook since not even the two basic documents for North American consumers of intelligence include a definition

[3] Lesourne, Jacques, "Plaidoyer pour une recherche en prospective", *Futuribles*, No. 137, November 1989.

[4] Heidenrich, *opus cit*.

[5] Entry "Tactical Intelligence". Joint Publication 1-02 (JP 1-02), *Department of Defense Dictionary of Military and Associated Terms*, Washington, Department of Defense, 12 April 2001, p. 526. http://www.dtic.mil/doctrine/new_pubs/jp2_01.pdf

of this concept[6]. In addition it has an essence very near to that which we might have found during the Cold War, an era with very different figures and needs to those at the beginning of the 21st century.

Nor does a text that, a priori, should reflect it, *ONCIX: Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage (2009-2011)* of October 2011, find space to define it[7]. Even an academic such as Jan Goldman[8], who dedicated one of his works to specifying the terminology used in the study of intelligence, does not provide clarity in his dictionary *Words of Intelligence*. The word *strategic intelligence* says to us that it is intelligence that is needed for the formulation of political and national plans at a national and international level and that its components would include aspects such as biographical, economic, sociological, transport, telecommunications, geographical, political and scientific and technical intelligence data but does not provide added value that may be relevant for the debate that I am trying to establish.

A representative case of the changes in the last decade, at the time, appears in Spain's very famous Defence White Paper of 2000[9] that brought us into the group of countries that were developing these types of thoughts. In our baptism into publicised defence planning we can see how reference is made 217 times to the words "strategic" and "strategy". From here I would conclude that we will find an intense and extensive reference to intelligence as an essential tool to deal with its development; however the word "intelligence" does not appear in the entire text and we have to be content with the 66 times where the term "information" appears. Without doubt, use of the word "intelligence" was not usual more than a decade ago, still very marked by the Cold War halo of secrecy, but its non-existence and therefore how our *policy makers* thought that "strategy" should be carried out is still remarkable.

Perhaps the White House *National Intelligence Strategy* of 2010[10] provides us with a clue, in which the only reference, indirectly, suggests to us that: "strategic intelligence [...] informs executive decisions since this is support for the decisions on internal, national and local security, tribal governments, our troops and essential national missions. We are work-

[6] Neither *U.S. National Intelligence: An Overview*, 2011. http://www.dni.gov/files/documents/IC_Consumers_Guide_2011.pdf nor the older *CIA: A Consumer´s Guide to Intelligence*, 1999 include it.

[7] http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf

[8] Goldman, Jan, *Words of Intelligence: A Dictionary*, The Scarecrow Press, Oxford, 2006.

[9] White Paper on Defence http://www.defensa.gob.es/politica/seguridad-defensa/marcolegal/

[10] *National Intelligence Strategy.* White House 2010, pp. 15 http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

ing to improve integration into the intelligence community at a time of strengthening the capacities of our intelligence community members. We are strengthening our collaboration with foreign intelligence services and maintaining strong links with our nearest allies". But above all because it includes an important element when it maintains that "the security and prosperity of our country depends on the quality of the intelligence we gather and the analysis we conduct, our ability to evaluate and share this information over time and our ability to counteract threats".

It includes two aspects such as security and prosperity. Regarding the first, we can assume a certain impact of a preventive nature attributed decades ago to intelligence, that is, to avoid the strategic surprise that Posner[11] analysed so well, but the second has always carried less weight, significantly less. However, we can find official documents from the seventies in which it is assumed that "our foreign policy can benefit if a more careful and analytical examination is conducted on the reality of other States"[12]. And it is specifically in economic intelligence where development makes more sense, although not in a peaceful way as we will see later. This document to which I refer, declassified in 1976, about economic intelligence states that a systematic and periodic review of high-level consumer needs is necessary, which shows that at a strategic and economic intelligence level we are speaking about high-level "civil" consumers, in other words the government.

I anticipate that for me the key to the present and future of strategic intelligence is in the debate that Kent and Kendall maintained at the end of the forties in the last century. Kendall[13] maintained that strategic intelligence consisted of "helping politically responsible leaders to reach their foreign policy goals, by identifying the elements susceptible to North American influence". At the same time, Sherman Kent was accused by Willmoore Kendall of having a "compulsive preoccupation with prediction and with the elimination of surprise from foreign affairs". What emerged from this and other accusations were differing visions of this new political element as intelligence was then.

In essence, Kendall saw intelligence as support for political decision makers to help them affect the progression of events so they could understand the operational factors on which the United States could have a certain impact. And this is what we speak about at the beginning of

[11] Posner, Richard A., *Preventing Surprise Attacks: Intelligence in the Wake of 9/11*, Rowman & Littlefield, New York, 2005.

[12] Letter from E. Richardson to W. Simon. "Re: Intelligence support for economic policymaking" (5 pp. in *Frank Zarb Personal Papers*. 12/20/76. DECLASSIFIED MATERIAL) http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

[13] Kendall, Willmoore, "The function of intelligence", *World Politics*, vol. 1, No. 4, July 1949, pp. 542-552.

the 21st century if we want to speak about something that is strategic intelligence, not preventing strategic surprises but understanding the environment to plan ahead for it and to some degree, configure it so that our foreign policy – and its economic dimension – can be developed and can generate prosperity for our country.

The other great theorist of the era, Washington Platt[14], focused on a military intelligence model, at a strategic level and not of a tactical nature, and therefore it does not help us in our current discussion, despite having been his most important contribution. In 1980, Harry Ransom[15] asked whether it was specifically "strategic" intelligence that guided the United States foreign policy, a question which only recently could begin to get a positive response.

There was a ray of light on the role of strategic intelligence in the 1993 *National Performance Review*[16] coordinated by vice-president Al Gore, where the then director of the CIA, John Deutch, confirmed that "the United States efforts in intelligence must provide decision makers with the necessary information on which to base their decisions with regard to defence abroad, economic policy and protection of the United States' national interests against foreign attacks". This agreed with Swenson and Lemozy[17] in that "strategic" attached to "intelligence" breaks down the most comprehensive concept – broad and widespread – of "intelligence for foreign policy", but I cannot agree with them that strategic intelligence excludes or supersedes the contribution of the diplomatic body in this process, although its role and structure evidently would have to be modified as the report by the ambassador Melitón Cardona, to which I will refer later, stated.

If we assume that strategic intelligence helps to provide context, develops national interests and delimits our problems and goals, the fact is that the current rapid cycles of political events mean that the political consumer requires an intelligence product that is not typical of strategic intelligence, that is, long-range, meaningful products, but rather early warnings against potential strategic surprises. In other words the recurring cycles mean that there is no space for strategic thought and that analysts and consumers are focused on the quantification of a product with little space for reflection. Therefore, in my opinion, a much more

[14] Platt, Washington, *Strategic intelligence production: Basic principles*, New York. Praeger, 1957.

[15] Ransom, Harry Howe, "Being Intelligent about Secret Intelligence Agencies", *The American Political Science Review* Vol. 74, No. 1 (Mar., 1980), pp. 141-148

[16] *National Performance Review*, 1993, http://www.fas.org/irp/offdocs/npr_sep93/index.html

[17] Swenson, Russell G. and Lemozy, Susana C. "Democratización de la función de inteligencia. El nexo de la cultura nacional y la inteligencia estratégica", *National Defense Intelligence College*, Washington DC., 2009.

intense presence should be demanded from strategic intelligence at the beginning of policies, at agenda setting and the prioritisation of goals, in other words at the design phase and not limiting it to implementation, because that way we will be using it mainly as an early warning against strategic surprises.

This complaint is covered in the report issued by the Commission on Arms of Mass Destruction in Iraq in 2005 that indicated that "managers and analysts of the intelligence community have, on repeated occasions, expressed their frustration at their inability to spend time on research and thought in the long term. This problem is intensified with the current incentives system for analysts where they are often rewarded for the number of reports they produce more than for the substantial knowledge or depth of their output[18]. A more recent episode we have is with the so-called "Arab spring", where the confusion it created in foreign ministries is only understandable due to the absence of quality strategic intelligence, of reliable knowledge about its roots and determining factors, not about tomorrow, not even about the day after tomorrow but about the essence of a phenomenon that will assist us in understanding its appearance and progress.

As a result, when we speak about the state and therefore the future of strategic intelligence we should not concentrate on the economic or military nature: strategic intelligence remains above these dimensions because it is more than a type of intelligence from signals, open resources or technique; I understand it is as evolution of this. Perhaps it will be better to proceed to understand how it has evolved and what its elements are in order to understand its possible future. And to understand what we are referring to and to try to conceptualise strategic intelligence and suggest a future for it, bear in mind the Kent Trinity: intelligence as an organisation, product and process, but firstly it is important to comment, however superficially, on the scenario in which strategic intelligence and its economic dimension should occur.

There are no longer any blue or red draughts on the new board

There are no doubts about what the current threats are, nor that they are different from a decade ago and from what they will probably be in the future, even though they may be reduced. And what is certain is that the markets – in that vague name – are the threats now. In modern democra-

[18] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President* (Washington, DC: Government Printing Office, 2005), Chapter Eight: Analysis, p. 175. http://www.gpo.gov/fdsys/pkg/GPO-WMD/pdf/GPO-WMD.pdf

cies, as Barry Buzan[19] saw, military conflicts lack logic so the polyarchies do not suggest military confrontation between themselves. However, it is entirely rational to put pressure on your business partners, suppliers of raw materials, bet against your public debt and ensure that your companies are at a bargain price on the stock exchange and can be bought by foreign capital; which without doubt Clausewitz would certainly consider a kind of "war using other means".

The European Security Strategy (ESS)[20] adopted by the European Council in December 2003 took responsibility for the European project in relation to global security, the axis of a security strategy for Europe. It pointed out that "the security context that gave rise to the end of the Cold War is characterised by ever greater opening of borders that permanently link internal and external security aspects". The ESS supports preventive agreement, an efficient multilateral strategy and the extension of the rule of international law. This strategy – that is more a *policy paper* – deals with how to make the European Union more capable, supporting an "ascending" approach, in other words, the focus is on how to increase the security of people considered individually in different parts of the world. The report develops both a set of principles on which European security policy should be based, and the skills needed to make a credible contribution to global security, on which its own security depends, but little attention is paid to the instruments to make this contribution effective.

The European Union brings the concept of Human Security to the table – as it is called in the ESS – and which is still another security concept; a narrative that reflects the goals and means of foreign policy and of highly diversified security and that is focused on different figures and aimed at varied audiences that, ultimately, would be too vague and difficult a concept. However, those who from the middle of the nineties defended Human Security maintain that unilateralism is not possible and they understand the need to develop new instruments as well as persistence with internal and foreign dimensions. If the European Union wishes to continue with this using this security concept, intense thought will be essential about how to use intelligence, not only strategic intelligence any more, but others in full development such as police-criminal.

However, ultimately, at a European level we do not have an operational concept such as that of *Homeland Security* which the Americans are consolidating; that is why, from Europe, they have continued to use others such as internal security, public security or domestic security. Going deeper into this concept should not lead us to close the con-

[19] Buzan, Barry, *Security: A new framework for analysis*. Boulder, London, Lynne Rienner Publishers 1998.

[20] *A Secure Europe in a Better World. European Security Strategy*, 12 December 2003. http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf

cept without fully understanding it. Therefore, some extensively speak about "protection space". This is how the European Union is perceived, its security perspective and the scenario from which to protect the European citizens.

Therefore, we would be advocating comprehensive security, definable as a system of defensive and proactive action that goes well beyond the classic dimension of national security, highlighting the need to influence – to guarantee said security – the energy, sanitary, food, environment, infrastructure, technological, military and internal security systems, which must be created in coordination using public management instruments in the political-institutional, technical, diplomatic and intelligence fields for the development of preventive strategies as well as the executive responses of varied scope with the ultimate goal of guaranteeing the meeting of people's basic needs and consumers' security, defending human rights and protecting the exercise of democratic rights.

Therefore, we have not only a national focus, but a global one. The majority of threats that the powers confront are global in origin and in results. That is why global cooperation has clearly been regionalised. The 2004 report *A Human Security Doctrine for Europe*[21] maintains that European citizens' security cannot be separated from human security in any part of the world and that the European Union therefore has a key interest in the development of capabilities that contribute to human security worldwide. They maintain that Europeans cannot be safe whilst millions of people live in unbearable danger. Where people live with anarchy, poverty, exclusive ideologies and daily violence there is fertile ground for criminal networks and terrorism and drugs and arms are exported or transported to the European Union from these regions in conflict.

Therefore, it is not difficult to conclude that we are dealing with more extensive security requirements than intelligence had to report on scarcely two decades ago. Using the different White Papers and reports on security scenarios, various States, the same as the European Union, have been reflecting on their future. In a kind of self-analysis these documents enable us to see how threats are seen from the Union and the member States. For example, in March 2008 the United Kingdom made public its new National Security Strategy[22], which comprehensively included a revised version of previous reports and initiatives. This new initiative will be considered original and welcome in the British approach to international

[21] *A Human Security Doctrine for Europe: The Barcelona Report of the Study Group on Europe's Security Capabilities*, 15 September 2004, http://www2.lse.ac.uk/internationalDevelopment/research/CSHS/humanSecurity/barcelonaReport.pdf

[22] *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, 2008. http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf

security but doubtful whether it will effectively overcome the traditional visions of certain aspects of international security and its consequences for the internal security of the country.

This *National Security Strategy of the United Kingdom* with the suggestive general heading of: *Security in an Interdependent World* establishes that the threat from the Cold War has been replaced by a series of different but interconnected risks and threats, at that time, international terrorism, weapons of mass destruction, conflicts in fallen States, pandemics and international organised crime. These would be interconnected by a series of underlying factors, including climate change, fighting for energy sources, poverty and weak governance in some States, demographic changes and globalisation, which does not differentiate it from other national reports.

The vast majority of powers have developed their strategic security scenarios to run for an average of 20-25 years. A review of them indicates that they are all based on comprehensive security but they find it difficult to move away from the design and the mechanisms of a traditional military threat, although they are beginning to do so. The National Defence Directive 2012 was drawn up clumsily, as analysed by Arteaga[23], who continues reflecting on the evolution that has occurred in recent years when the limited planning focused on defence efforts, understood as purely military. This has changed since the purely military threat has been eliminated and a plethora of others have now appeared.

The 2011 Spanish Security Strategy is joined to this vision of specific risks but also of general goals when it indicates that "we also have strategic interests that are related to the achievement of a peaceful and safe environment: consolidation and good operation of the European Union, establishment of a stable and just order, of peace, security and respect for human rights, preservation of freedom of exchange and communications and constructive relationships with our neighbours"[24].

This Spanish Strategy speaks about risk stimulators (globalisation malfunctions, demographic imbalances, poverty and inequality, climate change, technological hazards and radical non-democratic ideas) that coincide with others such as "La Seguridad Interior: España 2020" ("Internal

[23] Arteaga, Félix, "La Directiva de Defensa Nacional 1/2012: tiempos de cambio para cambiar a tiempo", ARI 58/2012, Real Instituto Elcano. http://www.realinstitutoelcano.org/wps/portal/rielcano/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari58-2012

[24] *Estrategia Española de Seguridad: Una responsabilidad de todos*, Gobierno de España (*Spanish Security Strategy. A responsibility for all, Spanish Government),* p. 16 http://www.lamoncloa.gob.es/nr/rdonlyres/d0d9a8eb-17d0-45a5-adff-46a8af4c2931/0/estrategiaespanoladeseguridad.pdf

Security: Spain 2020"), published some time before[25]. At the same time, it develops the threats that Spain must confront, such as: armed conflicts, terrorism, organised crime, economic and financial insecurity, vulnerability in energy, increase in weapons of mass destruction, cyber threats, uncontrolled migratory flows, emergencies and catastrophes and infrastructure, supplies and critical services. But these "national" goals match the international ones such as that of the *Reflexion Group for the Future of the European Union*, chaired by Felipe González in 2010 and therefore we are not faced with a myriad of new threats but, in any case, with an increase or decrease of them on state security agendas, if they exist as such.

Beyond the relevant cases of the great powers that place an extra emphasis on the global interests that they have, a necessary review of the White Papers and national security doctrines since 2001 show us agreement on four great threats: i) terrorism ii) organised crime iii) an increase in weapons of mass destruction and iv) energy-climate problems. It is true that, to a large extent, all of them try to avoid an approach based exclusively on defence-military terms and almost entirely connected to direct threats to the State. As López Espinosa[26] indicates, a new National Security concept is emerging in this direction, as a better concept that would move the centre of attention to others such as national defence or internal security. A new policy has not been created, nor have others been broadened in a sectorial nature – as a main feature – all the existing ones are adapted to the directions of the new strategy in a process of adjusting instruments, capabilities and State resources, including the economic element.

But within this clear change in national, international scenarios and, closer to home, Europe, the content of the most recent European Union documents does not appear to assign a new role to intelligence. Therefore, in the Stockholm Programme[27], we see how the European Council calls upon the Council and the Commission to define a strategy based on "reflection of a proactive and intelligence-led approach"; without a doubt this is positive but it is essentially the same approach. The 2010 Draft Internal Security Strategy for the European Union[28] indicated that "our

---

25 Jaime Jiménez, Óscar and Díaz Fernández, Antonio M., *La Seguridad Interior: España 2020*, Fundación Alternativas, Madrid, 2009, http://www.falternativas.org/la-fundacion/documentos/libros-e-informes/la-seguridad-integral-espana-2020

26 López Espinosa, María de los Ángeles, "Inteligencia y terrorismo internacional. Un panorama de cambios", *La inteligencia, factor clave frente al terrorismo internacional*, Cuadernos de Estrategia No. 141, Instituto Español de Estudios Estratégicos, Ministerio de Defensa 2009, pp. 197-239.

27 *The Stockholm Programme: An open and secure Europe serving and protecting citizens*, 2010. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:en:PDF

28 *Draft Internal Security Strategy for the European Union: "Towards a European Security Model"*, 8 March 2010, http://register.consilium.europa.eu/pdf/en/10/st07/st07120.en10.pdf

strategy must therefore emphasise prevention and anticipation, which is based on a proactive and intelligence-led approach as well as procuring the evidence required for prosecution. It is only possible to bring successful legal action if all necessary information is available".

To this reflection, which extends the security scenario at a global level, we can add that of the *National Intelligence Council,* which has updated its previous precautions by producing those with a time limit of 2030[29]. The three differences compared to the previous report would be the strong appearance of three key variables: i) the globalised economy, ii) demography and iii) new players (China and India). The report also suggests four possible scenarios that would be more important for a world power than for other countries, at that time:

- Scenario I entails a world in which the new powers replace the West as world leaders (food shortages, post-petroleum era, geopolitics of energy, water and food and climate change)
- Scenario II "surprise" or impact of the lack of attention to worldwide climate change (conflicts over power, reduction in instability, nuclear weapons, new conflicts over resources, terrorism, Afghanistan, Pakistan and Iraq, etc.)
- Scenario III, intense rise in emerging powers (BRICS) entering into a dispute over vital resources as a source of conflict (preparation for changes, multi-polarity without multilateralism, world networks, etc.)
- Scenario IV, expansion of policies that will no longer be domestic, and therefore the establishment of the environment on the international agenda overshadows governments.

And the most appropriate thing would be to finish this scenario into which strategic intelligence should be moved with the 2008 French report. This document has few conceptual novelties and is, in my opinion, the best in the "strategic" planning of documents of its kind. The *Défense et Sécurité Nationale: Le Livre Blanc*[30] states that: "development of knowledge and the capacity for anticipation is our first line of defence. [...] The battles of the 21st century will take place within the field of information, knowledge, people and societies. [...] Politicians must have access to all data that will serve as a basis for their decisions and to evaluate situations with full sovereignty. [It must be assumed that] public powers are doing everything possible on risks analysis for the future and trying to prevent them by preparing the means to confront them." Therefore, it is closer to the role that I understand must be assigned to strategic intelligence at the beginning of the century.

[29] *Global Trends 2030: Alternative Worlds* http://www.dni.gov/index.php/about/organization/national-intelligence-council-global-trends

[30] *Défense et Sécurité nationale: Le livre blanc 2008*, p. 66. http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/084000341/0000.pdf

The redesigned Kent trinity

Organisation: the Matrix has already been created

Intelligence organisations have had to suffer in the evolution process from the first intelligence system the world relied on: the Cold War model that was also very similar on both sides of the Berlin Wall. From then on and until today all intelligence models have been based on synthesis, with different roles and commitments from the armed forces, the police and the intelligence services although, obviously, with the latter having a central role as the more specialised structure. More specifically, the main characteristics that, in my opinion[31], defined the intelligence model that arose during the Cold War – and its specific understanding of "strategy" – were: i) the practice of misinformation, ii) the mass use of technology for controlling citizens, iii) the precedence of efficiency over citizens' rights and freedoms, iv) the presence of the intelligence services in all walks of life and v) the carrying out of covert actions.

This was clearly not a structural model for the challenges that would come at the end of the Cold War. The fall of the Wall meant an objective modification in intelligence requirements and the volatility of the Eastern Bloc produced two different dynamics. One of them wanted to understand that it was time to collect the "dividends of peace" and to use the funds invested in security and intelligence to other commitments even supporting the abolition of the army. The other united those who saw the need to change existing systems to meet the new reality full of threats that of necessity had to replace those that expired. Various commissions and working groups were set up, mainly in the United States, to discuss and deal with the emerging situation. Other countries did not think about the subject beyond some minimal contributions from some thought centres and the voluntary signing of limited cooperation agreements between the intelligence services of different countries to control the increase in weapons of mass destruction and the nuclear suitcases that might come out of the old Soviet Union.

During the decade between 1989 and 1999 the intelligence services were overloaded with a multitude of new and emerging commitments: the verification of arms reduction treaties, investigation into genocides, protection of communication networks, money laundering, organised crime, terrorism, etc. This responsibility that was so disproportionate to the intelligence services' goals was not planned but occurred gradually through a need, given the lack of alternative structures to which to assign them. Structurally the necessary thought had not taken place so that the

[31] For a more extensive analysis see, Díaz Fernández, Antonio M., "La adaptación de los servicios de inteligencia al terrorismo internacional", ARI 52/2006, Real Instituto Elcano, 2006.

services could undertake these missions with the necessary guarantees, leading to an incredible saturation of time commitments that wasted the chance to adjust to the developing scenario. This meant a delay of ten years for the services to adapt to the anti-terrorist fight. This decade was the key time for adapting intelligence to meet the requirements of the 21st century. But after this delay there was no longer the chance to think about whether it was more appropriate to undertake an evolutionary or revolutionary intelligence process; now the reaction time was too minimal to consider revolutions whose transition cost could only be acceptable when there is a truly peaceful scenario ahead and, unlike now, there were no individuals ready to sacrifice themselves at any time in the very heart of our cities.

This lack of an updated intelligence model led to 9/11 2001, tragically representing the end of the brief and superficial period of stability that came with the fall of the Wall. The new intelligence model that should have replaced that of the Cold War to contend with the threats relating to the era was still not ready, nor had the window of opportunity opened so that any of those designed by congressmen and the agencies could be implemented. To a large extent its absence was because it had been worked on in such an unhurried way that the State ended up being incapable of anticipating the new type of threat.

But all this meant – and means – a regret that the urgency of the moment does not allow us to spend time on. What is certain and obvious is that given the absence of a finished model the States had to turn to a refuge model which they were aware of from the Cold War and apply an incrementalist element to it in the hope that this would be useful for adapting it to the new situation. Both the greater number of resources and the technological skills that have appeared since this model was fully in force during the previous decades would have to be that incrementalist element that some considered sufficient for updating this model. In short, this signified that all the model's characteristics in the Cold War appeared again but with greater intensity. This model was scarcely useful for the needs of politicians during those years and would hardly, and only then by pure chance, be able to help in the growing anti-terrorist fight.

This emergency model applied after the attacks against the United States are characterised, in my opinion, by the following elements: i) the practice of misinformation, ii) the mass use of technology for controlling citizens, iii) the precedence of efficiency over citizens' rights and freedoms, iv) the presence of intelligence services in all walks of life, and v) the carrying out of covert actions. Structural reforms aimed at improving the "connecting the dots" that the report of 9/11 marked as one of the intelligence community's errors; that is, the State had the data but internal wars and lack of coordination prevented their appropriate treatment and resulted in the failures that led to the September attacks. But again, the underlying

idea is to improve the intelligence that prevents surprises; a physical or virtual Pearl Harbour, as this will be what we will see within a few years.

It is true that some opinions, including those of the 9/11 report, proposed the importance of a better understanding of the world at the beginning of the century to be able to organise intelligence in the most appropriate way. It is also true that in the period immediately after the 9/11 attacks some reforms occurred in some countries such as Austria, Holland, Spain, Latin American States and the Eastern Bloc. However, their dynamics and motivations were different to those generated by those attacks and relate to typical national contingencies. In some cases, such as Holland, going back to decisions taken years before that had led to dismantling foreign intelligence, in Spain a system generated during the transition to democracy had to be adapted and regulated within the range of the law without a prior model and by mutual agreement of bureaucracies. The Latin American countries sought to coordinate their domestic and foreign security agencies under a system that usually has the name "National Intelligence System", a structure already established in Portugal in 1986, but with similar and limited results.

Eastern Europe modernised its intelligence structures and gave them professional status after the culmination of its democratisation processes and they also reproduced this "National Intelligence System". However, Eastern Europe has a peculiarity since they keep police powers, the same as in Colombia until 2012 and as the Dominican Republic considered establishing. In addition, some States used the fact that they had to make their own reforms to introduce some original elements into their systems, such as making their units flexible and reducing the vertical nature of the service's structure so as to deal with more changeable environments.

It is this lack of adaptation that explains the failures of 9/11 and subsequently led to the attacks in Bali, Madrid and London, highlighting the lack of an alternative model and the overriding need to redevelop intelligence systems. The prevention strategies therefore turned into the basis for security in the 21st century, in the field prepared for the intelligence services and, without any doubt, into the basis for future security systems. Therefore, it is a fact that the intelligence services must snap out of their inertia and turn into structures more adapted to the changeable needs the 21st century brings, and be, shall we say, more strategic?

Reorganising the intelligence community so that it can adapt more quickly not only requires changes in organisational systems. In the United States, since 1947, when the intelligence system was established, nineteen commissions, committees and panels have tried to modify the role of the centralised authority of the director of the intelligence community and even proposed the creation of a director of intelligence. As early as 1985, the Turner proposal suggested the creation of a director for the in-

telligence community and what has happened since then has been more or less feeble support for this option. In fact, the reforms proposed by Boren-McCurdy in 1992 did not manage to get approval due to rejection by the Department of Defence; this is something that the members of the subsequent Aspin-Brown commission learned from. They avoided proposing it with too much bluntness and so softened this aspect by proposing the creation of two deputy directors to directly assist the director of the intelligence community with his tasks. Finally, the 9/11 Commission recommended the creation of a new authority, coordinating all the agencies and creating the position of National Intelligence Director. In short, many of the debates that are taking place today are another wave of proposals that have taken more than thirty years to occur.

Even when managing to introduce major advances in the construction of the intelligence community, the problem is that both the 9/11 Commission and the opinions and studies conducted in different countries have based the adoption of measures on preventing another attack similar to 9/11 but not to adapting structures to a new type of threat, organised crime for example. Without doubt this focusing of intelligence on counter-terrorism has taken attention and efforts away from other no less serious and long-term threats such as organised crime. It has to be understood that the incentive of intelligence reforms is the fight against terror, but it cannot be their only goal[32].

A potential loss of budget and influence by opening up intelligence work to other agencies from a broader intelligence community largely explains the Department of Defence's opposition to any change. What is very remarkable is that the great failures in military intelligence during the first Gulf War led American politicians and military to wish to transfer resources of "strategic" intelligence to the tactical, which is applied to combat; that is, not to redirect but to have more tactical intelligence. It has to be understood that during these years the Pentagon had put the majority of its total budget into intelligence, something that it did not want to give up and that would subsequently condition the definition of counter-terrorism as a military problem, for example. The Department of Defence's influence on the modifications that could have been undertaken to the intelligence system should not be underestimated.

The main study about the necessary evolution of the intelligence community occurred under the auspices of the Aspin-Brown commission (1994-96). This was a very ambitious task of great interest that covered all those dimensions that had to be modified or adapted into the intelligence systems. However, the lack of political leadership and, once again, strong opposition from the Department of Defence prevented their application.

[32] Díaz Fernández, Antonio M., Revenga, Miguel and Jaime, Óscar, *Cooperación Europea en Inteligencia: Nuevas preguntas, nuevas respuestas*, Aranzadi, Pamplona, 2009.

However, Holshek[33] makes a personal interpretation of the North American intelligence community evolution when he states that:

> *"The national security system the United States had finally adopted was more anticipatory, collaborative, agile, and innovative. It was more capable of combining all elements of national strength and power, integrating intelligence, making timely and informed decisions, and taking decisive action. It went beyond whole-of-government to whole-of-nation. American leaders had learned to think globally and act locally – strategically rather than operationally. They prioritized investments in strengths and opportunities over threats while lowering costs and risks. They placed economic development and diplomacy out in front of defence. Echoing changes in the business community, agencies became leaner and flatter, less redundant, more adaptive, teamed and networked. Resources were driven first by strategic goals, jettisoning the wasteful mindset of a surplus mentality. Shaped for collaboration among departments and between the public and private sectors, the system was more inclusive, engaging much more of America's still considerable soft power."*

Organisations must look towards the outside to be more competitive[34] and this logic means that the system has to be a part of our activity outside of our organisation but one we must know about and try to imitate. As Baumard[35] states, business intelligence is more structured in Western countries whilst, for example, in Japan it is more structured at the level of organisational culture.

We cannot conceive today of organisations – or intelligence communities – without their technological dimension, a burden that Mintzberg[36] has already warned would continue to increase. Technology is, however, a term mistakenly used since what we understand by technology is no more than a part of it, in our case the internet and data processing software in its many varied dimensions. Human beings have always been technological and this is what has enabled them to solve the problems with which they are confronted; technology is both the fire and the wheel and the intercontinental ballistic missile. And we must bear in mind that technology has always been an essential element in intelligence. Therefore, during

---

33 Holshek, Christopher, *America's first Quarter Millennium: Envisioning a Transformed National Security System in 2026*, Project on National Security Reform (PNSR), 2011, http://0183896.netsolhost.com/site/wp-content/uploads/2011/12/pnsr_americas_first_quarter_millennium.pdf

34 Arroyo Varela, Silvia, *Inteligencia competitiva: una herramienta en la estrategia empresarial*, Madrid, Ediciones Pirámide, 2005, p. 106.

35 Baumard, Philippe, "From noticing to 'sense-making': The use of intelligence in strategizing", *The International Journal of Intelligence and Counterintelligence*, vol. 7, No. 1, 1994, pp. 29-73.

36 Mintzberg, Henry, *La estructuración de las organizaciones*, Ariel, Madrid, 1979.

the world wars knowing what ships were crossing the Strait and their possible cargo was a key security element. In the same way, the Sherman Kent analysis was a success, impressing the military commanders to design spectacular scenarios as a result of the texts available in the Library of Congress that were sought and processed, as Davis[37] states.

Some writers[38] maintain that strategy has been very focused on the mechanical process and a model more focused on people should be developed. Although this is true, technology has increased the possibilities to prevent being surprised "strategically" while meaning an increase in the threat potential to us and our interests. To advance towards strategic intelligence also means understanding scenarios and being clear about how to carry out the processing and fusion of available data from the available multiple and enormous information sources. The necessary data fusion that it generates would refer, therefore, to the means not the purpose and has to include an entire series of techniques such as networks of sensors for data management, data collection with the machine-person interaction, organisational optimisation or the analysis of a large volume of data.

This data fusion at a high level is to a large degree intuitive for human beings but is a formidable challenge for computer systems. I will not go into aspects such as the Bayesian analysis, metadata or the use of ontologies, as it is not an area where added value can be contributed, nor would this be the right place for it. I'm focusing attention on the fact that strategic intelligence requires knowing what we are looking for to be able to find operation standards, if not, the emerging science of analytical reasoning that makes interactive interfaces[39] easier for analysts and decision makers will make them fall into a *Minority Report* style illusion. Willing to use resources and modify legislation relating to rights and freedoms, political decision makers would delegate authority to the powerful automated computer systems that track online and that would know how to deactivate threats before they materialise.

Combining automated analysis techniques with interactive viewing specifically designed to give support to analysts and political decision makers means an interaction should be achieved between the political decision maker's goals with real data for effective understanding, reasoning

[37] Davis, Jack, "The Kent-Kendall Debate of 1949", *Studies in Intelligence*, 1991, 35, No. 2.

[38] Martín Barbero, Isaac "Inteligencia economica. Tan lejos, tan cerca", *Inteligencia y Seguridad: Revista de análisis y prospectiva*, No. 2, 2007, pp. 107-120; Service, Robert W. "The Development of Strategic Intelligence: A Managerial Perspective", *International Journal of Management*, vol. 23, No. 1, 2006, p. 61; Solberg Søilen, Klaus, "Management Implementation of Business Intelligence Systems", *Inteligencia y Seguridad: Revista de análisis y prospectiva*, No. 9, 2010, pp. 41-65; Porter, Michael and Victor E. Millar (1985) "How information gives you competitive advantage", *Harvard Business Review*, July, pp. 1-13.

[39] Cook, K., Earnshaw, R. and Stasko, J., "Discovering the Unexpected", *IEEE computer Graphics and Applications*, September/October, 2007, pp. 15-19.

and decision making on the basis of enormous and complex databases[40]. This view is not so clear, for example, in the fight against terrorism, which seems dominated by an obsession for massive data collection and their exploitation through integrated platforms, some under development by large IT companies. The debate again goes back to the old one of a more basic nature such as the discussion between what emphasis needs to be put on the HUMINT (Human Intelligence) vs. SIGINT (Signals Intelligence) vs. OSINT (Open Source Intelligence) cocktail, but here is not the place to discuss this and its influence on strategic intelligence if we do not want to fall into commonplace themes which Rosales[41] studied some time ago.

A truly strategic new product

Economic intelligence existed in the past[42] and therefore under no circumstances is it a new concept. Beginning with Marco Polo, interest in broadening markets and obtaining commercial, industrial or economic information is well documented. For some time, as Rousseau published in 1925[43], economic intelligence was included as a complement to military intelligence, which made it possible to know the enemy's capabilities but was not a tool for the discovery of the potentials of others outside the sphere of war. However, this approach is no longer predominant.

According to the CIA, 40% of the information obtained from analyses conducted in the middle of the nineties was already about economic matters. The end of the Cold War meant that a lot of economic and commercial data was available and today no less than 95% of it comes from open sources. In theory the North American intelligence agencies are not involved in espionage for the benefit of their national industries. However, they are more and more involved in situations that entail identifying situations abroad where North American companies are in a disadvantageous situation due to unscrupulous actions such as bribery by foreign competitors.

Few doubt that intelligence services have usually focused on threats of a military and political nature or more recently on terrorist activity. That the intelligence services can supply a product of an economic nature, beyond its use to discover the enemy's capability in war, is also undeniable.

---

40 Keim, D. Kohlhammer, J., Ellis, G and Mansmann, F (eds.) 2011, *Mastering the information age: Solving problems with visual analytics*, Konstanza, www.vismaster.eur/book/

41 Rosales, Ignacio, "La inteligencia en los procesos de toma de decisiones en la Seguridad y Defensa", *El papel de la inteligencia ante los retos de la seguridad y la defensa internacional*, Cuadernos de Estrategia No. 130, Instituto Español de Estudios de la Defensa, Ministerio de Defensa, 2005, pp. 35-59.

42 Díaz Fernández, Antonio M., *Los servicios de inteligencia españoles*, Alianza Editorial, Madrid, 2005.

43 Rousseau, "Economic intelligence", *Journal Royal United Service Institution*, vol. 70, 1925, pp. 701-709.

In fact, they have been doing it for years, as Zelikov and Levet[44] explain. In my opinion, with all logic and sincerity, what Brander asks is whether the State must be involved in these tasks and, to support his questions, he puts forward three arguments in favour[45]. Firstly, failures in the market mean that the State must intervene, secondly, intelligence is public property that can only be borrowed by it, and thirdly, it has a role to play in protection the same as other State institutions.

Sherman Kent defined strategic intelligence as "the type of knowledge that a State must possess in order to guarantee that its interests do not suffer nor its initiatives fail due to the fact that its political decision makers or soldiers plan and act in ignorance"[46]. This definition is equally applicable to the business world but specifically there is one of the most essential differences in my opinion. Companies not only prevent their competitors stealing market share from them but they study thoroughly, and improve and try to attain it, about which Rodenberg[47] has written.

The potential for intelligence agencies that have adapted their instruments and resources to this new task is impressive. As Fraumann[48] states, this is because current economic espionage conducted by foreign powers goes beyond classic industrial espionage. Because "we cannot politically spy on an ally" some cases could be innocently justified, but what about economically? Both elements are subject to the action of intelligence but in the case of economic espionage, assuming that we spy on the economy of others, this means dividing this intelligence into two large dimensions, public-private and offensive-defensive, which I will discuss below.

On the one hand, globalisation has changed the concept of "ours" and "theirs", nationally and internationally. Markets are no longer strictly local, national or international but globalised, yet the governments and their instruments continue to be national. Therefore, the distinction between public and private that now is in itself more complex joins some States that have lost part of their regulatory and police power both at a State level and beyond their frontiers. It is in this environment where economic intelligence would operate, as an instrument for the strategy and

[44] Zelikov, Philip (1997) "American Economic Intelligence: Past Practice and Future Principles", Intelligence and National Security, vol. 12, No. 1, pp. 164-177; LEVET, Jean-Louis (2001) "L'intelligence économique: Mode de pensée, mode d'action", paperback edition.

[45] Brander, James A. "The Economics of Economic Intelligence". *Commentary, Canadian Secret Intelligence Service*. Reprinted in Evan Potter, ed. *Economic Intelligence and National Security*, Carleton University Press, Ottawa, 1998, pp. 197-217.

[46] Kent, *opus cit.*

[47] J.H.A.M. Rodenberg, *Competitive Intelligence and Senior Management*, Eburon Publishers, Delft, 2008.

[48] Fraumann, Edwin (1997) "Economic espionage: Security missions redefined", *Public Administration Review*, 5 (4), pp. 303-308.

management of companies and the State in a global world, although of course the latter accepts that it must have a pre-eminent role in it.

The second line of discussion is, therefore, not if the State can but if it must involve itself in direct economic espionage or exclusively develop its capacities for defence purposes[49]. But nor should we spend too much time on thought, since really the topic is the connection and balance between the two. If espionage exists it is due to need and reciprocity and therefore if we are developing a capacity for protection against threats it is because we assume what other States are actively doing so. And this is not only an assumption. The annual reports about the control and management of parliamentary control committees and intelligence services, respectively, unhesitatingly point to China and Russia as very active agents in economic espionage, including industrial espionage. Maybe that is why it is interesting that the two countries with the greatest interest in economic espionage make no reference to the importance of economic intelligence in their defence White Papers or in similar texts.

Therefore, in my opinion, although there is undeniable theoretical justification for the State to thoroughly research and establish itself in this area, the question is whether it should adopt an offensive-defensive role. Although we could speculate that if intelligence services worldwide were so successful at stealing commercial secrets, then research and development would drop rapidly since the private players would not be able to recoup their investments. On the other hand we would be speaking about information as public property – as Seiglie[50] mentions – in the sense that a product that because of its nature can only be provided by the State, and if this fails the private world cannot generate it since it is not produced by the private sector. But information is not property in the pure sense, although it is very close, as seen by the existence of private intelligence companies and their incredible expansion in the last five years.

Claude Revel[51] supports an offensive option for economic intelligence. This French expert says that economic security consists of prevention and avoidance of any situation that can interrupt the existence of both companies and the State. Without doubt it is a strange way of understanding "offensive". Economic counter-espionage is well known but not that of an offensive nature. The Canadian strategy, which is explained it its *Securing an Open Society: Canada's National Security Policy* of 2004[52], con-

[49] Brander, *opus cit*. 1998:205

[50] Seiglie, Carlos; Coissard, Steven and Échinard, Yann, "Economic Intelligence and National Security", *War, Peace and Security. Contributions to Conflict Management, Peace Economics and Development*, vol. 6, 2008, pp. 235-248.

[51] Revel, Claude, "Economic Intelligence: An Operational Concept for a Globalised World", ARI, Real Instituto Elcano, No. 134/2010.

[52] *Securing an Open Society: Canada's National Security Policy*, April 2004, http://publications.gc.ca/collections/Collection/CP22-77-2004E.pdf

nects intelligence with foreign espionage, that is, as a threat from other powers from which they should protect themselves.

Without doubt one of the most astute reflections on how to maintain balance was made by Mark Lowenthal – although extendible to all the participants – before the American Congress[53] and which Claude Revel[54] discusses in his last report *Développer une influence normative internationale stratégique pour la France.* In it Revel supports "the need for a national economic intelligence structure that will be a nerve centre for warnings, promotion and support and for monitoring strategies on information, security and influence that must be inextricably linked". The French writer continues by indicating that "there should be inter-ministerial cooperation, inevitably maintained at a State level, with access to all useful data from any of the State services and private players. The structure must centralise the data, direct strategy, tactics and action in international environments and monitor evaluation". He states that all this must be carried out in full coordination with all the State centres so that it can anticipate and make decisions on complex matters.

Returning to the debate between Kent and Kendall, here we would find an essential difference: either we want an organisation that wishes to anticipate threats – essentially attacks – or wishes to regulate the environment, something that is perfectly acceptable in (strategic) management. And the Carayon report shows, in my opinion, the evolution decided upon from this debate. On page 37 it states that a true economic security policy must impose on the State anticipation of threats and the active processing of attacks that its companies suffer. It is time to go from a static and reactive position (defence) to one of an active nature (economic security) including all the State's services and in the first instance the intelligence and security services.

Strategic process: the new plan

Russel Ackoff confirmed that the plan was "to conceive the desired future as well as the necessary means to achieve it"[55]. Shared strategic analyses make it possible to produce a synthesis of collective agreement, contrary to that which Henry Mintzberg[56] proposed. The most difficult thing

[53] *Hearing before the Select Committee on Intelligence of the United States Senate, One Hundred Third Congress*, First Session on Economic Intelligence, Thursday, 5 August, 1993 http://www.intelligence.senate.gov/pdfs103rd/103650.pdf

[54] Revel, Claude, *Développer une influence normative internationale stratégique pour la France*, 2013, http://proxy-pubminefi.diffusion.finances.gouv.fr/pub/document/18/14133.pdf

[55] Ackoff, Russel L. (1973) *Méthodes de planification dans l'entreprise*, Paris, Les Editions d'Organisation.

[56] Mintzberg, 1979, *opus cit*.

would not be making a good choice but being sure that the right questions had been asked. This problem has been well considered and collectively shared by those whom this problem concerns; we can say that it is an almost resolved problem. Therefore, we can say that we plan to resolve problems, in our case, the State in its different dimensions, including economic ones.

But time is and will be a key variable. Neither the analysts can use all they want in order to obtain deep knowledge, nor do political decision makers have enough to understand complex affairs for which they are responsible daily. The planning process starts from the clear allocation of commitments, and therefore leadership – in our case political – is essential for planning. Decision makers want information that helps them to prevent unpleasant surprises and, therefore, political decision makers, although they do not request strategic intelligence, need it. But the certain fact is that our future is planned by people who want to feel comfortable with their decisions but do not support receiving strategic intelligence that predicts difficult events that do not fit in with their politics, that is, they want to prevent strategic surprises but rarely develop "strategic" actions that go beyond the term during which they will be in office.

The flow of information from top to bottom is usually the traditional formula used by the State which coordinates, stimulates and finances these structures. However, the past shows us that the bottom to top approach comes from successful experiences that boost feedback in which the participation of the State is pragmatic and in response to initiatives that emerge from the field[57]. These preliminary elements, in my opinion, indicate that the role senior civil servants, who give permanence to a country's politics, have to play is key, although this is not the time to discuss it.

Maybe that is why an important document that passed unnoticed such as the report from the Commission for the Reform of the Foreign Service of the Spanish Cabinet Office, led by the ambassador Melitón Cardona in 2005[58], should be recovered. It is interesting because of its comprehensive approach, because of the date and because of the fact that Spain rarely produces this type of document. It was already established in it that the Foreign Service, on the one hand, had problems of an organisational nature that were reflected in problems with planning, coordination and the delimitation of capabilities and problems in the consular area. Among the planning problems was the limited capacity for planning and

[57] Marco, Christian and Moinet, Nicolas "L´intelligence économique", Paris, Dunod, 2006, p. 120

[58] *Comisión para la Reforma Integral del Servicio Exterior. Ministerio de la Presidencia* (*Commission for the Integral Reform of the Foreign Service. Cabinet Office*), 2005, chaired by ambassador Melitón Cardona, http://www.maec.es/SiteCollectionDocuments/Documentos/informe_CRISEX.pdf

strategic preparation for action abroad. The report mentioned that "this problem, which Spanish foreign policy has been suffering for decades, means that that our country's activity is moving within a new international context with a short-sighted approach. Also, the design for the network of Spanish missions abroad is inadequate. This problem is due to the limited planning for Spanish foreign policy and a lack of flexibility for opening and closing diplomatic missions, a result of the existing complex administrative procedures".

The report also adds:

> *"There is a failure to define the goals of Diplomatic Missions. The limited planning together with our foreign policy means that Spanish Diplomatic Missions do not have goals that make it possible to direct and control their activity. This means that they work in a reactive way and it is difficult to evaluate their actions objectively. The lack of Section Heads in certain areas means a lack of prompt monitoring of these topics, given that the Director of the Diplomatic Missions who is responsible for these issues must also be occupied with many other matters. The non-existence of certain Section Heads also means a need for continuous travelling by civil servants from ministries with the skills in these matters and as a result, a high cost in secondment".*

But ambassador Cardona also spoke about coordination problems. Specifically:

> *"about the lack of sufficient inter-ministerial coordination, due in part to the ineffectiveness of the collegiate bodies responsible for such purposes, such as the Foreign Policy Council which is the area where the government's general policy should be compatible with the priorities of all ministries with foreign activity. Also, there is a lack of systematic information flows which cause a large part of the coordination problems both in the Central Services and in the Diplomatic Missions. The information is not transmitted from top to bottom nor horizontally because no guidelines have been set so that the information circulates in all directions. There is a lack of coordination between the Mission's different departments, both due to poor circulation of information and the erratic regularity of the coordination meetings. There is a lack of suitable coordination of other national players with foreign activity".*

In France the Carayon[59] report, successor to the Martre[60] report, prepared a decade before, marked a starting point in the development of strategic intelligence that will be needed in the 21st century. Carayon explained

[59] *Intelligence économique, compétitivité et cohésion sociale*, July 2003. http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/034000484/0000.pdf

[60] *Intelligence Economique et Stratégie des Entreprises*, February 1994. http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/074000410/0000.pdf

that competitiveness needed economic intelligence policies and that these have to be coordinated in order to be efficient. However, although neither of the two reports establishes a unique definition of economic intelligence, the first does indicate that it should be based on four pillars: i) encouraging this practice at company level, ii) optimising information transfer between the public and private sectors iii) constructing databases based on users' needs and iv) mobilising the world of training and education. A series of challenges that are slowly being developed in most countries, including those where there is a clear wish to develop this type of intelligence.

In Spain economic intelligence is included in the Spanish Security Strategy (Estrategia Española de Seguridad). But, previously, the 11/2002 Act of 6th May, regulating the National Intelligence Centre (Centro Nacional de Inteligencia, CNI) included a key verb for developing the potentiality of strategic intelligence and clearly, of economic intelligence. Its article 4 indicates that "to fulfil its goals the National Intelligence Centre will carry out the following duties: a) Obtain, evaluate and interpret data and disseminate the necessary intelligence to protect and promote Spain's political, economic, industrial, commercial and strategic interests and be able to act within or outside national territory." The verb 'to promote' is key since it implies that the CNI can move from being an instrument focused on preventing threats to an instrument for development, including economic intelligence, without doubt an evolution in the development of our "strategic intelligence".

Conclusions

The excessive use of the description "strategic" is widely accepted and not only in the world of intelligence but also in that of marketing, personnel management and business decisions, among many others. The end of the Cold War, in the field of intelligence, generated the need to redirect the function of some structures created specifically to fight in eastern areas after the Second World War. And this is crystal clear. The forced evolution of intelligence agencies is a reason for them to be conceived and developed to basically fight against strategic surprise, no matter how much the word "strategic" fills reports and declarations and even leads to speaking about "strategic" nuclear arms, where we can find little that is strategic. Overnight, a world that was almost surgically divisible in half has been shown as plural, multi-faceted, complex and strange. This scenario is where true strategic intelligence has its place; intelligence that helps understanding, in its etymological sense, to enable political decision makers to understand what the challenges are in the medium and long term, accepting the inevitable existence of strategic surprises that, by definition, will always exist because uncertainty is inseparable from life on Earth.

To understand the world means evolving the Kent Trinity in its three dimensions. Organisations must be more adaptable, have analysts who are allowed extensive and extended thought over time, away from the management of goals that destroys this type of human capital based on know-how gained during years of experience and study. The product must also change. Beyond continuous updates, greater awareness by political decision makers and what their needs are is required, which means greater planning and monitoring by inter-ministerial coordination organisations, something almost unknown, at least, in the Spanish approach. Finally, processes must be modified, mainly through a new relationship that has to be established between intelligence consumers and producers, but above all by making use of technology's potential and escaping from continuous monitoring of the environment that will give us a lot of data, provided we know what we are looking for, and that is something that does not exist without a true strategic approach to intelligence.

The State often plays a pioneering role because it includes activities that are expensive or complex but that it usually abandons when the private sector comes into play. In the case of economic intelligence this approach is slightly more disputable since economic intelligence was important centuries before the Cold War produced the first intelligence services. We could say that the State – once the Machiavellian Prince – is returning to one of its original goals: economic information. The role that it will adopt, either offensive or counter-espionage to prevent other powers or companies draining its economic secrets, will be a debate that each state must have with its own businessmen in deep discussions, since we cannot speak directly about national companies as globalisation broke the "us-them" reasoning that worked for many years. However, the duty to help companies to protect themselves against economic espionage leaves us with few doubts.

Therefore, without including the privatisation of intelligence, a very noticeable rhetoric from the late nineties, there is a need not to duplicate resources and to let organisations such as universities, centres of thought, centres of analysis, computer centres and open sources take responsibility for part of the discourse about the new threats. We are not forgetting that although intelligence needs are now very short-term, the intelligence services' true role is long-term strategic support and they should concentrate the majority of their efforts there; to forget this aspect in the interest of daily effectiveness could lead to subsequent strategic surprises within a decade.

Although it is true that we cannot associate the future of strategic intelligence with that of economic intelligence, nor can we identify the current delay in some facets as being due to oversizing the intelligence apparatus to focus it on terrorism, in the same way that we are not looking at organised crime as the great threat that the parliamentary committee on

control of intelligence services 2001-2002 warned. But, ultimately and in conclusion, the key factors for the success of economic intelligence policies, both for the State and for companies, will have to be their skill in i) anticipating and not just comparing old scenarios ii) adapting structures and laws to increasingly rapid processes and iii) establishing cooperation networks mainly between the public and private sectors, especially between States that share the same general interests.

A visit to the oracle at Delphi in the centre of Greece is an illustration about how to understand intelligence. The fortune tellers only gave their predictions once a month and their preoccupation with the everyday was diluted since their vision was about life, about essential elements, and to do this they needed to dedicate time to thought. Various cities had their own sites in Delphi, where they also kept their treasures and offerings, a kind of meeting point for all those with an interest in knowing the future and who attended to hear the predictions. And finally, the predictions were not sure plans, they indicated how events or a person's life could progress and based on that, the integration between that "strategic thought" and a correct reading of the everyday, the traveller to Delphi could have a map to follow for perhaps whole years of his life. This means that it had a "reality" that could be known in advance. And for years this was the belief of politicians; that with more resources they would have the intelligence that would reduce uncertainty almost to zero, and of intelligence communities which put their emphasis on resources as an argument for achieving better analyses without acknowledging that what they did not want was to issue reports through which, inevitably, the next strategic surprise would be leaked. It is also true that in Delphi there were hidden passages and smoke that rose out of the subsoil that enabled magical appearances and disappearances but, the rhetoric of the occult will always have its small element of mystery beyond the strategic element.

Bibliography

Ackoff, Russel L. (1973) *Méthodes de planification dans l'entreprise*, Paris, Les Editions d'Organisation.

Arroyo Varela, Silvia (2005) *Inteligencia competitiva: una herramienta en la estrategia empresarial*, Madrid, Ediciones Pirámide.

Baumard, Philippe (1994) "From noticing to 'sense-making': The use of intelligence in strategizing", *The International Journal of Intelligence and Counterintelligence*, vol. 7, No. 1, pp. 29-73.

Brander, James A. (1998) "The Economics of Economic Intelligence". *Commentary, Canadian Secret Intelligence Service*. Reprinted in Evan Potter, ed. *Economic Intelligence and National Security*, Carleton University Press: Ottawa, pp. 197-217.

Buzan, Barry (1998) *Security: A new framework for analysis*. Boulder, London, Lynne Rienner Publishers.

Colby, William E. (1992) "Reorganizing Western Intelligence", in Carl Pete Runde and Gregg Voss (eds.) *Intelligence and the New World Order: Former Cold War Adversaries look toward the 21th Century*, Butstehude, International Freedom Foundation.

Cook, K. Earnshaw, R. and Stasko, J. (2007) "Discovering the Unexpected", *IEEE Computer Graphics and Applications*, September/October, pp. 15-19.

Davis, Jack (1991) "The Kent-Kendall Debate of 1949", *Studies in Intelligence*, 35, No. 2.

Díaz Fernández, Antonio M. (2005) *Los servicios de inteligencia españoles*, Alianza Editorial, Madrid.

Díaz Fernández, Antonio M. (2006) "La adaptación de los servicios de inteligencia al terrorismo internacional", ARI 52/2006, Real Instituto Elcano.

Díaz Fernández, Antonio M.; Revenga, Miguel and Jaime, Óscar (2009) *Cooperación Europea en Inteligencia: Nuevas preguntas, nuevas respuestas*, Aranzadi, Pamplona.

Ferrer, Juan (2011) *Seguridad económica e inteligencia estratégica en España*, Documento Opinión, Instituto Español de Estudios Estratégicos, No. 85.

Fraumann, Edwin (1997) "Economic espionage: Security missions redefined", *Public Administration Review*, 5 (4), pp. 303-308.

Goldman, Jan (2006) *Words of Intelligence: A Dictionary*, The Scarecrow Press, Oxford.

Holshek, Christopher (2009) *America's first Quarter Millennium: Envisioning a Transformed National Security System in 2026*, Project on National Security Reform (PNSR).

Jaime Jiménez, Óscar and Díaz Fernández, Antonio M. (2009) *La Seguridad Interior: España 2020*, Fundación Alternativas, Madrid.

Keim, D. Kohlhammer, J. Ellis, G. and Mansmann, F. (eds.) (2011) *Mastering the information age: Solving problems with visual analytics*, Konstanza, www.vismaster.eur/book/

Kendall, Willmoore (1949) "The function of intelligence", *World Politics*, vol. 1, No. 4, July, pp. 542-552.

Kent, Sherman (1949) *Strategic Intelligence for American World Policy*, Princeton, Princeton University Press.

Lesourne, Jacques (1989) "Plaidoyer pour une recherche en prospective", *Futuribles*, No. 137, November.

Levet, Jean-Louis (2001) "L'intelligence économique : Mode de pensée, mode d'action", Ed. Economica, Paris.

López Espinosa, María de los Ángeles (2009) "Inteligencia y terrorismo internacional. Un panorama de cambios", *La inteligencia, factor clave frente al terrorismo internacional*, Cuadernos de Estrategia, No. 141, Instituto Español de Estudios Estratégicos, Ministerio de Defensa, 2009, pp. 197-239.

Marco, Christian and Moinet, Nicolas (2006) *L´intelligence économique*, Paris, Dunod.

Martín Barbero, Isaac (2007) "Inteligencia económica: Tan lejos, tan cerca", *Inteligencia y Seguridad: Revista de análisis y prospectiva*, No. 2, pp. 107-120.

Mintzberg, Henry (1979) *La estructuración de las organizaciones*, Ariel, Madrid.

Platt, Washington (1957) *Strategic intelligence production: Basic principles*, Praeger, New York.

Porter, Michael and Millar, Victor E. (1985) "How information gives you competitive advantage", *Harvard Business Review*, July, pp. 1-13.

Posner, Richard A. (2005) *Preventing Surprise Attacks: Intelligence in the Wake of 9/11*, Rowman & Littlefield, New York.

Revel, Claude (2013) *Développer une influence normative internationale stratégique pour la France*, http://proxy-pubminefi.diffusion.finances.gouv.fr/pub/document/18/14133.pdf

Revel, Claude (2010) "Economic Intelligence: An Operational Concept for a Globalised World", ARI de Real Instituto Elcano, No. 134/2010.

Rodenberg, J.H.A.M. (2008) *Competitive Intelligence and Senior Management*, Eburon Publishers, Delft.

Rosales, Ignacio (2005) "La inteligencia en los procesos de toma de decisiones en la Seguridad y Defensa", *El papel de la inteligencia ante los retos de la seguridad y la defensa internacional*, Cuadernos de Estrategia No. 130, Instituto Español de Estudios Estratégicos, Ministerio de Defensa, pp. 35-59.

Rousseau, (1925) "Economic intelligence", *Journal Royal United Service Institution*, vol. 70, pp. 701-709.

Seiglie, Carlos;, Coissard, Steven and Échinard, Yann (2008) "Economic Intelligence and National Security", *War, Peace and Security. Contributions to Conflict Management, Peace Economics and Development*, vol. 6, pp. 235-248.

Service, Robert W. (2006) "The Development of Strategic Intelligence: A Managerial Perspective", *International Journal of Management*, vol. 23, No. 1, pp. 61-77.

Solberg Søilen, Klaus (2010) "Management Implementation of Business Intelligence Systems", *Inteligencia y Seguridad: Revista de análisis y prospectiva*, No. 9, pp. 41-65.

Swenson, Russell G. and Lemozy, Susana C. (2009) "Democratización de la función de inteligencia. El nexo de la cultura nacional y la inteligencia estratégica", *National Defense Intelligence College*, Washington DC.

Whitney, Merill E. and Gaisford, James D. (1996) "Economic espionage as strategic trade policy", *Canadian Journal of Economics*, XXIX Special issue, pp. 627-632.

Zelikov, Philip. (1997) "American Economic Intelligence: Past Practice and Future Principles", *Intelligence and National Security*, vol. 12, No. 1, pp. 164-177.

A study on economic warfare and associated problems

Christian Harbulot

Chapter II

Abstract

The history of mankind is dominated by the power relationship of an economic nature, identifiable at the different stages of progression: the struggle for survival, colonization and slavery, territorial conquest and trade, economic competition, the geoeconomic and competitive fighting. But there is no recognized written culture on economic warfare in the academic world. This gap can be explained by the lack of legitimacy of the concept due to the desire to conceal the purpose of economic fighting. The most visible expressions and irrefutable economic warfare as the most contentious phases of colonization or the two opium wars have not led to the beginnings of a reading grid. This article aims to fill this gap in thinking about a reality that everyday becomes more demonstrative. Unlike other countries such as the United States, South Korea and China, Europe is powerless to address this problem.

Keywords

Economic war, survival, colonization, conquest, read gate/obliged readings, concealment, strategy, increase in power.

Introduction

Economic warfare is becoming an undeniable reality in international relations, although it was considered for a long time as something exotic by the university community. The intellectuals that criticise the strong relationships between powers[1] have been obliged to give in, bearing in mind the clear development of international relationships. In addition to geopolitical events (such as the gas used by Russia as a weapon to reinforce their status as a power or the questioning of the financial supremacy of the dollar by Iran) there have also been geoeconomic events such as the diplomatic tensions between China and Japan over resources or the protectionist policy defended by the United States against China regarding the solar power industry. This diversity in situations emphasises the importance of a deeper reading of the conflicts linked to economic warfare.

The beginning of the 21st century was marked by a questioning of the positive vision of the development inherited from industrial revolutions and from the relative peace from the globalisation of exchanges, as the majority of liberal economists have stated. Similarly, the *Pax Americana* that became official due to the disappearance of the USSR, the beginning of the end of history myth[2], leaves room for risks of multi-polarised conflicts due to the progressive limitation of resources, growing tensions over the issue of energy, the structural crises of the Western world caused by de-industrialisation and the desire for commercial conquest by new players. In fact we are starting a long period of different tensions whose monitoring cannot be limited to a mere comforting discussion about the search for growth.

To analyse economic warfare[3] entails going from the implicit to the explicit, a difficult exercise taking into account the warring factions' almost universal desire to conceal the nature of their non-military conflicts. The works carried out in the last sixteen years under my direction at the School of Economic Warfare of Paris have enabled us to lay the foundations for some compulsory reading to decipher the strategies for increasing power through the economy and the strong relationships they generate.

Emergence of the founding principles of economic warfare

The history of humanity has been defined since our origins by two key stages: the priority given to survival and the opposition between seden-

1 Badie, Bertrand, *L'impuissance de la puissance*, Paris, Fayard, 2004.

2 Fukuyama, Francis, *La fin de l'histoire et le dernier homme*, Paris, Flammarion, 1992.

3 Harbulot, Christian, *Comment travailler sur l'absence d'histoire*, report of 7th November 2012, www.lesinfluences.fr.

tism and nomadism. The theme of survival had been a predominant situation for the greater part of the world population until the beginning of the industrial revolutions. It gave rise to the use of often systematic violence.

Violence and survival

Survival is one of the structural stages of the nature of economic conflicts without having to refer to economic warfare, given the mainly individual level of conflict that was therefore limited collectively. Opposition between sedentary and nomadic towns has entailed regular conflicts such as the origin of old Russia[4] shows.

"The Russian steppe is the extension of the Asian steppes and founded in the Hungarian steppe. This continent of steppes – from the yellow sea to Lake Balaton – is populated by nomads that, since pre-history, have travelled vast distances searching for pastures. Coming from the depths of Asia the nomads arrive at the steppe in waves. They expel the inhabitants who, in turn, occupy the pastures of weaker villages."

This warlike dance between the "barbarians" of the east and the town populations in the west arose from the river and land trade between the Baltic Sea and the Black Sea that lasted several centuries and played a decisive role in the construction of Russian geopolitical space. Similarly, the history of ancient China is marked by repeated invasions of Turkish-Mongolian nomad villages. The first version of economic warfare came from this dialectic nexus between the accumulation of wealth of the sedentary village and the rapid incursion of the nomad into foreign territory to carry out pillaging.

Resources and territories

The issue of resources is at the centre of the problem of developing civilisations. In the 15th century BC the Pharaohs of the new empire[5] needed three natural resources: wood for constructing monuments and ships, along with copper and tin, whose alloy in the form of bronze was used in those days to make tools and weapons. The maritime (the Mediterranean, the Channel and the Baltic) and land (the silk and tin routes) trade routes became sources of recurring conflict.

The progress of humanity between the Ancient and Modern Eras widened the spatial field in the process of economic conflict. Thus piracy became

[4] Heller, Michel, *Histoire de la Russie et de son empire*, Paris, Champs, collection histoire, 1999, p. 55.

[5] Grandet, Pierre, *Les pharaons du Nouvel Empire: une pensée stratégique (1550-1069 av JC)* Paris, éditions du Rocher, 2008.

a real power lever. Attracted by the gains of the triangular trade[6], the English pirates were warriors, precursors of future British Royal Navy. At sea and on land, the warring factions integrated the economic dimension to their military and diplomatic strategy.

At the end of the Middle Ages some monarchs turned to the economic weapon[7] to support military action. In his prolonged fight against Charles the Bold, Louis XI mobilised his fleet to disrupt supplies of grain and herrings from Flanders, belonging to the House of Burgundy. The king of France also pressured bankers to dissuade them from financing the cost of his rival's war and promote the creation of trade fairs in Lyon to reduce the income from the trade fairs in Geneva, which was an exchange point for the trade routes between Germany, Italy and Burgundy.

The security of territory and of its urban and rural wealth was perceived in the 17th century as a strategic priority for certain states in the process of constitution. The seven United Northern Provinces[8] against Spain produced the first survival model made up of a network of bastions, reinforced by the use of streams and rivers as a natural defence. The France of Vauban made its own by creating fortifications along the new frontiers that emerged after the conquest of territories in the north of the kingdom. This defensive barrier led to the "Pré carré"[9] concept that has a modern significance by including the external area of influence (diplomatic, military and economic).

Security of territory was also defended indirectly through economic concessions given to an ally State, taking advantage of its military supremacy. In 1373 Portugal signed a treaty with England[10] to benefit from its protection. Through this diplomatic act Portugal sought to escape voluntary annexing to Castile. This alliance ratified under equal conditions was gradually transformed into an English protectorate, as the English gave their military support in exchange for financial and commercial dominance over Portugal that lasted several centuries.

The difficult dynamics linked to colonisation

The constitution of empires is inseparable from the processes of colonisation that marks the history of humanity. Military conflicts that originate

[6] Triangular trade flows from the early stages of colonisation of America. It covered the slave trade between Africa and the U.S. as well as trade between the colonies and the European continent.

[7] Favier, Jean, *Louis XI*, Paris, Fayard, 2001, p. 754.

[8] Cornette, Joël, *Le roi de guerre, essai sur la souveraineté de la France du Grand Siècle*, Paris, Petite Bibliothèque Payot, 2010, p. 42.

[9] Bitterling, David, *L'invention du pré carré. Construction de l'espace français sous l'Ancien Régime*, Paris, Albin Michel 2009.

[10] Lacoye Mateus, Alice, Harbulot, Christian, *La complexité des rapports de force économiques*, Paris, Revue Française de Géoéconomie, April 2008.

from them are strongly related to economic challenges. Colonisation is the basis of empire creation that serves, in particular, to ensure dominance over underground riches and resources as well as over trade routes. The capture and exploitation of human beings was one of the clearest manifestations of the strong relationships generated by the desire for profit. As Jane Burbank and Frederik Cooper[11], lecturers at the University of New York, confirm: "In Great Britain, France and certain regions of the Portuguese and Spanish empires slavery was profitable to the empire and the empire made slavery possible". Economic warfare was present in all phases of colonial development, regardless of whether it referred to the dynamic of expansion of the Roman Empire or the construction stages of the European maritime empires starting from the 16th century. The most paradoxical element, from my point of view, about the formation of this principle is that it is not acknowledged as one of the recurring elements in conflicts linked to the globalisation of exchanges.

The colonisation of North America shows in a very educational way the superposition of conflicting rationalities created by economic challenges. The Thirteen Colonies, established along the Atlantic coast between French Canada and Spanish Florida, were firmly settled from 1733. The settlers had begun to plant cotton in the 17th century. This planting policy developed on a mass scale at the end of the 18th century, producing what would later be called "the triangular trade". The British ships carried manufactured products and spirits to West Africa to exchange them for slaves who were offloaded in the West Indies and in the south of the Thirteen Colonies. The ships later returned to Great Britain with a cargo of cotton, rum, sugar and tobacco, a result of the slaves' work.

The American settlers considered themselves as harmed by their relationship with England due to tax pressures and the trading restrictions with the rest of the world imposed by the Crown. Great Britain had the advantage in all cases since a substantial proportion of the merchandise imported from the New World was re-exported to continental Europe by the island's trading companies. The profits obtained from these transatlantic trade transactions contributed to the development of the British Empire's Asian trade.

The accumulated wealth intensified desires that gradually turned into tensions, into strong relationships and into armed conflicts between England and its colonies, between them and the native Indians and between the two rival kingdoms of the time, England and France.

Control of trade routes

England built its power through the sea and trade. Initially the England of the 16th century was a poor country without any real military capac-

[11] Burbank, Jane and Cooper, Frederik, *Empires, De la Chine ancienne à nos jours*, Paris, Payot 2011, p. 246.

ity for expansion abroad. Its power was much less than the kingdoms of Spain and Portugal, which at that time dominated the seas thanks to their navigation techniques, to their pioneering marine cartography and to their naval strength. Unlike the Spanish and Portuguese, the English were not missionaries or settlers. When the English decided to use the sea as a medium for expansion they had to find immediate profits. Their situation of weakness compared to their opponents' war fleets led them to turn to piracy. English pirates and buccaneers stole precious metals being transported by the Spanish and Portuguese from South America. During the reign of Elizabeth I the British trade networks extended towards Turkey and Russia. If the demand for sugar attracted the English merchants to the Caribbean, the demand for spices, tea and cloth led them towards Asia. The incorporation of the kingdom of Scotland into the kingdom of England, which gave rise to the birth of Great Britain in 1707, led to the creation of a major sector of the era's free trade and also to the appearance of the world's first mass consumer model for imported products, such as tea, coffee, tobacco and sugar.

During the 17th century the English made use of the enormous commercial potential of their overseas acquisitions. The creation of the *British East India Company* (BEIC) opened the way for colonisation in India. Commercial aggression by the English company from the East Indies led it to progressively adopt a political-military position on the Indian subcontinent. It had to recruit local troops to be able to carry out armed operations against regional sovereign states that protested against its supremacy. The increase in the colonial military framework was also the result of rivalry between the different European empires.

The development of exchanges between the continents thanks to triangular trade encouraged the English to take control of the main sea routes beyond Western Europe, not only towards the East Indies but also towards the Baltic, North America, the Mediterranean and West Africa. The origin of the economic challenges of the Anglo-Dutch wars between 1684 and 1784 was:

- Control of the main trade routes.
- Confiscation of trade traffic with the British colonies.
- Questioning of the dominant position acquired by the Dutch East India Company (Vereennigde Oost-Indische, VOC[12])

The Dutch had established the basis of a trade empire from one private dynamic. The VOC was a trading company that emerged from the matrimonial alliances of family and provincial groups. In two centuries it built

[12] Burbank, Jane and Cooper, Frederik, *Empires, De la Chine ancienne à nos jours*, Paris, Payot, 2011, p. 219.

a true commercial empire[13] that made it the most influential company among the European companies founded in the 17th century to exploit Asian wealth. But the private nature of VOC did not enable it to confront the warlike versatility of the Spanish and Portuguese empires that were seeking to gain control of the spice trade from the Indonesian archipelago. It had to incorporate the mechanisms of armed conquest inspired by the Portuguese model into its commercial development. In 1699 the VOC was the major private economic force in the world and had military strength in line with forty warships and ten thousand soldiers. Great Britain entered into the conflict with it to break its strategy of a monopoly on the trade between America and Asia.

Great Britain's protection of the trade routes and with it its economic prosperity defined British foreign policy and brought with it military operations during the empire's duration. Numerous examples of armed fights illustrate these events:

- From the time when Great Britain felt its interests were threatened in India by the Russians' expansion to the south and east, protection of India against them via land and sea became the main axis of Victorian foreign policy. Hence the military conflict with Tsarist Russia in central Asia that was still a "weak point", far from European colonial expansions. The two Anglo-Afghan wars, the first between 1839-1842 and the second between 1878-1880, show this strategy.
- The opium wars[14] (1839-1842 and 1856-1860) between the United Kingdom and the Quing Empire had an economic purpose. Great Britain wanted to force the Chinese Empire to open up to international trade. One of the goals of the British Empire was to obtain the cession of the territory of the city of Hong Kong from China, in order to store opium and trade with it in China. This is a clear example of a military act in service of an economic goal.
- Prime Minister Disraeli's decision to acquire part of the Suez Canal titles in 1875 was intended to stop France from taking control of a key trade route.
- The occupation of Egypt ensured the British Empire's maintenance and control of the strategic platform of Cairo.

[13] The VOC was a real State within a State. It ensured the main regulatory functions (police, defence, justice) in its business offices of the East Indies. It decided on war or peace with the native princes, therefore having autonomous diplomacy.

[14] In the mid-19th century westerners sold several tens of thousands of boxes of opium a year in China. The British demanded payment in silver ingots to recover part of the funds they paid the Chinese in the tea trade. This opium traffic enabled the British Empire to reverse the imbalance of the exchanges with this country in its favour. The opium war raised an unfair relationship that generated greater and greater corruption between Chinese civil servants and caused problems among the population.

- The war declared by the British Empire against the Boers was justified by control of the strategic point that the city of Cape Town represented. The British prepared this base at the tip of Africa with the aim of setting up an emergency maritime route in the case of Suez closing. Consequently part of the territory governed by the Boers was revealed as one of the greatest gold reserves in the world.

The British example showed how predominance of a power in the control of trade routes becomes a decisive weapon in geo-strategic conflicts.

The overlapping of war and the economy

The revolutionary and Napoleonic wars, spread out between 1792 and 1815, emphasised the influence of the economy on the development of strong relationships between the countries involved in this series of conflicts under alliances. In this regard, the economic repercussions of blockades were a great influence on the strategic changes in France and Russia.

The influence of economic conflicts on the war's direction

The Prime Minister William Pitt, whose family fortune came from Anglo-Indian trade, was fixed on a line of action to preserve Great Britain's dominant position in the trading world through control of the seas. His strategy was to support the *Royal Navy* that represented the only major force, compared to the military capacity of revolutionary and subsequently Napoleonic France. Whilst the Prussian alliance with Great Britain fought the French and their allies in Europe, the *Royal Navy* undermined the economic potential of the common enemy by preventing France from trading by sea. The key point of the policy followed by Pitt was to establish an indisputable maritime advantage. He obtained parliamentary support in London to increase the British fighting fleet up to 105 ships. This naval arms race gave England a decisive advantage since the French fleet only had 70 ships.

For the first time in history an economic war became global with the appearance of two blocking systems used by the warring factions: England's Maritime blockade against France's continental blockade[15] to cut British exports to Europe. Previously the blocking actions only had any effect on port cities. The origin of the two blockades was the reciprocal desire of the French and English to use economic reprisal

[15] The blockade was effective in countries allied to France and in countries occupied by its troops (Italy, Spain, the Netherlands, Lower Germany and Denmark).

measures strategically to achieve a favourable outcome to the conflict. This is what happened but not exactly as Napoleon had expected, since the removal of Russia from the "continental system" sought by France triggered the Russian campaign, which was so disastrous for the Napoleonic Empire.

This overlapping of war and economy gave rise to the birth of the first mechanisms in economic warfare that extended into peace time. At the end of the 18th century France was very weakened industrially by the war effort made during the revolutionary wars against Europe of the monarchies. Napoleon confided to Jean-Antoine Chaptal[16], a scientist, about a mission to find a way to revitalise French industry and protect it from British trade threats. This desire for revival in production required a recovery in terms of innovation. Napoleon wanted to know above all the strong and weak points of the British economy and confided this mission to a Society for the Stimulus of National Industry (*Société d'Encouragement pour l'Industrie Nationale*, SEIN) that organised a mechanism for observing discoveries on the other side of the channel. With a handicap of between fifteen and twenty years in technical knowledge, the French manufacturers had to imperiously cover that disadvantage through all media, including the use of illegal practices of smuggling in machines either bought or stolen on British soil.

In the context of the ban on the importing of English products that began in 1793, Napoleon consolidated this economic defence system by the militarisation of Customs[17]. His minister Chaptal considered this administration as "a guarantor of French industrial independence". Customs represented 20% of the administration's total staff in 1815 (excluding the army). This trade exclusion policy regarding Great Britain was extended in the Restoration period under the management of Saint Cricq, the Director General of Customs, who was kept in this position until 1824, the year in which he became Minister of Commerce under Charles X.

Ideological fight and strong economic relationships between powers

Despite the enormous economic cost of the wars against France, Great Britain stayed in a position of strength. The industrial revolution, which began many years prior to that on the continent, put its manufactured products in a very advantageous competitive position. Its colonies guaranteed a large supply of raw materials and its naval supremacy enabled it to block the main maritime trade routes. Consequently, London was

[16] At that time Chaptal held the roles of Minister of the Interior and of Industry.

[17] Todd, David, *L'identité économique de la France, Libre échange et protectionnisme, (1814-1851)*, Paris, Grasset, 2008, p. 64.

interested in promoting the disappearance of customs barriers in order to sell its products in other countries, especially in Europe.

To break the protectionist barriers maintained by France, the British government granted a greater strategic dimension to the techniques emerging from economic warfare in times of peace. The press and publishing[18] performed a decisive role in that strong relationship. London sent the political economist John Bowring[19] to Paris as head of the British commission responsible for negotiations on free trade. The reasons that led the university student David Todd[20] to present John Bowring as an influential agent at the service of the Crown were his working methods whose main goals were, firstly, to create pressure groups in France supporting British arguments and secondly, to use the local press so that his ideas would reach the circles of economic and political power. His management was summarised as follows:

"In 1834, through a series of letters sent to Lord Auckland, president of the *Board of Trade*, Bowring explains in detail the strategy he is developing in France on his travels. In each city he visits he tries to gather and form a group of supporters of free trade. Then he continues intense correspondence with these supporters to direct them towards a common goal: overthrowing the monopolies. The groups are responsible for the liberal ideas in the local press and formulating solemn declarations supporting a free market. Thus, they managed to favourably influence public opinion: *the opinion, the illustrated opinion – is the best instrument for achieving our goal – without it we will not have the least progress; with it we will achieve everything*".

John Bowring started to attack Saint Cricq's ideas, considering that he was an enemy of England[21]. He focused his activity on the exporting regions (silks in Lyon, wine in Bordeaux). The goal of his numerous interventions in the French circles of power was to encourage them to denounce the prohibitive French system. He sought support in regions snatched from the English in the 100 Years' War, such as Aquitaine, where many wine producers opposed the customs duties[22]. Another form of approach used by Bowring was the dialogue he established with French liberals such as Benjamin Constant and Jean Baptiste Say with whom he maintained contact as a politician. Bowring knew how to take advantage of the internal contradictions of the French political world, supporting organisations

18 In 1834, in Paris, 6,500 copies of liberal economy treaties and manuals were printed.

19 He was also involved in Switzerland, Italy and Germany.

20 Ibid. p. 183.

21 Ibid. p. 199.

22 French wine growers were very powerful at that time, representing a tenth of the population actively involved in either main or secondary grape producing activities, that is, two million people.

of anti-government republican press that ranged from the centre left to the extreme right. He knew how to collect the results of his labour on the ground and encouraged his supporters to draw up collective petitions, demanding the abolition of the protectionist barriers imposed by France.

Creation of structures dedicated to economic warfare

The First World War[23] established bases of economic weapons as a way to achieve a defined goal. From 1914, aware that the conflict would be long, the involved powers conceived a strategy for economic warfare, as the French note[24] below sent to the military attaché of the United States in Paris certifies:

"After the battle of the Marne, faced with the new movement from the war the high command understood that it would be long and it would not be enough to fight the enemy on the field of battle but it also had to be fought on their own terrain; preventing enemy armies having material available, morally and physically undermining the entire population, cutting off the necessary raw material supply for their industry, collapsing the economy, blocking their finances, even affecting the food supply. These are the basic ideas on which economic warfare is based".

In 1915 the French War Ministry organised a system dedicated to economic information. A Control Section was created, managed by Jean Tannery[25], a senior public official at the Court of State Auditors (*Cour des comptes*). This section organised the collection of information required to put into practice the activities of economic warfare:

- Identification of the axes for German supplies and study of the arrangements that would have to be made to hinder this supply.
- Monitoring of the organisation and development of the German war industry.
- Preparation of plans for destroying industrial centres.
- Preparation of lists of companies connected to the enemy.
- Application of restrictions and quotas.
- Control of economic flows in order to prevent German foreign economic relationships.

Great Britain organised itself differently using an independent body, the *War Trade Department Intelligence*, which in turn reported to the *Foreign Office*. In 1916 the Italians created the *Ufficio di raccolta e controllo di noti-*

[23] Soutou, Georges-Henri, *L'or et le sang, les buts de guerre économiques de la Première guerre mondiale*, Paris, Fayard, 1989, p. 566.

[24] Revue Historique des Armées, Paris, No. 4, 2001.

[25] Bourlet, Michaël, *Guerres mondiales et conflits contemporains, Jean Tannery (1878-1939) à l'origine de la guerre économique*, Paris, PUF, 2004.

zie economiche, linked to its War Ministry. These structures were coordinated by an Inter-Allied Bureau with its headquarters in Paris.

Throughout the war the activities of economic warfare were already focusing on international goals such as rationing the countries of Northern Europe, in order to force them to stop exports to Germany or with military operations carried out thanks to developments in aviation, such as bombing selected stations in Lorraine that, while occupied, provided three quarters of the iron ores needed in the German iron and steel industry.

In 1918 the French, British and Americans agreed on the criteria for the goals that had to be achieved. For Paris, the economic weapon was not only a weapon of war to force Germany to sign for peace but also the possibility of preserving the advantages won in the event of victory. France wanted to reach an understanding between the allies on how to keep Germany in a weakened economic situation by jointly controlling raw materials. For Washington the economic weapon took the role of a strategic and political influence that would force Germany to sign an acceptable peace treaty and put an end to its economic expansion[26]. Raising the principles of economic liberalism, the United States sought to find itself a place within the world market whilst London followed Washington's line although maintaining its own interests (protection of main industries, special relationships with the *Dominions* on the question of control of raw materials).

Economic warfare structures disappeared at the end of the war. At the beginning of the Second World War, in September 1939, Neville Chamberlain, the British Prime Minister, created a Ministry of Economic Warfare with similar powers to the structures developed during the First World War. In July 1940 Winston Churchill gave this Ministry a very offensive role by allocating it a new service, the *Special Operations Executive*, which was responsible for sabotage operations on the continent and for prompting rebellion and resistance in territories occupied by the German armies. The notoriety of this new organisation meant that specific aspects of economic warfare shifted onto a second level. This Ministry ceased its activity after the defeat of Nazi Germany.

If the overlapping of the economy and war was obvious, for some decades the problem of economic warfare in the second part of the 20th century again became invisible for the following reasons:

- The cold war forced the Western Bloc countries to squash or disguise their economic disagreements, prioritising the image of an ideological unit facing the Communist Bloc.
- The United States, the new world superpower, made the British strategy of applying pressure to end the protectionist barriers on

[26] Hauser, Henri, Les *méthodes allemandes d'expansion économique*, Paris, A. Colin, 1919.

continental Europe its own. The texts on free trade and free competition became obligatory reading in the economic reality of the Western political world. Strong economic relationships between powers were silenced or were considered within the university community, in particular by the majority of liberal economists, as unrepresentative anomalies of the competitive relationship between companies.

The geopolitical justifications of conquest

The search for obligatory reading on economic warfare involves simultaneously analysing the progress of the conquest mechanisms (territorial and commercial) and the States' methods of power development.

Commercial conquests began to replace territorial conquests during the 19th century. Unlike territorial conquest often carried out turning to traditional war, commercial conquest tends to increase the State's supremacy by expanding its circles of power over foreign markets.

Historically some powers did not hesitate, almost publicly, to discuss their expansion, which was necessary for their survival. This was particularly the case with Japan and Germany, which on several occasions spoke about their living space in terms of territorial conquest or commercial conquest.

The conquest against commercial imperialism

From 1853[27], Japan was under the control of Western countries. In the beginning the Japanese bowed to initial Western pressure, signing a treaty on 31st March 1854 in Kanagawa that confirmed the opening of Shimoda and Hakodate ports to commercial ships under the American flag. In the following years England and the main European powers obtained equal privileges. In 1867 when the young emperor Mutsuhito (whose reign would be called *Meiji Tenno)* came to the throne he modified the terms of the strong relationship. Listening to reformists the young king wanted to avoid falling back under the domination of the West (as was the case with China during the same period under the "unequal treaties[28]").

[27] This was the year during which an American fleet made up of four warships sent by Commodore Perry appeared in the Bay of Tokyo. He was carrying a "friendly" letter from the President of the United States for the *shôgun* of the Tokugawa family. After a second layover in 1854 Commodore Perry demanded the *shôgun* to open Japanese ports up to American merchant ships and whalers.

[28] The result of the Chinese military defeats against Western troops, the unfair treaties signed in the 20th century between China and Western powers as well as Russia tried to force China to open up its domestic market.

The strategy applied by Japan took a very significant slogan: rich country, strong army. The *Naimusho*, founded in 1873, was the ministry responsible for industrial development planning. It built state factories inspired by European manufacturer models and discreetly fought to prevent foreign capital taking over the strategic economic points of the emerging Japanese market (port infrastructure, naval shipyards, armaments industry). The modernisation of Japan was carried out within a policy framework of all types of knowledge acquisition acquired abroad, following the example of countries more experienced in the field.

At the beginning of the 20th century, Japanese expansion (the annexation of Korea, acceptance of a responsibility over China) caused antagonism with the United States, who wanted to leave a door open in China. Benoit Meschin[29] summarised the report on the strengths between the two countries after the Washington[30] Naval Conference in 1921 like this:

> *"Linked by the Washington agreements, excluded by the United States with its new immigration law, complicated in its economic development by the increasingly severe restrictions imposed by the American customs service on the importing of Japanese products into the United States; what could Japan do so as not to be confined to their islands and solve the dramatic problems originating from the ever faster rise in its population?"*

After initially seeking to break isolation by turning to a kind of colonisation of Korea, Japan considered that it would be essential to build up an area of shared prosperity at a regional level[31] that would regroup all the countries occupied by the Japanese Imperial Army during the empire's expansion phases. The occupation of Manchuria in 1931 is included in this perspective.

The founding of the State of Manchukuo, a year later, is an example of the reproduction of militarised conquest systems invented by the Portuguese and imitated by the Dutch and English at the beginning of colonial processes in Modern History. The Japanese copied the model of the old India Company but were also inspired by the development produced by the American railway companies that built an industrial empire by connecting the East to the Pacific coast. At the end of the thirties Manchukuo was under the Manchu railway company administration[32] that governed

[29] Meschin, Benoit, *Histoire de l'armée allemande*, volume 1, Paris, Robert Laffont, collection Bouquins, p. 847.

[30] The United States rejected marine equality with Japan and made it disarm part of its war fleet.

[31] The shared prosperity area project of eastern Great Asia was proposed by General Hachirō Arita, Minister of Foreign Affairs from 1936 to 1940.

[32] Over 75% of the company's income came from exporting soybean to Japan and Europe. In 1927 half of the world's soybean came from Manchuria.

this territory in a relatively autonomous way with regard to Tokyo. It directed the occupying Japanese troops, managed its own police force, ran a local administration of over 200,000 employees and had its own issuing bank as well as merchant fleet. The State of Manchukuo was used as an experimental laboratory for a new supremacy concept of power by using the economy.

Conquest of living space

German history is marked by the search for new territories to be conquered, whether peacefully or by using force. From the beginning of time Roman writings gave accounts of particularly difficult living conditions in German villages. Covered in forests and not very suitable for agriculture, the territories in Northern Europe did not enable its population's subsistence. To survive, German villages had to conquer more prosperous territories for subsistence. This conquest strategy was carried out on the land and by sea. At the end of the Middle Ages German colonies had started to be established in the east of Bavaria. Bankers, such as the Fugger family from Augsberg had financed the exploitation of Czech mines and forests. This commercial exchange enabled them to peacefully conquer the old markets of the Slav princes with this being the beginning of the development of the territories of Bohemia and Moravia. This colonisation was not always peaceful. The Polish rejected it and opposed the Teutonic Knights.

The foundation of the Hanseatic League[33] opened the path for maritime conquest. The expansion of the Baltic ports gave Germany as well as the cities in Northern Europe the resources to become established peacefully on the Polish coasts between the 16th and 17th centuries. Military campaigns carried out by the Prussian family Hohenzollern completed the creation of a sphere of influence to the east of Germany.

This constant search for living space outside borders permanently shaped a sharp sense of distribution of strengths in the spirit of the elite Germans. The debate about the strategic opportunity of territorial conquest or commercial conquest dominated political life in the Second Reich. Bismarck's preparation of Germany enabled the country to take on an influential global role. Germany's increase in power at the end of the 19th century was not limited to the movement by the German economy into the industrial era. The mobilisation of German economic figures is inseparable from the geostrategic positions of the Second Reich that were strongly determined by the attitude of the British and French colonial empires. The strategic German heart

[33] Association of German merchants and later of North German cities and Northern Europe that dominated Baltic trade between the 12th and 17th centuries.

(Konzern[34], banks, insurance companies) shaped in that era wanted to dominate other European powers.

This dimension to the debate did not escape German adversaries such as Georges Clémenceau who, from 1915, estimated that the danger from Germany was worse in peacetime than in war, due to the way in which Germany had discovered how to develop a competitive economy capable of competing on a worldwide level with the British Empire economy.

The First World War caused disputes to arise about how to manage hypothetical military victory in geoeconomical terms, once peace had been achieved. The result of this reflection on Germany appeared in 1915 with a work that can be considered today as the draft of an economic warfare manual. It was translated into French under the provocative title of "The German Business War Plan[35]". From the beginning of the book the connotation is obvious: "all business is a war, the world is a battlefield". It was later called by the Americans the Bernhardi[36] of Business; Herzog defined the economic action resources to be put into operation against the Reich's enemies. There were two types:

- The factors that may influence or control exports in commercial war.
- The factors that would enable Germany to overcome the passive resistance in defeated countries.

In the event of victory against the allies Germany knew that it had to face "world hate". Then it would have to face all kinds of reprisals in the defeated countries (supply or raw materials stopped, boycott on its exports, censure of its scientists at international meetings or the poaching of their cutting-edge technology). To justify its fears Herzog quoted an English technical magazine that, at the beginning of hostilities, insisted on the need to launch an economic war against Germany based on science. The British still held resentment from Victorian times due to the stealing of their techniques by the Europeans and Americans. The secret nature of inventions and therefore control of science was for them the basis of all economic warfare. To keep the economic wealth of his country Herzog suggested state control be applied "to the industries that foreign countries have not yet stripped of their capacities". Despite defending this measure he did not question the market economy. Private initiative had to be protected without prejudicing the nation's economic interests. The profit motive encouraged businessmen to relocate their companies to countries which appropriated manufacturing secrets and so became potential competition.

[34] Association of companies that were developed through horizontal and vertical concentration.

[35] S. Herzog, *Le plan de guerre commerciale de l'Allemagne,* Editions Payot, Paris, 1919.

[36] German General (1849-1930), theorist of Pan-Germanism.

As soon as the work of Herzog became known, the Americans had it translated and they spread it extensively. Herbert Hoover, the American Supplies Minister and future President of the United States, stated in the preface of the book's American version that the threat of economic conflict had been clearly understood in this book at the beginning of the century: "not satisfied with military supremacy, Germany was intrigued by commercial supremacy, with an insulting snub towards the rights of others and use of bad faith that has characterised its entire policy since Frederick the Great".

Covering up economic warfare

From ancient times until the time of industrial revolutions, economic supremacy was a constant in the nature of strong relationships between individuals, groups and States. Professor Edward Mead Earl of the Institute for Advanced Study has recalculated the dialectic relationship between the political and economic dimension of power[37]:

> *"If it were possible to separate economic and political power this would only occur in the most primitive societies. In modern times (with the emergence of the National State, expansion of European civilisation throughout the entire world, the industrial revolution and constant progress in military technology), it has been necessary to face the issue of the interdependence between commercial, financial and industrial strength on the one hand and political and military strength on the other. This correlation is one of the trickiest problems in the art of government. It affects a nation's security and, to a great degree, determines the quality of life, freedom, property and happiness that an individual can have".*

The same is true with the realist theory of international relations: despite having ignored the economic aspect in the search for power, the "*animus dominandi"* is described as a constituent element of all human associations and social relationships and therefore of national and international political life. Hans Morgenthau[38] emphasised that international policy is a fight for power. But power is not only military. However, unlike military war, economic warfare did not become a subject for debate in political and academic circles.

How to explain such an omission of strong relationships in compulsory reading with regard to the conflictive relationships between peoples? From the early Middle Ages the nature of the historical phenomenon that is economic warfare has been denied on the pretext that the political jus-

[37] Mead Earl, Edward, *Les Maitres de la Stratégie,* volume 1, Paris, Flammarion, 1986.

[38] Morgenthau, Hans, *Politics Among Nations. The struggle for Power and Peace*, New York, Mac Graw-Hill, 1948, p. 29.

tifications of economic warfare are perceived as actions of illegitimate aggression. The debate on war, barely started by Saint Augustine and Saint Tomas Aquinas, established the bases for the reasoning that identified economic warfare with "a negative vision of war triggered by greed and the desire to get rich at the cost of others[39]". The idea of injustice was quickly associated with wars of conquest. During the discovery of the New World the conquerors had to justify the use of arms against towns that opposed the conquest of their territories. The text *De jure belli* from the Salamanca School (16th-17th centuries) classified the indigenous rebels as disloyal enemies for adopting an impossible attitude against their conquerors. In this way, through the seizure of property and the capture of indigenous rebels (the spoils of war), punishment was justified in the eyes of the Christian world.

The results of this ideological debate, strongly instilled in the history of political ideas, encouraged state figures in economic conflicts to hide their strategy by using different pretexts such as the spreading of religious thought, the modernisation of third world countries and, the most recent way, the development of democracy. This policy, almost systematic in its concealment of the true goals of conquest, distorted the interpretation of the strong relationships linked to a people's survival process or caused by the search, maintenance and increase of a country's power. Maybe a relationship could be found in the fact that, today, there is no doctrine on economic warfare within international military organisations such as NATO (North Atlantic Treaty Organisation). Within the global focus defined by the new doctrine (NATO) 2010[40], the use of economic weapons never appears as an offensive option but as a factor for understanding the environment. This type of omission can be explained by the differences in domestic economic challenges within the community of member states[41].

The disguising of economic warfare is applied both to domination strategies put into operation by colonial empires and recovery strategies by countries that wanted to avoid colonisation or that later sought power.

Dominance strategies

The religious question contributed to hiding the true purpose of conflicts that involved considerable economic benefits. A papal bull of 1452 gave

[39] "Où en est la notion de guerre juste?", François Rigaux, Emeritus professor of international law at the Louvain Catholic University, published in the work *Colère, Courage, Création politique*, volume 1, Paris, L'Harmattan, 2011, pp. 163-177.

[40] OTAN "Concept et doctrine ", official site. http://.www.nato.int/nato_static/assets/pdf/pdf_publications/20120203_strategic-concept-2010-fr.pdf.

[41] Mazzucchi, Nicolas, "Alliance militaire et guerre économique", Revue de la Défense Nationale, No. 752, Paris, 2012, pp. 1-3.

carte blanche to the Portuguese to attack, conquer and subdue the Saracens, pagans and other infidels. A second papal bull of 1454 recognised the Portuguese acts of conquest in Africa by contemplating the possibilities of converting the local populations to Christianity and ratifying the Portuguese commercial monopoly in a territorial area on the Guinea coast as well as all the territories presumably located on the silk route.

In 1494 the Treaty of Tordesillas[42] was negotiated under the authority of the Catholic Church with the Spanish-born pope Alexander VI. He was looking for a resolution of conflicts caused due to the discoveries of Christopher Columbus and established the distribution of the lands of the New World between Spain and Portugal, which were the two emerging colonial powers. The Portuguese also obtained papal recognition of their conquests of African territories and claimed the right to inspect any ship in African waters. This treaty was not recognised by any other European kingdom. Above all, it explained the reality of the strong relationships between the two dominant maritime powers in that era.

After having been hidden under the pretext of evangelisation of peoples that were considered primitive, the disguising of economic warfare was the consequence of a new phase of development of power at the dawn of the industrial revolutions. If military war had evolved thanks to technical inventions, the notion of power had been the subject of an authentic metamorphosis under the impact of the creation of economic empires. The birth of liberalism championed a new way of increasing power through commercial conquest that in turn became an alternative to traditional territorial conquest. The Victorian empire integrated the dynamic of economic warfare, legitimising its reason for being and hiding its purpose through a debate on the opening up of markets supported by the theory of free trade. The imperialist dynamic of the British Empire represented a decisive decrease in the logic of territorial conquest, necessarily politicised, towards a system of commercial conquest, in other words, of control by markets. Therefore, free trade was transformed into the standard for the Empire[43]:

> *"In short, the first economic strategies for increasing power appeared through the creation of an economy-world under British influence. Great Britain, by multiplying economic relationships – based on the leitmotif of Adam Smith "laissez faire, laissez passer" ('let men do, let goods through') – with state units operating both inside and outside its*

[42] Almost all the Americas belonged to Spain, except Brazil. The Portuguese secured control of various coastal territories in Africa, the Middle East (Eritrea, Somalia), south-east Asia (Goa, Colombo, Malacca, Timor), except the Philippines that were claimed by Spain along with the Canary Islands (Atlantic).

[43] Blanot, Harold; Boyer, Adrien;, Kûhl, David and Spiess, Margo, *La guerre économique comme explication structurante de la construction d'un pays*, EGE, Paris, éditions de la Bourdonnaye, 2013.

economy-world, created a free trade zone in which liberalism spread and the market was institutionalised, even managing to venerate itself as a means of pacification in international relationships and the development of participating nations. Consequently the British Empire obtained great benefits from this system which was its great power centre, enabling it to influence the circulation of capital, merchandise and manpower. Aware of its supremacy, the centre of the economy-world (London) could therefore define or even impose commercial policy in accordance with its interests. In this way, between 1840 and 1860 the volume of trade between England and the rest of the world trebled: English industrialists exported their goods to the rest of the world in English ships with the support of English insurers and banks. In addition, the trade balance was approximately 10% in favour of England between the years 1870 and 1914. This growth enabled England to be at the head of those countries on the road to industrialisation, to be the leading maritime power and above all to control almost 25% of the world in 1901. The theoretical application of this change in the way of conquering was in the displacement of imperialist rationale – military and vertical – to that of economic supremacy, with the latter being the capability of one policy to exercise effective sovereignty over foreign political societies without absolutely controlling them[44]*. The transformation of power lead Benjamin Constant to confirm that, "war is no more than a savage impulse whilst trade is civilised calculation". The colonial empires meant the distribution of land in different spheres of influence.*

Commercial conquest could result in commercial war by turning into a resource for coercion when the countries coveted by the British merchants were opposed to voluntarily allowing the penetration of its domestic markets. To impose their products on the Middle East and East Asia markets, the British established the practice of "gunboat diplomacy" that reached its peak during the blockade of the Port of Alexander by the Royal Navy in 1840-1841 and, later, in the two opium wars that, successively, pitted China against Great Britain and China against a coalition of Western countries. It was at that point when the Western world commanded the drug trade through military means on a theoretically independent country.

William Jardine, who managed the opium company Jardine & Matheson in Hong Kong, legitimised this action by making himself the protector of "the freedom of the independent company without restrictions[45]". It is advisable to remember that the pretext given when using force by the British was the embargo and destruction by the Chinese authorities of

[44] Battistella, Dario, "La notion d'empire en théorie des relations internationales ", *Questions Internationales*, No. 26, July-August 2007, pp. 27-32, p. 30.

[45] Brizay, Bernard. *Le sac du palais d'Eté. Seconde guerre de l'opium*, Paris, éditions du Rocher, 2011.

20,282 boxes of opium unloaded at Canton in 1839. The Chinese emperor Daoguang decided to suspend trade with the English and condemn to death any foreign merchant engaged in the opium trade. The British considered the Chinese reprisals as a crime of "commercial treason[46]"and began hostilities that resulted in adopting unequal treaties that "were unfair and whose conclusion left, in the Chinese conscience, the germ of a desire for vengeance that would only increase through successive generations and would take its strength from the resentment that stirred the memory of humiliation[47]".

The opium wars gave such visibility to economic aggressiveness that it took countries like Japan[48] to mould national identity with a power policy based on economic expansion symbolised in the slogan "a rich country, a strong army".

The coming to power of the emperor Mutsuhito in 1868 was the beginning of a series of reforms whose goal was to catch up with the West. Japan took over a century to prepare the basics of an economy in the service of power. At the end of the eighties, the Central Intelligence Agency published the report *Japan 2000*[49] drawn up by a working group made up of figures from the civil and military worlds. This document was one of the few written contemporary examples of a governmental text on the strong economic relationships between two powers. The most explanatory part of the text condemned "Japanese propaganda" of disguising protectionist measures that the country applied to other market economies and its lack of respect for economic liberalism. Some passages in the report stigmatised the Japanese power strategy in these terms: "The members of the *Chrysanthemum Club* (who joined the elite Japanese political and industrial resources) considered that the Western system was doomed to disappear and they acted, as much as possible, in a way that brought forward its end." The Japanese recovery strategy pursued since the Meiji era enabled it to reach second place in the world economies in little more than a century of effort. At the end of the eighties, voices of complaint were heard regarding Japanese expansion and the use of economic warfare techniques in political and economic media by the United States and Europe.

Commercial aggressiveness in the ancient empire of the Rising Sun with regard to the West stopped with the adoption of different measures by the

46 Brizay, ibid. p 35.

47 Leger, François, *Les influences occidentales dans la révolution de l'Orient. Inde, Malaisie, Chine. 1850-1950,* Paris, Plon, 1955.

48 Souyri, Pierre-François, *La nouvelle histoire du Japon*, Paris, éditions Perrin, 2010.

49 The report *Japan 2000,* rapidly withdrawn from circulation due to protests from the Japanese authorities, announced the tension in negotiations between the United States and Japan over the opening up of its domestic market and access to shareholdings in its largest companies.

North American authorities (repeated attacks to break Japanese protectionism, the destabilisation of its banking system by the refusal to grant a currency snake during the Asian financial crisis, a blockade of its techno-globalism strategy[50], limitation of the Japanese games of influence in the North American political administrative system). The fall of the Berlin Wall deprived Japan of its implicit blackmail of the United States. If the United States did not grant Tokyo enough room to manoeuvre for the construction of its economic potential, the North American governmental authorities no longer had anything to fear from the instability of this ally/ancient adversary within the sphere of Soviet influence. Despite this, the brutal blockade of Japanese economic potential did not stop its strategic opportunities for recovery.

Recovery strategies

Recovery strategies were organised around elementary goals strongly dependent on geographic and cultural context. In the case of Japan, as a priority its insularity forced it to equip itself with an infrastructure for maritime purposes (shipyards, ports) and secondly, to establish bases for an industrialised economy. Several countries such as South Korea, India, Brazil and China later followed its example without having to copy its model. South Korea followed the Japanese style by favouring naval construction and the formation of large private industrial conglomerates, *chaebols*, the Korean equivalent to Japanese *keiretsu* or the ancient *zaibatsu* dissolved by the American occupying authorities after the Japanese defeat in 1945.

India followed other models to position itself as a dominant player in the worldwide IT industry. The authorities in New Delhi pursued educational reform between 1993 and 2004 to create a reserve of human resources needed for the development in the field of information technology. For a while the federal government decided to remove from the secondary education programme literary subjects to increase the number of hours spent on mathematics. The goal was to support guidance of the maximum number of students towards technical and IT engineering professions. Gradually from 2004, literary subjects were reintroduced by the authorities considering that the goal had been reached. This policy was also based on transforming the city of Bangalore into the high tech capital. The reasons for its selection were its climate conditions, with it being one of the few places in India where the monsoon's range is weak. In this

[50] Drawn up in 1987 by the Japanese Ministry of Industry and Commerce (MITI), techno-globalism sought to prevent parasitism of research due to competitive practices and thereby fulfil the separation between North and South, creating a common asset of humanity. This occurred after the American tightening up in the field of patents and scientific exchanges with Japan.

way a framework adapted to the return of Indian engineers was created and the life of Western expatriates made easier.

Brazil developed recovery strategies by supporting the energy sector (non-conventional petroleum thanks to its offshore deposits and its Amazon reserves, water for its hydroelectric dams, renewable energies). The Brazilian State[51] made the company Petrobras the vanguard for its strategy of geoeconomic influence. Brazil sought to acquire regional superiority in the energy sector, mainly by adopting numerous bilateral agreements signed with neighbouring countries that gave them a predominant influence in energy provision on the Latin American continent. Regarding soft power[52], Brazil was also improving its image as an emerging power in terms of sustainable development as well as claiming to be one of the cleanest countries in the world thanks to its electrical production.

China has built its recovery strategy by supporting opening up (creation of special economic zones and strong policies for attracting foreign investment), unlike Japan, which sought to gain knowledge by closing access to its domestic market. The meeting point between the two countries consisted of the priority given during their phases of mutual development to the conquest of foreign markets. In both cases this form of commercial aggressiveness resulted in hostile reactions by the United States and high profile debates about the problem of economic warfare[53] in the Western world. China was accused of pursuing a strategy of infiltrating the standardisation organisations for the purpose of imposing its own standards[54]. It has active members on 82% of the technical committees in the International Organisation for Standardisation (ISO) whose headquarters is in Geneva. This participation is higher than France (80%), Japan (79%) and the United States (75%). Suspicion towards China generated different types of reactions difficult not to compare with forms of economic conflict. As an example, let us use the protectionist measures of the Obama Administration regarding photovoltaic technologies and the refusal to allow shareholdings in Western industrial groups, such as the refusal to the request by the Chinese company Minmetal to own part of the Australian company Oz Metal by the Australian government in Canberra.

---

51 Mazzucchi, Nicolas, *L'énergie, source de la nouvelle puissance brésilienne*, Nouvelle Revue Géopolitique, No. 3, Paris, 2012.

52 Indirect action that seeks to place a power in a strong relationship that is to its advantage with regard to the topic of international interest under debate. The soft power strategies also delimit the influence strategies intended so that certain countries agree with the same positions of a power in accordance with its own interests.

53 Dossier *2013, l'année de la guerre économique*, l'Expansion, No. 780, December 2012, Paris.

54 Ibid. p. 44.

Change in the paradigm of economic warfare

The control methods and economic domination devised by colonial empires suffered a mutation under the effect of geopolitical, military and commercial supremacy that the United States assumed at the beginnings of the Second World War. Contrary to the coercive methods applied by the colonial empires in their territorial occupations, the United States established a new model for expressing economic power on the basis of the following principle: a superpower that seeks to dominate an allied country on economic or cultural issues must seek the best position at the top of a hierarchy of values, regulations and arbitrations of the market economy. This manoeuvre for monopoly from the summit entails a new method of understanding economic conflicts. The United States imposed this practice of silent economic warfare in peacetime on the industrialised countries of the Western Bloc. But a geopolitical factor and another of a geoeconomic nature modified this period of stability from economic conflicts:

- Opening of new spaces in the market emerging as a result of the disappearance of the Eastern Bloc.
- Commercial aggressiveness generated by the recovery strategies of emerging economies.

The tightening of worldwide competition caused by the joining of these two factors meant that the United States took economic conflicts into consideration in an almost official way.

Economic security policies

The growth of Asia and the construction of a European economic space affected the geoeconomic predominance of the United States from the end of the Second World War. This redefinition of strong relationships re-launched the problem of economic warfare from a new paradigm: the ally/adversary relationship replaced direct or indirect conflict between two enemies. Economic warfare practiced since ancient times had demonstrated direct conflict: the power that gained territories was directly opposed to the country that tried to resist this conquest. The centuries of colonisation were its clearest example.

The globalisation of exchanges modified the unsettled economic framework both in industrialised countries and in emerging economies. Competition went hand in hand with *co-opetition* (cooperation + competition). Strategic interests of the powers were diversified and became more complex. Military or geopolitical interest could clash with an economic interest or vice versa. In other words, a country could ally with another from a military viewpoint and clash with it on economic matters. In this way a new type of ally/adversary strong relationship

emerged. In practice, it resulted in a reduction in the strong economic relations that had been shown in the past. But this formal reduction did not erase the intensity of rivalry between the powers, in particular in geographical areas where new markets were organised and in areas rich in resources.

The leading economic world power felt legitimised during the nineties to make an economic security policy already started in the seventies, official with the establishment of section 301[55] of the Trade Act of 1974 and the super[56] and special 301[57] of the Omnibus Trade and Competitiveness Act of 1988. The American authorities used the pretext of fighting against unfair competition suffered by North American companies in some parts of the world. If the expression "economic warfare" was not mentioned in official texts the comments of some official representatives of the North American executive power underlined a hardening of their positions in their analyses of commercial exchanges. Carla Hills[58], trade representative from 1980 until 1993, expressed it in her own way using the inverse expression of the carrot and the stick, "we will open foreign markets with a stick if necessary but with a handshake whenever possible."

Despite protests from numerous countries, this unilateral regulation was not abolished. The United States used it from then on as a means of pressurising the body for solving differences in the WTO. The representative of the State Department[59] was equally explicit when commenting on the report on the gas pipeline between Thailand and Burma, "The Total Company has practically replaced Conoco and has obtained a contract that would have been more beneficial for Conoco. We want to punish those companies that have this attitude in the future".

The Torricelli (1992), Helms-Burton (1996) and D'Amato (2001) Acts completed these measures of commercial reprisal stopping hostile countries having access to the United States in order to prevent their companies being able to gain markets in those regions, thereby making them competition to North American companies. With the exception of Cuba, subject to a North American embargo since 1962, countries affected by these acts such as Iraq, Libya, Iran and Nigeria had major oil resources.

55 Section 301 enables the United States to oppose commercial barriers that penalise North American exports.

56 The Super 301 fights against the set of unfair practices registered by the Office of the United States Trade Representative.

57 The Special 301 was conceived to protect North American companies against violation of their intellectual property by foreign competition.

58 Jacob, Yvon and Guillon, Serge, *En finir avec la mondialisation déloyale*, Paris, La Documentation française, January 2012.

59 Revel, Claude, Pedron Liou, Isabelle, *La diplomatie exportatrice des Etats-Unis*, Observatoire du Marché International de la Construction, Paris, 1997.

The Clinton Administration completed this legislative regulation by creating the National Economic Council[60] in 1993, which worked closely with the National Security Council. The North American Secretary of State, Warren Christopher, emphasised the importance of the matter, "North American economic security must be the first priority in foreign policy".

Various countries followed the North American example with differing results. Firstly France created a Committee for Competition and Economic Security in 1995, chaired by the Prime Minister, Edouard Balladur. The life of this committee was short-lived. However, the adopted economic security measures were made permanent under the direction of the Ministry of the Interior. From the first presidency of Vladimir Putin the Kremlin reinforced the role of certain state organisations in the protection of economic wealth and made the governors of the states in the Russian Federation aware of this new mission. China had also followed this path in the previous decade.

The impact of economic strategies on increasing power

Can the mutation in strong economic relations of the ally/adversary confrontational kind be called into question by the economic strategies for increasing power of new figures in the Western world in the global market? Economic weakening of the Western world may emphasise, if confirmed in the medium/long term, tensions between the new conquering powers and industrialised countries that have dominated the global economy in the last century. Various factors might make the problems of conflict and domination reappear:

- Acquisition of energy and mining resources.
- Territorial challenges linked to geographical location.
- Problems of economic dependence.
- New forms of cultural colonisation by the information society.
- Possibilities of investment in alliances.

Currently there is an imbalance between the dynamics of power of the new figures and the way in which the Western world has become accustomed to managing its economic power without real rivals. The priority of new players is the conquest of foreign markets to finance their policy of increasing power whilst the countries of the Western world have separated the problem of power (mainly military and diplomatic) from the rationalities of economic warfare, silenced from the second half of the 19th century. The policy of deregulation that began in the Western world emphasises this paradox. National leaders are being broken up in Europe whilst the new players build their competitiveness focusing on the pow-

[60] Initially it was going to be called the National Economic Security Council but this name seemed too aggressive to European countries.

er of consortiums financed by banks, directly or indirectly controlled by the country's political power. This type of operation is incompatible with the competitive system of the Western world. A competitive imbalance originates from this that weakens the industrialised countries that have separated the question of increasing power from the problem of economic competition. Such an imbalance is reinforced by the importance of finances in the operation of the Western market economy. Financial markets influence the definition of strategic challenges to the extent that politicians prefer the short term as the criteria to define their timing in the construction and preservation of power.

Chinese leaders who have managed to adapt a communist dictatorship to the rules of the market economy have some more ambitious goals than the simple desire for profit. Aware of the hostile reactions that the growth of China might generate, officials of the Chinese People's Liberation Army have invented the term *off-limits warfare*[61]. The balance of the failure of the USSR in its weapons race against the Western world encouraged them to put a preference on methods of conflict that went outside the strictly military framework and that, in part, are a result of economic warfare. The concept of *unrestricted warfare* applied to the geoeconomic field is a way of diverting the rhetoric prepared by the Anglo-Saxon business field. It opens the path to another form of perceiving economic conflicts. During a Franco-American seminar in April 2012 in the United States, representatives of the Pentagon reminded their French counterparts of the sensitive report on computer hacking by China. Taking into account the range of the phenomenon they were asked whether it would be appropriate to classify this type of aggression as an act of war instead of an act of industrial espionage. This change of vocabulary reopened the debate on the issue of denial or validation of economic warfare. The United States managed to guide the debate in the direction of the denial of economic conflicts between powers (see the economists' dominant discussion). This pacification speech on the exchanges in the *global village* of globalisation is justified by the benefits obtained from its status as a superpower since 1945.

Limits of western ethnocentrism

The West has dominated the world thanks to the colonial empires and later to the North American superpower. The questioning of colonisation (the clearest example of economic warfare of all time) opened a geopolitical[62] split that remained hidden by the victory of the Western Bloc over the Eastern Bloc as a result of the collapse of the USSR. The promotion

[61] Liang, Qiao and Xiangsui, Wang, *La Guerre hors limites*, Paris, Payot et Rivages, 2003.

[62] The loss of colonies had political repercussions in some countries. In Belgium the linguistic conflict between the Flemish and Walloons became a national problem from 1962.

of emerging economies opened a geopolitical split shown by the process of deindustrialisation and the weakening of some Western market economies. These two splits emphasised the limits of Western ethnocentrism that caused strong relationships to be analysed, starting from the principle that the strong could only be from the Western side.

The contradictions between the United States and Europe

In this game of cards the Western world is weakened by numerous contradictions. The first recalls the tale of the "sprinkler sprinkled". Great Britain and later the United States used liberalism to legitimise the dismantling of protectionist systems of countries-clients in order to support the sale of their goods and their domination on international financial mechanisms. Today it is difficult to reverse this policy because it would mean delivering a fatal blow to the validity of the discussion. The second contradiction is American. Important private interests on the other side of the Atlantic, both industrial and financial, try in the short term to make use of opportunities that the globalisation of exchanges offers. The flexibility of liberal discussion enables them to legitimise relocations and the effects of deindustrialisation. The debates in the United States Congress show the often unfair fight between the power groups supporting the opening up of markets and the forces that prioritise the safeguarding of the interests of the resident population in America. The third contradiction is the inability of the European Union to be confirmed as a power that is aware of the importance of the challenges in economic warfare.

Since the post-war era, negotiations on the compensation for beneficiaries of the Marshall Plan opened strong debates in France on some of the American economic conditions such as the tax on American soybean used as animal feed or Hollywood cinema distribution in its cinema market. When he returned to power in 1958, General de Gaulle defined the criteria for a national independence policy that opposed American interests:

- The creation of Elf Aquitaine, an oil consortium, to reduce France's dependence on the seven Anglo-Saxon oil companies.
- The setting of quotas to limit the establishment of multinational American companies.
- The end of the argument about the predominant role of the dollar as the global reference currency.

The Gaullist vision of national independence did not resist the liberal allegation with regard to the opening up of markets. The liberal doctrine eliminated any possibility of structural discussion about the nature of economic conflicts despite there being commercial differences between the United States and Europe that occasionally disrupted the GATT and World Trade Organisation negotiations. The European market construc-

tion served as a pretext even for marginalising intellectual thought on the role of the economy in the construction of power.

In 1976, Giscard d'Estaing and Raymond Barre dismantled the instruments designed to provide French industry with the capability to respond in terms of economic power. This was how the Plan's Permanent Commission on Electronics was abolished. This commission was the meeting point for the general managers of the sector's large companies, representatives of professional organisations, SMEs and Ministries. The topics submitted for debate referred to French strategy in strategic sectors such as IT, telecommunications, aeronautics and electronics. This commission originated from the raising of awareness in the sixties about the essential need to provide France with a sufficiently powerful electronics industry in order to free it from North American domination. The Plan's Commissioner had even created an IT system called Mars that was a database created from information flows generated by 250 companies, 30 administrative services and 23 trade unions. Information flowed in both directions since the industries could access it under certain conditions and thereby improve their contribution to innovation *et leur approche du marché mondial*. On the state side, the Mars system enabled the measurement of the effectiveness of the credit injected into the electronic sector. Extending it to all French industry was considered. On that occasion *Le Monde* newspaper emphasised that French multinationals had never accepted playing the role of a power strategy focused on France and preferred to cooperate with American companies. In this way a fracture line arose between those who were in support of a globalised market and the defenders of an economic territory. This contradiction, despite being fundamental, was not taken into account when the Prime Minister, Dominique de Villepin, reopened the debate on economic patriotism at the beginning of 2000.

Far from being an artificial or obsolete debate, the topic of economic patriotism was fed by the negative effects of the emerging economies' recovery possibilities. Their appeal, represented by cheap labour, did not serve as an explanation for everything. Certain emerging countries have been transformed into *combat economies* to now be on the same level as Western economies. They have done nothing more than reproduce the techniques started centuries ago in the Western world. You only have to reread history. After the revolutionary wars France did everything possible to try to make up for its technical shortcomings compared to the United Kingdom, turning to the trafficking of machinery imported clandestinely from Great Britain and to industrial espionage on British manufacturers. The offensive strategies of the emerging economies have completed this panoply of offensive techniques using an engineering of information gathering, greatly amplified thanks to the internet, the theft of patents, the practice of dumping, to the industrialisation of imitations, without forgetting the illicit trafficking of metals such as copper due to

global demand. These unfair actions contribute to the degradation of the economic supremacy in the Western world and it is becoming a topic of concern in the United States. In Europe it is relegated to the category of exceptions that prove the rule, in other words there is a blind belief in the supremacy of the liberal model.

The bad effects of the liberal model

The United States did not hesitate to provide itself with a coercive system for the penalisation of acts of pillage or economic isolation by hostile countries. Brussels sometimes imitates Washington's behaviour but it does not usually put theory into practice. In 1984 the European Union was provided with an instrument of commercial reprisal[63] inspired by section 301 of the American Trade Act. Equipped with this weapon against the illicit practices of third party states in sectors not regulated in the GATT agreements, the European Union only exceptionally[64] resorted to this type of pressure that can be compared to a kind of economic warfare in peacetime.

The impossibility of a unified idea about the geoeconomic priorities of the country emerging in a country like France is not a result of a cultural blockade. The European Union is limited to agreeing the preventive regulations that the member states can take against risks of economic pillage and unfair competition. Protection of the perimeter of national defence and public order is the only room for sovereign manoeuvre recognised by the Brussels Commission. In 2006 the European executive decided on some infraction procedures that penalised attitudes contrary to the rules of the internal market by copying the decree against the French takeover, which required the request for prior authorisation from the French authorities by foreign investors that wished to take control or have a minority share of 33.33% in companies in 11 sectors of activity considered strategic.

Unlike Great Britain, the Netherlands or Germany, which integrated the disguising of economic warfare in their modus operandi, France sought validation of its room for manoeuvre through official texts recognised at a European level. During the first year of his term[65], Alain Juillet, the Senior Executive for Economic Intelligence, took months to convince his representatives on the European Commission to accept the industrial energy

[63] This type of tool made it possible to fight against countries that practiced unfair competition, imposing penalty measures on exchanges with European Union countries: quantitative restrictions on export, and an increase in customs duties.

[64] Used on six occasions within a ten-year period.

[65] His mission regarding commissioning of Economic Intelligence in the National Defence Secretary-General (Secrétariat Général de la Défense Nationale, SGDN) will last from 2003 to 2009.

sectors that France had wanted to protect better. To justify its refusal, the European Union claimed the exemplary application of liberalism standards as a pacifying element in the exchanges. This attitude was far from unanimous on the Eurasian continent. In December 2008 the Russian government established a list of 295 companies considered as strategic, without omitting those in the energy sector[66]. Vladimir Putin added 1500 companies that were essential for the national economy and qualified to receive state assistance, tax amnesties and customs privileges. The warning from the Russian Head of State to his European counterparts about the risk of a cut in the gas supply demonstrated the strategic fragility in Europe when providing energy during this period. On this specific topic the liberal doctrine that focused European thought on the deregulation of a market open to competition did not seem suitable for the situation. However, this defect did not force the search for a unified position between the European members[67].

Conclusion

Globalisation has long been rightly regarded as the carrier of positive factors such as rising living standards of the populations of industrialised countries, the process of negotiating trade disputes, progressive regulation of trade and the strengthening of protection thanks to the recognition of international patents. But this "mixed" world product of globalisation has not pacified the economy. The geoeconomic balance in the world playing field is much more deeply multipolar now that the market is global. The growing rivalry between the Western world and the new actors weakens the dynamics of appeasement driven by a dominant Western world.

The question could be asked of whether Europe has learnt its lesson from world wars that made it lose its supremacy or whether it has managed to correctly measure the importance of the threats that hang over its geopolitical and geoeconomic future. Devoid of analysis on economic conflicts and incapable of drawing conclusions on its strategic development over centuries, today Europe is still lagging behind the United States. Despite appearances it is more divided than ever by a co-existence that it does not want to name. Northern Europe is led by Germany, which plays a double game in discreetly supporting the rebirth of its power whilst projecting an image of a deeply pacifist country due to its previous military errors. Southern Europe is trying to overcome its infrastructure crisis. The Europe made up of former socialist countries is trying to find a path that is still heavily influenced by the strategies of America, Germany and Russia.

To escape this cul-de-sac without a strategic exit it is important to consider new obligatory reading on economic warfare. It seems logical to

[66] The gas group Gazprom and the oil companies Lukoil and Rosneft.

[67] Germany had signed a bilateral agreement with Russia in 2000.

consider a new political economy based on proper coordination between the construction of power in a state, command in the conquest of markets and the development of territories. These three strategic dimensions are not naturally compatible. Political power must be provided with the resources to define a programme of the challenges and priorities in the short, medium and long term. Today the European Union is incapable of doing so. However, this is an absolute priority.

Bibliography

Esambert, Bernard, *La guerre économique mondiale*, Paris, Olivier Orban, 1991.

Carayon, Bernard, *A armes égales*, Report to the Prime Minister, Paris, Assemblée Nationale, 2006.

Crouzet, François, *La guerre économique franco-anglaise au XVIIIe siècle*, Paris, Fayard, 2008.

Delbecque, Eric, Christian Harbulot, *La guerre économique*, Paris, Que sais-je, PUF, 2010.

Denécé, Eric and Revel, Claude, *L'autre guerre des États-Unis, Économie: les secrets d'une machine de conquête*, Paris, Robert Laffont, 2005.

Fonvielle, Dominique. *De la guerre économique. Défense et défis nouveaux.* Paris: Presses universitaires de France, 2002.

Fourquet, François, *Richesse et puissance, une généalogie de la valeur*, Paris, La Découverte, 1989.

Gauchon, Pascal, *Le Monde, Manuel de géopolitique et de géoéconomie*, Paris, PUF, 2008.

Harbulot, Christian, *Techniques offensives et guerre économique*, reedition, Paris, éditions de La Bourdonnaye, 2012.

Harbulot, Christian, *La main invisible des puissances*, éditions Ellipses, Paris, 2007.

Harbulot, Christian, *Manuel de l'intelligence économique*, collective work, Paris, PUF, 2012.

Huissoud, Jean-Marc and Munier, Frédéric, *La guerre économique, Rapport Anteios*, Paris, Puf, 2010.

Laïdi, Ali, *Aux sources de la guerre économique, fondements historiques et philosophiques*, Paris, Armand Colin, 2012.

Laïdi, Ali and Lanveaux, Denis, *Les Etats en guerre économique*, Paris, Le Seuil, 2006.

Leonetti, Xavier. *La France est-elle armée pour la guerre économique?* Paris, Armand Colin, 2011.

Lucas, Didier and Tiffreau, Alain, *Guerre économique et information*, Paris, Ellipse 2001.

Luttwak, Edward, *Le rêve américain en danger*, Paris, Odile Jacob, 1995.

Nadoulek, Bernard, *L'intelligence stratégique: philosophie de l'action face à la mondialisation cultures, économies et rapports de puissance*, Paris, Centre de Prospective et d'évaluation, Ministère de la Recherche, 1990.

Nora, Dominique, *L'étreinte du samouraï, le défi japonais*, Calman-Levy, Paris, 1991.

Liang, Qiaoand Xiangsui, Wang, *La Guerre hors limites*, Paris, Payot et Rivages, 2003.

Soutou, Georges-Henri, *L'or et le sang,* Paris, Fayard, 1989.

Chapter III

Legal intelligence: the strategic value of the law in economic security

José L. González Cussac

Abstract

In the present context of globalization, where new technologies have taken on prime importance, the idea of *legal intelligence* is developed. In addition, in this area there has been a development in the idea of geopolitics towards the idea of geoeconomics, with the rise of the notion of "economic warfare" or "fourth generation warfare". The basic premise is that all human activity is subject to regulations that influence the economy and intelligence. On this basis, the paper examines the law as a matter of intelligence and the law as a tool of intelligence. The conclusion is that the law is strategically valuable. The one who is capable of creating and imposing rules commands a decisive advantage, and the competitors who do not know the meaning of those rules are not in a position to compete on equal terms.

Key words

Legal intelligence, regulatory Trojan horse, economic security, legal security, national security, economic and competitive intelligence, rules and law.

Approach

Politics, Law and Economics show different patterns of marriage throughout history. They are actually ways of exercising power. Power is domination, within a scenario of confrontation or competition, and in the framework of the rules of the game. In the past century we witnessed a model of colonial domination, and later another post-colonial domination during the Cold War. Currently we are witnessing a new geopolitical scenario in which domination is exercised by other mechanisms. Globalisation is the key, and in the words of Juillet brings together two types of economy that are far from coincidental: the market and the state. However, the end of the "East-West" confrontation has led the confrontation towards economic competition, which has placed the "market economy" in the geoeconomics of the Great Powers. This universal competition in which both traditional and emerging powers participate, reaching over two hundred countries, requires new rules, both national, regional and international, to referee the game between multiple interests and to determine the distribution between dominant and subordinate countries. And in this great game of power, interests and rules, and new technologies play a fundamental role[1].

In this context, various authors (following Clausewitz) now speak of the economy as a continuation of the war, so that we would be dealing with a "covert economic war" (Harbulot)[2]. Therefore, we would have gone from *geopolitics* to *geoeconomics*[3]. Countries gamble their sovereignty and the citizens their welfare. On this new board, non-state factors and actors with exclusive economic motivations (financial markets) are also involved, but there are also actions of influence and destabilisation led by government actors. And closely linked with this starting point is the idea that the "new war" is playing out, mainly, on the World Wide Web (*cyber war*)[4], and largely, within what we usually call economic espionage (Clarke and Knake)[5].

The economy and its resulting economic and competitive intelligence are today more than just an essential component of national security

[1] Juillet, Alain (2006), "Principios de aplicación de la inteligencia económica", *Intelligence and security: Journal of Analysis and Prospective*, No. 1, December, 2006, p. 123.

[2] Harbulot, Christian (1992), *La machine de guerre économique: États-Unis d'Amérique, Japon, Europe*, Paris, Economica. Also Carayon, Bernard (2006), *Patriotisme économique: De la guerre à la paix économique*, Monaco, Editions du Rocher.

[3] An excellent development and explanation at Olier Arenas, Eduardo (2011), *Geoeconomía,* Pearson Prentice Hall.

[4] Olcott, Anthony (2009), "Revisiting the Legacy: Sherman Kent, Willmoore Kendall, and George Pettee - Strategic Intelligence in the Digital Age", *Studies in Intelligence* Vol. 53, No. 2 (Extracts, June 2009), pp. 21-32.

[5] Extensively in Clarke, Richard A. and Knake, Robert K (2011), *Guerra en la red: los nuevos campos de batalla,* Barcelona, Ariel.

as we used to know it (Potter)[6]. And as Juillet might warn, globalisation and lack of regulation have essentially defined the geopolitical arena, in addition to traditional state actors, companies and other subjects of civil society[7].

Perhaps by sharing this analysis, although from different angles, authors such as Joseph Stiglitz, Paul Krugman and Alain Touraine, among others, believe that the initial financial crisis of 2008 has become not only a global economic crisis, but a real political and social crisis. In a way, we are witnessing a true and complete global paradigm change: geoeconomics has entered the scene. And with it the development of various models of "economic security" (Buzan, Waever, Wilde)[8]. National security can no longer be reduced to its classical content, or economic security, without a human dimension. Thus, economic security as a component of national security is not only measured by traditional economic criteria of wealth (also the availability of goods and services, stability, levels of protection, etc.) and transfers the centre of gravity from the idea of security of States to the security of people.

However, the deregulation of trade and investment, that is, certain effects of globalisation, involves a progressive loss of the ability of nation states to regulate these activities and in turn to deliver goods and services to its citizens. Therefore, States, including all their domestic legislative frameworks, have lost decision-making capacity but continue to support the security demands of their citizens.

The current global economic crisis must be added to this aforementioned panorama of profound change, which has revealed (when not caused), a serious instability and insecurity throughout the international system, and not just in economic terms. The availability of strategic resources and raw materials, capital flows, the burden of the welfare state and institutional operations are to some degree determining factors in regions and countries, which are now at the crossroads. And like any great economic crisis this causes a deep expansion with effects (with varying degrees of impact) in all areas and actions, and therefore carries an additional risk of utmost importance for political stability. We know that the evolution of these factors accentuates social differences and therefore represents an ideal scenario for social unrest, the rise of populist movements and the rise of radicalism. All of which, combined and agitated,

---

[6] Potter, Evan H (1998), editor, *Economic Intelligence and national security,* Carleton University Press. Cfr. Arnett, Dennis, Menon, Anil and Wilcox, James B. (2000), "Using Competitive Intelligence: Antecedents and Consequences", *Competitive Intelligence Review,* Vol. 11, Issue 3, pp. 16-27.

[7] Venegas González, Álvaro (2008), "Inteligencia económica: un componente estratégico por desarrollar", in *AA Intelligence*, Year 1, No. 2, Chile, pp. 10-19.

[8] Buzan, Barry, Weaver, Ole and De Wilde, Jaap (1998), *Security. A new framework for Analysis,* London, Lynne Rienner Publishers, pp. 95 *et seq*.

constitutes the greatest of dangers to the democratic systems and the Rule of Law[9].

The above demands a need to change, update and revise regulatory models, in order to strengthen their own institutional system of democratic Rule of Law, which is the only system capable of offering minimal legal security to guarantee civilised coexistence.

This task involves the development of standards and interpretive practices of self-protection and cooperation, as well as legislation likely to provide a greater capacity to compete on equal terms with other countries in its sphere. The law is viewed from this perspective as a first-rate strategic weapon to deal with a "fourth generation" war, where asymmetric actors alone or in alliance with other states, can coordinate attacks on countries, companies or financial systems with serious damage to national security, in which the economic rights of citizens are an essential component.

In this scenario, economic intelligence, as part of the global economic policy and a basic component of national security, should organise its strategy in a regulatory system that allows it to achieve its objectives. These specific objectives are focused on the following basic aspects: **a)** to ensure strategic surveillance in order to facilitate public and private decision making; **b)** to sustain the competitiveness of companies and the ability to transfer technology from research centres, and **c)** to ensure the economic security of companies and research centres.

Consequently, an economic intelligence system must today be based on an adequate regulatory policy, both nationally and internationally[10]. That is why we can speak about the need to develop a *legal intelligence* with value and a strategic projection.

The law as a collection of regulations

Wittgenstein staged an authentic revolution in philosophical thinking of the twentieth century, particularly towards a "conceptual clarification". This thinking has led to a decisive turn in philosophy, social science and the Law[11]. Therefore, for the purposes of this work, I wish to underline that I take as a starting point one of its central ideas: that all activity

[9] González Cussac, José Luis and Larriba Hinojar, Beatriz (2011), *Inteligencia Económica y Competitiva: Estrategias legales en las nuevas agendas de Seguridad Nacional*, Valencia, Tirant, pp. 13-14.

[10] Pooley, James and Halligan, R. Mark (2000), "Intelligence and the Law", in Miller, Jerry (ed.) *Millennium Intelligence: Understanding and Conducting Competitive Intelligence in the Digital Age,* CyberAge Books, Medford, NJ, pp. 171-187.

[11] A masterful development and application of criminal Law from the thinking of Wittgenstein can be seen in Vives Antón, Tomás Salvador (2010), *Fundamentos del sistema penal*, 2nd Edition, Valencia, Tirant lo Blanch.

is subject to rules – beginning with language itself – or better yet, that activities only have meaning and significance from their understanding through rules. The law, economics, economic security and economic intelligence are no exception: without rules it is not even possible to speak of them[12].

The law is a positive collection of regulations, i.e. imposed by the authority that has the power to do so. Therefore, the Law also regulates the economy and intelligence: all human activities are regulated, subjected to the "Rule of Law", this is the essence of democracy.

Therefore, the constant tendency in the last decades of the policies of deregulation, *self-regulation* and "codes of good governance" in certain economic areas, have from the start represented a thorny issue, to say the least.

A second central aspect lies in the emergence of a new global legal order, with spatial and temporal conditions different to the traditional ones, framed within the globalisation process. The central categories of law such as sovereignty, nation-state, and the constitution are facing new challenges and restructurings (Jáuregui)[13]. In particular, this highlights the need to structure time, taking into account not only the present but also the future, a major challenge for the Law that will involve the drafting of a new "social contract". And secondly, the transition from one scenario of nation states to another of supranational scenarios, which in turn demands a conceptual change from the idea of "government" to "governance" that is broader and less formalised. This emphasises the impossibility, in an era of globalisation, of states not subject to external restrictions. To this must be added a lack of international order, an unbearable asymmetry in international relations and therefore a constant delegitimisation process of all existing institutions. In short, we are faced with the need to transform legal institutions to adapt them to new social, cultural, political and economic parameters.

Therefore, in this new context, **economic intelligence** also cannot be burdened with the macroeconomic analysis of regions, sectors and countries, or directed solely to the scrutiny of organised crime in its many facets, or only offer protection of industry and technology in a dual use,

[12] On the ambiguities and difficulties of language, and in particular applied to the legal environment of industrial secrecy, espionage and competitive intelligence, can be seen the magnificent exhibition of Horowitz, Richard (2011), *Competitive Intelligence, Law and Ethics: The Economic Espionage Act Revisited Again (and Hopefully for the Last Time),* SCIP, Vol. 14, No. 3, July/September 2011, pp. 45-46.

[13] Jáuregui, Gurutz (2011), "La emergencia de un nuevo orden jurídico-institucional: el Estado y la Constitución de la era de la globalización", in Innerarity, Daniel, and Solana, Javier, editors, *La humanidad amenazada: gobernar los riesgos globales,* Barcelona, Paidós, pp. 237 *et seq*.

or even just trying to stabilise the financial system[14]. When speaking of economic intelligence we normally stress the risks associated with the profitability of an investment, but often ignore both the examination of the political risks associated with the investment itself (although these are increasingly taken into account), such as the risks associated with its legal insecurity. Both risks being, as evidenced by recent world events, much more important than financial ones.

Consequently, to transfer this approach to the Law intelligence can also not stop at providing legal tools in all these areas, or by adding the need to develop counterintelligence work. It should also encourage, for example, rules that stop or reduce external actions aimed at altering the normal functioning of markets and of course it has to enable the deployment of actions of influence within and outside of national borders.

In this sense, the proven experience of the legislation on the defence industry and the regulation of technologies of "dual use", that specifies a strong link between seemingly different matters, such as military and commercial, are an excellent example of the path to follow. But they are just good guidelines or necessary indicators of a sophisticated regulatory policy.

In any event, the Law is the only instrument that provides an essential value in the coexistence and human relationships of all kinds: ***legal security***. The measurement of this essential concept, with its complex interweaving of rights and guarantees, of times, delays, procedures, of a legal independent power, of the quality of legislation, stable applicable practices and, ultimately, order and guaranteed formalised institutional functioning, decisively influences the actions of the various economic, political and social interests. Legal insecurity has a high economic cost. And this cost is also related to the degree of corruption in a state and its association with transnational criminal organisations and groups[15]. And of course we must not forget the cost of social exclusion, with its levels of conflict and consequent risk of instability[16]. This is a tremendous political risk.

Thus, the Law, as a collection of regulations of mandatory compliance, is crucial in any human activity, especially in the following fields specific to this problem.

---

[14] Bégin, Lucie, Deschamps, Jacqueline and Madinier, Héléne (2007), *Une approche interdisciplinaire de l´intelligence économique*. Cahier de Reserche No. HES-SO/HEG-GE/C--07/4/1-CH, Haute École de Gestion de Genève, 2007.

[15] All indicators show a significant increase in prosperity in Latin American countries and the consolidation of an emerging middle class. However, this progress is hampered by social inequality and civil insecurity. Serrano Monteavaro, Miguel Ángel, *La nueva clase media Americana. Hacia una mayor seguridad económica y social*, Information document, IEEE 02/2013, December 2012.

[16] Essential explanation by Stiglitz, Joseph E. (2012), *El precio de la desigualdad*, Madrid, Taurus.

Firstly, the collection of regulations applicable to the intelligence cycle, in particular, to intelligence and economic and competitive counterintelligence[17], and especially to covert actions and influence[18]. What is particularly important here is the serious problem of industrial, commercial and technological espionage[19], and all the new problems associated with cyberspace and its regulation[20].

Secondly, the Law must offer sufficient and effective protection to companies and research centres, preserving their security and competitiveness. This involves coordinated regulation from various government bodies with competency in areas as diverse as foreign affairs, international relations and cooperation, security and justice, tax, industry, tourism, agriculture, fisheries, public works and infrastructure, education, culture, science, research, technology, entertainment, and the environment. But besides a protective regulation of all these fields, states must also implement another policy capable of increasing the transfer capacity of public and private research centres to companies and also offering regulated encouragement to companies.

Ultimately, economic policy must be translated into effective laws that support sustainable economic development, which is not incumbent solely on institutions and companies but also on individuals. And intelligence should also be applied to this task, and to do this we need to have different organisational models[21]. This is about the understanding of regula-

[17] Bradford, William (2007), *The three faces of competitive intelligence: defection, collusion and regulation*, University of Florida, Warrintong College of Business, 19th February.

[18] Extensively in González Cussac, José Luis and Larriba Hinojar, Beatriz (2011), cit., pp. 89 *et seq*.

[19] As stated by Horowitz, Richard (2011), *Competitive Intelligence, Law and Ethics: The Economic Espionage Act Revisited Again (and Hopefully for the Last Time),* SCIP, Vol. 14, No. 3, July/September 2011, p. 43, one of the biggest problems in this area is that although theoretically there is a difference between espionage and the lawful obtaining of information, in legal practice it is very difficult to draw the difference between legal and illegal methods.

[20] Larriba Hinojar, Beatriz (2013), "Ciberespionaje Económico: Una amenaza real para la Seguridad Nacional", in *Nuevas amenazas a la seguridad nacional. Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación,* (Directors José L. González Cussac and María Luisa Cuerda Arnau; Coordinator Antonio Fernández Hernández), Valencia (Tirant) 2013, where the author emphasises that economic cyber espionage is one of the most serious threats to national security in the twenty-first century. Also see González Cussac, José Luis, "Estrategias legales frente a las ciberamenzas", in *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*; Instituto Español de Estudios Estratégicos, Ministerio de Defensa, Strategic Dossier No. 149 (Madrid 2010), pp. 85-127; and also see**:** "Tecnocrimen", in *Nuevas amenazas a la seguridad nacional. Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación,* (Directors José L. González Cussac and María Luisa Cuerda Arnau; Coordinator Antonio Fernández Hernández), Valencia (Tirant) 2013.

[21] Ugarte, José Manuel (2005), *La relación entre inteligencia y política, y sus consecuencias en las estructuras y normas de los Sistemas de Inteligencia,* Brasilia.

tions that govern any human activity. This involves not only quantitative or descriptive analytical work regarding laws, but essentially a qualitative understanding or interpretation of their significance and their effects and consequences.

The law as an object of intelligence

In the previous section we assumed that all activity, as if it were a game, including economic and correlative intelligence activities, is subject to rules: for better or worse, defined or vague, sufficient or insufficient. Even the absence of rules expresses the application of a rule: that of the strongest. But at the end of the day there are always rules. Therefore, it is obvious that the player who produces, creates and enforces rules has more advantages. And in any case, the player who does not know the rules of the game properly is a daredevil and a more than likely a loser.

Both aspects, creation and knowledge of the rules, must be present and will be dealt with separately.

Whatever is the objective to be reached, the *players* or competitors must try to impose their rules. In legal theory the effect is distinguished between the material sources and the formal sources of creating regulations. The first, the materials, refers to the different social powers with the ability to drive, to influence or to condition legislation. The second, the formal sources, allocate the different procedures formalised regarding the creation and manifestation of the Law. Both state and non-state actors operate on this plane. And the playing field is basically limited to two spatial environments: the *territory* where a state has sovereignty (domestic legislation) and beyond its borders, in the international scenario.

In principle, within its territory the state is sovereign to produce the Law that it deems appropriate and necessary, reconciling different conflicts of interest. On this plane the state has *potestas and autoritas* to decide, at least theoretically, the relevant law according to its national interests and according to its material and formal procedures of legislative output. From the outside, their international commitments are only bound and conditioned when transferred and included in internal regulations (treaties, conventions, agreements, associations, etc.). Naturally the degree of real sovereignty will depend on multiple internal and external factors, which does not exclude the need to monitor and control them sufficiently in order to avoid external regulation causing dependency and subservience to outside interests.

In the international circuit the state and non-state actors also play an essential role in the material and formal production of legal rules. Hence the need for the presence of any state in all international institutions of decision or deliberation. Equally essential is to have a regulation that makes

it possible to exercise influence on foreign actions, within international law. Therefore, states should encourage proactive action legislatively over any organisation or actor capable of generating an impact on economic activity, either through communication, public relations, influence or lobbying. For many authors, the global economy is determined by the power of no more than 120 large multinational corporations. Combining this material power with that deployed by states is what today constitutes the major challenge in this field.

The second aspect to be developed lies in the need to utilise ***legal intelligence*** resources to know the best possible laws and legal practices of a country or of international regulations, for without knowledge of the rules it is impossible to compete on equal terms, let alone at an advantage.

Knowledge of legislation, case law and other practices and customs is essential to ensure an investment in a foreign country. It is not enough to know or master employment, commercial, criminal or tax laws. A fundamental task of economic intelligence, developed by both public and private services, is to detect highly unstable environments that are dependent on the total discretion of their governments, or those managed by pressure groups or even corrupt groups. This is not just to provide merely descriptive information, but genuine *legal intelligence*, that is, qualitative. This also implies the knowledge of the parties involved.

Legal intelligence in general we could define as the type of intelligence that deals with the collection, processing and protection of strategic information that is useful for all legal economic acts. It is a process that includes among its key objectives giving strategic and legal meaning to environmental information. This means that the value added to the information comes precisely from the capture of its meaning, interpreted from a strategic perspective. The "search, treatment and transformation of information of regulatory use in legal knowledge" and their purposes include:

- Protecting individuals and companies from litigation, or at least, to deal with it in the best possible conditions. This demands a precise knowledge of applicable rules and practices, and in any event requires deploying preventive or defensive strategies through the anticipation of the search and consolidation of evidence.
- Guaranteeing the recognition and legal protection of social or corporate rights and intangible assets of companies and citizens. The protection of sensitive information of a company is achieved, firstly, through profound and accurate knowledge of the regulations and practices on intellectual and industrial property. Secondly, recognition and proper legal protection of a company is obtained through "lobbying" awareness of all actors involved (legislative, administrative, economic, media, etc.) to the needs of a company.

These types of actions of influence cannot be confused with undue influence or corruption, as it is limited to expressing the opinion of the company about the type of laws and the applications that they favour[22].

- Defence of the company image, reactive communication, and campaigns exposing the agreement to practices that are always legal and ethical. Here the key lies in internal action protocols designed to prevent or mitigate destabilising actions through various mechanisms of use of the Law. The need to provide specialised means with internal protocols of reactive legal strategies that are immediate, compared with media campaigns orchestrated by a competitor, by initiating legal processes that, although risky, make it possible to denigrate or diminish the value of a company *("informational risks"),* for example, before a market exit or entrance. Or a search in legal proceedings to obtain sensitive information about a company or individual. Remember that also in the legal sphere the advantage is always with he who attacks, who demands or claims. Hence the need to reduce the possibilities of surprise[23].
- Legal surveillance offered by competent and reliable advisors to safeguard tangible and intangible equity, contractual confidentiality rules, a patents policy, that is, deciding whether to patent or to operate the invention before but with an adequate protective system, tackle fraudulent practices like "bait patents" or the flooding of patents on the market to confuse them compared to the genuinely useful, etc[24.]
- Before negotiation processes with other companies, and possible takeover attempts by larger competing companies, they should organise agreements between shareholders that reinforce these

[22] In the last few months we have seen a strong debate on various legal initiatives by countries such as the United Kingdom, Spain, France, Germany and Italy, in order to reduce "tax competition" between several European countries. Indeed, for several multinationals, such as Amazon, Microsoft, Apple, Facebook, Inditex, Samsung, Starbucks etc., imitating the giant Google, took advantage of the opportunities provided by the different domestic tax laws, to avoid or reduce the payment of taxes. Therefore, the profits are attributed to subsidiaries, which act as intermediaries, declared in states with a low tax rate, such as Ireland, Luxembourg, Netherlands and even Bermuda. To prevent this leakage of revenue, these countries are trying to standardise their domestic laws with the intention of fixing the obligation of contributing to the place of business and generation of profits, and not in the place of corporate residence.

[23] A recent good example is the surprise legal attack suffered by the Argentinean frigate "Freedom" in Ghana, triggered by a foreclosure lawsuit filed in a New York court by NML Capital investment fund, which persuaded the Tribunal of the Law of the Sea, based in Hamburg (Germany) to instruct the courts of the African country to confiscate the Argentinean Navy Training Ship, due to a debt of $300 million, unpaid since 2002.

[24] Cfr. Larriba Hinojar, Beatriz (2006), *La tutela penal del diseño industrial*, Valencia, Tirant lo Blanch.

foreign entries of new partners, that on occasions seek the control and destruction of the brand, or at least the corporate domain.

Therefore, the fundamental mission of the Law is "to ensure economic security" by identifying the risks of interference in national companies and research centres. In this sense it must develop procedures which offer sufficient protection and deterrence. Legislation must tackle competition in an open global economy, which faces advantages in terms of growth but must also confront established powerful actors and emerging ones.

It is essential, therefore, to develop a concept of economic security linked to the broader category of security and in particular national security, detecting threats and thus promoting regulation that is both preventive and penalises noncompliance. This would include economic security in a strict sense (commercial deregulation, tariffs, protectionism, inflation, financial instability, market volatility, lack of transparency in investment), commercial security (international crime, terrorism, espionage, cyber-attacks, corruption), food security (food reserves, agricultural and fisheries subsidies, genetically modified foods, bio fuels), energy security (reserves and continuity of supplies, rising prices), environmental security (global warming, nature reserves, prevention of natural disaster emergencies), consumer safety and health (infectious diseases, genetically modified foods, biotechnology), social security (employment, coverage and assistance, pensions).

In fact, the ***economic security*** category would include a broader one together with other more established ones such as the aforementioned national security, collective security, common security, human security, cooperative security and sustainable security[25].

Legal intelligence must cover both the domestic market as well as overseas, and it must encourage a regulation that allows fluid coordination between central, regional and local administrations with different types of companies. Here lies the convenience of the creation or improvement of public companies in strategic sectors, as well as the promotion of stable cooperation forums between the public and private sectors.

New information technologies also make work in this field easy, quick and in real time by enabling knowledge about the Law and applicable practices that is both quick and accurate. Its combination with the use of highly-trained human sources allows the bringing together of unlimited technical capabilities that provide detailed analyses for decision making, and at the same time also enable the deployment of multiple actions of

[25] Ballesteros Martín, Miguel Ángel and Joyanes Aguilar, Luis (2011), "Los efectos de la globalización en el ámbito de la seguridad y defensa", in *Inteligencia y Seguridad: Revista de Análisis y prospectiva*, No. 10, pp. 14 *et seq*.

influence through social networks, media, specialist publications and professional forums, and, of course, also access to decision-making circuits.

Legal Intelligence must enable knowledge about contracts, opportunities, projects, needs, and even profiles of the competition, accompanying national offers domestically and abroad. This work involves the study and promotion of regulations that promote research and enhancement of public research, whose priority is to benefit domestic companies by offering legal advantages to technological inventions to open or established markets and promote exports. Similarly, they must organise contractual models to ensure a return on the investment.

Patents, brand notoriety, contractual basis (conditions, applicable law and jurisdiction) are indispensable elements. Today the key issue in economy lies, more than the productive process such as simple manufacturing, in design and in added value. Hence the importance of investment in technology, innovation and in the regulation and instruments for their protection (anti-espionage)[26] and operating in secure conditions.

The preference is for strategic contracts: attracting "direct investments" to encourage investment overseas and especially exports in priority sectors. The creation, knowledge and legal handling of these areas are at present absolutely decisive.

And in this context of international competition it must be assumed that domestic laws are not identical, as is obvious between the Europeans, the Americans and the Asians; therefore the legal treatment of companies is very different from one place to another[27]. Nor is the degree of compliance with international treaties reciprocal, as we can see with the anti-corruption convention of the OECD, signed by all European countries and that reduces competitiveness against other states that have not signed and therefore cannot apply it to their companies.

Consequently, the national security strategy must contain the national and international regulatory policies that support its growth and stability, as well as the mechanisms of external influences[28].

---

[26] A significant example can be seen in *National Counterintelligence Center (USA, 1997), The Economic Espionage Act of 1996: A Brief Guide. Cfr.* Szott Moohr, Geraldine (2009), "The problematic role of criminal law in regulating use of information: The case of the Economic Espionage Act", *Public Law and Legal Theory Series*, 2009-A-5, University of Houston Law Center.

[27] Illustrating these differences is the current acrimonious debate within the European Union on the implementation of a tax on financial transactions. Cfr. Montoya Cerio, Fernando, Sambeat Vicién, Andrés and Fabra Rodríguez, Óscar, *La tasa Tobin europea. Un impuesto sobre las transacciones financieras*, Opinion document, Instituto Español de Estudios Estratégicos (IEEE), 06/2013, 16 January.

[28] In the matter of international business alliances, the development of The Trans Pacific Partnership (TPP) undoubtedly represents a global change of the first order, to

The law as an intelligence tool

At present, economic intelligence includes any information that could have an influence on the results of company activity and from there can transcend the common welfare (national security). And knowledge about laws and legal practices is a substantial part of these data with a potential impact on the social order, as it is part of the competitive environment in an economic sector. Regulation is one of the key elements of decision making.

The use of the Law as an intelligence tool is shown openly within the framework of covert actions and actions of influence.

The North American model of the OSI (*Office of Strategic Influence*)[29], that since 2001 has begun the creation of regulatory lobbying, represents one of the best examples in this respect.

As a paradigmatic example, we can study the regulations on companies about "information gathering", particularly Google. These corporations hoard multiple ways of obtaining information and data from consumers and economic actors from anywhere in the world. Once acquired this also raises its hypothetical communication, within a strategy of U.S. economic intelligence, to competitor companies of this nationality - even just one set of miscellaneous data in order to build profiles of Internet users. Knowledge is power[30]. But not only in the sense of acquiring mass information

now bring together the United States of America, Canada, Mexico, Peru, Chile, Australia, New Zealand, Malaysia and Singapore, and the likely inclusion this year of Japan and South Korea.

[29] It should be noted that the existence of the OSI as such is so far unknown. Apparently it was a section created by the Department of Defence of the United States in October 2001 to support the war against terror through "psychological operations" in target countries, including the United States. Although initially its closure was announced in 2002 by the then Secretary of Defence Donald Rumsfeld - once its existence became public knowledge - various sources claim that the OSI continues operating - under another secret name - and that it only removed its name, passing the majority of its "public" powers to the *Information Operation Task Force*. But obviously, being secret activities nobody really knows if they are now still being carried out and if so what the competent body is. The OSI was originally authorised to employ what is called military deception of public opinion, presenting information, images or false declarations in order to deceive enemy armies or agencies and civilian populations through disinformation.

[30] Solove, Daniel, J (2006), *A Brief History of Information Privacy Law*, George Washington University Law School, Public Law Research Paper, No. 215. Ibid. (2006), "A Taxonomy of Privacy" in *University of Pennsylvania Law Review*, Vol. 154, No. 3, January, pp. 484-486; p. 478. Without doubt the obtaining of information has a strategic value, but likewise constitutes an interference with the fundamental right to privacy of citizens; therefore these activities should be carried out in strict compliance with the Law, even in situations concerning national economic security. González Cussac, José Luis and Larriba Hinojar, Beatriz (2011), *Inteligencia Económica y Competitiva: Estrategias legales en las nuevas agendas de Seguridad Nacional*, Valencia, Tirant lo Blanch, pp. 89 *et seq*.

from around the globe, also from the standpoint of benefiting through legislative coverage. A similar capability of the creation and enforcement of the rules applicable to these large information companies expresses an intelligent power[31]. Here we could launch an eloquent discussion on the territorial and extraterritorial application of the domestic law of the United States of America and on its nebula and different regulations regarding cloud computing[32].

We are actually talking about what NYE baptised as "soft power"[33]. In this case the export of legal systems, the ability to apply domestic law outside its borders (extraterritoriality), the power to create protectionist rules in a domestic market, a dominant position in international organisations, or the influence on the process of the creating of laws of other states[34]. These regulatory capabilities allow real advantages and in many cases absolute ones, and have been ingeniously called real **"regulatory Trojan horse".** Some clear examples are the following:

- Promotion from the United States of America of **IFRS** *(International Financial Reporting Standards).* Some analysts understand that these rules are applied with great flexibility in the U.S., while in Europe they are more rigorously regulated in terms of accounting[35].
- However, we cannot lose sight of the final objective: the continued convergence between U.S. GAAP and International Accounting

[31] Geradin, Damien and Sidak, J. Gregory (2008), *European and American Approaches to Antitrust Remedies and the Institutional Design of Regulation in Telecommunications*, Howrey LLP and Criterion Economics, L.L.C., Working Paper Series, Liége, April 07.

[32] González Cussac, José Luis (2012), "La verificación de los ordenamientos internos en los países de localización como garantía de la seguridad y la confidencialidad de la información", in *Derecho y Cloud Computing* (Ricard Martínez Martínez editor), Madrid (Civitas), pp. 289-307.

[33] Nye, Joshep S. Jr (2011), *The Future of Power*, New York Public Affairs (ed.).

[34] The ability to influence other states legally bears a close link with those conventionally called "cultural norms", and hence the relevance of the term "geoculture". Cfr. Mejía Velásquez, Hernán (1998), "La geopolítica de la geoeconomía", *Revista Pensamiento Humanista*, No. 4, Medellin.

[35] Since the promulgation of the stable platform of International Financial Reporting Standards (IFRS) in 2005, subsequently revised and modified, a large number of companies and countries around the world have adopted these standards (formerly called IAS) as a basis for their financial reports. This collection of accounting standards of a global nature, approved by the Council of International Accounting Standards, is intended to require comparable, transparent information and of a high quality in the financial statements and other types of financial information, in order to help participants in the capital markets around the world and other users to make economic decisions. Today, one of the main challenges faced in this area is the development of a commitment for convergence established between IFRS and generally accepted accounting principles in the United States of America (U.S. GAAP). See, in detail, Peñalva Acedo, Fernando (2007), "NIFF versus US GAAP: resumen de las principales diferencias", in *Revista de Contabilidad y Dirección*, Vol. 4, Year 2007, pp. 55-69.

Standards. Certainly today it is carrying out a convergence project to further align the rules included in the International Financial Reporting Standards (IFRS) and Generally Accepted Accounting Principles (US GAAP).

- The SOX, abbreviation of ***Sarbanes Oxley Act***[36], is an American law passed in 2002 in response to financial scandals such as ENRON, undermining the confidence of investors and the American State itself on the data contained in the financial accounting reports of companies. The name of the law is derived from the surnames of its two main sponsors, Representative Michael G. Oxley and Senator Paul S. Sarbanes.
- The main objective of this Act is to promote greater transparency and accountability in relation to the data of the reports issued by both public companies in the United States and its worldwide subsidiaries, such as the foreign companies that are listed on any stock exchange in the United States. Specifically, and amongst other things, it establishes a new supervisory board, supervised by the Security Exchange Commission (SEC) and includes new reporting requirements and more severe punishments regarding corporate fraud.
- In reality it is an American regulatory addition (**Sarbanes Oxley Act**) of the IFRS that allows the PCAOB (Public Company Accounting Oversight Board) to extend research on companies in terms of financial and strategic data beyond its borders[37]**.**
- The **Patriot Act,** which requires financial institutions such as the PCAOB, to transmit financial reports to the intelligence services (CIA, NSA etc.) without the permission of the companies and without their knowledge[38]. After which, the CFIUS (Committee of Foreign Investment in United States) evaluates the sensitivity of the company to American interests according to its elastic National Security Act[39]**.**

As Zunzarren sharply summarised, *"if **CFIUS** believes that the data held by **Google** are sensitive to American interests by the **Sarbanes Oxley Act** and*

[36] Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745, 30 July, 2002.

[37] For a more detailed analysis of this rule, see: Romano Roberta (2004), "The Sarbanes-Oxley Act and the Making of Quack Corporate Governance", in *NYU, Law and Econ Research Paper* 04-032; Yale Law & Econ Research Paper 297; Yale ICF Working Paper 04-37; ECGI - Finance Working Paper 52/2004.

[38] Phillips, Heather, A (2005), "Libraries and National Security Law: An Examination of the USA Patriot Act", *Progressive Librarian,* Vol. 25, Summer.

[39] A supplement to this legislation, in the sense of attributing federal jurisdiction to the United States of America to investigate and prosecute any business, is found in the Economic Espionage Act in this sense, extensively and critically in HOROWITZ, Richard (2011), *Competitive Intelligence, Law and Ethics: The Economic Espionage Act Revisited Again (and Hopefully for the Last Time),* SCIP, Vol. 14, No. 3, July/September 2011, p. 41 *et seq*.

*by the **Patriot Act**, they can obtain them without the agreement of **Google** and without the knowledge of the company under investigation **even if not American**. And let us not forget that the company **Concileo** is one of the giants in terms of **moderation of Web content**, which some dubbed as censorship; and is American. There are those who can **cut to the chase** regarding the contents of the Web; but under what criteria?"*[40].

Juillet has already highlighted the importance of the Law and its use, saying, *"Americans, inspired by the world of business, have chosen to modify the environment leading to a new configuration system, turning to technological innovation. The aim is to change the game, to dictate new rules, after taking the lead in a competition that is currently lopsided. Technological power linked to the definition of the battlefield means the adversary can only choose the type of defeat and speed of realisation"*[41]. This is the model that leading countries, particularly in the West, are trying to emulate.

Indeed, as the aforementioned author continues to underline, the basis of sovereignty of a state is not just the standard of living, gross domestic product or export capacity. Nor even its nuclear capacity. The global scenario has changed and there are a small group of strategic technologies that ensure real independence of nations. But the scientific expertise required to work in these fields and the volume of investment required will prevent many countries remaining in the technological race. Therefore, the launching of communal programmes at European level is essential, since, *"for more than fifteen years, Americans have had a clear and perfectly identified strategy. They invest relentlessly in information technology as well as in the development of knowledge and learning, elements that are at the heart of power and modern independence. Encouraged by its state, American industrialists have no hesitation in establishing partnerships and in buying companies, throughout the entire world, when they want to acquire a technology, complete their experience or neutralise a competitor"*[42].

On the international level there are countless examples[43], sufficient for our purposes here to cite the ongoing conflict in Nigeria, where the ap-

---

[40] Zunzarren, Hugo, in http://idinteligencia.wordpress.com/archivos-2/posts-precedentes/inteligencia-juridica-en-los-eeuu/

[41] Juillet, Alain (2006), "Principios de aplicación de la inteligencia económica". *Inteligencia y seguridad: Revista de análisis y prospectiva*, No. 1, December, pp. 123-132.

[42] Juillet, Alain (2012), this text is a summary of his speech to the Coloquio Independencia de Europa y Soberanía Tecnológica, held in April in Paris and titled *"Cambian las bases de la soberanía mundial. Se desplazan de factores económicos y de seguridad a algunas tecnologías clave que Europa no ha cultivado"*. Reproduced with permission from the author. French translation: Eduardo Martínez. http://www.tendencias21.net/Cambian-las-bases-de-la-soberania-mundial_a337.html.

[43] González Cussac, José Luis and Larriba Hinojar, Beatriz (2011), *Inteligencia Económica y Competitiva: Estrategias legales en las nuevas agendas de Seguridad Nacional*, Valencia, Tirant, pp. 72 *et seq*.

proval of a law is being debated that would enable the imposition of heavy fines on oil companies for damages caused in the Niger Delta in its crude oil extraction activities. But naturally, the powerful lobbies of these multinationals, supposedly supported by the institutions and services of their home countries, are trying to influence to stall the proposal, delay it, or at least limit its application.

The recent French military intervention in Mali is also analysed not only as a determined curb to terrorism, but also with a geoeconomic purpose: to protect their investments in neighbouring Nigeria (it produces 8% of worldwide uranium), where its multinational AREVA, with 80% of public ownership, extracting uranium that imports to France and which represents around 40% of its consumption. *Energy security* has undoubtedly also been influential in China not opposing this intervention, which also protects its giant companies CNIUC and CNPC with interests in uranium and oil.

The importance of rules in the global economy has a remarkable exponent today in the regulation of so-called "sovereign wealth funds". Their strategic importance is clear from the fact that they are treated as public funds, i.e. handled by governments, but invested in the private sector. But just one of the major criticisms of these financial instruments is their lack of transparency, besides some signs of protectionism, the cession of strategic control to particular sectors (banking and technology) and their possible use by some states as an instrument of political and economic pressure on other countries.

All this controversy gave rise to the creation in April 2008 of the International Working Group of Sovereign Investment Funds (IWGSIF), which culminated in October 2008 in Chile, with the approval of a code of professional ethics. This agreement was called "Generally Accepted Principles and Practices" (GAPP) or "Santiago Principles". Yet despite its decisive importance in the twenty-first century global economy, they remain a model of self-regulation and not authentic binding legal rules. Therefore, although their purpose is said to be purely economic and financial, it is not expressly excluded that their use is subject to "other considerations"[44]. Here is a large calibre *geoeconomics* weapon to consider as central to any analysis of legal and economic intelligence.

This panoramic view should also underline the so-called "Basel Accords" and the World Trade Organisation (WTO).

In 1974, the Basel Committee, composed of central bank governors of the G-10 countries, approved the first "Basel Accord"; a collection of recommendations aimed primarily at establishing the minimum capital a bank

[44] Coronas Valle, Daniel and López Jiménez, José Mª (2013), *Crisis y Fondos Soberanos: ¿El abrazo del oso?,* Opinion document, IEEE 14/2013, 5 February 2013.

should have taking into consideration the risks it faces. It was a simple recommendation, so that the signatory states were not obliged to incorporate it into their laws, or they could do so with modifications. Over a hundred countries signed it. However, two major drawbacks were detected: their insensitivity to the variations of risk and the lack of assessment on credit quality.

To overcome these criticisms the "Basel II Accord" was adopted in 2004, creating the subgroup responsible to drive its international implementation *(Accord Implementation Group, AIG)*. Today it applies throughout the European Union (mandatorily imposed by directives), in Japan, Australia and in more than 95 different countries by the members of the Committee. This shows the extent of its unquestionable progress towards a unified international practice, and its possible technical deficiencies, once again called attention to its legal nature, which allows a different degree of compliance worldwide. This in spite of its implications in the genesis of the current financial crisis and its extraordinary value in a strategic market such as the financial one. Once again we are faced with a shortage of obligatory regulations and a notable lack of transparency.

The World Trade Organisation, although not forming part of the UN, or of the "Bretton Woods" organisations (the IMF, World Bank), includes more than 158 countries and 26 in an observer capacity. Its objective is the multilateral regulation of international trade, and currently administers about 60 agreements. The original provisions, called "GATT 1947", were expanded from the celebrated "Uruguay Round", known as "GATT 1994", i.e. "General Agreement on Tariffs and Trade". It is known that the initial impetus was the result of an agreement between the most developed countries, especially the United States of America and the European Community, with the aim of deregulating international trade, reducing customs tariffs, subsidies and other instruments of "trade distortion". However, it was objected that they only covered sectors that suited their interests, but exempted those that needed to maintain protectionist measures (textiles and agriculture). From the "Uruguay Round" this situation began to change. However, the flexibility measures were insufficient in the opinion of the least developed countries, and also, as compensation, they would introduce new sectors such as Trade Services and particularly relating to intellectual property, as required by North America[45].

The WTO requires adherence to all its agreements, without exception. This way trading rules apply to all, exactly the same, irrespective of the level of human, technological and social development. This contrast raises the essential critique, demanding special and differential treatment

[45] In this respect, see Arcos Martín, Rubén (2010), *La lógica de la excepción cultural*, Madrid (Cátedra).

commensurate with the degree of development of each country. The so-called "Doha Round" of 2001 ("Doha Development Agenda") pursued this objective, which was still very distant and abandoned with the outbreak of the great crisis of 2008. Consequently at present, the most developed countries affected by the crisis maintain agreements that clearly favour them in international trade and do not seem very willing to make concessions to either the emerging countries or the underdeveloped. Once again we can see the value of law, the advantage of who has the capacity to create the rules and therefore its strategic value[46].

In the Spanish case, among others recently, we could cite the dispute over REPSOL-YPF in Argentina, which is highly significant regarding what we are discussing. Also very controversial was the reform of 27th September 2011 of art. 135 of the Constitution. For some this constitutes a manifestation of a loss of economic sovereignty, influenced by the interests of international creditors and something that guaranteed the maximum regulatory level. For others, however, it was a need to correct the public budget deficit (structurally of 5% of GDP and that soared after the current crisis), with the introduction of a limit on spending and borrowing or a principle of budgetary stability[47]. Indeed, the determination to impose strict rules on budget deficits should also be extended to the imbalances in trade balances, to reform tax laws towards a flexible and adaptable understanding to periods of expansion or recession of the economy[48].

The strategic importance of a strong alliance between technological innovation and regulatory accompaniment is nowadays expressed as a paradigm in the energy industry[49]. According to the report of 12th November 2012 of the EIA (Energy Information Administration), the United States of America will in 2017 be the largest oil producer and in 2030 the largest exporter. This is thanks to what has been allowed legally (in spite of obstacles and environmental risk warnings); the development of an innovative technology of horizontal drilling and of "hydraulic fracturing", which allows the extraction of crude oil and gas through water pressure *(fracking)*. This change is already having decisive geopolitical effects and multiple consequences on other countries as diverse as Saudi Arabia

[46] Reynaud, Julien P. M. and Vauday, Julien, (2008), *IMF Lending and Geopolitics*, (14 November 2008). ECB Working paper No. 965, International Monetary Fund.

[47] Worth considering is the theory that advocates a classification between countries which accumulate wealth (favourable trade balance, technology and savings) and countries that accumulate debt.

[48] For a more complete view about the geopolitics of oil today, see MAUGERI, Leonardo (2012), Oil: The Next Revolution Discussion paper 2012-10, Belfer Center for Science and International Affairs, Harvard Kennedy School, June 2012.

[49] Youngs, Richard (2007), Europe's External Energy Policy: Between Geopolitics and the Market, (20 November 2007), Centre for European Policy Studies Working Documents No. 278.

(and other Asian Gulf countries), Russia, China, Venezuela, Ecuador and Bolivia[50].

These "**regulatory Trojan horses**" express the allegorical construction of Bentham's *panoptic*, masterly description of the form of power under which we live, and especially in the digital age. Moreover, new technologies may even dispense with the central monitoring tower and any other material tool, as with these infrastructures they exercise complete control. The large financial, energy, internet service and telephone companies are more than just good examples. Their alliance or collaboration with the governments increases their powers and extends the watched and the watched over. However, the Internet presents a problem for vigilantes, since to watch leaves traces of their observation and in turn can be watched. But to make this two-way possibility real, regulations must be implemented. In the international environment, treaties that limit and regulate global monitoring. At the domestic level, freedom of information laws and especially regarding transparency, where citizens can control the vigilantes.

In short, it is essential to have national and international law that enables a powerful organisation that will deter external hostile actions. This will update the doctrine of deterrence, as it becomes clear that the negative consequences for those who try will outweigh any benefit. We need special and exceptional rules for times of profound change in social relations, or if you prefer, in times of "economic war". The rules should contribute to diminishing or abolishing the vulnerabilities and to generating common wellbeing. It could be stated as the necessity of a **new economic Law** for a new global context.

To achieve basic results to improve institutions, providing them with real capacity to implement a protective and penalising law to attacks on economic, scientific, technological, historical, artistic, cultural and environmental wealth, of a special guardianship against data espionage sensitive to intrusions. To organise public mechanisms of control over the capital of strategic companies, and surveillance on investors, especially over those *unwanted* ones.

This complex regulation should extend especially to SMEs, permitting the development of networks that will allow them to defend their rights throughout the world, contributing to the reduction of oligopolies, to the impositions of large multinational companies and, in short, enabling the old liberal aspiration of free competition. Along with this it is necessary to provide incentive rules to encourage implementation abroad and domestic consolidation, and to implement formalised advisory mecha-

[50] Nye, Joseph S. Jr (2010), "American and Chinese Power after the Financial Crisis", *The Washington Quarterly*, 33:4, Center for Strategic and International Studies, October 2010, pp. 143-153.

nisms to eliminate bureaucratic obstacles, lack of data or misinformation actions.

Conclusions

The first conclusion is to support the value of the Law, both as the power to create rules and its knowledge and application to economic intelligence. The interplay between the three levels outlined above is therefore essential. Thus, if today the dependence between national security and economic prosperity is obvious, it is also obvious that both are proxies for the current rules.

The second is to point out the hitherto insufficient attention which, regarding economic security as an integral part of national security, has been paid to the phenomenon of organised crime, its close links with corruption and its tremendous institutional impact. Very recently this attitude has been corrected, as shown, for example, by the attention paid to different strategies of national and regional security, or the European Parliament in its report of 2011 on international organised crime in the European Union.

The third and essential point refers to the underlying causes of the current international crisis. In this panorama the predominance of policies of "non-Law" is rightly highlighted, using euphemisms such as deregulation, self-regulation, or state anti-interventionism. Obviously these policies are part of an ideology behind which are hiding notorious economic interests, and in no way express any kind of "natural law of markets". Supported by large financial energy and new communication and information technology oligopolies, they make it possible to impose their particular interests above general interests, whether in collusion with some states or even against the wishes of other weaker ones[51]. The result is the burden of the constant impoverishment of these countries and of their citizens. But they also cause an erosion of institutions and a continual loss of legitimacy. Better for them, because the weaker public institutions are, the more power they accumulate.

This state of affairs, together with direct damage to the quality of life of millions of people, feeds the discourse of radical and extremist ideologies. And it also resurrects the historically failed discourse of economic protectionism. Hence proposals arise for de-globalisation. In particular, some are in favour of a return to protectionist state regulations[52].

[51] Of great interest is knowledge of the operation of the global financial market, especially the so-called "Credit Default Swap". Cfr. Álvarez Rubial, Gregorio Pablo: *"El Credit Default Swap como agente transformador del paradigma financiero internacional",* Opinion document, IEEE, 04/2013, 9 January.

[52] Todd, Emmanuel (2010), *Después de la democracia,* Madrid, Akal; MONTEBOURG, Arnaud (2011), *¡Votad la desglobalización!,* Barcelona, Paidós.

Certainly capitalism exercises its economic control by allowing governments, through the Law, to satisfy specific social demands. However, with the fall of the counterweight represented by the communist states, this balance was broken. The neoliberal ideology of modern capitalism has been built on a dual argument: state intervention reduces individual freedom and restrains the initiative of civil society. From this assumption there was unleashed a constant and systematic process of reductionism of the public sphere towards the "minimal state". The explicit message was simple: all state intervention is synonymous with domination, of restriction of freedom. Therefore, any product of the state is negative: thus, legal regulation, with its formalities and requirements of control and publicity is presented as useless bureaucracy; politics is always equivalent to corruption and justice, with its procedural guarantees, a hindrance from the past, slow and inefficient. The subliminal message hides the interested identification of civil society with free markets, i.e. with the monopolies of financial power, and consequently progress requires the agility and flexibility of deregulation, ***self-regulation***, arbitration, mediation and any other non-formalised mechanism.

In short, the discrediting of the state and its ongoing delegitimisation calls for fewer rules, less law, less *res publica*. But as Epicurus warned, *"if they eliminate the laws, men need the claws of wolves, the teeth of lions."* Only the Law provides rules, values, reasons, interests, and imperatives capable of the transit from a society where the power of the strongest governs – historically military force, today the financial oligopoly – to an orderly coexistence that is plural and transparent: the Rule of Law. Only with legal security can there be a real free economy. And economic and competitive intelligence must first know these rules, and then encourage their correct application and reform in accordance with the general interest. That is the aspect of the economy as part of national security.

In this line, some proposals seem essential to achieve the objective of a greater economic security. Firstly, to underline that the international community already has useful and effective rules that, largely, can solve many of the issues raised here. Its recognition, application and control of compliance are essential to economic activity.

Secondly, promoting stricter laws on competition and enabling their effective application, particularly on institutions of finance, energy and new technologies of information and communication. This involves dealing with disproportionate end bonuses, tax subsidies and public aid, more transparency and an end to tax havens. But also tax reforms to correct current gross inequalities, modifying legislation on bankruptcy and ultimately, a new regulation that, in the words of Stiglitz, "softens globalisation"[53].

[53] Stiglitz, Joseph E (2012), *El precio de la desigualdad,* Madrid, Taurus, p. 343.

This crisis must be overcome by using more democracy (greater citizen participation), and more Law (an updated and precise regulation). It is essential to increase transparency, which is an essential way to the control of citizens over public representatives, who cannot continue holding back public information and thus aspiring to exclusively retain the ability of decision making on general matters, protected in the false assumption that they are the only knowledgeable and therefore uniquely qualified people. As Hobsbawm has categorically expressed it, *"The States with a stable and buoyant economy and a distribution of relatively equitable wealth are less likely to suffer a social and political earthquake than those poorer, where inequalities are the order of the day and whose economy is anything but stable. Similarly, the possibility of peace would be affected by a drastic increase in economic and social inequality, both in individual countries and between all of them"*[54].

Historical experience shows us the consequence for the democratic Rule of Law of having economic and social instability, manifested constantly by periods of inflation that are devastating to the middle classes. And we already know that without them a regime of freedom is not possible. The risk of inflation now lies in wait for many developed countries and consequently its control must constitute one of the priorities of our governments[55].

Likewise, the legally developed States – which entail an important degree of implementation of civil, social and individual rights (especially labour rights) – favour sustainable growth and consequently attract economic investment. This premise is a historical constant, and currently begins to loom with the incipient end of the trend toward off-shoring and outsourcing of large companies. Indeed, many of them have started the return "home" as a reaction to the enormous problems of legal uncertainty, corruption and political instability, insufficient technological development and infrastructure of many of the countries that initially attracted their residence due to their low costs.

With Berlin, we can reject monistic analysis and response: nor is there a single crisis, but several intertwined ones, nor is the answer unique – only financially and economically – but also institutionally, with a demand and pressing need to develop rules built on shared values. Indeed, because as economists also remember, this financial and economic crisis is primarily a crisis of values, that is, a moral crisis and consequently a crisis of rights, insecurity and lack of confidence[56].

[54] Hobsbawm, Eric (2006), *Guerra y paz en el siglo XXI*, Barcelona, Crítica, p. 16.

[55] Touraine, Alaine (2011), *Después de la crisis*, Madrid (Paidós).

[56] Stiglitz, Joseph E (2010), *Caída libre El libre mercado y el hundimiento de la economía mundial*, Madrid (Taurus), pp. 324 *et seq*. On this point integral education becomes a fundamental value; this is humanistic, because without it there are no truly free citizens (critics); and without them, democracy remains a hollow idea.

I will conclude with an idea expressed with great clarity by Juillet, *"Facing the pressure exerted by all those who want to increase their global market share, the only true answer consists in creating clear game rules that are applicable in all countries. It is a rare event now because many have the tendency to seek privileges or to slip away. Faced with the difficulty of enforcing international agreements, it is necessary to convince people that the absence of rules, the non-compliance of rules and violation of patents are ruinous for companies and economies. The recognition and supervision of the rules as well as the control of compliance with the rules applicable for all are therefore at the heart of economic intelligence activities"*[57].

In conclusion, as I have tried to emphasise in this work, all human activity is subject to rules, their knowledge, handling, application, and especially their creation, are an essential strategic value (*Auctoritas, non veritas, facit legem*). As Aristotle warned, intelligence consists not only in knowledge but also the skill to apply knowledge in practice.

Rules, values, interests, imperatives, all this is Law. Without reliable laws a truly free economy cannot exist, in other words, without legal security there can be no economic security. And without a free and secure economy for everyone, a peaceful and orderly coexistence is impossible (*Salus populi suprema lex*). Therefore, only the Law is the future of democracy.

Bibliography

Álvarez Rubial, Gregorio Pablo (2013), *El Credit Default Swap como agente transformador del paradigma financiero internacional,* Opinion document, IEEE, 04/2013, 9 January.

Arcos Martín, Rubén (2010), *La lógica de la excepción cultural*, Madrid (Cátedra).

Arcos Martín, Rubén (2012), "Hacia un sistema español de inteligencia para la seguridad económica y la competitividad", in *Inteligencia y Seguridad: Revista de Análisis y Prospectiva*, No. 11, pp. 103 *et seq.*

Arnett, Dennis, MENON, Anil and WILCOX, James B. (2000), "Using Competitive Intelligence: Antecedents and Consequences", *Competitive Intelligence Review,* Vol. 11, Issue 3, pp. 16-27.

ARMENTA DEU, Teresa (2009), "Exclusionary Rule: Convergencias y divergencias entre Europa y América", Revista de Estudios de la Justicia, No. 11, 2009.

AA.VV. (2012), *Modelos de reflexión estratégica europea e inteligencia económica*, Universidad Rey Juan Carlos, Instituto Juan Velásquez de Velasco y Cátedra de Servicios de Inteligencia y de Sistemas Democráticos.

[57] Juillet, Alain (2006), "Principios de aplicación de la inteligencia económica". *Inteligencia y seguridad: Revista de análisis y prospectiva*, No. 1, December, pp. 123-132.

Ballesteros Martín, Miguel Ángel and Joyanes Aguilar, Luis (2011), "Los efectos de la globalización en el ámbito de la seguridad y defensa", in *Inteligencia y Seguridad: Revista de Análisis y prospectiva*, No. 10, pp. 14 *et seq*.

Buzan, Barry; Weaver, Ole and De Wilde, Jaap (1998), *Security. A new framework for Analysis,* London, Lynne Rienner Publishers, pp. 95 *et seq*.

Bégin, Lucie; Deschamps, Jacqueline and Madinier, Héléne (2007), "Une approche interdisciplinaire de l´intelligence économique", Cahier de Reserche No. HES-SO/HEG-GE/C--07/4/1-CH, Haute École de Gestion de Genève, 2007.

Bradford, William (2007), "The three faces of competitive intelligence: defection, collusion and regulation", in *University of Florida, Warrintong College of Business*, 19 February.

Carayon, Bernard (2006), *Patriotisme économique: De la guerre à la paix économique*, Monaco, Editions du Rocher.

Clarke, Richard A. And Knake, Robert K. (2011), *Guerra en la red: los nuevos campos de batalla,* Barcelona, Ariel.

Comai, Alessandro (2009), "El Sistema de Inteligencia Económica de Francia: Una Política Pública", in *Puzzle* (*Revista de Inteligencia Competitiva)*, Year 8, Edition No. 30, July-September 2009.

Coronas Valle, Daniel and López Jiménez, José Mª (2013), *Crisis y Fondos Soberanos: ¿El abrazo del oso?,* Opinion document, IEEE 14/2013, 5 February 2013.

De Nardis, Laura (2012), *Governance at the Internet's Core: The Geopolitics of Interconnection and Internet Exchange Points (IXPs) in Emerging Markets*.

Esteban Navarro, Miguel Ángel, coordinator (2007), *Glosario de inteligencia*, Ministerio de Defensa, Madrid, 2007.

Equipo de Inteligencia Económica del CNI (2011), "Aproximación a la inteligencia competitiva", in *Inteligencia y seguridad: Revista de Análisis y prospectiva*, No. 9, 2011**,** pp.19-40.

Ferrer Rodríguez, Juan (2011), *Seguridad económica e inteligencia estratégica en España,* Opinion document, Instituto Español de Estudios Estratégicos, 85/2011, 5 December.

Geradin, Damien and Sidak, J. Gregory (2008), *European and American Approaches to Antitrust Remedies and the Institutional Design of Regulation in Telecommunications*, Howrey LLP and Criterion Economics, L.L.C., Working Paper Series, Liége, April 07.

González Cussac, José Luis (2010), "Estrategias legales frente a las ciberamenzas", in *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*; Instituto Español de Estudios Estratégicos. Ministerio de Defensa, Cuadernos de Estrategia No. 149 (Madrid 2010), pp. 85-127.

González Cussac, José Luis and Larriba Hinojar, Beatriz (2010), "Un Nuevo Enfoque Legal de la Inteligencia Competitiva", in *Inteligencia y seguridad: Revista de Análisis y prospectiva*, No. 8, 2010, pp. 39-73.

González Cussac, José Luis and LARRIBA HINOJAR, Beatriz (2011), *Inteligencia Económica y Competitiva: Estrategias legales en las nuevas agendas de Seguridad Nacional*, Valencia, Tirant lo Blanch.

González Cussac, José Luis, coordinator (2012), *Inteligencia,* Valencia, Tirant lo Blanch.

González Cussac, José Luis (2012), "La verificación de los ordenamientos internos en los países de localización como garantía de la seguridad y la confidencialidad de la información", in *Derecho y Cloud Computing* (Ricard Martínez Martínez editor), Madrid (Civitas), pp. 289-307.

González Cussac, José Luis (2013), "Tecnocrimen", in *Nuevas amenazas a la seguridad nacional. Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación,* (Directors José L. González Cussac and María Luisa Cuerda Arnau; Coordinator Antonio Fernández Hernández), Valencia, Tirant lo Blanch.

Guiora, Amos N. (2008), "Anticipatory Self-Defence and International Law. A Re-Evaluation", *Journal of Conflict and Security Law*, U of Utah Legal Studies Paper, No. 057-08-10.

Harbulot, Christian (1992), *La machine de guerre economique: Etats-Units, Japon, Europe,* París, Economica.

Hidalgo Schnur, Diego (1998), *Europa, globalización y Unión Monetaria,* Siddarth Mehta.

Hobsbawm, Eric (2006), *Guerra y paz en el siglo XXI,* Barcelona, Crítica.

Horowitz, Richard (2011), *Competitive Intelligence, Law and Ethics: The Economic Espionage Act Revisited Again (and Hopefully for the Last Time),* SCIP, Vol. 14, No. 3, July/September 2011, pp. 41 *et seq*.

Jáuregui, Gurutz (2011), "La emergencia de un nuevo orden jurídico-institucional: el Estado y la Constitución de la era de la globalización", in Innerarity, Daniel and Solana, Javier, editors: *La humanidad amenazada: gobernar los riesgos globales,* Barcelona, Paidós, pp. 237 *et seq*.

Juillet, Alain (2006), "Principios de aplicación de la inteligencia económica". *Inteligencia y seguridad: Revista de análisis y prospectiva*, No. 1, December, pp. 123-132.

Juillet, Alain (2012), this text is a summary of his speech to the Coloquio Independencia de Europa y Soberanía Tecnológica, held in Paris in April and entitled *Cambian las bases de la soberanía mundial. Se desplazan de factores económicos y de seguridad a algunas tecnologías clave que Europa no ha cultivado*. Reproduced with permission from the author. French translation: Eduardo Martínez. http://www.tendencias21.net/Cambian-las-bases-de-la-soberania-mundial_a337.html

Larriba Hinojar, Beatriz (2013), "Ciberespionaje Económico: Una amenaza real para la Seguridad Nacional", in *Nuevas amenazas a la seguridad nacional. Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación,* (Directors José L. González Cussac and María Luisa Cuerda Arnau; Coordinator Antonio Fernández Hernández), Valencia (Tirant) 2013.

Larriba Hinojar, Beatriz (2006), *La tutela penal del diseño industrial*, Valencia, Tirant lo Blanch.

Lodeiro, Andrea (2006), "Ámbito de la inteligencia económica: significación, teoría y práctica", in *AA Inteligencia*, Digital version (2006/12).

Maugeri, Leonardo (2012), *Oil: The Next Revolution*, Discussion Paper 2012-10, Belfer Center for Science and International Affairs, Harvard Kennedy School, June 2012.

Mejía Velásquez, Hernán (1998), "La geopolítica de la geoeconomía", Revista Pensamiento Humanista, No. 4, Medellín.

Montebourg, Arnaud (2011), *¡Votad la desglobalización!,* Barcelona, Paidós.

Montero Gomez, Andrés and Martin Ramirez, José (2008), *Inteligencia económica como vector internacional de seguridad*, Working document No. 18/2008. Real Instituto Elcano.

National Counterintelligence Center (USA, 1997), The Economic Espionage Act of 1996: A Brief Guide.

Montoya Cerio, Fernando; Sambeat Vicién, Andrés and Fabra Rodríguez, Óscar (2013), *La tasa Tobin europea. Un impuesto sobre las transacciones financieras*, Opinion document, IEEE, 06/2013, 16 January.

Nye, Joshep S. Jr (2011), *The Future of Power*, New York Public Affairs (ed.).

Nye, Joshep S. Jr (2010), "American and Chinese Power after the Financial Crisis", *The Washington Quarterly*, 33:4, Center for Strategic and International Studies, October 2010, pp. 143-153.

Olcott, Anthony (2009), "Revisiting the Legacy: Sherman Kent, Willmoore Kendall, and George Pettee - Strategic Intelligence in the Digital Age", *Studies in Intelligence,* Vol. 53, No. 2 (Extracts, June 2009), pp. 21-32.

Olier Arenas, Eduardo (2011), *Geoeconomía,* Pearson Prentice Hall.

Peñalva Acedo, Fernando (2007), "NIFF versus US GAAP: resumen de las principales diferencias", in Revista de Contabilidad y Dirección, Vol. 4, 2007, pp.55-69.

Phillips, Heather, A. (2005), "Libraries and National Security Law: An Examination of the USA Patriot Act", *Progressive Librarian,* Vol. 25, Summer.

Pooley, James and Halligan, R. Mark (2000), "Intelligence and the Law" in Miller, Jerry (ed.) *Millennium Intelligence: Understanding and Conducting Competitive Intelligence in the Digital Age,* CyberAge Books, Medford, NJ, pp.171-187.

Potter, E. (1998), *Economic Intelligence and National Security,* Ottawa Carleton University Press and the Centre for Trade Policy and Law.

Reynaud, Julien P. M. and Vauday, Julien, (2008), *IMF Lending and Geopolitics*, (14 November, 2008). ECB Working Paper No. 965, International Monetary Found.

Romano, Roberta (2004), "The Sarbanes-Oxley Act and the Making of Quack Corporate Governance", in NYU, Law and Econ Research Paper 04-032; Yale Law & Econ Research Paper 297; Yale ICF Working Paper 04-37; ECGI - Finance Working Paper 52/2004.

Sanz Roldán, Felix (2011), "El Centro Nacional de Inteligencia ante el reto de la seguridad económica", in *Inteligencia y seguridad: Revista de Análisis y prospectiva*, No. 9, 2011, pp. 11-18.

Serrano Monteavaro, Miguel Ángel (2012), *La nueva clase media Americana. Hacia una mayor seguridad económica y social,* Information document, IEEE 02/2013.

Solove, Daniel, J (2006), *A Brief History of Information Privacy Law*, *George Washington University Law School*, Public Law Research Paper, No. 215.Solove, Daniel J. (2006), "A Taxonomy of Privacy", in *University of Pennsylvania Law Review,* Vol. 154, No. 3, January, pp. 484-486; p. 478.

Stiglitz, Joseph E (2010), *Caída libre El libre mercado y el hundimiento de la economía mundial*, Madrid (Taurus).

Stiglitz, Joseph E. (2012), *El precio de la desigualdad,* Madrid, Taurus.

Szott Moohr, Geraldine (2009), "The problematic role of criminal law in regulating use of information: The case of the Economic Espionage Act*"*, *Public Law and Legal Theory Series*, 2009-A-5, University of Houston Law Center.

Todd, Emmanuel (2010), *Después de la democracia,* Madrid, Akal.

Touraine, Alaine (2011), *Después de la crisis,* Madrid (Paidós).

Ugarte, José Manuel (2005), *La relación entre inteligencia y política, y sus consecuencias en las estructuras y normas de los Sistemas de Inteligencia*, Brasilia.

Venegas González, Álvaro (2008), "Inteligencia económica: un componente estratégico por desarrollar", in *AA Inteligencia*, Year 1, No. 2, Chile, pp. 10-19.

Vives Antón, Tomás Salvador (2010), *Fundamentos del sistema penal,* 2nd Edition, Valencia, Tirant.

Youngs, Richard (2007), *Europe's External Energy Policy: Between Geopolitics and the Market*, (20 November, 2007), Centre for European Policy Studies Working Documents No. 278.

Zunzarren, Hugo, in http://idinteligencia.wordpress.com/archivos-2/posts-precedentes/inteligencia-juridica-en-los-eeuu/).

Chapter IV

Competitive intelligence: a new paradigm in the strategic direction of organisations in a globalised world

Fernando Palop Marro

Abstract

The author starts from the challenges that organizations cope with in the global world of the twenty-first century with a dynamic of changes in their markets, technologies and socio-economic context. Those changes often **behave disruptive character of the prevailing** by both its content and its complexity and uncertainty derived in part from the speed with which they occur. This dynamic requires a new paradigm to be taken into consideration. First in terms of culture and learning processes of the organization in relation to the changes taking place around them but as well in the way decisions are built and made. That is how the organization and its sphere of influence detects, anticipates and "reads" the meaning and stakes of those changes. But also how it integrates and transforms the results of that learning capability into actions, decisions.

This integration need is stressed in the decisions field, affecting the management and strategic direction of the business. This new paradigm that requires intelligence to compete is collected by the proposal formulated as competitive intelligence and other denominations also known. Competitive intelligence is not as such a "new" proposal, it takes more than half a century of practice in many companies and organizations as we un-

derstand it today[1], and has precedents from many centuries ago. But it is still unknown and partially or completely unexploited by a large number of them. So it can be said that not exploiting today the potential posed by CI in organizations is a competitive disadvantage. The article reviews the term, its foundations and the processes involved. The main benefits and some application examples are put forward and the relationship between competitive intelligence, CI, business security and the importance of the influence concept are reviewed. Focused on the business world, this paper also addresses other applications of the same concept, as in the case of territorial intelligence. Finally some evolutionary trends in this field are provided.

Keywords

Competitive intelligence, strategic planning, decision process, organizational learning, knowledge management, organizational intelligence.

[1] Masson, J.L. (2005)

Executive summary

CI forms part of the responses developed by organisations (of all kinds and sectors) to provide the management of organisations with the keys to drive strategy and many of the tactical matters in a modern world with a high grade of uncertainty and speed of change.

This grade of uncertainty and speed of change has made part of the traditional practices that deal with information gathering and analysis of non-structured decision making obsolete.

CI does not eliminate uncertainty but it does reduce it to the extent that the systematic nature of its practice makes identifying a greater percentage of relevant information possible. This percentage varies significantly depending on the context of the matter to be decided. On the other hand it does not eliminate risk, but it does help to manage it.

Competitive intelligence creates a change in the paradigm of the traditional way of dealing with the development process and decision making by directors. Traditionally, intelligence generation for decision making has been almost exclusively assumed by decision makers. Within the new paradigm, the organisation is not generally limited to providing the decision maker with data and information. The organisation starts by involving the decision maker in the CI process and collaborates with the decision maker by generating intelligence (implications and significance of events, trends, alternatives, action proposals) to make the decision.

CI forms part of the characteristics of modern organisations considered as learners. From CI the organisation actively participates through different roles and purposes in the tasks of information observing, gathering, organisation and analysis and finally in its communication. There is extensive involvement and participation by the organisation in the process, not reduced to a few people from the management "staff". Even from the network concept, the involvement of people outside the organisation but within its sphere of influence is managed.

CI is above all an inter-disciplinary process in the organisation's traditional vertical functions, of continued performance over time (through its warning and anticipation aspects), focused on its support priorities and on the future.

CI as a process enables management within all of a company's processes, its results are measured through indicators and have regulatory references regarding innovation and quality such as from AENOR (Spanish Standardisation and Certification Association) UNE (Spanish Standard) 166.006.

CI takes many of its tools from other areas of knowledge (such as strategic planning, marketing, financial analysis, knowledge management or forecasting). But also, in addition to the process, it generates, especially in the analysis stage, an important store of practical experience (in part

originating from its application in the area of defence, security and geopolitics) with contributions and proposals in the field of cognitive biases in the use of analogies, inductions, deductions, inferences etc.

CI represents a competitive advantage for those organisations that know how to make use of the untapped potential in their organisations. CI, according to what has been empirically compared through surveys, increases a group's degree of cohesion based around goals and strategic priorities and their achievement.

Today, possibly one of CI's most typical and unique characteristics is its capacity for risk detection and anticipation. Unlike other functions in organisations that also collect data and information from the outside environment, CI focuses on providing context to the facts, their significance and implications for organisations and their possible progress. These facts will appear from CI only as evidence of support for the reasoning that leads to the provided intelligence. In this sense Gilad, B. (2008) maintains that CI creates a specific perspective of the risks and external opportunities for the global performance of companies and therefore is part of an organisation's risk management activity.

Introduction

In recent decades the merging of a group of changes in organisations' socio-economic and technological environment has represented major challenges in order to adapt to these changes. Behind this need for adaptation is their capacity for learning about the changes and the integration of this capacity into the decision making process in organisational and strategic plans. For this adaptation to be effective it is dependent, as I will explain, on the way in which said learning occurs and on the way decisions are constructed and made.

This group of changes includes challenges created by the globalised world. Accelerated technical change modifies not only products and services but also their consumption and appropriation habits. The obligatory international presence that very many companies, not only large corporations, have today is also represented in order to achieve maximum performance in their business models. The reality of a world with less economic security, where new aspects of competition appear to be considered as an influence, cannot be ignored. All of this has contributed to the fact that in their management organisations face increased risk and high levels of uncertainty.

It is in this context where organisations are faced with today's unavoidable need to manage the aspect of monitoring and learning about the changes that occur in their surroundings, particularly those that go beyond an operational or divisional sphere. Not long ago this aspect was considered a general obligation for any director's position, not needing

to be allocated to any job definition in particular, nor did it seem necessary for some tasks or specific processes. Everybody knows about it, but it is nobody's responsibility. It was not measured and as a result not managed, apart from exceptions such as in the case of marketing[2], but remained restricted to its sphere. However, history has shown numerous cases of organisations, and in particular companies, that have passed the first company generation when their directors have been able to connect strategic reflection with the capability transferred to their organisations to keep them up to date with events that determine how they understand organisations, and as a result act and make decisions. This has been much more frequent in sectors dependent on science; as is the case, for example, in bio-pharmaceuticals used to working with a long-term view.

This outlook penalises all those organisations that are not capable of detecting the signals that generate these changes in time, or that having detected them, do not take decisions as a result. This shortcoming ends up becoming a weakness in these companies and organisations when competing in a global market. This has been highlighted by Ansoff, I. (1975) by introducing the concept of *"Strategic Management"*. In that year he had already put emphasis (at a time when companies were facing problems in the environment) on the need to focus on their capacity to anticipate threats and opportunities. Later, other leading writers, among them Michael Porter (1980), Gary Hamel and C.K. Prahalad (1994), emphasised the importance of strategic positioning based on analysing information from the local environment. The former, in addition to proposing techniques for analysing the sector and competition, suggested generating intelligence about competitors through an "intelligence system". The latter pair emphasised the importance of management teams in order to compete to obtain a prospective vision of the sector. Later Clayton M. Christensen *et al*. (2004) returned to obtaining certain types of signals of change as the starting point of analysis to predict changes in the sector.

With regard to the benefits of anticipating competitors' actions and understanding their strategies and other market forces or assessing the consequences and implications of technological changes, today this does not require great justification. It is as clear as the negative consequences of decision making based on incomplete or non-reliable information or information not available in time.

But as far as decision making is concerned, we have a process of obtaining information (increasingly collective and linked to the learning capacity) and another complementary analytical process and then the subsequent decision. It is here where a competitive disadvantage is again

[2] The idea linked to this analysis function or environment intelligence – "*environmental scanning*", market intelligence, although limited to its field, shares approaches with competitive intelligence.

occurring between organisations that continue under the traditional paradigm (the director assumes the initiative and the leading role) against the more participatory paradigm, for instance those based on models such as learning organisations (Peter Senge, 1990). In this regard, he underlines in Chapter 1 that, "*there are surprising examples where the intelligence of a team exceeds the intelligence of its members*".

It is in this context that we talk about competitive intelligence, also known by other descriptions such as corporate or economic strategy and similar to other concepts such as technological or strategic security or to that of market intelligence. It does not seem to us that the name today is an important matter but rather a consequence of the youth of this field. That is why we call this contribution competitive intelligence, hereinafter CI. Competitive intelligence, although it has prior precedents, strictly speaking started in the eighties in the business environment as a response to the context explained at the beginning of this introduction. It refers to making use of the capacity to understand the environment in the process of making non-structured or strategic decisions, as well as some operational decisions.

CI and strategic direction

CI represents current methodology that is increasingly linked to the needs of strategic management and corporate innovation. D. Bernhardt (1994) noted how intelligence was the energy of strategy and even went on to suggest that strategy without intelligence would make it necessary to return to speculation. Recently Roger Martin (2013) recalled how on more than one occasion when asking company directors about the company's strategy they answered that they did not wish to or could not develop it to match the high degree of change in their operating environment. According to them, particularly in high technology sectors (although it would also be possible to find other cases) there was not enough certainty to develop strategy efficiently. The danger for them, of course, is that whilst they are using uncertainty as an excuse to postpone strategic decision making, the competition can be doing something completely different such as anticipating, thanks specifically to its strategy. Therefore, it is no coincidence that directors complain after the event of having been surprised by something unexpected. Their story tends to be that when it happened it was too late to do anything constructive in this regard. The failure was not their fault at all, because for them it is the sector that is uncertain and this type of thing only occurs "naturally" and is unpredictable.

As the lecturer in Administration at Toronto University aptly remembered, each company has a strategy (Martin, R. 2013). Whether its execution is explicit or not, the decisions that are taken daily affect the company's performance on some part of the playing field (for example, making a choice of "where to compete") and how to compete there (in other words, making a

choice on "how to win"). Without making an effort through "making strategy" and let us not forget that it requires feeding with intelligence, a company runs the risk that its numerous daily options will not be connected to each other, will be contradictory regarding their divisions and levels and will finally have a reduced impact compared to the goals that have been set.

Summarising the practice of strategy, it is supported by the existence of a competitive intelligence process and in turn CI requires the existence of some strategic priorities in order to be able to effectively contribute and support the organisation's performance.

CI field of activity

CI activity focuses its attention outside the organisation but to do this it has to start from solid inside knowledge. Fleisher (2001) pointed out how with regard to CI's outside role it focuses on the comparison of:

- The industry structure and its evolution: special emphasis on the attractiveness of the sector;
- The macroeconomy seen in another way, as those social, technological, economic, ecological and political/legal (Steep[3]) aspects of the environment associated with the company itself;
- The interested parties: those organisations that can affect or are affected by the achievement of the organisation's competitive goals, and
- Issues or problems: these are the gaps that exist between the organisation's actions and the expectations of those (for example, stakeholders such as clients, suppliers, etc.) that can affect its competitive goals.

Benefits that ci provides to the organisation

Professional practice and literature on the subject lists the most common benefits:

- It reduces risks and uncertainty. Gilad (2008) stated, "it proposes a specific perspective for risks and external opportunities… and therefore it is part of the organisation's risk management activity".
- Warnings about technological and commercial surprises and those from the local environment. This benefit originates from the ability to manage anticipation. This will be dealt with later in the chapter on CI Basics.
- It contributes to the companies' non-structured decision making process, both in strategic decisions and in many of the tactical ones.
- It identifies "opportunities, threats, weaknesses and strengths".

[3] Also known as PESTEL.

In the case of strategic planning we should emphasise its capacity for characterising the business sector through the preparation of profiles about the sector itself, its players, special competitors or the technology that determines it, thereby satisfying the specific needs of the decision maker. Prescott (1989) pointed out the capacity to provide answers to questions that demand the preparation of these profiles, such as:

- What are the basic characteristics of my industry and the competitors?
- What is the current position of my competitors?
- What could my competitors' most likely movements be?
- What movements can our organisation make to achieve a competitive advantage?

It transforms collected information into practical intelligence aimed at action:

- The collaboration of all members in an organisation in the intelligence process as "antennas" or "lookouts".
- Its adaptation to the time dynamic, to deal with the evolution of critical matters and thereby make organisational reform easier.
- The monitoring and anticipation of changes in market structure and competitive activities such as: the emergence of new businesses, new alliances, capacity expansion, mergers and acquisitions (Fleisher, C., 2001).
- The analysis of competitive models: processes, products, organisations.
- Technology security and monitoring and its implications: R+D activities, innovations based on technology, emerging technologies.

CI as a process

In general terms CI is the process through which organisations collect and analyse information (evidence that can be translated into action) about competitors and the competitive environment and that ideally can be applied to their decision making and planning processes to improve their performance. It involves understanding the significance and implications of changes and innovations to the environment in time. CI connects informative signals of changes, with no apparent relationship, spread over different sources, events, perceptions and data, establishing guidelines and trends relating to the market environment.

According to the UNE 166.006:2011 standard, *"competitive intelligence includes... analysis, interpretation and communication of strategically valuable information about the business environment, about competitors and the organisation itself that is sent to those responsible for decision making as a support element to adjust direction and indicate possible paths of devel-*

opment that are useful for the organisation". This standard defines CI in its chapter 3.3 as: "Ethical and systematic process of collecting and analysing information about the business environment, about competitors and about the organisation itself and notification of its significance and implications used for making decisions" (Aenor, 2011).

CI uses public access sources to find and develop information about competition, competitors and the market environment (Vella and McGonagle, 1987, quoted by Fleisher, 2001). CI is not corporate espionage; it is ethical, legal and legitimate, while corporate espionage is clearly illegal, unnecessary and does not form part of the description of CI tasks. Information from public sources does not necessarily involve published information. There is a set of data and evidence which can be accessed legally without it needing to be published. (Fleisher, C., 2001).

Today, most organisations carry out CI in some basic form whether they are aware of it or not. Many directors practice CI in their daily activities when it involves understanding how to best position their organisation's products or services in the market. Not only large corporations but also small companies (especially in sectors such as capital goods or those more dependent on science such as biotechnology or health sciences) are often more sensitive to the gathering of information and to the use of IC effectively. Perhaps because their size does not allow many levels and everyone has "their feet more on the ground". It is not unusual in these cases for motivated businessmen to be the ones that lead this demand in their organisation, as they are personally used to finding out as much as possible about the market that surrounds them and their competitors.

Case 1: Example of a small casting company.

Such is the recent case of a casting company with thirty employees in a South American country. For years it had performed comfortably in its local market using a highly manual process carried out with professionalism but with one weakness; a high percentage of its turnover depended on projects for an outside company. The development experienced in recent years in the country led that foreign company to decide to invest in its own casting plant in the country, thereby terminating the long-standing relationship. Just at that same time, the small company made an investment to extend and modernise its facilities and process. The small company, after taking part in a CI transfer of skills process and conducting market analysis for the first time, carried out a strategic reflection exercise to redirect its current position before the consequences of the changes forced it to do so.

Source: own preparation with the collaboration of technicians and staff of the company Templamos.

CI, its concepts and practices are shown to be of great potential value for different types of organisations, not only companies but public entities,

local bodies, institutions, universities and research centres with a need to make decisions based on evidence, looking for risk anticipation and reduction. This is the case with a hospital institution making decisions about investment in order to expand its accident and emergency department.

Case 2: Example regarding the introduction of Surveillance Technology and CI in a leading hospital.

In 2011 Pablo Tobón Uribe Hospital (HPTU), Medellin, Colombia decided on an ambitious plan to expand its healthcare capacity, which entailed improving the services in the accident and emergency department to put it among the leaders in its field in South America. In the same year the HPTU management decided to take part in an initiative[4] that a local innovation agency, Ruta-n, coordinated, to define and install CI practices among companies in the Antioquia region. Health institutions increasingly have to face strategic investment decisions that are more dependent on technology. At the same time these can determine its future performance. As a CI pilot exercise, the HPTU management selected the decision concerning efficiency in the accident and emergency department. As a result, a hospital team in collaboration with the local university institution, ITM (Metropolitan Technology Institute), previously trained in CI, followed the known CI methodology and in twelve weeks prepared an international report on best practices, trends and processes in the organisation of the hospital emergency department. It identified two communication technologies applied to emergency units that up until then had only been installed in the USA. The management endorsed the report's results and gave approval to this surveillance technology (ST) and CI practices in the hospital. The quality control manager and the systems and ICT manager were integrated into the ST and CI task force.

Source: own preparation with the collaboration of HPTU technicians and medical personnel.

Adapting a work by Professor Craig Fleisher (2001), a way of understanding a CI operation is to see it as a progression from raw materials or consumables up to finished products. From this perspective CI starts with scattered pieces of raw basic data. This raw material is organised by CI practitioners and turned into information. The information is turned into intelligence when, after obtaining the information originating from it (meanings, implications and consequences for the organisation), it is put into a useful format for the key or unique intelligence needs of a decision maker (known as Key Intelligence Factors or KIF); good CI is driven by needs. Without CI customer orientation, it does not make the slightest bit of sense. The decision maker's involvement in the CI process starts with the definition of the need and culminates in the interaction with the results or communica-

[4] This initiative had the writer of this article's address from the Polytechnic University of Valence and was financed within a programme known as ERICA with support funds from Spain's cooperation through the AECI and local institutions.

tion to make the decision. Therefore, intelligence is the information that is analysed, interpreted and communicated with the explained implications. Competitive intelligence is the more specific intelligence product that satisfies the unique needs of a decision maker to understand a competitive aspect of the organisation's internal and/or external environment.

CI as an organisational function or management approach

CI is the aforementioned process but to fulfil all of its potential it also needs to be administered as a management approach or system that makes use of the learning potential of the entire organisation and of its area of influence as a support network and by obtaining warning signals about those changes that to a great extent involve the organisation.

In this regard it is considered as an organisational function and therefore we should also discuss a system's formalisation and organisation.

In fact this is the approach of UNE 166.006 when mentioning the purpose of surveillance technology and a competitive intelligence system in Chapter 1: "formalisation and structuring in the organisation of the listening process and environment observation to support decision making at all levels in the organisation, evolving into the introduction of permanent surveillance technology and a competitive intelligence system. In this regard the system will contribute to establishing bases for defining the competitive position that the organisation has to take, its goals *(in the case of this particular standard its purpose especially relates to matters of R&D+i)* and the appropriate organisational diagram for said position and goals".

CI can provide the foundations for the construction, assessment and modification of both market and technological strategies and tactics and in other fields. As a function mainly aimed at management, CI is cross-functional. That is why in practice, organisations coexist where the CI approach is functionally developed based on marketing and/or planning and to a lesser degree on other functions, such as R&D. While these other practices appear, there are less common ones where CI is used, depending on the need in question, whether purchasing or a corporate need, including marketing, engineering, human resources, finance and planning and there is CI coordination for the entire process. Later in the chapter its organisation will be discussed in more depth.

On the other hand, CI can consider two possible approaches to work, which are often complementary; contributing intelligence for decision making at a particular time, and continuous tracking regarding the time, surveillance and monitoring of a particular subject of interest. This is included in the UNE 166.006 standard Chapter 7.1 as:

- The search and research into what is unknown, and

- The search and systematic monitoring of innovations in areas that have already been previously defined.

Essential stages in the ci working process

The CI process or cycle that is shown in Figure 1 brings together a series of the usual steps or stages in a CI exercise or project that with some minor variations in terminology and in the number of steps meet the standard model in this scope of the intelligence function (Aguilar, F.J. 1967, Porter, M. 1980, Bernhardt, D. 1994, whilst in Equipo CNI we can find an abridged Spanish version). Madureira, L. (2013) claims how the OODA (Observe, Orient, Decide, Act) Loop model by the American John Boyd is more suitable, by prioritising immediate answers. It is important to emphasise that although the stages appear as consecutive within a cycle, in reality it is not like this. This means that it is good for clients/decision makers, as they are up to date and direct the research advances throughout. Neither does the analysis stage begin once the previous stages have finished. At the end there is a high degree of group work and interactions that enable delivery times to be cut from that of a strictly sequential process of these stages.

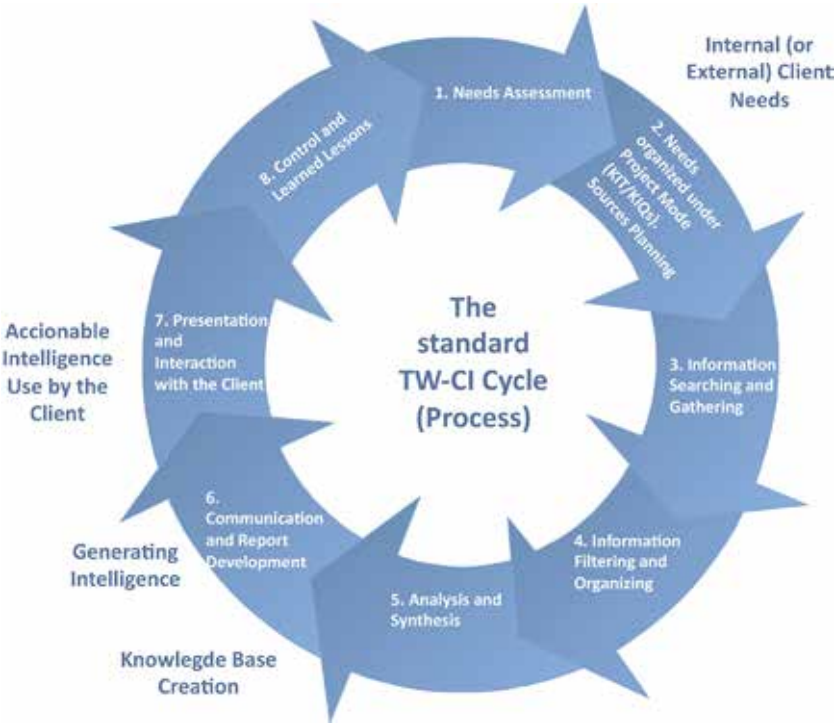

Figure 1. Competitive Intelligence process or generic cycle

Source: own preparation from the traditional Competitive Intelligence Cycle/Process in Palop Marro, F. and Martínez, J.F., 2012.

Planning

The CI process or cycle usually starts with a decision maker who has a specific intelligence need (key intelligence factor or need or KIF) and people who collaborate to construct it. It is important to determine what needs to be discovered, for whom and how and when it is going to be used.

Writers such as Herring, J. (1999) speak about three types of need that are most common. These in turn make up the basis of the approach for structuring the work process around the ST/CI subjects as projects or Key Intelligence Factors, KIF. Each one of these three groups of needs requires a different type of result and this determines the sources to be consulted, the analysis techniques to be applied and also the structure/ report that will contain the answer.

Strategic decisions and actions. Including the development of strategic plans and strategies. For example, decisions appear that are connected to investments in technology, entrance into a market or alliance with a company.

Early warning subjects. Possible initiatives regarding competition, technical and technological advances that can surprise, socio-economic and geopolitical changes and their implications, modifications, regulations and standards that have to be complied with.

Descriptions of the players and of a certain market. These include competitors, suppliers, clients, possible allies or the regulator of a market.

When CI is developed with a "spontaneous" nature there are no predefined formats for reports to organise the intelligence that it generates. But this does not occur when we are in a planned CI situation. As a result of seeking productivity in tasks and flexibility in the delivery periods, some types of reports or CI products are defined, such as competitor profiles, warnings about risks/opportunities, reports on the status of state-of-the-art technology, comparisons or "benchmarking" of products/services, monitoring services or synthesis reports etc., the communication of which will be discussed later.

Each one of these reports or products is differentiated from each other by considering variables such as:

- Purpose and expected value in relation to the need that arises and type of decision.
- Main client and other recipients.
- Sources of information to be used.
- Models, analytical methods and software tools to be used, as appropriate.

- Forms of communication and type of template for the report.
- Cost in terms of hours of commitment and acquisition of information.

Obtaining information

The arrival of the internet, web sites and social networks meant a new paradigm in the way in which electronically published information is accessed. However, despite its indisputable value, the role of primary contact sources on the ground with the main players involved in the subject cannot be underestimated. This in the Anglo-Saxon world is known as "humint" or intelligence from information and tacit knowledge that only resides in people. The need to access these "experts" or players about the matters of interest, mainly by telephone, e-mail or professional meetings has been shown as essential on numerous occasions in order to compare and complete substantial pieces of the "puzzle" that enables completion of the intelligence. It is also irreplaceable for the managing of the other experts that finally enables completion of the task. In this regard it must not be forgotten that globalisation also gives these experts access from a global viewpoint. We should also take into account that in the full "kingdom" of the internet and electronic sources an entire series of markets coexist, for example energy markets in distant countries, where the scarcity of data from conventional sources takes preference and where verification "in situ" of the interlocutors is needed before negotiating[5].

Case 3: Example of how companies watch over each other: Microsoft – Google

MICROSOFT spent months on a massive project to bring down Google when the truth began to dawn on Bill Gates. It was December 2003. He was browsing on the web site of the company Google and found a page with descriptions of all the jobs available at the company. Why, he asked himself, were the requirements for many of these positions identical to the specifications for working at Microsoft? Google started as a search engine on the web, however, here on the screen were jobs for engineers with experience that had nothing to do with search engines, whereas all were connected with Microsoft's main business; people qualified in things such as operational system, compiler optimisation and distributed architecture systems design. Gates asked whether Microsoft could be facing much more than a war in search engines. In an e-mail that he sent to a handful of executives that day, he effectively said, "we have to watch these guys. It appears that they are building something to compete with us".

Source: adapted from Fred Volgestein, 2005.

[5] I owe this teaching to a technique of a gas industry company.

Analysis

From the CI approach, data and information are the starting point not the finishing point. Therefore, data and information collected in the preliminary stage are not intelligence. So that "sense making" is brought to decision making (Jaworski, 2002), meaning and value, that is, intelligence, must be selected, validated and organised through its analysis and interpretation (Kahaner, L. 1996). In other words, this refers to constructing, from unconnected fragments made up of data, personal testimonies and information, a puzzle or outlook that makes it possible to understand what the analysed scenarios are and intuit possible ways forward. In short, building CI is transforming information into elements for deciding and acting.

In this regard, although much has been written on the role of intuition in CI and on the nature of the "art" of interpreting the collected facts, while not ignoring its contribution, it does not appear to us that it is an appropriate starting point to approach the learning of analysis. In accordance with what we have explained in the basics of CI, we believe that the construction of CI reasoning based on the interpretation of the collected evidence and its significance for the context of the company to be key. A CI construction based on evidence and analytical models makes it possible to involve the decision makers within a transparent chain of the decision making process. At the same time, intelligence gains in objectivity by reducing its dependence on the person(s) who formulate(s) the conclusions and interpretations. Finally it supports learning of this key stage in the CI process. This said, of course over time experience accelerates the analyst's capacity to sense consequences derived from facts, but the analyst must try to justify them through evidence so as not to introduce excessive biases in the results.

The results produced by the analysis, as Fleisher, C. (2001)[6] recalled, must be able to induce action, have a prospective nature and be directed towards the future, provide the perspective of the facts within the context of the business, (Gilad, B. 2008), help the decision makers to develop better competitive strategies, provide a better understanding of the competitive environment than their competitors have and identify not only the current and future competitors, their plans and strategies but also the key risks and opportunities. The final goals of the analysis are to obtain better business results, not achieve intermediate results from better decisions or analysis. Good analysis provides a response to the well-known question in CI, "if this is true, then what?" – in other words collected information tells me something new and original that I need to

[6] Adapted from Craig Fleisher with changes.

know about the market that can satisfy the matter or KIF proposed by the decision maker.

Fleisher, C. (2001) also completed this description of analysis when he pointed out how an efficient CI practitioner must know about the interaction between the collection and analysis stages, use creativity and alternative thought[7], use deductive and inductive reasoning, understand basic analytical models, introduce interesting and attractive models to induce the idea of discovery from the analysis rather than a more unexciting research approach, know when and why to use the different analytical tools, recognise the inevitable existence of gaps and blind spots and know when to stop analysing in order to prevent paralysis due to over-analysing.

The relationship between people immersed in analysis using the CI process with the different analysis tools must be that of experts regarding the possibilities that each of them offers within the "toolbox" and their ability to apply the most appropriate tool in each case. Professors Fleisher and Bensoussan (2002), made a commendable effort to compile analytical tools used in the business environment, many of which were ignored or underused, and they also gave guidelines for their application.

Finally, analysts need different training to people with an informational profile, more focused on obtaining and organising information from different cultures. Large organisations develop a different function within CI and sometimes from a different place.

Communication, application of what has been provided and evaluation

The communication stage presupposes an interactive process between the decision maker who is going to put the intelligence into practice and those who contribute to it. What is provided does not become intelligence that is directly applicable by the decision maker unless the decision maker gets involved and interacts especially in this team stage so that the team directs and personalises its results just as the decision maker needs. This is why the reports mentioned earlier in the planning stage give the specific decision maker different types of communication such as personalised reports, personal communications, scheduled presentations, special notes, archives, computerised databases, along with memos, regular meetings, training seminars, electronic notice boards in the intranet or the removal of tasks.

[7] Writer's note: in the sense of outside the box of conventional thinking.

Generally, application of the results also includes certain sub-processes that are no less important. Among these is control of the CI process. In other words, the evaluation and communication of what is provided, its effectiveness regarding the decisions taken and their result. In short, the capacity shown by the CI to contribute to generating value. Also, from the point of view of quality, the experience acquired and its development, resources used, etc., will be taken into account in the feedback for improving the CI process – the driving force of quality – as UNE 166.006:2011 proposes. Finally the results can also influence the need to review or reconsider some aspect of the organisation's strategy.

When measuring and controlling the performance and value provided by the resources spent on CI it is necessary to go beyond the quantitative indicators of activity to the result. We must focus on measuring its capacity for generating value. In this regard some questions of the following types, frequently asked, can help to evaluate it. Who are the clients of the CI process? What type of needs are they demanding? How do they value the intelligence they receive? How are they applying the intelligence? What are the costs of the resources spent on CI? To what extent has the work of the CI team and this process contributed to turnover/profits and savings in costs for the organisation?

How CI is organised

Not only one organisational reference model can be mentioned but different scenarios that depend on the degree of maturity, on a person's experience in CI, the sector in which it occurs, etc. Writers that have studied this aspect (from Rouach 1996 to Michaeli or Singh, 2006 among others) essentially agree, although using different terms, in defining between three to five situations. A first, which is widely used, of reactive CI, practiced spontaneously individually as a response to an urgent need for collecting information and making decisions given the appearance of certain changes. In many organisations these practices are formalised as a work process in a team with a coordinator within any of the operational divisions or any business unit but without developing synergies between them. Finally, in some companies CI is organised as a cross-departmental corporate process already consolidated with an assigned director or a CI unit within the management personnel.

Although in many cases an evaluation process is confirmed among the different aforementioned situations from the spontaneous/reactive to the planned and consolidated, each organisation finishes by finding the model with which it is most comfortable. The most typical situations are summarised below:

From operational departments independently or jointly using the figure of a coordinator or project manager.

- Michaeli, R. (2006) suggested evolution of their organisation as from "islands" in the operational divisions or departments to being organised as a "centre".
- Fleisher (2001) highlighted the organisation starting from a company's own specific programme.
- Cartwright, Boughton and Miller (1995), mentioned by Fleisher (200) described 1) *ad hoc*, 2) continuous overall 3) continuous focused and/or 4) project-based CI. *Ad hoc* would be the most extensive CI, done on demand and producing results that are by their nature one-off and are focused on a particular competitor, event or competitive product/service.

Regarding large corporations, Martín (2010) proposed a model for the CI unit and operations manual where a study on the risks agenda was provided.

From the nineties we see how CI has contributed to strategic decision making integrated into formal dedicated units, whether independently or more usually within marketing or planning. The activities of competitive intelligence are focused on both tactical and strategic decision making and include qualitative and quantitative analysis starting from the evidence. Competitive intelligence receives moderate attention from senior management and is often a useful factor for taking strategic decisions.

Reference countries in the CI practice. The situation in Spain. The range of training.

If we prepare an indicator for said purpose based on variables such as the offer of CI training with degrees and postgraduate studies in the academic field, courses for companies, conferences and seminars and companies with formalised CI processes it is probable that among the countries having a better score will be most countries in the OCDE (Organisation for Economic Cooperation and Development). Among them some are traditionally mentioned as leaders: USA, Canada, France, Germany, United Kingdom, Israel, Japan, South Korea, Finland, Sweden and Switzerland. Many of the multinational companies from these countries are known for involving their employees as antennas of observation in their business environment.

With regard to Spain, it is confirmed that CI public visibility still appears well below its use for business and its potential for generating value in a globalised world. It is true that since the nineties, driven

by internationalisation of many of its companies and the acceptance of more complex risks, it has seen significant promotion. However, its awareness and practice is not comparable to the situation in neighbouring countries. In any case, the role played in recent years in its dissemination by institutions such as AENOR with its UNE 166.006:2011 standard, ICEX (Spanish Institute for Foreign Trade), the National Intelligence Centre (Centro Nacional de Inteligencia, CNI) or the Inter-University Masters between the Carlos III and Rey Juan Carlos Universities in Madrid that the Autonomous University of Barcelona recently added, should be considered.

CI promoted from institutions

Countries such as France, Germany, Israel, Japan, South Korea or Sweden maintain different policies and support instruments for their companies with institutional information networks. From there they have been generating interactions and transfers to the commercial and economic sphere.

We highlight the French approach of "intelligence economique" as France is a neighbouring country and for the particular interpretation and involvement of the institutions from that country in the development of CI in the business environment as policy.

This idea was introduced in recent decades, driven by government initiatives and through working groups with extensive involvement in the business world. It contains an appropriate interpretation for the interests of France and its economy regarding the consequences of globalisation. Therefore, it went from the priority consideration of strategic surveillance to the appearance in 1994 of the Martre Report in which the current concept of "intelligence economique" was already mentioned and presented in relation to its important role in improving the country's competitiveness and its social cohesion[8]. It was in January 2003 when there was a new step by motions from the French government's Prime Minister and what is known as the Carayon Report (2003) was prepared. It was the Prime Minister Jean-Pierre Raffarin who asked his MP Bernard Carayon "to make an inventory of how our country integrates the functions of intelligence in its educational system and training into its public performance and into the business world" and he pressured him to make recommendations to improve this function. Said report considered the public policy of competitiveness, economic security and influence, especially with international organisations and training. It is de-

[8] Martre (1994), *Intelligence économique et stratégie des entreprises*, Commissariat Général au Plan, 1994.

rived from an original reading on globalisation that took into account the daily life in markets, avoidance of their rules, games of power and influence. Economic intelligence is considered in the report as a public policy more aimed at the identification of sectors and strategic technologies and at organising the convergence of interests between the public and private spheres.

The report emphasised the trio formed by obtaining information (surveillance of the environment...), protection and influence. Emphasis on influence was presented as a characteristic of French researchers (both in the form of pressure groups, of political influence to endorse market conquests by companies, but also as an ability to impose international standards, images, values and general ideas supporting their economic intentions).

Therefore, today the concept of economic intelligence in a neighbouring country is especially linked to:

- Surveillance and business intelligence (obtaining of important information).
- Protection of the wealth of information assets (stopping secrets from being revealed).
- Supporting decisions (analysis, decision mapping, scenarios and a "war room"...)
- Influence (spread information or forms of behaviour and interpretation that support the strategy)

Therefore, the policy has involved different institutional and territorial levels. So the French Chambers of Commerce have been very active for years making this approach reach small and medium-sized companies. Meanwhile in the territory around the concept of a group or "cluster", different "technological poles" of specialisation throughout the country have been prioritised with the idea of intelligence playing an important role. This will be returned to later when discussing the concept of territorial intelligence.

Harbulot and Baumard (1997) provided historic background to the French concept of economic intelligence and, among other references, cited writers such as the aforementioned Harold Wilensky (1967), on his vision of organisational intelligence. This writer proposed two main issues that remain valid:

- Collective and cooperation strategies between institutions and companies in the production of common knowledge for the defence of a competitive advantage.
- The importance of knowledge on the economy and industry as a strategic fact of development and change.

Training offer

It is necessary to distinguish between programmes from academic institutions for degree and postgraduate qualifications and informal training programmes.

Apart from exceptions in countries such as France, Canada, USA, Sweden and Finland, CI studies are still not present as such in degree programmes, although they are reflected in closely related areas of knowledge (information sciences and librarianship). In postgraduate studies there is a better range of Master qualifications in different countries; in Spain particularly there is the aforementioned Inter-University course of Intelligence Analyst and some short courses offered by the UOC (Catalonia Open University).

Informal training is full of courses with different contents and different durations that involve the term CI. Recently the ESIC Business Marketing School, Madrid, has become involved in this market with a specialised seventy-hour course.

Specifically with a programme designed for company directors there are programmes in various European Union countries from the Institute for Competitive Intelligence (ICI) with headquarters in Germany to the North American Academy of Competitive Intelligence LLC (ACI). The certification of the qualifications that they issue is one of the key elements of these programmes.

CI basics. The state of the art

I am not aware of an accepted model that integrates learning about the business environment and the non-structured decision making process into organisations. In this regard, I agree with Day and Schoemaker (2006) when they, regarding the concept that they called the *"peripheral vision"* of the organisation, particularly necessary when referring to intelligence on emerging changes, considered that a universally assumed and accepted model did not exist that sustained it. In this regard, one of the challenges to be covered by competitive intelligence in its current context is the analysis and forecasting of future opportunities that are still distant from the activity itself.

That is why we write as a starting point in order to establish the CI basics; the reflections that for this purpose these writers carry out of the "peripheral vision". Among our many sources we have turned to the decision-making fields (decision sciences), marketing, strategy, organisation theory and economy as well as to scientific fields applied as scenario planning, competitive intelligence, market research, environment scanning and technological forecasting. This leads us to a first

conclusion; we are faced with a field of an *interdisciplinary* nature and still, as Fleisher and Blenkhorn (2003) stated, in the standardisation process. These apply - starting with Ashley and Morrison (1995) - the phases in the evolution time cycle of problems to the solution and regulation of some of the issues that are still under debate within CI, including its name.

The non-existence of a reference model for CI or the persistent lack of consensus with regard to certain issues has hindered its dissemination in this still young field as we understand it today, but not in its precedents as we will explain below. On the contrary, as argued previously, the current market challenges have helped to expand the concept and put it into practice.

From a historical perspective, professors Juhari, A. and Stephens, D. (2006), from the University of Loughborough in the United Kingdom, carried out a valuable review on the background and development of CI. They outlined the beginning of intelligence starting from military confrontations, companies' needs for information and government practices. This process for configuration of the CI field meant a continuum that dated back in time many centuries until reaching the current CI situation, where it was positioned at the end of the 1970s.

This is how a multidisciplinary environment has been configured in recent years. This includes the management of work processes, Competitive Intelligence (CI) that requires a culture and skills in knowledge management by the organisation and a process that integrates it for decision making. In this regard it has obvious synergies with the concept of organisational intelligence. This idea includes management of the organisation's knowledge and learning. It has a final purpose by directing knowledge management towards its strategic adaptation to the environment and fulfilment of business goals, Halal, W.E. (1998). Its precursor was Harold Wilensky (1967).

This process is necessarily cross-departmental in organisations as it involves and needs contributions from people, from different departments and operational departments in the organisation and the use of a set of techniques inspired within strategic and prospective planning. Finally, the model that the management of this effort requires is company strategic management and innovation.

Palop Marro (2012) previously tried to show this interdisciplinary nature but relating in particular to the field of Surveillance and Intelligence in technologies (see Figure 2). This had already been done by Masson, JL. (2005), who, by confirming how CI resulted from the integration of some areas of knowledge, referred also to Information Technologies, Linguistics and, within knowledge management, to Information and Documentation Management.

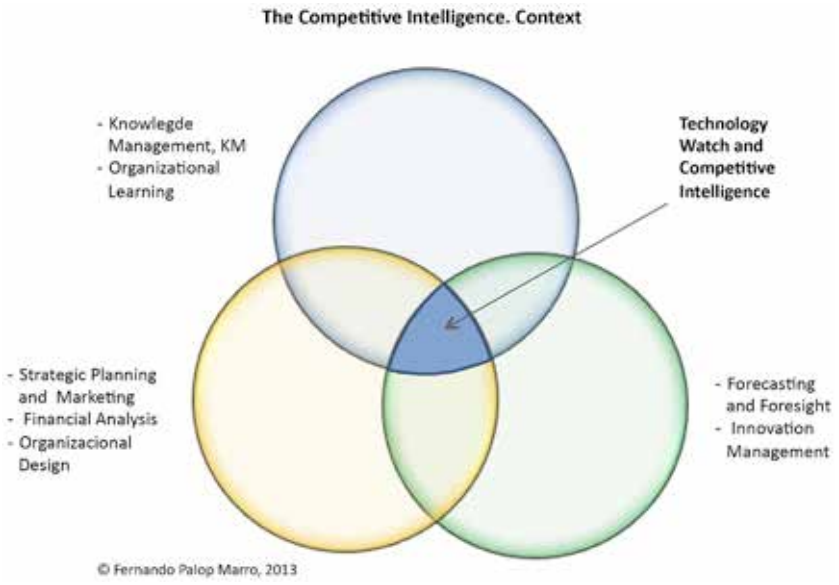

FIGURE 2. Inter-disciplinary nature of CI

Source: adapted from Palop Marro (2012).

Having confirmed its inter-disciplinary nature, we are next going to outline to what extent CI represents a proposal for a change of the paradigm on which the current strategic decision making process is based. In particular the decision maker's role in this process is interesting, as is that of the people that make up the organisation and the value of the evidence obtained as main support that is irreplaceable in CI proposals for decisions. This role is explained below on three axes: the information process aimed at decision making, learning mechanisms for changes in the environment by organisations and the third is the need to generate the anticipation that this learning demands. The first two start from the Day and Schoemaker (2006) approach and we add the third here.

It is confirmed from a planning and decision making perspective how individuals are the receivers of the organisation and its internal procedures are those that ultimately impose the matters that must receive attention. There are major challenges on an individual, group and organisational level to take responsibility for the appropriate issues at the appropriate time (Stoner and Wankel 1989). To assess these matters, Day and Schoemaker (2006) proposed incorporating:

- At an individual level different criteria and choice biases.
- At a company level the organisational and strategic dynamic.

Implications for organisations. Their use vs. Their protection

Three axes on which to locate the CI basics in organisations:

1. The information process focused on decision making.

In the past, Palop (2012) maintained how the slow rhythm of change made it easier for a small group of directors with access to information and the ability of prospective vision to successfully define an organisation's evolution. Today what we are seeing is that these same directors must consider changing their traditional paradigm for decision making, relying more on their organisation, in which it actively participates in the timely integration of multiple sources of information and its analysis. In a world where to compete means making decisions with a high degree of uncertainty, the reasoning and construction of intelligence that these decisions demand must be based on evidence. Senior management must discover, if it has not already done so, that in this task its own organisation must play a leading role, including the networks of relationships that it acquires.

Alan Newell and Herbert Simon proposed "a perspective of information processing in the organisation's decision making". The heuristic nature of human reasoning as understood by cognitive psychology continues to fail to resolve interaction between emotion and cognition. When applied to the problem of periphery vision of what surrounds an organisation, Day and Schoemaker (2006) understood that the processing paradigm of information indicates the presence of four key phases: perception, judgement, action and feedback. At an organisational level the parallel stages to this process can be described as: information acquisition, information dissemination, shared interpretation, coordinated action and collective learning. This interpretation of Day and Schoemaker seems important to us as it shares the elements that in our opinion the new paradigm requires.

Nor must we ignore how these writers remind us that "In all stages the process is guided by a set of models or mental sketches that reside in very deep levels of the organisation". In other words it is not enough to generate value with CI by implanting a process or investing in a costly software tool. A new type of leadership must be demanded that also changes those aspects of the corporate culture linked to information management and knowledge.

2. Learning about the changes in the environment by organisations and their implications in the management of knowledge required by CI.

There are many precedents and points of intersection with the point of view of the information process for decision making.

Peter Senge's book *The Fifth Discipline* (1990) could be considered as a turning point, by translating for a wider audience of directors the evaluation of the importance of a focus on learning[9]. Senge combined his contributions with other points of view, especially the importance of systematic thought, to provide a comprehensive perspective of an organisation that learns. The related work carried out by John Sterman[10], Chris Argyris and others helped to configure organisational learning as a different intellectual perspective. The basic point of view is that in dynamic environments learning is complex and therefore it is neither simple nor automatic. To try to determine what happened and why, we find – by following Day and Schoemaker (2006) – the following: ambiguous "feedback", late reactions, multiple partial causality, interesting contributions, missing information, processing effects, random noise and the illusion of controlling all attempts to destroy the organisation.

When we add to this the probability and ambiguous nature of the signals, lower in as much as it comes from the organisation's business periphery, the problem becomes a lot worse. Some writers have demonstrated that people show a great aversion to ambiguity when faced with decisions that involve unknown hazards. People prefer "the devil you know" to the supposed known good. Consequently they never experience or learn well in environments of great ambiguity. This tendency can be aggravated at an organisational level where it is expected and desired that rationality and the capacity for prediction dominates. However, new opportunities usually lead to a high level of uncertainty and therefore demand a high degree of tolerance to ambiguity. These thoughts by Day and Schoemaker (2006) coming from an analysis of emerging technologies are perfectly valid for many mature markets where the socio-political circumstances give them high uncertainty. For example, decisions about nationalisation that are being taken in some Latin American countries with populist governments or the situation recently in some Arab countries emerging from long periods of dictatorship.

For Day and Schoemaker (2006) the idea of cultures that are capable of learning from complex environments might require some management principles and values different to those that are necessary for maximising the organisation's legal business. In this case a conflict arises be-

[9] In addition to P. Senge's book the strategic importance of learning – above all about the future – is underlined by Gary Hamel and C.K. Prahalad in their book *Competing for the Future* (Boston, Harvard Business School Press, 1994). Chris Argyris in his book *Strategy, Change and Defensive Routines* (Boston: Pitman Publishing, 1985) tackles the organisational obstacles to learning and change. In the field of new technologies these obstacles are a threat, as is shown by Clayton M. Christensen in *The Innovators Dilemma* (Boston: Harvard Business School Press, 1997).

[10] Morecroft, John and Sterman, John "Modelling for Learning Organizations", Portland, 1994, *Business Dynamics: Systems Thinking and Modelling for a Complex World* (McGraw Hill, 2000).

tween the culture of performance and that of learning and it is senior management that is responsible for determining the correct balance between them.

3. The need to generate the anticipation that this learning requires.

Different studies frequently connect failures in business management to the inability to: anticipate rapid changes in the markets, respond to new competition and to its proliferation or to redirect a company's new technologies and strategic management towards the changing needs of clients and a sector's new standards (Fleisher 2001). Gilad expressed the same idea that organisations frequently failed because they were not capable of reading typically weak and ambiguous signals that were ubiquitous in their environments and markets.

By introducing the expression "Strategic Management", Ansoff (1975) highlighted the need to focus on organisations' capacity to anticipate threats and opportunities in order to confront the turbulence in the environment surrounding a company.

In fact, different field studies confirm this point of view. Successful organisations are among those that detect the most important events through "warning signals". When uncertainty is high the directors report on a greater frequency in the monitoring and surveillance of the environment and a greater use of sources of personal information. The top directors in high performance companies respond to strategic uncertainty by monitoring the environment more frequently and extensively than their equals in low performance companies (Daft *et al.*, 1988).

But in practice this challenge does not provide a simple solution (Ansoff *et al.*, 1979, Porter, 1980). Even organisations that have implemented CI systems often do not anticipate strategic surprises (Gilad, 1988; Blanco and Lesca, 1998). In both cases (with and without CI systems) the majority of them seemed to suffer from both an information overload and from a lack of "strategic information" which for Blanco and Lesca 1998 led to a questioning of their strategies of information collection.

However, in my opinion this situation is also due to a failing in the other two aforementioned axes. Here we are to go a little deeper into the identification and selection of the signals of change as a basis for anticipation and into its management overcoming barriers and "blind spots".

Ansoff confirmed the existence of a series of filters in the organisation, shown in Table 1, which prevented the relevant signals getting to the decision makers on time. Today these contributions continue to be very valuable. I personally had the chance to confirm it. Such is the case of rapid international growth in the last two decades of a new competitor in the sector of lemonade drinks, the Peruvian family group AJE, by making the most of opportunities for changes in the traditional business model. This

growth occurred and people within one of the affected competitors told me they were conscious of the appearance of the threat but did not have the mechanisms available in their organisation to make senior management aware of it and catalyse a change. This is an example that confirms how knowledge of events is not enough - the signals of change. Their meaning and implications must be made available to senior management so that it can set up the strategic direction before it is too late. Among other challenges, this means overcoming these Ansoff filters and communicating not the events but the intelligence about them.

Table 1. Barriers to early signals of change: the CI process helps to reduce them.

Filtro o barrera	Causa de la existencia del filtro
Filtro de vigilancia	Error al centrar el foco de atención. No hay directrices ni prioridades
Filtro de mentalidad	No se reconoce la importancia de la novedad porque sale del modelo o esquema mental predeterminado. Se reduce la información
Filtro del poder	En la toma de decisiones lleva a los actores menos poderosos en la organización a contener la expresión de sus percepciones

Source: Ansoff, I. 1984.

The existence of a CI process helps to reduce these barriers as Ansoff, I. (1984) pointed out, to those early or "weak" signals of changes and to communicate not only the evidence but its implications for the business, in short, intelligence. In this regard, supporting with evidence and with a transparent process for everybody improves the credibility of the team that promotes the CI exercise while minimising the possible power filter by integrating decision makers into the CI process itself. That is why the CI working team must try to differentiate at all times between what are valuations or interpretations regarding their facts. Once the case has arrived it must be explicitly documented in such a way that the decision makers are always clear about the process or the chain of value of the information transformation[11]. In other words the sources from where the data and information starts, the gathered evidence, and the perceptions and meanings gathered from them that are managed for their decision.

The underlying supposition of "*Early Warning Signals" (EWS)* is that discontinuities do not arise without prior warning. These warning signals

[11] This idea is from the French engineer Paul Degoul, Director for many years of ARIST (Annual Review of Information Science Technology) Alsace and ADIT (Design, Industrialisation and Technology Consultancy).

can be described as "weak signals" as they have a value while they are scarce, scattered and fragmented. The capacity for anticipation and margin for reaction still exists there. The goal of the "weak signals" (Ansoff, 1975) concept is early detection of the signals that could give rise to strategic surprises and to an event that would have the potential to put the organisation's strategy in danger. The CI process must integrate an organised and systematic response to the detection of these signals.

A major problem for organisations is to resolve the choice of these "*Early Warning Signals" (EWS)*. To conclude, Blanco and Lesca (1998) confirmed that EWS could not be approached objectively, but was a construct that represented the knowledge of individuals. Therefore, the choice must be necessarily considered as a collective process in which interpretation played an important role. This led them to formulate both practical implications and theories. Mendonça *et al.* (2007) came to the same conclusion when he stated that the practical meaning of weak signal information is that it can be transformed into meaningful knowledge for action. However, they confirmed that as the value of this information did not materialise automatically, the carrying out of this potential required a collective cognitive framework through which the weak signals could be collected, evaluated and from there action be taken. The theory of stakeholders was proposed by Comai and Tena (2006) to understand figures in a specific industry within a EWS system.

Therefore, the approach from a CI process on how to focus the response to EWS is not obvious, as has now been pointed out. Its solution has been shown not to rely solely on information technologies. These are an instrument and not an end and can help the human team's productivity but not replace it. The combination of information technologies and the human team is shown as the approach with greatest potential.

As a result of the existence of these aforementioned filters reported by Ansoff, certain blind spots of incorrect perception regarding the view of the environment appear in certain managers. This idea of a "blind spot" was raised by Porter (1980, pp. 59-60), who used the term to refer to elements of knowledge about the environment that were not certain but that still guided business strategy. Specifically this writer mentioned that, "they are areas in which a competitor or not sees the importance of events absolutely (such as for example a strategic movement) or perceives them in an incorrect way or only perceives them slowly".

Behind the analysis of blind spots lies an assumption about the biases inherent to decision making among an organisation's senior management (companies and institutions), which overcomes those of their employees or outsiders. Their foundations can be found in the Ansoff filters. In 1994 and later, Ben Gilad developed a three-stage analysis method for these blind spots that has been incorporated into the CI analyst's toolbox. From

a first examination of five market forces and their driving factors an analysis is carried out on the directors' assumptions and perceptions of a certain company to identify in them these possible blind spots in a third step. The deterioration of the capacity of the managers to see reality as it is and the most objective analysis of analysts and the medium-level planners (with less ego involved) means that this third step in the analysis of blind spots can be a tool to manage those potential blind spots.

Influence and security inside companies.

Although the benefits for the business and for world globalisation development have been confirmed, the fact remains that it represents an increase in risks which companies must face in conflictive and/or distant markets. It is obvious that the complexity/uncertainty increases in those countries where an information value chain does not exist or is incomplete and therefore the performance of conventional sources will be very much reduced. On the other hand, and purely as an example, recent events such as those experienced in 2012 by the Spanish company Repsol YPF in Argentina (complexity of political and economic "drivers", subsequent entry of a competitor Chevron, "a dark horse" into the scenario) or the limited situation experienced at the beginning of 2013 with the occupation of the BP gas plant, the Norwegian Statoil and Sonatrach in Tiguentourine, in southern Algeria (again the triggering factors were socio-political) are reflected in that growing complexity and uncertainty of the existing potential for CI and of the need to emphasise risk management.

But today security also has to be considered in the EU's own market. In this regard, as an example we include some of the advice about economic security that the French Chambers of Commerce, Chardon, V. and Bauquis (2012) propose to research companies and entities based on three goals:

1. Identification and analysis of the threats when French companies are the target;
2. Protection of research companies and institutions, by their size or sector in which they operate. In fact any business can be subject to "attacks" when it is a prominent innovator and operates in a competitive sector; the same is applied to research institutes;
3. Dissemination of a security culture for tangible and intangible assets in all companies, both in large groups such as SMEs and research institutions.

The strong tendency of organisations towards dependence on knowledge management, their reflection on the growing value of management of intangible intellectual assets, and global electronic commerce also underlines threats of a different kind to these intellectual assets and their need for protection from a global viewpoint. An example of it is shown in the aforementioned French idea of "intelligence economique". This in-

cludes, as has been seen, two additional dimensions to the surveillance or monitoring of the environment and to the generation of intelligence for decision making, which are:

1. The capacity for influence, in other words, the technique for using the information for the organisations to project their influence into the markets;
2. Protection of information assets, in other words, the company's ability to preserve the information relating to its knowledge, experience, strategy and prevention of risks connected to negligence or fraud in the handling of the company's information and knowledge.

Here we will limit ourselves from this confirmation to explain the negative consequences of a type of traditional crime for the security of companies and research institutions, as is case with industrial espionage. This situation, which nowadays takes on new forms through cyber crimes, requires the ability to respond with active protection policies that also deal with the organisation's intangible assets. One of those derived from CI is that the organisation as a collective becomes more aware of what is really important to preserve (tangible and intangible assets) from the knowledge, where their most vulnerable points are and as a result how to adequately protect them.

The illegal nature of industrial espionage and its negative consequences on CI in companies

Throughout history attacks on organisations' intangible and tangible assets have occurred. The attempt to use shortcuts breaking the law to steal a competitor's unique know-how has a lot of precedents. In fact, now we will be using examples on how this type of crime has an importance today that cannot be dismissed. What attracts attention is that within this field this crime, which is called "industrial espionage", leads the media to eclipse the work of the great majority of the professionals, associations and training entities that respect legislation and are used to generate value for their organisations by analysing the information obtained from public access sources. In addition, as Gilad (2008) emphasised, this negative connotation is the result of ignorance and confusion in general interest media, of the meaning of the concept of intelligence with something more suitable to a military environment, where obtaining information is the end that justifies the means. This is where a crime can appear if extrapolated to the civil sphere, but that is information obtained illicitly and therefore unacceptable on principle. These same methods can ignore that the meaning and value for the company lies in the result of the information analysis; that is the CI. In all events, this confusion represents a clear impediment to greater knowledge of CI and its role in companies. Here are some examples and economic data about these crimes.

Case 4: the German company Enercon GmbH was spied on at the order of a North American competitor.

The facts place this criminal act in March 1994. At that time its in-house technology of turbines with direct drive (without gears) and variable speed gave incomparable advantages in the maintenance of machines that gave it a differentiation strategy. Its product was sold at prices higher than its competitors. During this period, 1993-1994, the German manufacturer negotiated with New World Power Corp. (NWP) for its E-40 machine's export to the USA. What the Germans were unaware of was that its North American competitor, Kenetech, in violation of the law, obtained the intimate details of an E-40 and armed with them, directed a defensive battle against the planned exports declaring a breach of one of its patents before the federal body, the US Int. Trade Commission. The litigation lasted years and kept Enercon out of the US market.

Subsequent to these events Wobben and its American lawyers received – possibly accidentally – the evidence from the other party. In addition to a large number of photos that showed the complete interior of the E-40, there was also an eight-page report on the espionage by Ruth Heffernan. The report describes in detail the way in which she and her Dutch colleagues from the US competitor Kenetech, Jans-Robert "Bob" and Ubbo de Witt from Oldenburg, spied on the Enercon system. According to it "they left Groningen in the early hours of Monday 21st March 1994 with Bob". In Oldenburg they collected Ubbo, a physicist and meteorologist who had worked as a "freelancer" for Kenetech. He was in contact with a farmer who owned an Enercon-40 on his land and it was in use. The rest of the events are summarised as the nocturnal and criminal entry of those persons into this machine, the discovery of the facts, their statement and the scandal that in its day merited the condemnation of the European Parliament.

Source: adapted by the writer from the original by Schröm, Oliver in *Die Zeit* (1999).

Case 5: Convicted for stealing Motorola secrets including an unproved accusation of selling them to China.

Jin Hanjuan, a nationalised American citizen, was about to board a flight to Beijing on 28th February 2007 *when a random check stopped her short. In accordance with the judicial file and the sworn declaration of the FBI presented as a case of economic espionage against her, when the customs officers at O'Hare airport in Chicago inspected the bags of the 40-year-old software engineer they found over 1,000 confidential documents that were allegedly stolen from Motorola, the US electronics group, for which Ms Jin had worked until two days before the flight.*

The court documents said that the Chinese officials also discovered military manuals, catalogues of a European military products company, documents

that detailed Chinese military applications for electronic equipment, etc. that had been drawn up by an unidentified Chinese telecommunications company and 30,000 USD in cash[12]*. In the criminal case against Ms Jin, held in a Chicago court, Motorola alleged the research and development costs of the information in the accused's possession was more than 600 million USD. The company lost major global revenue when the contents were made public, it alleged. For her part Ms Jin pleaded not guilty.*

In another civil case brought by Motorola, Ms Jin was one of those accused along with Huawei, the Chinese telecommunications equipment manufacturer, through an allegation that her and the others were "secretly involved" in the development of products for the Chinese company at the time when she was employed by Motorola. Huawei said that the case presented by Motorola was "inadmissible" and denied to comment on the criminal case.

Source: extract translated from the Financial Times original, 1st February 2011.

The economic losses that these crimes represented were, as seen in these two cases, significant. The figures involved were very inconsistent according to sources. A report to the US Congress in 2002 included some estimates (Xerox White Paper, 2003). The writers of the report in the Financial Times (2011) confirmed a growing preoccupation with the appearance of these cases. Some of the most well-known recent cases involved Renault and its battery technology for electric cars or Google and its source code subject by cyber attacks. But cases were also presented in very different sectors, such as the accusation of espionage in 2009 by Starwood Hotels and Resorts against Worldwide Hilton, (Reuters 2012).

Among other protection measures, given these crimes, the work of the Financial Times in 2011 set out to reduce the possibility of leaks to a minimum, whether through methods prepared with the help of information technologies, or sometimes by starting from ideas that were due more to common sense. Another approach can be to abandon hope that all leaks can be avoided and concentrate on a continual innovation process regarding the most advanced technologies and products that are difficult to reproduce by any unconnected person due to their complexity and the use of original ideas.

In any case, this type of crime has led to some OECD countries to actively transfer advice on prevention and protection to their companies against

[12] Bloomberg subsequently added at the start of the judgement that her flight ticket to China was one way only, that the Chinese companies could be Kai Sun News Technology Co., also known as SunKaisens, and the Chinese army and iDEN the technology in question. On 29th August 2012 the judge, after examining the proven facts, condemned the accused to 4 years in prison for stealing secrets, but exonerated her from the crime of selling them to the Chinese http://www.huffingtonpost.com/2012/08/29/han-juan-jin-sentenced-for_n_1840304.html

espionage. This is the case in Canada, whose national research services on security are published on the Internet[13].

Implications for territories: territorial intelligence

The development of a territory depends on various factors and variables and the information and knowledge generated in it play an important role. It makes use of this knowledge and of this information, through coordination of the players that work and participate in the same region; this has come to be called *territorial intelligence* (TI). Although TI encompasses more aspects than information management, this is one of its cornerstones (Ortoll, Eva, 2012).

This term arose in France in the nineties and is used to name the function and the intelligence process carried out by public administrations on a local, regional or national scale. The goal is, through the use of information, to know about the territory and its resources, to create wealth and plan development policies and sustainability, (Bertacchini 2004). For Ferrari, T. (2007) TI consists of systematically approaching the development of a territory through the work of its players in a network aimed at its sustainable development.

This TI concept cannot be understood without starting from concepts such as strategic territorial planning, triple helix, territory capital, "clusters", districts or poles of economic specialisation due to competition, drive to innovation and CI. The Carayon Report, 2003, dedicated a large part to EI (economic intelligence) and the territory. The idea of "territorial intelligence" basically serves to promote innovation in the territory. In practice it is explained by the collection and analysis of information about the environment with a focus on competitive intelligence and confrontation of the viewpoint of local players to generate the most consistent policies to be applied.

For Ferrari, T. (2007) territorial intelligence is the domain of the methods and resources of economic intelligence at the service of the territories; its use is carried out with the goal of:

- Identifying projects and helping to put them into operation, creating employment, wealth and business in line with the strategy.
- Anticipating changes, risks and future evolutions, with regard to the prospective vision and safeguarding assets.
- Assessing the territory and its most attractive performance in terms of influence.
- Encouraging the territory's technological and economic development through networks.

[13] The addresses are: www.csis-scrs.gc.ca/nwsrm/wr/wr2-eng.asp and www.csis-scrs.gc.ca/nwsrm/wr/wr3-eng.asp

Development perspectives

The present and future CI is linked to the way in which it is capable of serving strategic decisions and integrating the decision maker. In many cases a lack of client focus has been demonstrated. This deficit in the attention that is paid to the client and its involvement in the CI process limit intelligence generation and the process becomes a mere supply of information and documentation and this leads to the marginalisation of the organisation.

This is why conversion of information into intelligence has become one of today's central CI issues. Wright, S. (2013) has recently worked on it by starting from a consideration of how to make use of an organisation's unique intangible assets: its explicit and implicit acquired and derived knowledge, and from a concept such as the traditional intelligence-based competitive advantage or "IBCA". For Gilad (2008) this was done through interpretation (or what many call analysis) of information. For me, the correct definition of intelligence must therefore be that of a viewpoint regarding the facts and in this regard must be clearly distinguished from information. This is why two currents are mentioned, the main one, the "reporting school", with emphasis on the collection and organisation of information and another that responds to its position, and the "analysis school" focused on generating intelligence.

Madureira (2013) put the emphasis on the CI proximity[14] or generation time. For him the CI competitive advantage does not come from access to the data, nor only from the quality of the analyses, but from the balance between speed and quality of the vision, which we call "flexible insight". This means being first to detect an opportunity or a threat and transform it into applicable perceptions and understanding that can lead to strategy and be put into practice to gain position in the market.

Professor Prescott, J.E. (1999) after analysing the evolution of CI spoke about a tendency towards it becoming a central ability for companies, its generalised integration into the training programmes of business school, with an emphasis on attributes such as qualitative and strategic abilities and its communication using direct components to the decision maker provided by CI, marketing or planning units. In the past decade, I have worked on the standardisation of a body of standardised contents that define the curricular contents for teaching CI.

If this is a more academic vision, interesting proposals also arise for the future of CI from business practice. For example, that made by the American Brenner, M. from the corporation Air Products and Chemicals, who saw the effectiveness of the CI specialists as facilitators or "coachers" of

[14] I owe this term to Marcelino Huerta, former manager of FAMOSA.

group decision-making sessions. This approach is supported by Fahey, L. (2009) when he showed how intelligence ultimately is not the result of intelligence professionals by themselves. It is co-created through interaction between intelligence professionals and decision makers. That is why he insisted: "the key result of intelligence is understanding "insight". This is all the game consists of: this "insight[15]" involves the decision makers.

Specifically in line with the creation of mechanisms that will involve participation together with CI specialists and decision makers and their staff, there appears a form of developing the technique of analysing scenarios that are known as the "war room". Specifically for its capacity to confront uncertainty in a timely way it has great potential in business.

Interesting integration experiences for librarianship professionals are arising from university libraries in the academic field, which are added temporarily to research groups to provide them with access to the analysis results.

This need to obtain results from the analysis together with an explosion of scientific, technological and market knowledge increasingly obliges the incorporation of software tools for mining technical scientific texts or 'Tech Mining' or of syntactic and semantic analysis in order to understand the emerging guidelines and their relationships.

Finally, standardisation is opening a path in this field through R&D+i. Therefore, the UNE 166.006:2011 standard in its latest revision has been opened up to CI. The studies in progress by the group of the European Standardisation Committee, CEN 389: on Strategic Intelligence Management point towards an international presence in the near future with a regulatory reference for companies in this field.

Dedicated to Antonio Rico Gil, economist and teacher, in memoriam (1947-2013).

Bibliography

Aenor, (2011), *Gestión de la I+D+i: Sistema de vigilancia tecnológica e inteligencia competitiva,* UNE 166.006:2011.

Aguilar, F.J. (1967), *Scanning the business environment*. New York, Macmillan Co.

Ansoff, I. (1975), "Managing strategic surprise by response to weak signals", *California Management Review*, 18(2) pp. 21-33.

Ansoff, I. (1984), *Implanting Strategic Management*, Prentice Hall International, New Jersey, 1984.

[15] Understanding, vision or perception of the facts and of their implications for the business.

Bertacchini, Y. (2004), "Le territoire, une entreprise d'intelligence collective à organiser vers la formation du capital formel", *Revue Communication & Organisation* No. 25, *Les vallées: sens, territoires & signes*, GREC/O, ISIC, Université de Bordeaux 3, 1st Semester 2004. Retrieved 2010.05.13 from http://isdm.univ-tln.fr.

Bernhardt, D. (1994), "Tailoring Competitive Intelligence to Executive Needs", *Long Range Planning*, Vol. 27, 1, 5-17, February 1994.

Blanco, S., Caron-Fasan, M. and Lesca, H. (2003), "Developing Capabilities to Create Collective Intelligence within Organizations", *Journal of Competitive Intelligence and Management,* SCIP, Vol. 1, No. 1, Spring 2003.

Blanco, S. and Lesca, H.(1998), *Business Intelligence: Integrating Knowledge into the Selection of Early Warning Signals*. Retrieved 17.11.2002 from http://www.veille-strategique.org/docs/1998-Blanco-Lesca-Articlewksp.pdf

Carayon, B.(2003), *Intelligence économique, compétitivité et cohésion sociale,* La Documentation française; Paris; p.176. Retrieved 14.06.2004 from http://www.ladocfrancaise.gouv.fr/brp/notices/034000484.shtml

Chardon, V. and Bauquis (2012), *Intelligence Économique,* Guide du Routard, Hachette.

Christensen, C. M. *et al.* (2004), *Seeings What's Next*. Harvard Business School Press.

Comai, A. and Tena, J. (2006), *Mapping and Anticipating the Competitive Landscape,* Emecom Ediciones, Barcelona.

Daft R.L., Sormunen, J. and Parks, D. (1988), "Chief executives scanning environmental characteristics and company performance: an empirical study", *Strategic Management Journal,* Vol. 9, pp. pp. 123-139.

Day, G. and Schoemaker, P.J.H. (2006), *Visión periférica*, Ediciones Deusto.

Equipo CNI (2010), "Aproximación a la inteligencia competitiva. Inteligencia y seguridad", *Revista de análisis y prospectiva,* Vol. 2010, 9, pp. 19-40.

Escorsa, P. and Maspons, R. (2001), *De la Vigilancia Tecnológica a la Inteligencia Competitiva,* Prentice Hall, Madrid.

Fahey, L. (2009), "The Future Directions of Competitive Intelligence: Some reflections", *Competitive Intelligence Magazine,* SCIP, Vol. 12, 1, pp. 17-22.

Ferrari, T. (2007), *Intelligence Territoriale,* ADIT, Documentation for the training course in CI for Madri+d.

Fleisher, Craig S. (2001), "An Introduction to the Management and Practice of Competitive Intelligence (CI)", Chap. 1 of the Monograph edited by the author and David Blenkhorn, *Managing Frontiers in Competitive Intelligence,* Quorum, Westport, CT.

Fleisher, Craig S. and Bensoussan, Babette (2002), *Strategic and Competitive Analysis: Methods and Techniques for Analyzing Business Competition,* Prentice Hall, p 457.

Fleisher, Craig S. and Blenkhorn, D. (2003), "What are the enduring Issues in Competitive Intelligence CI?", Chap. 1 of the Monograph edited by the authors *Controversies in Competitive Intelligence,* Praeger Publishers, Westport, CT.

Fleisher, Craig and Wright, Sheila, (2009), "Causes of Competitive Analysis Failure", pp. 36-50. *Proceedings III European CI Symposium*, ECIS, Stockholm. Sweden. Retrieved 23.01.2013 from http://www.bth.se/fou/forskinfo.nsf/all/d44c704148b7adbac12576e0003d87e8/$file/ECISproceedingsFinal3.ppppdf.pdf.

Financial Times (2011), "Industrial espionage: Data out of the door", 2011.02.01.

Gilad, Ben. (2008), "The Future of Competitive Intelligence: Contest for the Profession's Soul", *Competitive Intelligence Magazine*, 11(5), pp. 21-25.

Gilad, B. and Gilad, T. (1988), *The Business Intelligence System: A New Tool for Competitive Advantage,* Amacom Books, p. 242.

Halal, W.E. (1998), "Organizational Intelligence: What is it, and how can managers use it?", *Knowledge Management Review,* Vol. 1, March-April 1998. A copy is published in www.strategy-business.com/article/12644?gko=4a546.

Hamel, G. and Prahalad, C.K. (1994), *Competing for the Future,* Harvard Business School Press.

Harbulot, C. and Baumard, P. (1997), "Perspective Historique de l'intelligence économique", *Revue Intelligence économique,* École de guerre économique.

Herring, J. (1999), "Key Intelligence Topics: A Process to Identify and Define Intelligence Needs", *Competitive Intelligence Review*, Vol. 10(2) pp. 4–14.

Jaworski, B.J.; Macinnis, D. and KOHLI, A. (2002), "Generating Competitive Intelligence in Organizations", *Journal of Market-Focused Management*, 5, 279–307.

Juhari, A. and Stephens, D. (2006), "Tracing the Origins of Competitive Intelligence Throughout History", *Journal of Competitive Intelligence and Management,* Vol.3, 4, pp. 61-82.

Kahaner, L. (1996), *Competitive Intelligence: How to Gather, Analyze, and Use Information to Move Your Business to the Top*. Touchstone -Simon & Schuster. N. Y.

Lesca, H. and Lesca, N. (2011), *Les signaux faibles et la veille anticipative pour les décideurs,* Ed Lavoisier, Paris.

Madureira, L. (2013), *Social Market Intelligence. An Introduction to Future Ready CI*. SCIP insight e-bulletin. January 2013 | Vol. 5, 1.

Masson, JL. (2005), *Inteligencia Competitiva. Bases teóricas y revisión de literatura,* Univ. Autónoma Barcelona, Dpto. de economía de la empresa, Barcelona.

Mendonça, S.; Cardoso, G. and Caraça, J. (2007), *Some Notes on the Strategic Strength of Weak Signal Analysis,* LINI working papers No. 2, Retrieved 23.01.2013 from

http://www.lini-research.org/np4/?newsId=9&fileName=SMENDONCA_ETAL_LINI_WP2.pdf.

Michaeli, R. (2006), *Competitive Intelligence. Strategische Wettbewerbsvorteile erzielen durch systematische Konkurrenz-, Markt- und Technologieanalysen,* Springer Verlag, Berlin-Heidelberg. English translation since January 2013 (2012 Edition).

Ortoll, Eva (2012), "Inteligencia territorial: iniciativas y modelos", *Revista de los Estudios de Ciencias de la Información y de la Comunicación,* UOC, 9 March. Retrieved 20.02.2013 from http://www.uoc.edu/divulgacio/comein/es/numero09/articles/Article-Eva-Ortoll.html.

Palop, F. and Vicente, J.M. (1999), *Vigilancia Tecnológica e Inteligencia Competitiva: Su potencial para la empresa española,* Colección Estudios No. 15, Madrid: Fundación COTEC.

Palop Marro, F. and Martinez, J.F. (2012), *Guía metodológica de práctica de la Vigilancia Tecnológica e Inteligencia Competitiva*, ERICA.

Prescott, J.E. (1989), "Competitive Intelligence: Its Role and Function Within Organizations", pp. 1-14 in the Monograph edited by the author in *Advances in Competitive Intelligence*, Vienna, VA, Society of Competitive Intelligence Professionals.

Prescott, J.E. (1999), "The Evolution of Competitive Intelligence", *Journal of the APMP,* Spring, pp. 37-52.

Porter, M. (1980), *Competitive Strategy*. Free Press.

Martín, R.A. (2010), "Modelo normalizado de unidad de inteligencia competitiva y manual de operaciones: una propuesta. Inteligencia y seguridad", *Revista de análisis y prospectiva,* Vol. 2010, 9, pp. 67-93.

Martin, R (2013), *Strategy and the Uncertainty Excuse,* HBR Blog Network. 8 January 2008. Retrieved from http://blogs.hbr.org/.

Rouach, D. (1996), *La veille technologique et l'intelligence économique*, Paris, Presses universitaires de France.

Senge, Peter M. (1990), *The Fifth Discipline*, Doubleday/Currency.

Singh, A. and Beurschgens, A. (2006), "Benchmark Your CI Capabilities Using a Self-diagnosis Framework", *Competitive Intelligence Review*.

Schrom, O. (1999), "Verrat unter Freunden" © *DIE ZEIT,* Dossier. Retrieved 4.04.2006 from www.zeit.de/archiv/1999/40/199940.nsa_2_.xml?page=all.

Stoner, J.A.F. and WankeL, Ch. (1989), *Administración. Planeación y toma decisiones*, 3rd Edition, Mexico, Prentice-Hall, Hispanoamericana SA, 1989.

Volgestein, F. (2005), "Search and Destroy", *FORTUNE Magazine*, 2 March 2005.

Wilensky, H. (1967), *Organizational Intelligence: Knowledge and Policy in Government and Industry*, New York: Basic Books, p. 226 .

Wright, S. (2013), "Converting input to insight: organising for intelligence-based competitive advantage" in Wright, S. (ed.) *Competitive intelligence, analysis and strategy: creating organisational agility,* Abingdon: Routledge, pp. 1-35.

Xerox White Paper (2003), *Economic Espionage and Trade Secret Theft: Defending against the pickpockets of the new millennium.* XEROX CORPORATION, p. 10. Retrieved 2013.01.17 from http://www.xerox.com/downloads/wpaper/x/xgs_business_insight_economic_espionage.pdf.

Chapter V

The economic risks of cyberwar

Henning Wegener

Abstract

The increasing acceptance and introduction of digital technologies in military planning and armament opens the perspective of a cyber warfare that, given the global interdependence of net structures, would unavoidably and deeply affect the economy and vital societal assets. Hostile military use of these technologies could, for factual and legal reasons, not be cleanly separated from cyber conflict in general and raises serious questions of controllability and legitimacy, thus opening up highly disturbing damage perspectives. There is the perennial dilemma that the exponential growth and ultra-rapid development of cyber technologies and new sophisticated uses are in conflict with the equally exponential growth and sophistication of attack options. The amazing quantitative and qualitative growth of digital systems and infrastructures in *a second digital revolution* comes accompanied by an equal or even superior growth in attack options and thus in vulnerabilities. Yet, the benefits of the digital age accrue only if there is trust in the functioning, availability, integrity and safety of the underlying technologies; thus, cybersecurity has come to be a global challenge. The article describes actual and possible future cyber developments and the evolving threat landscape in terms of new attack modes, new perpetrators, and new dimensions of economic risk and loss.

The article argues that the deliberate military use of digital technologies in a cyberwar mode should be delegitimized or that at least its offensive

component be deemphasized, but that the best course for all stakeholders, including economic actors, would be to optimize strategies for the prevention and mitigation of cyber damage. The key concepts – for all forms of cyber conflict – are self-defense, resilience, security improvements in the IT industry, standard setting including standards for cloud safety, technical redundancies, restraint, national and international cooperation, emergency responses, effective information exchange and warning systems, increased efforts to harmonize cyber penal law and sanctions, advances in international law enforcement, and building international norms of behavior for the cyber age The article concludes emphasizing the need for a universal culture of cybersecurity, and offers an outline of a concept of cyber stability and "cyber peace".

Keywords

Cyberwar, cybersecurity, cyber conflict, cyber attack, cyber infrastructure, critical national infrastructures, new digital technologies, cyber law, threat landscape, resilience, culture of cybersecurity, cyber law, cyber stability, cyber peace

Cyberwar and Cyber Conflict: the Economic Dimension

An earlier volume of this series of *Cuadernos de Estrategia,* published in December of 2010, concentrated its analysis of cyber threats on the national security dimension[1]. The current essay will examine the consequences of cyber insecurity and cyber conflict for economic security and economic intelligence. As the underlying threat factors are the same or similar – and economic security is, after all, an essential ingredient of national security – the analysis will build on the earlier publication, which remains entirely timely and valid, although some more recent developments and figures have of course been incorporated.

Understood literally, our topic appears to focus on the economic damage that may be inflicted by the hostile use of cyber technologies in a *military* context, thus positing a direct relationship between economy and war.

Indeed, history has shown that war – traditionally conducted with kinetic weapons – has always spelled enormous risks and damage to the economic assets of a belligerent country: by its *indirec*t effects on infrastructure, consumption patterns, economic processes and client relationships, the general functioning of society, etc.; as *unintended,* collateral damage where the effect on strictly military targets spills over into society at large including essential infrastructures – or *directly*, as part of a deliberate strategy to destroy the economic grid of an enemy country, especially with regard to its armament industry or transport infrastructure, the "war economy", or beyond, to break the morale of the adversary and to undermine the will of its populations to fight and resist.

Modern war has increasingly engulfed societies as a whole. Its intended comprehensive destructive effect has certainly seen its climax in the Second World War, a "total" war, where the practically unlimited explosive power of weapon systems, including nuclear weapons, and the strategic will of the parties entailed the wholesale destruction of enemy territory, economic assets, cities and populations included, with new dimensions of violence and human suffering.

When we enter the digital realm, other laws govern. Digital attacks including those with a military purpose are primarily non-violent and relatively low-cost – "bits instead of bombs", exclusively by way of electronic invasion of systems and net structures. That also holds for military assets. ITCs, Information and Communication Technologies have revolutionized military affairs, including battlefield information and communication and weapons systems, but at the same time increased vulnerabilities to such invasions. A cyber attack comes from an invisible enemy, is hard

[1] *Ciberseguridad, Retos y Amenazas a la Seguridad Nacional en el Ciberespacio,* Ministerio de Defensa, Madrid

to track and trace, is asymmetric, difficult to assess in its amplitude and final effect, uncertain in the overall damage caused to assets beyond the accountable economic consequences. And while there will be less bloodshed and physical destruction, the consequences could yet be disastrous and touch profoundly on the economy.

Many definitions where authors venture to define cyberwar, describe it as politically motivated actions by a nation state to inflict upon an adversary damage of military relevance – damage to military computer networks, command-and-control systems, air defense networks and "network-centric" weapons systems by digital means[2]. More than 100 countries have reputedly established cyber commands and understand cyberspace as the fifth domain of warfare, just as critical to military operations as land, sea, air, and space. More than 30 countries are known to have developed explicit cyberwar doctrines; more than a hundred possess the technical prowess to develop offensive military capabilities. There is a general understanding that cyberwar is a real and portentous military warfare option that has to be taken very seriously, although scenarios and predictions as to its likelihood differ. One concern in this respect is the autonomous growth of cyber commands and cyber war doctrines that may follow traditional military thinking patterns as if afflicted by autism, oblivious of the interconnected cyber context. Thinking in terms of cyber*war* may lead one into a terminological trap. We will return to this worrying aspect.

However, a brief review and juxtaposition of the various available definitions of cyberwar quickly reveals that they clarify little, and that cyberwar remains an elusive concept at best. The naked minimum substratum is that we are dealing with digital attacks on systems and cyber infrastructures. Almost any further definitional criteria are open to doubt or ambivalence. Politically motivated attacks? If espionage, including espionage in armament industries and national infrastructures, is a prominent element in cyber war, as most of the definers claim, political and economic motives are naturally intertwined, and economic gain or data theft may well be the dominant motive[3]. Cyber terrorism (a concept to which this

[2] Wikipedia, *Cyberwar.* See also Glenny, Misha, *Das Ende der Nettigkeiten. Cyberkrieg und Sicherheit im Internet,* Internationale Politik, November/December 2012, p. 80

[3] Recent reports about cyber exploitation from China do not only demonstrate the huge and indeed alarming dimension of cyber espionage from that country, but also the great variety of perpetrators: big spying units that steal technological blueprints, negotiating strategies, corporate and government databases from the US in terabyte quantity appear to be part official, part contracted, part independent, and as these studies claim, at least linked with, if not coordinated by, a Chinese army unit. This opaque relationship shows a mix of actors and purposes that defies definition and renders the cyberwar notion ambivalent. See David E. Sanger, David Barboja, Nicole Perlroth, *Chinese Army Unit Is Seen as Tied to Hacking Against US,* New York Times, February 19, 2013, and the *Mandiant Report* cited therein and widely commented in other organs.

analysis will return) certainly has political motives, but does not pursue state-to-state war aims. Action by States and governments? Yes, attacks may be state-run, but the more likely and more effective scenario is that crime consortia, digital mercenaries as it were, are employed to inflict digital havoc at least as auxiliaries – unholy alliances between rogue States and organized crime as a provider of "crime as a service". "False flag attacks" could occur when states or non-state actors undertake a cyber attack in the disguise of another state; the resulting misperception could entail consequences that defy imagination, as generally misperception that follows from errors of attribution or wrong interpretation of an innocuous intrusion as a preparation of major attack could be fatal. Ambiguities abound. ¿Military targets? Indeed, should governments lead a determined attack on an enemy country, cyber commands may be spearheading the campaign, military assets will be at the center of any attack, and modern network-centric military systems are sure to be aimed at as preferential targets. Yet, what about comprehensive military and industrial espionage? Even a schematic outline of principal scenarios proves that the spectrum of targets is much wider, and that military planners already include by implication at least critical infrastructures and vital non-military communication systems in their target list, as most of these are dual purpose. All four of the scenarios most frequently mentioned in military-political analysis – the Estonia "cyberwar" in 2007 with its massive attacks on government and important infrastructures by distributed denial of service saturation, the combination of cyber attacks and kinetic means in the Georgia conflict in 2009, the persistent "low level" threat of military espionage, or the hypothetical "all out" cyberwar on defense assets, governments, the economy and infrastructures described in a somewhat sensationalist, but in the last analysis realistic way by Richard A. Clarke[4] – are multi-target, half military, half civilian attacks and show that cyberwar in its pure definitional form is very difficult to find; the heuristic value of the cyberwar concept is thus very limited, and an *integral assessment* of cyber conflict and cyber threats is by consequence unavoidable. It is exactly such an integral perspective that can demonstrate the tremendous destruction potential of a far-reaching cyber attack. This author is not given to dwelling on dramatic doomsday scenarios, but the extant literature on possible "digital Pearl Harbour" events can neither be disregarded nor trivialized[5].

The key factor that renders any definitional effort to characterize cyber war as a distinct category of hostile behavior so difficult lies in the digital

[4] Clarke, Richard A. and Knake, Robert K., *Cyberwar. The Next Threat to National Security and What To Do About It,* New York, 2010.

[5] Citable literature with plausible assumptions and calculations is hard to find, but it can be assumed that governments and security institutions dispose of substantiated threat assessments shielded from the public eye.

technology itself: the means of attack between civilian and military are identical, almost always dual-use, whatever the motives and targets. Any attack on the now all-pervasive net structures affects (all) digital participants in an unforeseeable and often uncontrollable way. One may regret the absence so far of a systematic investigation on the likely *cascade effects* of even a limited military cyber attack and its international repercussions, which is to say, a lack of estimates as to the basic risk of the use of cyber weapons[6]. Digital interdependence between various sectors of the economy is likely to create situations where failure in one sector not only creates damage in another, but various mutually reinforcing feedbacks. It is thus clear that the cascade effect of any attack on systems and net structures in a closely interconnected world may be enormous – and, as the assets of the attacker may also be endangered this may in the best case serve as an implicit deterrent[7]. Characteristically, all efforts to define cyber *weapons* have failed in the past, although some partial identification of dedicated attack malware has resulted.

The truth is thus that cyber attacks pose an even greater threat to society at large and its social and economic fabric than indicated in any variant of military doctrine, planning and forebodings. The growing dependence on digital technology puts public and private facilities, electricity supply, telecommunications, banking and finance, transportation, manufacturing, medical installations, education and government just as much at risk as military assets (more on these critical infrastructures further down). We must speak of an *integral risk exposure* of our countries and their economies. In this perspective, the differences between cyberwar, cyber terrorism and cybercrime become blurred, and it appears more adequate to speak of cyber attacks and cyber conflict when analyzing the broad threat pattern now emerging and impinging so clearly on the economy. In popular parlance, cyberwar has often been understood with this broad connotation, as a reflection of the unspecified, but massive fear cyber

[6] It is as yet an open question whether the often-cited Stuxnet virus, a very sophisticated malware, specifically geared to attacking the Siemens-produced dedicated control software (SCADA) of nuclear enrichment installations in Iran, breaks this cascade effect and can be the precursor of smart surgical cyber attacks. In any event, the Stuxnet attacks were not directed at a military installation, and did not emerge in the Internet, but were applied via smuggled flash memory sticks within a plant, thus posing a problem more of physical access control and insider misbehavior. See in this context, James P. Farewell and Rafal Rohozinski, *The New Reality of Cyber War,* Survival, August-September 2012, p.107

[7] The cascade effect may be less effective if data – for instance, military data – are managed in Intranets, or if other forms of net segmentation have been installed. Yet, the insulation is only relative, and network defense is always needed to combat the same invisible enemy. The same logic holds with respect to presumed plans of certain countries to opt out of the worldwide Internet structure, creating national digital borders in a "cybered Westphalian age". Such a national net segmentation will never be complete and finally ineffective.

conflict evokes among citizens. These public intuitions demonstrate that cybersecurity, or rather cyber insecurity, is among the great challenges of our time.

It is these broad threat patterns that most directly impinge upon the economy by way of an integrated threat perspective, and on which this essay will concentrate in keeping with the general theme of this book. A realistic economic risk analysis requires a comprehensive, integrated analysis of the entire spectrum of cyber risks, whether the primary purpose of a cyber attack is to reach economic gain or not, and an integrated strategy to combat cyber conflict. The vital contribution digital technologies make to our era and especially to economic security, depends on the functioning, integrity and reliability of these technologies, and of the confidence they inspire. Cybersecurity must thus be a central theme of this essay, as it was in the 2010 publication cited above.

We will, then, first explore the extent to which digital technology has already permeated all economically relevant segments of society. In a predictive mood, we will then analyze, even if somewhat speculatively, the likely growth and mutation of the digital world in years to come. The following chapter will focus on the vulnerabilities and exposure to risk this ever more interconnected world will generate, and the security threats thereto as they are shaping up. An attempt will then be made to measure the resulting economic damage, and the tenuous relationship between cyber attack and cyber defense, i.e. the state of the security industry. In the second part of the essay, the accent will be on counterstrategies, damage mitigation and prevention, exploring the full panoply of cyber defense. An important emphasis will be placed on the legal aspect, as there is as yet little provision made to effectively control the escalation of cyber conflict by norms, and as there is at best an incipient understanding of how the existing norms of international law would apply[8].

Cyber as the Agent of an Economic Paradigm Shift

Any realistic threat assessment requires an overview over the state-of-the-art digital technology employed by key economic actors. Information and Communication Technologies (ICT) increasingly become the new dominant paradigm of all aspects of human endeavour, providing the all-encompassing operative system of human societies. Cyber Technology has become a defining characteristic of our age. The well-nigh total dependence on ICT confers vital importance upon the performance robustness, security and reliability of digital systems and networks, con-

[8] Further down more detailed reference will be made to the "Tallinn Manual on the International Law Applicable to Cyber Warfare", Cambridge University Press 2013, the first comprehensive treatise on the subject

fidence in their functionality and integrity, and in the protection of privacy. These increasingly become framework conditions for the functioning of society. Information security thus needs to be ranked as an overarching societal challenge of global proportions.

The progress and growth of ICT which we currently observe in the economy and elsewhere, including in military affairs, is breathtaking and justifies designation as a *second digital revolution.*

As mentioned by different sources and studies, rapid advancements regarding the integration density and performance of very large-scale digital circuits which form the base technology in the digital age will be going on for at least another decade. Moore's law of doubling computer performance every 18 months continues to be valid. As these digital components are getting smaller and cheaper, more and more of these components like microprocessors, sensors and actuators are embedded in technical or physical systems and interconnected via various kinds of networks. According to a recent paper by Manfred Broy, currently about 98% of all microprocessors are embedded (and invisible), and are connected via sensors (e.g. RFIDs) and actuators with the physical world and with the internet. As Broy mentions, "... the physical world merges with the virtual world of cyberspace leading to Cyber-Physical Systems and to an Internet of Things, data, and services"[9].

With more than 2,3 bn computers on-line, billions of microprocessors and microcomputers thus employed in embedded systems, RFIDs and other sensors, mobile devices, evolving network technologies and bandwidth, ultra-miniaturization of digital circuits and the resulting ubiquity of new miniaturized computing elements, the steady progress towards an "Internet of Things" with miniature computers soon inserted in cloths or the frames of eyeglasses, the possible resulting threat spectrum goes infinitely beyond traditional computers and the current Internet. Basically, *all* digital devices and networks are vulnerable, and increasing interconnectivity of digital systems can easily result in "snowball"-like distribution of errors, faults and failures – or damage caused by cyber attacks. And these are ongoing processes. We are already witnessing an explosive growth of digital actors and an exponential growth curve of interconnectivities, an all-pervasiveness that automatically spells a parallel increase in vulnerabilities.

The phenomena of *migration* – migration of fixed line telephone to mobile systems and to VoIP, migration of computing processes, software management and data storage from individual and business computers to huge server farms (grid computing in the "cloud") with petabyte capac-

[9] "IT" – Information Technology, Special Issue, 6/2012, p. 255, Manfred Broy, Editorial, *Cyber Physical Systems (Part 1),* München 2012

ity (1PB = 10^{15} bytes) and cloud computing services – and *convergence* – resulting in an undistinguishable mesh of mobile and fixed systems – add up to a huge integrated global network structure with a universe of connectivity.

Counting traditional computers, mobile devices, embedded systems – omnipresent, but sophisticated microprocessors often miniaturized to the size of a sugar cube – some analysts estimate that the total number of interconnected systems, civilian and military, has already reached – or will soon be reaching – the level of 50 bn. The exponential propensity of their mutual connectivity potential – and thus also their vulnerability to cyber attack if not specifically protected – is difficult to calculate, but in any event a matter of evidence and concern.

The development of mobile devices is particularly noteworthy. Recent statistics indicate that worldwide smartphones trading alone will have reached more than 650 million units in 2012, bringing the worldwide mobile subscriber base to nearly 8.5 bn by 2016, an annual growth rate of more than 7%, with mobile penetration exceeding the point of 100% soon. The annual business figure of the mobile handset business stands at appr. US$250 bn[10]. This does not count in other mobile devices, nor the innovative potential of all smart mobile systems: such as smartphones, tablet computers etc. with mobile Internet connection. They are making computing ubiquitous.

In OECD countries and in emerging markets, nearly all companies are connected to the Internet, and an increasingly higher percentage of business sector value-added can be attributed to Internet-related activities; developing countries are catching up with increasing speed, often predominantly based on mobile techniques.

The production apparatus of our societies is already digitized to a large extent. Internet-connected machines that operate comprehensive autonomous machine-to-machine information exchange systems within factories, often interconnected through wireless protocols, so-called cyber-physical production systems, increasingly characterize today's – and tomorrow's – production processes and are the basis of the fourth industrial revolution, even though this development is as yet incipient. Net-connected and imbedded IT systems like RFID responders become the driver of innovation, replacing central production control and management by self-organization and fine-tuned process adjustments.

"Smart factories" go hand-in-hand with smart grids for essential public support functions. A rational energy economy has to move to smart grids, a production and consumption control and steering process predicated upon the functioning of millions of sensors. Smart systems are by no

[10] Figures from Portio Research Report Smartphone Futures 2012-2016

means the property of OECD countries: New Delhi has recently introduced smart grids for the energy management of the metropolis.

The *second digital revolution* manifests itself also in the unprecedented quantitative growth of data traffic. The new dimension of information storage, transfer and processing, and the availability of new ICT services is specifically enabled by the tremendous growth of data centers, "Big Data", colloquially referred to as the "cloud", which have become a prime driver of economic growth. The various and fast-growing "cloud" services (Infrastructure as a Service, IaaS, Software as a Service, SaaS, etc.) allow for the reduction of company hardware and software acquisition and maintenance, and offer flexibility, savings, and universal availability of company data from anywhere. The explosion of data production is indeed fomented by the cloud phenomenon. Cloud computing is the fastest growing segment of IT operations, with data in the cloud expected to grow sixfold over a five year span, and to produce, for the EU alone, almost €600 bn additional revenue, creating 2.5 mn new jobs in the process.

The Cyber World of Tomorrow

Before appreciating fully the threats and economic risks of cyber conflict, one must also appreciate, if in a summary manner, *evolving* cyber developments, although predicting is risky business by itself. Yet, the grand lines can be drawn, as they develop from current trends, provided a realistic accelerator is built in. It is safe to assume that miniaturization and the all-pervasiveness of devices – the Internet of things, based on the much more potent Internet Protocol IPv6 – will continue at an even faster pace, that the ubiquity and pervasiveness of invisible computing will grow, that data growth will accelerate and that new forms of computing leading to different and novel structures of processing configurations in digital nets, e.g. neural computing, will evolve. We will see the development of minute computers with self-organizing potential ("organic computing"), able to communicate autonomously with other digital devices, new human mind-machine communications (to name just some of the "next generation" computing trends[11]). These developments will generate a continuing explosive growth wave of digital devices, dwarfing the quantitative evolution we have seen so far. Computing power, especially through grid and cloud computing, becomes virtually unlimited. The incorporation of *smart* processing modes in industry will accelerate, and *smart grids*, today still in an experimental stage, will be a regular feature of the economic environment.

[11] A more complete list would look to the advancements of nanotechnology, material science, new semiconductor-based sensor technology, the formation and management of virtual systems, new architectural concepts etc.

Broadband availability and coverage, and bandwidth, will increase to a point of providing entire societies, including in the developing world, with effective and powerful on-line access, in many third world countries predominantly by mobile techniques[12]. We will see new very high speed fiber connections, and new high-speed wireless connections, two technologies that will shape the near future of connectivity. Mobile devices will become more sophisticated and versatile – serving as means of payment, replacing traditional keys and even chip cards, able to receive high resolution television anywhere.

Mobile technologies will be so efficient that they allow work at home with full access to company data as a normal feature, thus changing the work structure and enabling savings in infrastructure and travel. *Bring your own device (BYOD)*, a work form where the employee takes on his computing and data management tasks from anywhere, fully connected, already in use in some companies today, will become a routine procedure. Nothing will be as before.

Threat Development – the New Economic Reality of Cyber Insecurity

The foregoing analysis has placed emphasis on the exponential current and future growth of systems and actors, all interconnected, that make up the cyber world. And it is evident that the multiplication of systems and actors are the principal indicators of new opportunities to imperil cyber security on a grand scale, military and in a civilian context. Growth of objects, at this exponential rate, indicates growths of threats, equally exponential. One must bear in mind that *any* digital object, if not protected, can be an object of cyber attack, and if it is part of a connectivity mesh, this spells multiple infection potentials and profusion of damage.

The tremendous growth process simultaneously affecting cyber systems, actors and net structures has generated the famous quantity to quality jump. Rather than old-style crime merely going on-line, cyber attackers are today taking advantage of the increasing dependence of our day-to-day life on IT by developing creative strategies to exploit the vulnerabilities of IT systems.

The resulting change is nothing less than dramatic. The various dimensions of the threat surge have to be assessed in conjunction. The explosive growth of systems and interconnectivity – here already described – the growing intensity, sophistication and diversity of attack modes and attack technology, and the radical change in the characteristics of cyber conflict perpetrators, all interact and multiply the damage potential. With

[12] For current percentage figures see *OECD Internet Economy Outlook 2012*

the *second digital revolution* we enter a new world of perils which makes analyses of the cyber threat of, say, ten years ago, appear idyllic.

All operations in cyber conflict have in common that they intervene in the functioning of digital processes, whether they affect data, their storage, their handling, or their transmission, thus undermining the reliability and authenticity, integrity and privacy of data and processes.

But the aim of an attack can differ. Some leave the normal functioning of the systems and computing processes unaffected: their purpose is to observe and possibly to copy ("steal") data. The key applications are military and industrial espionage, data and personality theft. If the attack remains undiscovered for a length of time, it can be pursued, and even more data can be retrieved as they emerge; espionage and data theft operations aim at this long-term covert use. The usual term for these practices is *persistent threat*, or in case of an organized crime perpetrator and systematic use over time, *Advanced Persistent Threat (APT).*

Other attacks, using for instance "logic bombs", aim at altering or destroying the functions of the attacked system, falsifying its effect (e.g. the operating instructions of a weapons system) or making it inoperative. Still other attacks change the normal functions for abusive or illegal purposes for a given time, for instance in bank or credit card fraud, or more permanently by defacing the sites. The massive sending of *spam,* unsolicited bulk e-mail, frequently with commercial content, to an indiscriminate set of recipients, can also be termed an attack, as it is frequently used to dispatch viruses and other malware as a technique to enact financial theft, identity theft, data and intellectual property theft, fraud or simply deceptive marketing.

Evolving Attack Modes

The conflict modes which we will review subsequently, together with their development trends and evolving dimension, fall in one or several of these attack scenarios. As this essay does not purport to deal with their information-technological characteristics, the references to them will be general.

Topical information and figures are amply collected and made available by the globally operating cyber security companies Symantec, Norton, McAfee, Microsoft, KasperskyLabs, PandaLabs and CISCO, among others[13]. In addition, many national cyber security services like the German BSI, the US Homeland Security Department, and the European agency

[13] *Symantec Internet Security Threat Report, Norton Cybercrime Report, McAfee Threat Reports.* These reports are issued periodically, and 2011 and, in part, 2012 data and developments are already covered in their latest editions.

ENISA[14] collect and often publish data. While extremely revealing, such compilations still have to be read with a grain of caution. Commercial IT security companies, while certainly correct and conscientious with their information, tend to highlight the perils of attack in the interest of their business. And victims tend to underreport incidents – businesses too, like banks, in order to protect business confidence, individuals because of shyness or lack of interlocutors, national security services, especially when information networks relate to military secrets, weapons systems, or an essential security dispositive that has been penetrated.

But it is exactly the exploitation of espionage possibilities that have been displaying lately one of the highest growth factors. As they access the secure systems of target states, organizations and industries encounter increasingly lower barriers to entry, and the ubiquity of techniques used to undertake such collection, many of which have been developed by criminal groups, is evident – some States make an increasingly aggressive use of cyber espionage. There is detailed information on China's cyber operations in the US, where the intruders concentrate on key corporate infrastructures aiming at the theft of intellectual property[15]. For many years China has been practicing nuclear espionage, collecting highly classified information on long, documented lists of nuclear warheads, while also accessing networks of major defense and financial institutions. The most commonly used penetration technique is Trojan attacks, where a virus is introduced and can over long periods be instructed to download data without being perceived by the target system's operator. While China's cyber exploitation operations have received special publicity because of their extent and aggressiveness, all other great powers are also involved in intense espionage battles. At the moment, viruses with espionage functions enjoy a positive business cycle. Lately the spyware variants Madi and Flame have become particularly prominent[16]. Their appearance shows that even relatively simply constructed spyware can serve to obtain very valuable and sensitive information on a large scale.

From state-run espionage networks with a high Trojan penetration, it is only one step to the direct attack, degradation of weapons systems, and sabotage, e.g. through sleeping logic bombs, although these need to be

[14] ENISA's Reports, as recently the *ENISA Threat Landscape: Responding to the Evolving Threat Environment,* of January 2013, stand out because of their broad database, incorporating findings from most other reports, and because of the systematic and definitional analysis of the various types of threats and risks.

[15] Wikipedia, *Chinese Intelligence Operations in the US;* IISS Strategy Survey 2012, *Intelligence Agencies and the Cyber World,* p. 33. See also Nigel Inkster, *Chinese Intelligence in the Cyber Age,* Survival, February-March 2013, p. 45. See also fn. 3 above.

[16] The Duqu virus, often cited in the Flame context, also has excellent espionage and data theft properties, but is substantially more complex, possibly related in structure and origin to Stuxnet. Its primary target is also control software like SCADA. Duqu disappears from the affected systems after 36 days which complicates detection.

able to resist the vigilance and ongoing software upgrades of the soon-to-be attacked party.

All reports from security companies agree in their latest editions that malicious attacks continue to grow rapidly and, according to McAfee, have presently reached an all-time high in database breaches. At the same time there is growing sophistication of attacks and malware development. Mobile malware, a new central focus of attack, has almost doubled in a one-quarter period. With the number of vulnerabilities in the mobile space rising – Symantec has detected a 93% rise in one year – and malware authors creating specific malware geared to mobile opportunities, 2011 was the first year that mobile malware presented a tangible threat to businesses and consumers, not least because workers tend to bring their smartphones and tablets into the corporate environment faster than many organizations are able to secure and manage them. "BYOD" poses enormous new security challenges. It may lead to a further long-term increase in data breaches. The new threats to mobile are designed for activities including data collection, the sending of content, and user tracking.

There are quantitative jumps in all categories of attack mode. Symantec alone blocked more than 5.5 billion malicious attacks in 2011, an increase of 81 percent over the previous year. In addition, the number of unique malware variants increased to 403 million during that period.

Financial damage to banks and individual customers (credit card fraud, phishing and carding, spearphishing, direct financial extortion) continues to rise fast. Last year cybercriminals set up an automated transfer system (ATS) that was used to attack European financial institutions, and set out to target a major U.S. multinational financial institution. "Mobile Money Transfer", MMT, a catchword for novel digital financial systems, services that are bringing banking to millions of people in the Third World, will, if not quickly and effectively regulated, display the "dark side of cyber finance" and will become a playing field for cyber attack and crime[17].

Given the still persisting quasi-monoculture of operating systems where one producer dominates the market, the vulnerabilities inherent in its products are particularly widespread and, if exploited, lead to substantial damages. The main source for distributing computer viruses are therefore innocent users of personal computers and company computers, who often are not aware of the risks inside the web.

Virus attacks have also been greatly facilitated by the huge presence of "new social networks" that act as gratuitous distributors for infection.

[17] Bronk, Christopher; Monk, Cody and Villasenor, John, *The Dark Side of Cyber Finance,* Survival, April-May 2012, p. 129. A specific virus, Gauss, targets financial transactions; there are others.

Moving beyond spam attacks, cyber criminals are turning to these social networks. Their seemingly very innocent nature makes users incorrectly assume they are not at risk, and attackers are using these sites to target new victims. Due to social engineering techniques and the viral nature of social networks, it is much easier there for threats to spread from one person to the next. Yet spam, although now better controlled by anti-spam filters of the Internet Service Providers, and in addition in many countries subject to anti-spam legislation, is still rampant; more than 86% of Internet traffic – 62 bn messages globally per day – was spam in 2010, (with a slightly lower percentage of 75%, 42 bn messages, in 2011)[18], which by inundating the accounts causes appreciable damage in lost production time, apart from its potential to spread virus attacks.

There is another move away from indiscriminate spam: attackers individualize their attack, focusing on those victims on whom they have previously accumulated actionable knowledge through data and personality theft. One individualizing method is spearphishing. The term denotes a targeted email attack on persons who are known to frequent specific online businesses and may have relevant account information for banks, specific businesses or distribution chains. It is so called because the move to target is precise and narrow, like the tip of a spear. Although credit card data may not be stolen, email addresses are compromised, and these addresses can be sold on the black market. Furthermore, the information gathered from spearphishing can also beget more sophisticated phishing attacks on other customers acting upon the legitimate looking message from a retailer or bank with whom they are already doing business. Targeted attacks are increasingly directed at smaller companies, because they may be less well defended or occupy an important place in a given supply chain.

At the same time, malicious code is less and less programmed to directly cause irreparable damage. Rather, attackers try to bring infected computers under their control so that they can continue to misuse them by way of Trojan infection and remote control.

One important and effective element in such schemes are targeted DDoS (*Distributed Denial of Service*) attacks. In this attack method, the attacker floods the server with useless data packages, thus overloading the system in order to provoke business interruptions in the victim's systems and net structures. In a business context, such attacks could be launched by competitors, dissatisfied personnel, or otherwise motivated groups of people. Obstructing the smooth operation of web sites massively can re-

[18] Figures from Symantec. Spam may grow less rapidly also because there is increased pressure on spammers; some huge specialized spam botnets having been taken out over the last two years. By contrast, the content of criminal spam has become more sophisticated.

sult in considerable economic consequences, especially for companies practicing or relying on e-commerce. In military or political conflict scenarios, DDoS attacks – a central feature of the cyber attack on Estonia in 2007, where, however, economic damage was minor – can paralyze defense installations and communications, neutralize or destroy weapon systems, paralyze government services, provoke breakdowns in critical infrastructures and economic sectors, and may thereby, in extreme cases, lead to massive loss of life.

While the latest reports of the security companies clearly put their finger on the new threats to mobile devices – and through them to the whole interconnected universe – they do not yet quantify the new vulnerabilities that spring from the explosive growth of the cloud centers. Yet, apart from the mobile threat, the insecurity of massive migration of data to the cloud has for some time been a hot topic in security discussions, in the words of an ENISA report from 2009[19], "The massive concentrations of resources and data present a more attractive target to attackers", although the agency believes that "cloud-based defences can be more robust, scalable and cost-effective".

Underpinning this list of new attack modes is the emergence of a wide array of new highly sophisticated destructive software programs appearing with an ever increasing rapidity and sophistication[20] and targeting precision. National boundaries are of course no longer relevant to this type of threats, and it is impossible to confine the protection of information technology and IT infrastructure to domestic policies. The authors and vendors – and profiteers – of computer viruses and other malware are operating globally, and cyber defense has to adopt that same mode.

The New Enemy: Collective Actors of Cyber Conflict

Internet criminality is more and more conducted in a professional and commercial manner. Targeted attacks are increasingly carried out by organised criminals. Financial interests are the decisive driving power. Cyber conflict is developing into a powerful branch of the international organized crime scene. Crime consortia command armies of cyber experts and malware developers and systematically organize crime campaigns for gain. Over years of operation they have built professional teams for sophisticated malware development, benefitting from massive crime-generated resources. This also allows for a new magnitude of at-

[19] *Cloud computing: benefits, risks, and recommendations for information security,* November 2009, www.enisa.europa.eu

[20] One example is a new technology to segment malware into minute data packets that enter a target system, unrecognized by firewalls and anti-virus systems, but reassemble automatically once inside the host system

tacks. Already in 2004, sixteen percent of hacking activities were aimed at e-commerce companies. This represented a 400-percent-increase compared to the previous year, but since then the individual hacker has terminally faded into the dark, and organizations have taken over.

They systematically plant Trojans into large numbers of computers – increasingly also into mobile devices, and thus have thousands and even millions of devices at their command where they can activate malware and use it for attacks, *Botnets* – the word is composed of robot and net – are on the rise. These aggregates of *zombie computers* have several uses. Their operators – the *botherders* – can proceed to money-making directly, or collect espionage knowledge, commit data and identity theft. Botnets provide an effective and increasingly used infrastructure to distribute spying programs in a wide range of variants, and to do business in online banking. Botnets are the ideal platform for DDoS attacks, as these need a large number of activated email-emitters to reach the desired large-scale saturation effect. Botnets can also be rented out to other criminal perpetrators – or to governments, as digital mercenaries, creating an opaque state-non-state actor mix. They are not the only merchandise on the black market, accessible to criminals and governments alike; aggressive attack software, email addresses and credit card numbers in huge packages are available for almost token prices. There is no lack of *zombies* either. Almost every 10th email is estimated to be infected by relevant viruses, and, accordingly, the botherders can count on large herds, functioning unbeknownst to their owners. Already in 2010 McAfee had estimated that the number of *zombie* computers grow by at least 5 million systems per month, and that identified malware variants increase annually by a factor of 5. At the best time of the *Conficker* virus which was, and is, autonomously able to recruit new computers into the botnet, the dimension of that net alone may have reached more than 10 mn devices. Without the push of the new collective actors this growth would be inconceivable.

One alarming aspect of the new criminal cyber scene is the aforementioned technical and financial prowess to develop malware *ahead* of cyber defense and in spite of the undoubted efficiency of the international cyber security industry. At the same time, the digital dependency of modern societies is growing; infrastructures are ever more net-dependent (e.g. smart grids). Even the numerical aspect alone is worrying. McAfee's reports indicate that identified malware variants increase annually by a factor of 5. The timeless dilemma of attack vs. defense thus takes on a new meaning, especially due to these new collective operators in cyber space, and the defenders of a functioning, peaceful and crime-free cyber space do not always have the upper hand[21]. The attack potential of these

[21] "There is and always will be a permanent race in cyber space between attackers and defenders. Unfortunately, at the moment attackers are one step ahead." ENISA

organized evil forces also gives an idea of the possibilities of a true cyber war if states and organized crime cooperate.

There are several analyses with theories about the countries or places of residence of these crime groups, based in part on the URL of the attack messages. But given the unlimited possibilities of station-hopping and combining inputs from various sender countries, this essay refrains from any such attribution.

With all these developments it has certainly become clear that the term *security* has reached an entirely new meaning and dimension in cyber space; national boundaries provide less protection today than ever before. Such terms as internal and external security are increasingly difficult to define or might indeed merge in most cases.

Cyberterrorism can also be subsumed under the new collective threats. Under the dominant definition, cyber terrorism denotes the use of Internet attacks by political-ideological groups, aiming at large-scale disruption of systems and networks, potentially creating destruction, alarm and panic. If the purposes of these terrorists are not economic gain, they would not be genuinely within the purview of this study. If they go economic, for instance, to extort funds for the financing of terrorist activities, they are not essentially different from other criminal operators, and would only form part of the integral cyber conflict and threat landscape here described. That does by no means trivialize the dangers they pose, especially with attacks on critical infrastructures, and they are rightfully within the focus of governments in their anti-terrorism and general security campaigns[22].

Measuring the cost of cyber conflict: is quantifying possible?

Several international cybersecurity companies periodically undertake to put a price tag on overall economic damage caused by cyber conflict, based on their own activities and insight.

The Norton Cybercrime Report 2012 calculates the immediate financial loss to come to US$110 bn for 24 countries (Symantec arrives at 114 bn), with 556 mn victims; but if the money equivalent of lost time trying to respond to incidents and resolve cybercrime is added, the figure rises to roughly 390 bn. Whatever the exact methodology in arriving at these figures, it is certain that – apart from the limited number of countries

Threat Landscape, January 2013, cited above.

[22] See Candau Romero, Javier, *Estrategias Nacionales de Ciberseguridad. Ciberterrorismo.* In: Ciberseguridad, Retos y Amenazas a la Seguridad Nacional en el Ciberespacio, Instituto Español de Estudios Estratégicos, Cuadernos de Estrategia nº 149, Madrid 2010.

covered – the cost of long-term damage and business disruption, direct cash spent in incident response, and the damage to business reputation have not been fully factored in, and, for all countries, if included, should reach important additional proportions. And as pointed out before, any damage statistics have to cope with the huge number of unreported and unassessed attack cases[23].

Preventive and cyber defense measures do not appear to be covered either. Taking the US Government efforts at enhancing its cybersecurity capabilities (protecting critical infrastructures, cybersecurity operations, information sharing and analysis, etc.) as an example, the budget allotment of the Department for Homeland Security for these purposes alone amounts to US$1,2 bn for FY 2013[24], surely less than the private sector, all businesses told, has to invest in cybersecurity and cyber vigilance. Such amounts of funds have to be scaled up for the entire international community. The cybersecurity industry itself runs a multi-billion euro or dollar business.

Estimating the budgets for safeguarding military installations, communication systems and weapons will be even more difficult. But it is evident that the availability and maintenance of one's own military communications and command structures as well as the capacity to neutralize hostile military action – cyber defense – must enter, as they do, into calculation and planning.Given the uncertainties of calculation, it is thus not surprising that there are no handy overall figures. Yet, at the recent First World Summit on Cybersecurity organized by the East-West Institute in Dallas, Texas, in 2010, authoritative speakers have estimated the total economic damage of cyberinsecurity at appr. US$ 1 tn (1000 billion) annually, and this indicative figure has been used since without anybody seriously objecting. In the same order of magnitude, an authoritative speaker from the US House of Representatives has estimated the annual loss from cyber espionage – presumably from Chinese intruders – to have reached $300 bn in 2012, no breakdown of figures included[25]. At the World Economic Forum at Davos 2013 it has been assumed that over the next decade there is a 10% chance of a major digital breakdown – presumably of criminal origin – costing

[23] The European Commission through its Vice President Neelie Kroes is currently contemplating to establish a legal obligation for business to report cyber attacks. *News agencies*, 26 November 2012. The EU Commission is preparing a Directive in this sense. EU-wide, more than 40,000 enterprises would have to submit to the reporting obligation. The initiative has encountered resistance from industry and IT service providers. ENISA has estimated that 25% of attacks in the EU and the US are not reported to law enforcement authorities. For an initiative calling for voluntary industry reporting, see fn. 55 below.

[24] www.dhs.gov

[25] Article in El País and US press, February 21, 2013

over a quarter of a tn dollars[26]. These figures, and at least their order of magnitude, are enormous.

While the *first part* analyzed current and evolving cyber threats and their enormous economic cost, and emphasized that an integral risk situation required also a comprehensive and integral response, this *second part* will concentrate on combating cyber conflict, developing cyber defense strategies and devising strategies for the mitigation of consequences.

Limits on Cyberwarfare Proper

Although we have found the concept of cyberwar to be ambiguous and of doubtful relevance to the present analysis of economic risks, a brief summary of the constraints international law places on hostile cyber action appears in order, as they may limit the potential of damage.

International law and especially the law of armed conflict antedate the cyber age, but as cyber space is now increasingly recognized as a new theater of war, it is generally assumed that the *jus ad bellum* and the *jus in bello*, suitably adapted, also govern hostilities in cyberspace. There is much academic literature on the analogies that can and must be drawn from the UN Charter, the Hague, Geneva and ICRC Conventions and Additional Protocols and other treaties on Humanitarian Law, UN General Assembly resolutions announcing general principles for state conduct, extant international case law and customary International Law. Governments have published manuals and cyber strategies that also define constraints, but at the same time provide the underpinning for huge investments in cyber armament. Much of the debate centers on the definition of "attack" and "armed attack", but also cyber-suited definitions on the principles of the laws of armed conflict (necessity, distinction, proportionality, non-discrimination, prohibition of attack on civilian objects and certain persons, objects and activities, neutrality, etc.[27]

The views expressed range from the acceptance of broad options of attack, where targeting critical infrastructures is considered within the realm of legality[28], to more restrictive interpretations[29].

---

[26] Cited by Vice President Kroes at the Global Cyber Security Conference, Brussels, 30 January 2013

[27] For a summary of the issues, see Westby, Jody R. *A Call for Geo-Cyber Stability* in ITU (Hamadoun Touré and the Permanent Monitoring Panel on Information Security, World Federation of Scientists), *The Quest for Cyber Peace*, ITU, Geneva, 2011, p. 66. In the same publication, see Barletta, G.A., Barletta, W.A. and Tsygichk, V.N., *Cyber Conflict*, p. 53.

[28] For a cautious assessment, stressing the complexity of "line-drawing" in the use-of- force debate, see Waxman, Matthew C., *Cyber Attacks and the Use of Force: Back to the Future of Art. 2(4),* The Yale Journal of International Law, Vol 36 (2011), p. 421.

[29] In 1999 Amato, *Anthony* D,, *International Law, Cybernetics and Cyberspeace,* 76 Intern. Law Studies, p. 59, predicted that "attacks in the Internet will soon be seen as clearly

There is no point in belaboring these various perspectives, as the principal reference work is now quite clearly the recently published "Tallinn Manual on the International Law Applicable to Cyber Warfare"[30] elaborated by "The International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence". This comprehensive treatise seeks to establish 95 "Rules" covering the *jus ad bellum* and *jus in bello* for cyber conflict exhaustively.

The Manual has obvious merit. The prestigious assembly of co-authors proposes under the international regime *de lege lata* plausible definitions and rules and puts an end to many previous controversies. Yet, the members in dealing with the military-civilian relationship, and in trying to distinguish between military and civilian assets, and dealing with non-discrimination, etc. have to admit that cyber "weapons", "by their nature generate effects that are incapable of being controlled and therefore can spread uncontrollably into civilian and other protected computers and computer networks that create an uncontrollable chain of events" (p.122), and that most possible targets, especially critical infrastructures and cyber infrastructures, are dual-use, and that an attack on them creates more than the "collateral damage" to be assumed in kinetic conflict. Could a critical infrastructure of mixed military-civilian use also be targeted if it supports targets that are protected by the Geneva Conventions? The Manual seems to give preference to the military purposes. Rules such as "The civilian population as such, as well as individual civilians, shall not be the object of cyber attack" (Rule 32), thus they are likely to lose their protective effect. Rules 14 and 55, specifying that cyber operations in self-defense must be necessary and "proportionate" become blurred, if, because of lack of controllability, the proportion cannot be measured reliably. Other uncertainties concern the treatment of hidden non-state actors, combatant status, definition of "war-sustaining" economic objects, neutrality, anticipatory self-defense – when can a cyber attack that occurs with lightning speed be judged to be imminent? The authors are more successful in defining "attack" and "armed attack", employing the "effects" rule in the latter ("Whether a cyber operation constitutes an armed attack depends on its scale and effects", Rule 13)[31]. Yet even here

illegal in international law, and customary international law may already have reached that point", but clearly developments since then have not gone that way.

[30] See footnote 7 above.

[31] The Manual also makes clear that not all transfrontier cyber attacks, even though issuing from a state, constitute a violation of the law of armed conflict or international law generally. Thus cyber espionage, in "peace" or armed conflict, does not fall within the purview of international law (except in special cases, e.g. when disregarding the inviolability of diplomatic archives and communications). One of the important elements of cyber conflict, massive intrusion into digital systems for purposes of espionage, an Advanced Persistent Threat, is thus to be judged under *national* cyber laws and sanctions, such as the Budapest Convention defines.

the ambiguities are preoccupying. The "armed attack" rule is so broad that it lowers the barrier to war; it is unwise and dangerous for international stability to treat conflicts that imply no clear threats to human lives or essential societal disruption as "armed attack" with the accompanying consequences under international law[32].

On the whole, the Manual, far from constraining the cyberwarfare option, rather underlines the great new possibilities of cyber attacks and the uncontrolled damage it can inflict. Very little harnessing is done. Instead, the uncertainties and the risk to civilian cyber structures become more apparent. That refers specifically to Critical National Infrastructures which are not only predominantly privately owned, i.e. part of the national economies, but indirectly penetrate the whole social fabric so much that economies are ever more dependent on them. Cyber attacks on them not only generate massive economic damage, but also seriously compromise the security and safety of society, putting human life at peril.

More importantly, the Manual accepts the option of warfare in cyberspace in an unreflecting way and dodges the question of whether unbridled cyber armament in view of future use is a wise course for civilized nations to take. The Manual starts of course from the underlying assumption that state-sponsored cyber hostilities respect the UN Charter, and are only invoked in self-defense. Yet, the final impression is that the wholesale transfer of the traditional Law of Armed Conflict and the thinking in military terms does end up as a cloak of legitimacy for the cyberwars of the future, neglecting the huge dynamics both of digital developments, and the growing societal vulnerabilities and unpredictability of consequences.

A similar approach can also be detected in the military cyber manuals many governments have prepared, to the extent that they are publicly accessible.

Some countries are incorporating offensive cyber capabilities into conventional warfare strategy, foreseeing conventional military responses even to information sabotage on the Internet, even independent of the presence of an "armed attack" or human casualties. Others call for unlimited use of cyber weapons ("exploit potential fully, maximum effect, joint firing process, retaliation, punishing blow") indicating that planning also follows military lines ("war-fighting doctrine") with the corresponding analogies and thinking patterns[33]. Yet, concepts like deterrence, retaliation, "rules of engagement" do not take account of the specificity of cyber attacks and, for instance, the problems of attribution and proportionality.

[32] Barletta, Barletta, Tsygicho, op.cit. p.60

[33] A brief list of the various "warfare" modalities has been offered by ITU Secretary General Touré in *The international Response to Cyberwar, in* The Quest for Cyber peace, op. cit, p. 86

Fortunately, these concepts do not stand uncontradicted. The destruction potential and unpredictability of cyber attack options are increasingly recognized, and have nuanced the purely military viewpoint or are juxtaposed to it. In many military and political doctrine documents, cyberwar prevention, prioritization of cyber defense, and cooperation of all stakeholders are now moving to the foreground. One interesting example is the US Department of Defense Strategy of Operating in Cyberwar of July 2011 which clearly opts for cyber defense, close cooperation between Government agencies, Government and industry and international cooperation. NATO's summit documents, like the Declaration of Lisbon (20 November 2010), do not conceal defense needs, placing the emphasis, however, on central cyber protection and the optimization of collective cyber self-defense and internal alliance cooperation as well as international cooperation (§ 40). It is also significant that cyber attacks are not subsumed under the attack concept of Art. 5 of the NATO Treaty, but rather mentioned in the context of the consultation regime under Art. 4.[34]

This indicates that the mastering of cyber attacks is in many quarters healthily recognized as falling under a new security paradigm that places prevention, "resilience", strengthening of threatened digital infrastructures and a defense "network of partnerships" up front.

As this article will substantiate further down, this movement to a defensive mode should lead one to introduce the concept of *cyber peace*.

To opt for the positive side in the war-peace antinomy implies an important change in perspective and scale of priorities, as it orients the mind towards the benefits and positive potential of the Information Society and provides a goal post to that effect, reinforcing the negative connotation of cyberwar and related terms and calamities – delegitimizing it as it were – and fomenting dynamic movement towards a global culture of cyber security.

In attempting to reverse the above described belligerent perspectives, one must be fully aware that digital infrastructures are now all-pervasive, and will unavoidably also be used for hostile, non-peaceful purposes. The overriding objective, then, is to harness such uses and to provide the strictest possible limits for any attack situation. As the very term

[34] Another good example for this emerging instinct of prudence can be found in current reports on a draft US Presidential Directive embodying legal rules for the military in defending or retaliating against a major cyber attack, fully respecting International Law. The rules will reportedly endow the President with broad powers, including for a preemptive strike, but, given the consequences and the attribution problems, also reflect an attitude of substantial restraint, ruling out "automatic" retaliation, and reserving the prerogative of ordering strikes to the President as Commander-in-Chief. David E. Sanger, Tom Shanker, *Broad Powers Seen for Obama in Cyberstrikes,* New York Times: February 2, 2013. See also Jamie E Condliffe, *Obama Has Signed a Secret Directive to Stymie Cyber Attacks,* Washington Post, Nov. 15, 2012

"cyberwar" is conducive to stimulating thinking in military categories, an attempt must be made to combat this mental automatism and to substantiate a plea for peaceful behaviour in cyber space.

Active and Passive Cyber Defense

If an "armed attack" is carried out by a state – or if such attack is presumed – the victim, the attacked state, has, under the UN Charter, the right to proportionate self-defense. But if the attack inflicts damage on private interests, e.g. an enterprise or a privately owned infrastructure (energy, banking, aviation, etc. – for a more precise definition see fn. 42)? Can the attacked then slap back? And can he do so also if there is uncertainty as to attribution and the perpetrator is, or may be, a non-state actor or simply an ordinary cyber criminal? Here national cyber law with its penal sanctions and law enforcement tools comes into play. The debate as to whether "active" defense is legal, even though it implies intrusion into systems and networks and inflicts damage, has been waged for some time[35].

Active defense tactics such as have been proposed could include hacking back into systems to retrieve data, shutting down systems, sabotaging data, infecting the attacker with malware, taking over the attacker's botnet, or hiring a botnet to attack the attacker. Feeding an attacker data (so long as it is not malware) may not be illegal, but these other active defense actions likely are. Just because actions are being taken against a criminal attack does not make them legal in most jurisdictions. Moreover, these actions can trigger lots of other laws (particularly if botnets are involved), such as intellectual property, spam, fraud, contract and tort laws. Plus, they can cause collateral damage to third party systems[36].

Some of the justifications that are being suggested for active defense tactics include self defense, hot pursuit, and ownership of stolen data. However, none of these justifications hold water; self-justice will not do, and the right course to take instead is to make systems and nets more resilient, and to improve (passive) cyber defenses and national and international law enforcement[37].

[35] See article of Jody R. Westby on Forbes blog http://www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk/

[36] Examples taken from Westby, fn. above

[37] If attribution of origin of an economic attack is reasonably certain, some economic counter measures, like discontinuation of relationships, refusal to deliver, withdrawal of trade benefits, or – for a government – withholding of most favored nation status or other punitive trade measures, may be legitimate. Responding to the current surge of cyber attacks on US corporate assets and infrastructures, President Obama has recently spoken of such measures.

An Emerging Comprehensive Information Security Management System

After the foregoing excursion into the territory of cyber warfare with its ambiguities, deficits and scary implications, the discussion shall now once again focus on the overall threat panorama, with cyber conflict originating from states, non-state actors – or a combination of both – terrorist groups, organized crime consortia, and cyber criminals in general. Commensurate with the near total penetration of our societies by cyber technologies, one can now increasingly observe that international organizations, governments, the economy in general, the IT industry and IT security industry, as well as civil society, the entire *stakeholder community* as the accepted term goes, join forces to combat and mitigate threats in cyberspace. In a paper of limited length, this movement, in part concerted, in part autonomous, is impossible to cover. Thus, an attempt will only be made to list and evaluate its major forms of expression. The overriding key words are cyber defense, self-protection and resilience.

Resilience – the defensively oriented policy that maximizes the ability of possible target systems to prevent, deter and withstand cyber attacks and, if they occur, to minimize and mitigate their effects – is a multidimensional concept and has technical, organizational, political and legal components that need to be combined to be effective[38]. We will discuss in turn the legal framework requirements, the requirements of self-defense at enterprise and end-user level, the improvement of attack-resistant technical design, the potential of standard-setting and best practices, the benefit of redundancies and societal assistance and cooperation, international cooperation and law enforcement, the role of information exchange, warning systems and emergency responses, and, of crucial importance, the national and transfrontier protection of Critical Information Infrastructures.

Creating a harmonized legal framework to combat cyber crime and cyber conflict

Cyberspace could not remain a lawless space, and, with the advent of ICT legislators, has faced a double task: capturing the new technologies within their national legal system, and providing a harmonized international framework for penal prescriptions and sanctions and law enforcement, as

[38] The European Commission, a trailblazer in constructing digital strategies for the 27 members of the European Union, thus unifying their digital policies and defense, is using the "resilience" concept as an overriding finality, for instance by creating – through ENISA – a "European Public Private Partnership for Resilience" (EP3R), and placing its recent draft Cybersecurity Strategy of the EU in a major way under the plank "Achieving cyber resilience".

cyber attacks can take their origins in any part of the globe. Most industrialized countries have now cyber laws and cybercrime laws, many of them very adequate, but significant variances in defining what constitutes a cyber offense, in detecting and identifying cyber crime, and in the applicable procedural provisions have until recently significantly hindered cybercriminal investigation. The Council of Europe Convention of Cybercrime[39] (Budapest Convention, signed in 2001 and entered into force in 2004) has brought a major advance in the harmonization of global cybercrime laws, and I join Professor González Cussac in his praise of this instrument; I also agree with him that new digital developments and attack mode will make a revision of the text necessary over time, however valuable it is at this moment[40]. Yet, the Convention, as of this writing, has only been signed and ratified by 39 countries, with 10 ratifications pending. Significantly absent are Russia, China, as so often Israel, and most third world countries, presumably reticent to adopt a document of European origin. The ITU Toolkit for Cybercrime Legislation has been developed as an alternative, with proposed legislative language that is harmonized with the Convention and cybercrime laws in industrialized nations. Broader use of these texts, or adopting comparable autonomous language by countries not yet party to the Convention, will hopefully soon advance the harmonization process further. This is time-critical. The Convention, of course, has to be translated into national legislation by countries ratifying the international legal commitments..

Self-Protection

Cyber defense begins at home or at enterprise level. Among the obvious obligations of the Chief Information Officer should be the introduction of state-of-the art firewall, antivirus and incident information technology, encryption of confidential information, access control for premises and digital equipment, including a rigorous and differentiated password management ("need to know") and other sophisticated authentication techniques. If BYOD is permitted, rigorous controls should cover the brought-in equipment. Vigilance is especially required as regards the SCADA systems of critical infrastructure installations, as these are particularly vulnerable to state, non-state or terrorist attacks with a military or otherwise disruptive purpose. This should be obvious, but experience demonstrates that theft of confidential information, both in enterprises and governmental agencies, is predominantly due to negligent insiders. More than 9 out of 10 breaches would have been prevented if the organizations had followed data protection and information security best practices[41].

[39] www.conventions.coe.int

[40] *Estrategias legales frente a las ciberamenazas,* Cuadernos de Estrategia nº 149, op. cit., p. 116

[41] Figures from ENISA

One of three top causes of data breach is physical theft or loss of devices. Also, a report from German industry shows that only a small percentage of e-mails with highly sensitive information, like industrial design blueprints, are encrypted. There is a systematic lack of encryption on mobile company devices. In many cases, no provision is made for redundancies that could, in case of attack, conserve or rapidly re-establish functionality of systems or connections.

Designing for Security

One important loophole for attackers almost from the inception has been that hardware and software designers, focusing primarily on design benefits arising from technical advances for performance, have given less interest and effort to information security and privacy. Also, building in security from the outset may entail additional cost reducing profit margins. Traditionally, there has been a gap between the production and the security industries, helped by the lack of awareness of end-users of information security and privacy risks inherent in their equipment; for a long time, there has been incongruence between factual and perceived security. Many smaller enterprises may not have the resources or profession skills set to design the means of protection themselves. These gaps are now increasingly filled by a more security-conscious industry, higher end-user awareness, closer cooperation and even common ventures of the various stakeholders (see, for instance the recent acquisition of the important IT Security company McAfee by Intel).

Also it would be wrong not to give credit to major industry alliances formed to promote the security performance of hardware, software and net architecture, collective exercises that started mostly in the nineties of the last century. Most prominent is the Trusted Computing Group with more than 100 members, contributors or adopters from industry. Its Trusted Platform Module (TPM) has been standardized by ISO/IEC[42].

Yet, given the threat landscape, the obligation of the hardware and software industry to "design for security" remains permanent, and there is also a permanent responsibility for public and private institutions and for countries to establish security procurement and certification policies and standards[43]. Collective efforts to securize SCADA system design would

[42] www.trustedcomputinggroup.org. The TPM is used in the operating systems of most major providers. Trusted Computing does, however, face severe criticism from the free software community on the ground that it produces customer lock-in.

[43] The ITU in its Global Security Agenda is committed to the "Development of strategies for the creation of globally accepted minimum security criteria and accreditation schemes for hardware and software applications and systems". See also the chapter *Designing for Security* in *Information Security in the Context of the Digital Divide,* Recommendations submitted to the World Summit on the Information Society (November

appear particularly useful. All this is based on the insight that there is still a lack of design and analysis methods, scientifically proven, to master the enormous complexities of future interconnected digital systems, especially regarding safety, reliability, functioning and security. The IT security industry deserves high marks for keeping abreast, at a very professional level, of the challenges it increasingly has to confront; the security companies run a rapidly expanding and highly demanding and competitive multi-billion dollar business.

Standard-Setting and Best Practices

Government action and self-organization by industry have created a universe of technical and operational standards to secure IT structures. Many of these are voluntary, but a system of certifications provides incentives to adopt them with public visibility. Enterprises that do not vie for excellence in this area, and consequently suffer attacks and data breaches, not only lose money, but also reputation and clients. The most important standards for the management of IT technology, of practically global applicability, have been elaborated by ISO/IEL[44] in the series 27.000 and 13.335, for the aforementioned Trusted Platform Module in norms 11889-1 to 11889-4 on information technology (2009). In the USA the norm-setting function is entrusted to the American National Standards Institute ANSI. For years, the community of users, developers and vendors of Internet technology have joined in the Internet Engineering Task Force (associated with the Internet Society) to develop and promote standards for the Internet infrastructure, routing, transport security. Then, on the special problems of distributed computing, there is the Open Grid Forum for standard-setting in grid computing and grid architecture.

The International Information Systems Security Certification Consortium (ISC), described as "the world's largest IT security organization" ("security transcends technology"), promotes the standardization idea by awarding certificates for excellence in secure IT operations (Certified Information Security Professional, CISSP); the areas eligible for certificates also include software development, security architecture and design; 85,285 members from 143 countries currently hold the certificate. The issuers of certificates beyond the traditional norm-setting agencies – institutes, associations, individual enterprises, intergovernmental agencies – are many, obviously reflecting a need for recognition of excellence and con-

2005) by the Permanent Panel on Information Security of the World Federation of Scientists, Doc. WSIS-05/TUNIS/CONTR/01 at www.itu.int

[44] www.iso.org, www.iec.ch. The Spanish member organization of both is AENOR, which is also setting standards of its own (in this context see UNE 71502) and provides certification.

fidence-building. An indicative compilation on the Wikipedia web page of CISSP lists 70 different certifications[45].

Protection of Critical Infrastructures

CIIP, the protection of critical information infrastructures[46], has for many years been at the center of attention of information security policies and strategies to enhance resilience, both on the part of Governments and international bodies, and of the operators of these infrastructures themselves. Indeed, in a "cyberwar" context , it would be the centerpiece of defensive strategies and of any effort to optimize system resilience. Given their vital importance for the functioning of society, the increasing vulnerability of infrastructures in an interconnected and Internet-dependent environment, and the possible cascade effects of their failure, this priority is understandable. Critical infrastructures are first in the line of fire of military attack, terrorists, and crime consortia – organized crime – in the latter case as a basis for blackmail.

In the US, presidential directives since the time of President Clinton have ordered the necessary protective measures. Securing critical infrastructures and information systems is an essential part of the brief of the Department of Homeland Security, generously endowed in each annual budget. CIIP policies figure prominently on the DHS home page www.dhs.gov. Capping intense previous efforts, the US President on February 13, 2013 signed an *Executive Order (EO) on Improving Critical Infrastructure Cybersecurity* and *a Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience*, which provide instructive reading. Another major actor is the European Commission, assisted by its net security agency ENISA. Mindful of the still existing differences in systems and levels of protection in the 27 member countries, the EU has been working on CIIP and the harmonization of protection standards for some time. In 2009, the Commission adopted an Action Plan and a Communication on

[45] The *Revista Seguridad en Informática y Comunicaciones*, www.revistasic.com, an excellent publication, and certainly the best journal in Spain in the information security field, helps the non-professional reader to keep track of these various distinctions as they are earned by Spanish enterprises. The editor of this journal, SIC, also organizes periodic cybersecurity conferences in Spain.

[46] These infrastructures are generally understood to include, in the broadest sense, electricity generation, transmission and distribution, gas production, transport and distribution, oil and oil products production, transport and distribution, telecommunication, water supply (drinking water, waste water/sewage, stemming of surface water (e.g. dikes and sluices), agriculture, food production and distribution, heating (e.g. natural gas, fuel oil, public health (hospitals, ambulance transportation systems (fuel supply, railway network, airports, harbors, inland shipping); financial services (banking, clearing), security services (police, military). The energy component is often considered the most vulnerable part.

CIIP[47] and has organized a EU Ministerial Conference on CIIP[48]. The European Public- Private Partnership for Resilience has already been referred to. ENISA has been organizing several European Cybersecurity Exercises with broad government and private sector participation, the latest in 2012[49], aiming at strengthening the cyber incident management community. On February 7, 2013, the Commission published, in a Joint Communication with the other major EU bodies, the Cyber Strategy of the European Union which, in a broad sweep, intends to set common minimum requirements at the national level for each member of Network and Information Systems (NIS), touching very much on resilience and infrastructure protection[50]. The European Parliament is also active; it held its latest meeting on CIIP on February 6, 2013.

For more than a decade the International Telecommunication Union (ITU) has been dealing with Critical Infrastructures Protection in a global perspective, lately in reference to its Global Cybersecurity Agenda, although no uniform regulatory framework has as yet emerged. Yet there is a wealth of studies, publications and conference reports, easily to be found at the ITU web page and that of its executive arm, the International Multilateral Partnership Against Cyber Threats (IMPACT)[51]. The foregoing survey is no more than indicative; supplementing it with an overview over national initiatives would exceed the possibilities here. Yet many, if not most, countries participating in the cyber world deal with CIIP in their national organs, complementing international efforts. The German Federal Information Security Agency, for instance, runs a specialized Internet Platform for CIIP and sponsors a series of publications[52]

Resilience in Cloud Computing and Mobile Computing

The rapid advance of cloud computing in huge data centers, and the massive migration to mobile, as described in earlier sections of this article, make it useful to analyze the resistance to attack of both these new venues of data management and cyber operations, and to point to novelties in this respect.

Cloud computing is a new way of delivering computing resources, not a new technology. The concentration of data and services delivery, scalable to demand, offers huge economic benefits and accordingly has attracted

47 COM/2009/149, endorsed by the European Council in Resolution 2009/C 321/01. See also the Directive 2008/114/CE on the Protection of European Critical Infrastructures

48 www.tallinnciipeu.eu/?id=conference

49 For key findings, see www.enisa.europa.eu

50 JOIN (2013 1 final). The Strategy is accompanied by a draft directive on measures to ensure a high common level of cyber protection

51 www.itu.int; www.itu.int/ITU-D/cyb/cybersecurity/impact.html

52 www.bsi.bund.de, for the CIIP platform see www.kritis.bund.dE

massive global investment. The worldwide forecast for cloud services in 2013 indicates a likely volume of $44.2 bn. As ENISA has tangibly expressed it, the cloud's economies of scale and flexibility are both a friend and a foe from a security point of view. The massive concentrations of resources and data present a more attractive target to attackers, but cloud-based defenses can be more robust, scalable and cost-effective. Attacks on data centers of this dimension offer a military or terrorist attack important new opportunities, including tampering with the energy supply entailing massive loss of data (if energy supply redundancies are overcome), physical destruction, or cyber intrusion into the data bases. Clients' fears are heightened as data masses are moving seemingly arbitrarily and untraceably from rack to rack, as supervisory personnel becomes anonymous, and as confidence in the integrity and privacy of the data becomes harder to maintain. The risks in cloud computing are major, and provide a major security challenge.

It is thus not surprising that cloud security has become a central theme of the current cybersecurity debate. In the very competitive cloud market, suppliers and security companies outdo one another in confidence-building. They can indeed show that there is also a premium in cloud security management. All kinds of security measures are cheaper when implemented on a larger scale; the same amount of investment in security buys better protection (cheaper physical perimeterisation and access control, better scaling of resources, timeliness of response, more effective threat management, etc.). Clients – governments among them – make their economic choices in good measure on the resilience of security services offered, reputation of confidentiality, and transparency of the internal center procedures. Lately, one important differentiating factor for European enterprises has been that they judge the legal data protection in Europe better than in the US, given the more intrusive data policy of the Department for Homeland Security.

Cloud security currently appears to be everybody's business. The references of this article to current analytical work and recommendations on the subject are therefore limited to ENISA's recent studies, "Cloud Computing: benefits, risks and recommendations for information security" – mentioned before – and "Critical Cloud Computing: A CIIP perspective on cloud computing" (14 February 2013), both at www.enisa.europa.eu.

Further up, figures have been cited on the breath-taking growth of the number of mobile digital devices, mobile services and applications, and the consequences of the migration to mobile technologies. It had also been pointed out that the threat to mobile computing and communication is growing out of proportion, making cyber attacks to mobile one of the dominant features of the threat landscape. Although exceedingly vulnerable to cyber attacks, mobile systems have long gone virtually unprotected. Only at this juncture, new anti-attack software for most mobile

operative systems appears on the market. But the future may well lie not in software downloads to individual devices, but in central vigilance of mobile customers from the cloud, such as an alliance between Vodafone and BAE Systems that is presently being introduced into the market via a 5 year strategic partnership[53]. The promise of this cloud vigilance approach is that not only smartphones, but also tablets, and eventually smart RFIDs, the controlling systems in smart factories and other cyber-physical systems could be effectively protected.

National and International Cooperation in Cybersecurity

Given the seamless and global nature of the digital net structures, broad national and international cooperation of the entire stakeholder community in combating and mitigating the consequences of cyber conflict is a matter of indubitable necessity – and this necessity is globally recognized. The cooperation patterns that in part already exist, and need to be enhanced, include effective information exchanges including incident reporting, mutual assistance, also to activate redundancies, organized incident responses, warning systems, contact points within and between nations, improved cooperation on law enforcement – and the organizational prerequisites to make all these desiderata function.

These measures – and other, related ones – appear quite straightforward and their usefulness within a strategy of preventing, defending against, sanctioning and mitigating incidents of cyber conflict is fairly self-evident. It is thus not surprising that the categories and numbers of stakeholders involved in them are huge and multifarious. We are dealing here with ongoing and expanding processes, very hard to capture in a brief analysis. Suffice it to mention a few recent developments to indicate tendencies.

Entrusted by the World Summit on the Information Society with coordinating cyber security responses, the ITU has worked out a Global Cybersecurity Agenda that promotes many of the cooperation tasks globally, culminating in "a framework of a global multi-stakeholder strategy for international cooperation, dialogue and cooperation". The Agenda has dynamically pursued its goals, as can be gathered from the ITU web pages.

One important element of cooperation strategy is time-critical information across borders. The key mechanisms is the "24/7" approach, the permanent availability of contact points for cyber incident management. The first international plan originated with the G8 in 1998. The group created a 24-hour network of law enforcement experts among its members, but other governments joined. In the EU, the first 24/7 program came with the Council Framework Decision on attacks against information systems

[53] *BAE and Vodafone in cyber safety deal,* Financial Times, and news services, 18 February, 2013

of 2003. A more systematic approach is part of the (Budapest) Convention on Cyber Crime, which, apart from harmonizing criminal substantive law of cybercrime, has provided for domestic criminal procedural law powers necessary to investigate and prosecute such offenses, but has also set up a fast and effective regime of international cooperation and mutual assistance (art. 23 et.seq. of the Convention) for "tracking and tracing" that includes rules on the expedited preservation of stored computer and traffic data, etc. In art. 35 a permanent 24/7 network with appropriate equipment and trained personnel is set up in order to ensure the availability of immediate assistance for purposes of investigation and prosecution, including the collection of evidence and the locating of suspects. Many governments, even beyond existing treaty obligations, participate in the 24/7 set-up.

An element of growing importance in the incident reporting, mutual assistance, early warning, risk information etc. area are the Computer Emergency Response Teams (CERT), also labelled Computer Security Incident Response Teams (CSIRT). Pioneered by Carnegie Mellon University with funding from the US Department of Defense in 1988, the CERT is now a network of global dimension. In many countries there is a central government CERT, mostly charged with the coordination of other national CERTs and specifically with securing government digital infrastructures.

CERTs are teams of IT experts that follow and process information on computer incidents, analyze, advise, coordinate, lend assistance in combatting cyber attacks and in restitution, and often issue news bulletins and warnings on new threats. Worldwide there are presently more than 250 organizations that use this name and deal with cybersecurity responses. In many countries industry and academic institutes have taken the initiative to establish CERTs. In the US, the Department of Homeland Security has established the US CERT. It coordinates CERT/CC, the in part federally funded US CERT community led by Carnegie Mellon. In Germany, a similar task is fulfilled by the BSI with its CERT-Bund, in Spain with the Centro de Respuesta a Incidentes de Seguridad TIC by INTECO, an organ of the Ministry of Industry and its executive office red.es. The ITU, as part of its Global Cybersecurity Agenda, assists developing countries in creating national CERTs. In September 2012, the EU set up a CERT-EU, at first for the protection of its own entities, but also to liaise with national and government CERTs in the EU area. At the same time, in its Digital Agenda for Europe of 2010 the EU called on members to establish their own national CERTs, a development to be completed by 2012, thus paving the way for an EU-wide network of effective incident responses.

In a related move, the EU has, in February of 2013, created a European Cyber Crime Centre (EC3) at EUROPOL that is to focus specifically on organized groups aiming at large criminal profits, and their hostile impact on infrastructures with enhanced investigative powers.

In the future it is necessary that the CERT movement be universalized, and that CERTs become more operative and interconnected, but they certainly form a major defensive weapon against cyber attack and to harness cyber conflict[54].

At the time of this writing, one does not only observe a surge of cyber attacks on governments and industry, mostly in the APT vein, but also a growing awareness that all stakeholders must become more active and forthcoming in information exchange and sharing of cyber defense resources. One prominent example of such broad industry self-help endeavors is the collective cybersecurity alliance pioneered in Europe by René Obermann, the CEO of Deutsche Telekom, who has called for more voluntary incident reporting and transparency[55]

A Culture of Cybersecurity: Norms of Behavior for the Cyber Age

So far, only *some* broad legal aspects have been dwelt upon: International Law as it ambiguously defines the limits to cyber warfare and "armed attack", and the harmonization of criminal cyber law in its national and crossfrontier dimension. Not mentioned, but valid in most countries, is, of course, a civil law regime that governs torts and damages, as well as the pertinent International Private Law.

But all that is far from filling the requirements of a functioning cyberspace regime able to combat and withstand cyber conflict. Legally speaking, the new area of cyberspace was initially a void, in need of a comprehensive framework of norms not only for states, but for all stakeholders. The task was to develop over time a set of norms for convivial behavior – of a culture of cyberspace and cybersecurity, including a comprehensive legal framework to manage and control the all-pervasive, infinite potential of digital technologies. Consequently, there is as yet little or no ability to effectively control by law the escalation of cyber conflict and to guarantee the peaceful use of cyberspace – and as we have seen no unambiguous understanding of how the existing norms of international law would apply. A dangerous, precarious state of affairs indeed. The cybersecurity group within which I have been active, the World Federation of Scientists, has early on ambitiously called for a UN-led effort to create a universal and comprehensive Law of

[54] CERTs since 1990 are coordinating and exchanging information in an informal international organization FIRST; there is room for more effective coordination. Already in 2004 this author has recommend that the CERT approach should not only be universal, but should, beyond individual information processing and assistance, develop a systematic lessons-learnt approach, see Henning Wegener, *Learning Lessons from Cyber Attacks: Broadening the CERT Framework*, at www.unibw.de/infosecur

[55] See, for instance, Obermann, René, *Uniting for Cyberdefense,* New York Times op.ed. page, February 21, 2013

Cyberspace[56]. Yet, for many reasons a one-shot cyber treaty has not proved to be a realistic option. Fortunately, collective thinking about the necessary processes of cyber strategy has notably evolved. To make a long story short, a new age of cyber diplomacy has begun around 2008 with a manifestly emerging international consensus to concentrate efforts on an alternative to formal treaty-making: the elaboration of confidence-building measures or codes of conduct as normative tools. We may be witnessing a turning point in cybersecurity diplomacy.

The prevailing view now is that CBMs and codes of conduct open a window of opportunity to make real progress towards common definitions and behavioral standards. CBMs have the potential to reduce threat, enhance transparency, make State behavior predictable, are flexible, voluntary, and offer a variable geometry in terms of participants – it is possible to include non-State actors – and follow-up: contrary to coherent treaty-making, participants are free to adopt partial solutions and enact them without delay and independently or with other like-minded stake-holders. CBMs which States embrace do not require ratification; they invite emulation, and are at most – and at best – politically binding. They are thus uniquely suited to foment international consensus-building on an evolutionary scale. A well negotiated package of CBMs with a critical mass of participants may set in motion a process of further incremental change and heightened sensitivity. Clarification of behavioral standards may provide an incentive for going for more.

There are currently many parallel international activities that jointly contribute to consensus-building. Suffice it to cite some. A UN Group of Experts has been instituted in 2011 with the concrete mandate to define "cooperative measures ... including norms, rules of principles of responsible behaviour of States and confidence-building measures with regard to information space"[57] and will report out in 2013. Governments have provided numerous inputs to the Group at the request of the UN Secretary General[58]. Their views have strongly supported the idea of identifying CBMs. In a short time, flurries of other national statements to the same effect have surfaced: from Australia, the UK, Germany, at least by implication

[56] *Toward a Universal Order of Cyber Space: Managing the Threat from Cybercrime to Cyberwar,* Document WSIS-03/GENEVA/CONTR/6-E,, www.itu.int/dms_pub/itu-s/md/.../S03-WSIS-C-0006!!PDF-E.pdf,, also at www.unibw.de/infosecur. See also Kamal, Ahmad, *The Law of Cyber Space: An Invitation to the Table of Negotiations,* UNITAR, Geneva 2005, www.in.int/kamal/the_law_of_cyber_space. At the United Nations, Russia has, as of 1998, in a series of resolutions advocated a Cyber Treaty, proposing to some extent conflictive and probable unimplementable contents, see Res. A/53/70 up to A/65/41. These resolutions had, however, the undoubted merit of keeping the argument alive that a major universal normative effort was required.

[57] A/Res/66/24 of 13 December 2011

[58] A/66/152 and A/66/152 Add.1

the US, among others[59]. An authoritative academic voice from India has joined the concert[60]. China, Russia, Tajikistan and Uzbekistan, reflecting work within the Shanghai Cooperation Council, submitted to the UN Secretary General, in September 2011, a draft international code of conduct for information security[61]. Although the document, by virtue of its choice of authors, did not seem to display a sufficient flavor of political correctness, the catalogue of commitments, offered for voluntary subscription by states, should not be disdained. In the meantime, member countries have organized prestigious international conferences, where the CBM idea has been ventilated, and more or less detailed catalogues of CBM contents or contributions to it have figured in the conference summaries (London, Berlin, Beijing, Vienna, Budapest). Apart from the ongoing UN exercise, regional organizations are also getting into the act. The ASEAN Regional Forum with its representative membership and participants, 27 nations going much beyond Asia, has zoomed in fully on the CBM theme[62]. The OSCE, mindful of its earlier experience with East-West CBMs, is intensively working on a draft code of conduct (see "A Comprehensive Approach to Cyber Security")[63] and APEC[64], as well as the Shanghai Cooperation Organization[65] are also working on regional arrangements. The Council of Europe, famous for its contribution to a world penal law on cyber crime through the Convention on Cybercrime, has adopted 10 Principles on Internet Governance[66]. UNIDIR helps to provide the academic underpinning

[59] See previous footnote and the positive utterances at the cyber session of the Shangri-La Dialogue, IISS news July 2012. For Germany, see also "Challenges in Cyber Security: Risks, Strategies and Conference Building, Conference Report, December 13 and 14, 2011, Berlin, http://www.auswaertiges-amt.de/DE/Aussenpolitik/Friedenspolitik/Abruestung/Projekte/ Cybersicherheit.html. The German Federal Foreign Office, in addition, supports a 2012 UNIDIR project on International Cybersecurity and CBMs

[60] Gupta, Arvind, CBMs in Cyber Space: What Should Be India's Approach?, IDSA, Institute for Defence Studies and Analysis, June 27, 2012

[61] A/66/359. See also the Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, signed in Yekaterinburg on 15 June 2009

[62] Secretary of State Clinton at the Pnom Penh ASEAN meeting on July 12, 2012, "This Forum includes some of the world's largest cyber actors. So this is an appropriate setting for a sustained, meaningful dialogue on cyberspace issues. In the years ahead, we should work together in support of responsible norms and standards, and pursue practical measures to build confidence and reduce risk". The ARF is organizing a Seminar on Confidence-Building Measures in Cyberspace in Seoul next September. In May of this year ASEAN defense ministers called for an ASEAN "master plan of security connectivity".

[63] www.osce.org

[64] See the APEC TEL Strategic Action Plan 2010-2015, www.apec.org

[65] No home page in English of the SCO could be detected. News is best gathered from the web pages of the member countries.

[66] www..coe.int

for these endeavors[67]. ONGs in the cyber area, as well as individual researchers, offer catalogues of rules of conduct of their own. These catalogues can obviously not be reproduced or analyzed here but provide effective tools for spurring the debate and facilitating CBM negotiations[68]. It is to be hoped that the present dynamics in moving to negotiations on such confidence-building measures and codes of conduct be maintained, and that agreement on an appropriate negotiating venue is reached soon.

In order to provide the reader with at least some ideas of content on the current normative endeavors, a brief reference to a short list published by the ITU Secretary General is included:

1. Every government should commit itself to giving its people access to communications.
2. Every government will commit itself to protecting its people in cyberspace.
3. Every country will commit itself not to harbor terrorists/criminals in its own territories.
4. Every country should commit itself not to be the first to launch a cyber attack on other countries.
5. Every country must commit itself to collaborate with each other within an international framework of co-operation to ensure that there is peace

For the ITU this concise list constitutes the essence of cyber stability and an important part of cyber peace. In the same direction goes the *Erice Declaration on Principles for Cyber Stability and Cyber Peace*, (2009) emanating from the World Federation of Scientists, whose list of tenets culminates in the plea "to avoid the use of cyberspace for conflict". Cyberwar can be avoided, and it should not be considered a legitimate instrument of military conflict. That would go a long way to alleviating the ambivalence of cyber technology, and would sensibly reduce economic preoccupations and economic risks. Cyber peace is the better choice[69].

[67] UNIDIR, www.unidir.org, organizes conferences and participates in others. Particularly relevant the 2012 conference on *The role of Confidence-Building Measures in Assuring Cyber Stability.*

[68] For a tentative listing of principles to be embodied in a global code of conduct, see Henning Wegener, *La 'ciberguerra' se puede evitar,* Política Exterior, Madrid, No. 146, March/April 2012, p140; from the same author, *Die Diplomatie des Cyber-Friedens, 2011* at www.unibw.de/infosecur, and also *Regulating Cyber Behavior: Some Initial Reflections on Codes of Conduct and Confidence-Building Measures,* August 2012, The Science and Culture Series, World Scientific, Singapore 2013 (in press).

[69] See also Henning Wegener, *A Concept of Cyber Peace* in *The Quest for Cyber Peace,* op. cit., 2011. In the same publication, the Erice Declaration is also reprinted.

Composition of the working group

Coordinator:	**Mr. Eduardo Olier Arenas** *President of the Institute Choiseul Spain* *Director of the Department of Geoeconomics at San Pablo CEU University*
Member Secretary:	**Ms. María José Caro Bejarano** *Analyst at the Spanish Institute of Strategic Studies*
Members:	**Mr. Antonio M. Díaz Fernández** *Professor of Political Science and Administration Faculty of Law, University of Cadiz*
	Mr. Christian Harbulot *Director of l'École de Guerre Économique in Paris.* *Associate Director of Spin Partners*
	Mr. José L. González Cussac *Professor of Criminal Law, Faculty of Law,* *University of Valencia*
	Mr. Fernando Palop Marro *Co-Founder of Triz XXI.* *Associate Professor at the Politécnica University of Valencia.*
	Mr. Henning Wegener *Former Ambassador of Germany in Spain.* *President of the Permanent Observatory for Cybersecurity of the World Federation of Scientists*

Strategic Dossier

01 La industria alimentaria civil como administradora de las FAS y su capacidad de defensa estratégica

02 La ingeniería militar de España ante el reto de la investigación y el desarrollo en la defensa nacional

03 La industria española de interés para la defensa ante la entrada en vigor del Acta Única

04 Túnez: su realidad y su influencia en el entorno internacional

05 La Unión Europea Occidental (UEO) (1955-1988)

06 Estrategia regional en el Mediterráneo Occidental

07 Los transportes en la raya de Portugal

08 Estado actual y evaluación económica del triángulo España-Portugal-Marruecos

09 Perestroika y nacionalismos periféricos en la Unión Soviética

10 El escenario espacial en la batalla del año 2000 (I)

11 La gestión de los programas de tecnologías avanzadas

12 El escenario espacial en la batalla del año 2000 (II)

13 Cobertura de la demanda tecnológica derivada de las necesidades de la defensa nacional

14 Ideas y tendencias en la economía internacional y española

15 Identidad y solidaridad nacional
16 Implicaciones económicas del Acta Única 1992
17 Investigación de fenómenos belígenos: método analítico factorial
18 Las telecomunicaciones en Europa, en la década de los años 90
19 La profesión militar desde la perspectiva social y ética
20 El equilibrio de fuerzas en el espacio sur europeo y mediterráneo
21 Efectos económicos de la unificación alemana y sus implicaciones estratégicas
22 La política española de armamento ante la nueva situación internacional
23 Estrategia finisecular española: México y Centroamérica
24 La Ley Reguladora del Régimen del Personal Militar Profesional (cuatro cuestiones concretas)
25 Consecuencias de la reducción de los arsenales militares negociados en Viena, 1989. Amenaza no compartida
26 Estrategia en el área iberoamericana del Atlántico Sur
27 El Espacio Económico Europeo. Fin de la Guerra Fría
28 Sistemas ofensivos y defensivos del espacio (I)
29 Sugerencias a la Ley de Ordenación de las Telecomunicaciones (LOT)
30 La configuración de Europa en el umbral del siglo XXI
31 Estudio de «inteligencia operacional»
32 Cambios y evolución de los hábitos alimenticios de la población española
33 Repercusiones en la estrategia naval española de aceptarse las propuestas del Este en la CSBM, dentro del proceso de la CSCE
34 La energía y el medio ambiente
35 Influencia de las economías de los países mediterráneos del norte de África en sus respectivas políticas defensa
36 La evolución de la seguridad europea en la década de los 90
37 Análisis crítico de una bibliografía básica de sociología militar en España. 1980-1990
38 Recensiones de diversos libros de autores españoles, editados entre 1980-1990, relacionados con temas de las Fuerzas Armadas
39 Las fronteras del mundo hispánico
40 Los transportes y la barrera pirenaica
41 Estructura tecnológica e industrial de defensa, ante la evolución estratégica del fin del siglo XX

42 Las expectativas de la I+D de defensa en el nuevo marco estratégico

43 Costes de un ejército profesional de reclutamiento voluntario. Estudio sobre el Ejército profesional del Reino Unido y (III)

44 Sistemas ofensivos y defensivos del espacio (II)

45 Desequilibrios militares en el Mediterráneo Occidental

46 Seguimiento comparativo del presupuesto de gastos en la década 1982-1991 y su relación con el de Defensa

47 Factores de riesgo en el área mediterránea

48 Las Fuerzas Armadas en los procesos iberoamericanos de cambio democrático (1980-1990)

49 Factores de la estructura de seguridad europea

50 Algunos aspectos del régimen jurídico-económico de las FAS

51 Los transportes combinados

52 Presente y futuro de la conciencia nacional

53 Las corrientes fundamentalistas en el Magreb y su influencia en la política de defensa

54 Evolución y cambio del este europeo

55 Iberoamérica desde su propio sur. (La extensión del Acuerdo de Libre Comercio a Sudamérica)

56 La función de las Fuerzas Armadas ante el panorama internacional de conflictos

57 Simulación en las Fuerzas Armadas españolas, presente y futuro

58 La sociedad y la defensa civil

59 Aportación de España en las cumbres iberoamericanas: Guadalajara 1991-Madrid 1992

60 Presente y futuro de la política de armamentos y la I+D en España

61 El Consejo de Seguridad y la crisis de los países del Este

62 La economía de la defensa ante las vicisitudes actuales de las economías autonómicas

63 Los grandes maestros de la estrategia nuclear y espacial

64 Gasto militar y crecimiento económico. Aproximación al caso español

65 El futuro de la Comunidad Iberoamericana después del V Centenario

66 Los estudios estratégicos en España

67 Tecnologías de doble uso en la industria de la defensa

68 Aportación sociológica de la sociedad española a la defensa nacional

69 Análisis factorial de las causas que originan conflictos bélicos

70 Las conversaciones internacionales Norte-Sur sobre los problemas del Mediterráneo Occidental

71 Integración de la red ferroviaria de la península ibérica en el resto de la red europea

72 El equilibrio aeronaval en el área mediterránea. Zonas de irradiación de poder

73 Evolución del conflicto de Bosnia (1992-1993)

74 El entorno internacional de la Comunidad Iberoamericana

75 Gasto militar e industrialización

76 Obtención de los medios de defensa ante el entorno cambiante

77 La Política Exterior y de Seguridad Común (PESC) de la Unión Europea (UE)

78 La red de carreteras en la penísula ibérica, conexión con el resto de Europa mediante un sistema integrado de transportes

79 El derecho de intervención en los conflictos

80 Dependencias y vulnerabilidades de la economía española: su relación con la defensa nacional

81 La cooperación europea en las empresas de interés de la defensa

82 Los cascos azules en el conflicto de la ex-Yugoslavia

83 El sistema nacional de transportes en el escenario europeo al inicio del siglo XXI

84 El embargo y el bloqueo como formas de actuación de la comunidad internacional en los conflictos

85 La Política Exterior y de Seguridad Común (PESC) para Europa en el marco del Tratado de no Proliferación de Armas Nucleares (TNP)

86 Estrategia y futuro: la paz y seguridad en la Comunidad Iberoamericana

87 Sistema de información para la gestión de los transportes

88 El mar en la defensa económica de España

89 Fuerzas Armadas y sociedad civil. Conflicto de valores

90 Participación española en las fuerzas multinacionales

91 Ceuta y Melilla en las relaciones de España y Marruecos

92 Balance de las primeras cumbres iberoamericanas

93 La cooperación hispano-franco-italiana en el marco de la PESC

94 Consideraciones sobre los estatutos de las Fuerzas Armadas en actividades internacionales

95 La unión económica y monetaria: sus implicaciones
96 Panorama estratégico 1997/98
97 Las nuevas Españas del 98
98 Profesionalización de las Fuerzas Armadas: los problemas sociales
99 Las ideas estratégicas para el inicio del tercer milenio
100 Panorama estratégico 1998/99
100 1998/99 Strategic Panorama
101 La seguridad europea y Rusia
102 La recuperación de la memoria histórica: el nuevo modelo de democracia en Iberoamérica y España al cabo del siglo XX
103 La economía de los países del norte de África: potencialidades y debilidades en el momento actual
104 La profesionalización de las Fuerzas Armadas
105 Claves del pensamiento para la construcción de Europa
106 Magreb: percepción española de la estabilidad en el Mediterráneo, prospectiva hacia el 2010
106-B Maghreb: percepción espagnole de la stabilité en Méditerranée, prospective en vue de L'année 2010
107 Panorama estratégico 1999/2000
107 1999/2000 Strategic Panorama
108 Hacia un nuevo orden de seguridad en Europa
109 Iberoamérica, análisis prospectivo de las políticas de defensa en curso
110 El concepto estratégico de la OTAN: un punto de vista español
111 Ideas sobre prevención de conflitos
112 Panorama Estratégico 2000/2001
112-B Strategic Panorama 2000/2001
113 Diálogo mediterráneo. Percepción española
113-B Le dialogue Méditerranéen. Une perception espagnole
114 Aportaciones a la relación sociedad - Fuerzas Armadas en Iberoamérica
115 La paz, un orden de seguridad, de libertad y de justicia
116 El marco jurídico de las misiones de las Fuerzas Armadas en tiempo de paz
117 Panorama Estratégico 2001/2002
117-B 2001/2002 Strategic Panorama
118 Análisis, estrategia y prospectiva de la Comunidad Iberoamericana

119 Seguridad y defensa en los medios de comunicación social
120 Nuevos riesgos para la sociedad del futuro
121 La industria europea de defensa: presente y futuro
122 La energía en el espacio euromediterráneo
122-B L'énergie sur la scène euroméditerranéenne
123 Presente y futuro de las relaciones cívico-militares en Hispanoamérica
124 Nihilismo y terrorismo
125 El Mediterráneo en el nuevo entorno estratégico
125-B The Mediterranean in the New Strategic Environment
126 Valores, principios y seguridad en la comunidad iberoamericana de naciones
127 Estudios sobre inteligencia: fundamentos para la seguridad internacional
128 Comentarios de estrategia y política militar
129 La seguridad y la defensa de la Unión Europea: retos y oportunidades
130 El papel de la inteligencia ante los retos de la seguridad y defensa internacional
131 Crisis locales y seguridad internacional: El caso haitiano
132 Turquía a las puertas de Europa
133 Lucha contra el terrorismo y derecho internacional
134 Seguridad y defensa en Europa. Implicaciones estratégicas
135 La seguridad de la Unión Europea: nuevos factores de crisis
136 Iberoamérica: nuevas coordenadas, nuevas oportunidades, grandes desafíos
137 Irán, potencia emergente en Oriente Medio. Implicaciones en la estabilidad del Mediterráno
138 La reforma del sector de seguridad: el nexo entre la seguridad, el desarrollo y el buen gobierno
139 Security Sector Reform: the Connection between Security, Development and Good Governance
140 Impacto de los riesgos emergentes en la seguridad marítima
141 La inteligencia, factor clave frente al terrorismo internacional
142 Del desencuentro entre culturas a la Alianza de Civilizaciones. Nuevas aportaciones para la seguridad en el Mediterráneo
143 El auge de Asia: implicaciones estratégicas

144 La cooperación multilateral en el Mediterráneo: un enfoque integral de la seguridad

145 La Política Europea de Seguridad y Defensa (PESD) tras la entrada en vigor del Tratado de Lisboa

145 B The European Security and Defense Policy (ESDP) after the entry into Force of the Lisbon Treaty

146 Respuesta europea y africana a los problemas de seguridad en África

146 B European and African Response to Security Problems in Africa

147 Los actores no estatales y la seguridad internacional: su papel en la resolución de conflictos y crisis

148 Conflictos, opinión pública y medios de comunicación. Análisis de una compleja interacción

149 Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio

150 Seguridad, modelo energético y cambio climático

151 Las potencias emergentes hoy: hacia un nuevo orden mundial

152 Actores armados no estables: retos a la seguridad

153 Proliferacion de ADM y de tecnología avanzada

154 La defensa del futuro: innovación, tecnología e industria

154 B The Defence of the Future: Innovation, Technology and Industry

155 La Cultura de Seguridad y Defensa. Un proyecto en marcha

156 El gran Cáucaso

157 El papel de la mujer y el género en los conflictos

157 B The role of woman and gender in conflicts

158 Los desafíos de la seguridad en Iberoamérica

159 Los potenciadores del riesgo

160 La respuesta del derecho internacional a los problemas actuales de la seguridad global

161 Seguridad alimentaria y seguridad global

161 B Food security and global security

162 La inteligencia económica en un mundo globalizado