

Economic Espionage

التجسس الاقتصادي

M.Sayeh Boussahia¹, M.Lassoued Moussa²¹ university of Larbi Tebessi, Tebessa (Algeria), sayeh.boussahia@univ-tebessa.dz² university of Larbi Tebessi, Tebessa (Algeria), Lassoued.moussa@univ-tebessa.dz

Received: 09/05/2020

Accepted: 12/06/2020

Published: 30/06/2020

Abstract:

The Economic espionage concept refers to any unlawful act targeting of stealing critical economic secrets, such as trade, intellectual property and technology. The term refers to the secret acquisition or the theft of private information that is invaluable in a number of areas, including technology, finance, and government policy. Through this mean, perpetrators could gain cheap access to important information, which results in severe economic losses for victims.

Espionage has evolved throughout history, where opponents make competitive efforts outside the battlefields, avoiding the use of traditional means, and following what drives growth and prosperity, by penetrating the secrets behind technology and targeting nuclear and military secrets. Today, intelligence services, criminals and spies focus on industry and commercial information and important technology as a fast, effective and safe way to penetrate the foundations of the economy.

Keywords: economic espionage, spy, economy, evolution, information, loss, criminality...

JEL Classification Codes: A2, F5, H8

ملخص:

يشير مفهوم التجسس الاقتصادي إلى أي فعل غير قانوني يستهدف سرقة الأسرار الاقتصادية الهامة، مثل التجارة والملكية الفكرية والتكنولوجيا، فهو يتضمن الاستحواذ السري أو سرقة المعلومات الخاصة التي لا تقدر بثمن في عدد من المجالات، بما في ذلك التكنولوجيا والتمويل وسياسة الحكومة. من خلال هذا الوسيلة، يمكن للجنة الحصول على معلومات رخيصة الثمن، مما يؤدي إلى خسائر اقتصادية فادحة للضحايا.

تطورت عملية التجسس على مر التاريخ، حيث يبذل الخصوم جهودًا تنافسية خارج ساحات المعارك، ويتجنبون استخدام الوسائل التقليدية، ويتبعون ما يدفع النمو والازدهار، من خلال اختراق الأسرار وراء التكنولوجيا واستهداف الأسرار النووية والعسكرية، أما اليوم، تركز المخابرات والمجرمون والجواسيس على المعلومات الصناعية والتجارية والتكنولوجيا المهمة كوسيلة سريعة وفعالة وأمنة لاختراق أسس الاقتصاد.

كلمات مفتاحية: التجسس الاقتصادي، التجسس، الاقتصاد، التطور، المعلومات، الخسارة، الإجرام...

تصنيفات JEL: A2, F5, H8

Corresponding author: Sayeh Boussahia, e-mail: sayeh.boussahia@univ-tebessa.dz

Comparative law and social and prospective studies Lab., under high patronage of DGRST

1. INTRODUCTION

Economic espionage is as old as the economy itself, and it appeared thousands of years ago in ancient Greek, when the chefs who presided over holidays complained about their rivals who stole their recipes, just as the Byzantine Empire, the Chinese Empire, the Ottomans, Great Britain and America in particular knew economic and industrial espionage in all its forms and means.

Economic Espionage is a process that aims to obtain crucial economic and industrial information usually not available to the public, and it is one of the types and twisted means used in ancient and modern wars, so it has become an imminent danger for all parties. The ancient Egyptians carefully organized spying operations, the Hebrews, Greeks, and Romans asserted it during the 13th and 14th centuries BC.

The Cold War witnessed the massive participation of economic espionage activities between the United States and its allies, the Soviet Union, China and its allies, especially related to nuclear weapons secrets. Recently, spy agencies have targeted the identification of natural resources and knowledge of the country's internal and external economic policies, employing sophisticated and unfamiliar tools.

Today, economic espionage has become the best way to compete for international trade and deals, as some countries resort to espionage in the economic and industrial field to match companies, and thus it took an important dimension and great importance for economic decision makers in various countries, especially industrial ones, to make great efforts and monitor huge budgets to this espionage activity in order to achieve its strategic goals and objectives.

The theft of state technologies by another country was characterized by the passage of years, so economic and industrial espionage was a logical choice, in which the types of technologies and the diversity of means increased rapidly, in which countries and multinational companies and even privates were touched; for that

What is the concept of economic espionage, how did it develop, and what are its dimensions?

2. Conceptual Background:

Economic espionage is a broader phenomenon, and in the specialized literature in economic espionage, we notice the confusion between the definitions of economic espionage and industrial espionage, because this topic is under research and under consideration, because the various academic fields (sociology, criminology and law) that deal with it use

different terms, and each one of them focuses on a separate aspect of this phenomenon (Konstantopoulos, 2006).

The distinctive link to this confusion can be found in Richard Bennett's "Encyclopedia" as it does not include an introduction to economic espionage, but it deals with this term in an introduction to economic intelligence. Moreover, Bennett referred to economic intelligence, commercial and industrial intelligence, economic espionage and corporate espionage, without defining it, defining it, and distinguishing one from the other, whereas it does not even mention the distinction between total economic espionage and microeconomic espionage (Richard, 2002).

2.1 General definitions:

According to Samuel de Porteous, the security analyst for the Canadian Security Intelligence Service, the term "economic espionage" refers to "secret or unlawful attempts by foreign interests to assist their economic interests by obtaining economic intelligence information that can be used to sabotage or obstruct another country's economic security" (Samuel, 1995).

Through the term "Economic Intelligence", Porteous means "commercially relevant economic policy or information, including technological, financial, and commercial data and government information, which in the event that foreign interests could get them, , either directly or indirectly, assist relative productivity or the state's competitive economy status; Philip Zelikow, a professor at the University of Virginia, defines economic intelligence as "information related to how to develop, produce, or manage material affairs, goods, services, and resources from people outside the United States (Zelikow, 1997)."

Randall M. Forte defines economic espionage as the acquisition by secret means of information related to economy, trade and/or intellectual property by a secret agency/service agency that uses secret sources and methods (Fort, 1993).

For Hedieh Nasheri, economic espionage is "one nation that collects economic data for another country" (Nasheri, 2005)(1) and the term "economic data" means "information such as national gross domestic product and inflation rate figures, which can be obtained from published sources, or more distinctive information such as defense budget allocations

(1)- This book is the only academic book published and although it examines economic espionage from a criminological point of view and not from an international relations or strategic studies/intelligence approach, it is extremely valuable because it covers the whole phenomenon.

and national research and development expenditures, which are usually obtained by illegal means."

2.2 The legal definition of "economic espionage":

It is the unlawful targeting and theft of the nation's critical economic intelligence, and it can include secret acquisition or outright theft of invaluable secret information in a number of areas including technology, finance, and government policy; the economic espionage differs from industrial espionage or on companies⁽²⁾ in a number of ways - it is usually state-sponsored, has motives other than profit or interest and much larger in size and scope.

According to the FBI, foreign competitors practise economic espionage in three main ways:

- Recruiting insiders working in American companies and research institutions that usually share the same national background.
- Use of methods such as bribery, electronic attacks, "diving in the garbage", and eavesdropping on phone calls.
- Establishing seemingly innocent relationships with US companies to collect economic intelligence information, including trade secrets.

Industrial and economic or corporate espionage is a form of espionage that has been conducted for commercial purposes instead of purely national security (Wikipedia, 2020). It's conducted or managed by governments and is international in its scope, while industrial or corporate espionage is often national and occurs between companies or institutions (Nasheri, 2004).

2.3. Distinguishing economic espionage from some other terms:

Economic espionage and Geopolitical espionage:

What distinguishes economic espionage from geopolitical espionage is that the aim of the latter is the early warning of the capabilities and intentions of the opponent's state to wage war, while economic espionage is related to gathering economic and technological intelligence, however, there are two factors that make the distinction between traditional/geopolitical espionage and economic espionage difficult, **firstly**, some of the high-tech materials and equipment are necessary for the defense industry in the state as well as for its civilian industries. **Secondly**, the common ground where the political and military strategies of countries -

(2)- The FBI recommends that to counter this threat, companies should take a number of steps that include implementing a proactive plan to protect trade secrets, securing physical and electronic versions of intellectual property, and training employees.

especially the great powers - always have an economic milestone (Kennedy, 1987) (Klaus, 1973).

Another important difference between economic intelligence espionage and commercial intelligence espionage - is that the latter refers to the collection and analysis of information from the company, usually multinational, against another company, and if these companies collect information using secret means, the term "Industrial espionage" would be acceptable. While industrial espionage is carried out by a private sector entity, economic espionage is carried out by the government of a country using its secret agencies.

According to the FBI, economic intelligence espionage refers to a situation in which state secret services collect economic intelligence, while industrial espionage has to do with the collection of economic information by private companies (Michal, 1994).

Economic or industrial espionage and Competitive espionage:

The "competitive espionage" levels are subdivided into two descriptive scenarios as a legal and ethical activity, systematically to collect, analyze and manage information about industrial competitors in order to become useful (Nasheri, 2004), it may include activities such as examining newspaper articles, corporate publications, websites, patent filings, specialized databases, information on trade fairs, etc... Similar to identifying information about the company and collecting these critical elements which are sometimes called competitive espionage solutions or competitive response solutions and with its depth in market research, "competitive espionage" was described as "an implementation of the principles and practice of military and national intelligence in the field of global business" (Nick, 1996). It is the equivalent of the open source business intelligence.

The difference between competitive and economic or industrial espionage is not clear, so one of us needs to understand the legal basics to know how to draw the line between the two (Horowitz, 1998); others say that it is sometimes very difficult to know the difference between legitimate and illegal methods, especially when looking at the moral side of collecting information, making the definition more elusive.

2.4 Forms of economic and industrial espionage:

Economic or industrial espionage occurs in two main forms. In short, the purpose of espionage is to gather organized knowledge or organizations, it can include the appropriation of intellectual property, such as information about industrial manufacturing, ideas, technologies, and processes, recipes

and formulas, or it may include confiscation of owned or operational information, such as those related to customer data sets, pricing, sales, marketing, research and development, policies, possible bidding, planning or marketing strategies or variable compositions and production locations, and may describe specific activities such as trade theft, bribery, extortion, and technological control as well as spying management on commercial organizations where governments can also be targeted - for example, define tender terms for a government contract so that another bidder can offer cheaper offers (Wikipedia, 2020).

Targeted industries:

Economic and industrial espionage is more commonly associated with heavy technology industries, including computer software and hardware, biotechnology, space, communications, transportation, engine technology, automobiles, tools and machines, energy, materials, paint and so on, and it is known that "Silicon Valley" is one of the regions of the world most targeted for espionage (Nasheri, 2005).

Theft and sabotage of information:

Information can make a difference between success and failure; in the case of theft of trade secrets, the field of competition tends to favor the competitor, and although much of the collected information is legally obtained through competitive intelligence, companies sometimes consider that the best way to obtain it is the economic or industrial espionage behavior (Sarah, 2003) that poses a threat to any information-based trade.

In recent years, economic or industrial espionage has taken a broad definition, for example, attempts to sabotage can be considered industrial espionage on a company and in this sense, this term takes broader connotations than the mother word, so espionage and vandalism become more clearly related to each other and is also manifested through a number of typical studies, some governments, and some companies.

The United States government currently has a lie-detector (Polygraph) called "Spy and Subversion Test" which is increasingly popular, albeit not by consensus, and for the idea by those who study espionage, counter-sabotage and the interrelationship between them, in practice, especially by "reliable and knowledgeable sources", it is generally considered to be a functional match for the purpose of counter-notification (Baesler, 2015).

Agents and the combination process

Economic or industrial espionage usually occurs in one of two ways. **First**, an employee seizes information in order to achieve his own interests

or harm the company. **Second**, a competitor or foreign government seeks information to develop its technological or financial interest.

The "moles" or trusted insiders are generally considered the best sources for economic or industrial espionage purposes, and they are historically known as "idiots". He can cause internally, voluntarily or coercively, by providing information, then he is asked at first to hand over unimportant information and then endangers him by accusing him of committing a crime, bribing him to deliver the most sensitive information (Palmer, 1974); some individuals leave one company and work with another while taking sensitive information about it and such behavior was evident to focus on many industrial espionage cases that led to legal battles (Reuters, 1996).

Some countries hire individuals to do espionage instead of making use of their intelligence agencies; it is often believed that academics, business representatives, and students are used by governments to collect information. Some countries, such as Japan, question students when they return home (Nasheri, 2005).

The spy may take the form of a tour guide and he can also be an engineer, a maintenance man, a cleaner, an insurance sales representative or an inspector - the basis of anyone who has legal access to the workplace (Palmer, 1974).

The spy may break into a headquarters to steal data and may search through waste paper and waste known as "diving in garbage"; the information may be endangered through informal requests to obtain them, or through surveys and marketing or the use of support, research or technical programs (Nasheri, 2005); computers have facilitated the process of collecting information, due to the ease of obtaining large quantities of them through physical contact or through the Internet.

Computer and Internet use

Personal computers

The computer has become the main device in the practice of industrial espionage due to the huge amount of information it contains and the ease of copying and sending; it has increased rapidly in spying in the nineties, the stolen information are usually copied by an unattended computer or in offices without supervision or through subsidiary functions such as cleaners or laptops repairmen, which are still a major target for those who travel abroad for business and being cautious not to leave them for a period of time. It is known that the perpetrators of espionage find many ways to trick individuals and enable others to access and steal

information; the term "reference bag" refers to "To use hotel personnel to access data, through laptop computers in the rooms, so information may be stolen during transit, in taxis, at baggage meters at the airport, luggage carousels, on trains and so on."

2.5 Economic espionage dimensions:

First, macroeconomic espionage refers to the use of secret services on behalf of the government of a country in order to obtain information about global economic developments and activities with the hidden aim of advancing its strategic interests (Loch, 1996).

In its basic form, macroeconomic espionage helps the political leaders of the state in managing its internal and external economic policy with optimal results. In 1949, Sherman Kant⁽³⁾, emphasized that the intelligence services must follow the current economic developments in the world as well as doctrines and external economic theories (Shapira, 2020) and, moreover, we should see the supply segment of the armed forces, the new development of crops and farming methods, changes in agricultural machinery, land use, fertilizers and reclamation projects, and we should pay close attention to the development of new facilities and those already established, as well the changes in distribution techniques and tools, new transportation methods and changes in transport units but, more importantly, in the nuclear age, we must track new discoveries as much as they care about natural resources, especially those used to build nuclear weapons.

Second, espionage is called microeconomics (or microeconomics intelligence, commercial espionage), and according to it, the government of a country participates through its secret agencies in collecting intelligence information in order to help a company (usually a multinational), and by that method creates cooperation between the government and the company, the latter's aim is to win over opponents in the international economic arena (Loch, 1996).

Third, countering economic espionage, which Randall M. Forte defines it as "identifying and neutralizing foreign intelligence services' spying on US citizens or companies and stealing information and/or technology for use within their own countries" (Fort, 1993).

(3)- *The father of U.S. intelligence analytical domain, who had full knowledge of the value of macroeconomic espionage.*

Thompson Strong⁽⁴⁾ expresses the view that "the goal of the process of counteracting competitive espionage is to make investment in competitive espionage ineffective or very costly, at least perceptually (Thompson, 1995)."

Samuel Porteous distinguishes counter-espionage as not only a very important job for intelligence, but also less controversial, and according to his definition of the term "anti-spy service to the nation", he simply sought to advise the government and report on the activities of foreign intelligence services or their agents involved in secret activities directed against the country's economic and commercial interests (Samuel, 1998).

2.6 Incentives and constraints:

Decision-makers decide to assign their intelligence services to collect and analyze macroeconomic intelligence information for some specific reasons, and may refrain from that activity for some other reasons.

Incentives:

Decision-makers order intelligence agencies to commit total economic espionage for the following reasons:

- Achieve the most effective monitoring of international economic and technological developments in the world.
- The economic result of analyzing the costs and benefits of macroeconomic espionage operations is always positive.
- Intelligence services have a structural advantage compared to other government agencies.

Obstacles:

The obstacles that deter states from participating in macroeconomic espionage are:

- Macroeconomic espionage causes problems during the establishment of effective bilateral and multilateral diplomacy by the state.
- Some analysts and politicians support the view that the role of intelligence is not to study the international economy and steal trade secrets, but to ensure national security.
- According to some analysts, the information gathered by macroeconomic espionage is useless at the tactical level because its members do not have the economic knowledge available to exploit it.

(4)- Strong makes the usual definitional mistake. He uses the term competitive espionage instead of economic espionage and he identifies competitive espionage with economic espionage and industrial espionage, although he distinguishes their difference.

- Intelligence services cannot compete with the quality of analysis of government and academic institutions dealing with the study of economic issues.
- The majority of macroeconomic intelligence is collected via open source.

3- Historical Background:

Industrial espionage - especially for luxury goods - had been around for thousands of years and an important event in the mid-6th century AD, and it can be said that it took off from the late Roman era to the early centuries of the existence of the Byzantine historian Procopius, where a delegation of Eastern Orthodox monks under Justinian command broke two monopolies in eastern - China silk production and in Persia silk trade routes to the west - and this destruction was through smuggling silkworms to the west, and ensuring new production of western silk, and this change made silk available easily and less costly in the West by stabilizing Constantinople (Byzantium) As a new source of silk, which intermediaries in the cost equation.

By the sixth century AD, knowledge and technology of raw silk production had spread out of China, the Christian monks who lived in China had hidden some silkworms in bamboo canes as an act of industrial espionage that allowed the silk industry to be woven and woven independently to take root in the Byzantine Empire, and it happened that the Koreans The Japanese, Indians, and Persians also learned how to produce this precious tapestry.

3.1 The origins of industrial espionage:

Going into history, we can find many examples of total economic espionage, and the great importance of economic and technological intelligence can be checked throughout the ages, when the Israelites made a picnic in the Sinai, Moses instructed spies for him to "get to know on the ground" and this first attempt at espionage was really helpful and includes the issue of total economic espionage as the spies not only gave a concrete description of the city and its defenses and the strength of its residents, but also provided useful economic intelligence by verifying that Canaan was the land of "milk and honey" and giving details of the quality of the land (B.J.C, 1992).

Collecting macroeconomic intelligence was not known in ancient Greece, and according to Professor Andrew Gerolimatus, in 416 BC the Athenians sent a delegation at Egesta in order to know the economic capabilities of the city in order to finance a joint offensive military

operation.

The works of Father Francois Xavier to discover ways of making Chinese ceramics for Europe in 1712 are sometimes considered an early case of industrial espionage (William & Timothy, 2009). Historical accounts of industrial espionage between Britain and France are attributed to the emergence of Britain as an "industrial creditor". The second decade of the 18th century witnessed the emergence of state-sponsored efforts to transfer British industrial technology surreptitiously to France; witnesses have confirmed the existence of temptations for craftsmen abroad and the training of trainees in England (John, 1998), on the other hand, protests such as those by iron workers in the British city of Sheffield and steel workers in Newcastle on the advantages and temptations of skilled industrial workers abroad have led to the first English legislation designed to prevent this method of economic and industrial espionage (John, 1998).

3.2 In the Ancient History

Events involving espionage have been documented throughout history, thus writings of ancient Chinese and Indian military strategists such as Sun Tzu and Chanakya contain information about deception and sabotage. Moriya, a student of Chanakya and the founder of the Moriah Empire in India, used assassinations, spies and secret agents, which were described in the ancient Indian treatise on the art of government, economic policy, and military strategy written in the Sanskrit language (Cthulhu).

The ancient Egyptians had a sophisticated system of intelligence; the Hebrews used spies as well, as stated in the story of "Rahab", just as spies were prevalent in Greek and Roman empires (N.O., 2020), and during the 13th and 14th centuries, the Mongols relied heavily on espionage in their conquests in Asia and Europe.

Feudal Japan often used a ninja to collect intelligence, and recently, spies played an important role during the Elizabethan era in England and many modern espionage methods were largely created until then.

The Aztecs used merchants as spies and diplomats with diplomatic immunity, and alongside these people, before any battle or war, secret agents and quimitchin, were sent to spy on enemies and usually wore local uniforms and spoke in the local language, and used techniques similar to those used by contemporary undercover agents (Soustelle, 2002).

During the 6th century, the Byzantine Emperor Justinian dispatched Christian monks to China in order to undermine its monopoly on silk production, and years later, monks returned to the empire carrying silkworm eggs, mulberry seed and knowledge needed to produce silk, and

this industrial theft was a blessing for the West, despite it has hurt the economies of China and Persia (Hagon, 2012).

In the era of the Greek democratic city-states, espionage was mainly used as a political tool, as agents spied on their competitors from other cities and revered information on military power and defenses to rulers; the most far-sighted contributions to the ancient Greek intelligence community was to create a complex and effective means of communication between cities where couriers deliver intercity messages, but important messages are also relayed between a series of outposts or towers using a signal, a form of communication that uses signals to transmit messages so Greek connections were so effective that they remained unparalleled even in the modern era.

In the Middle East, after Byzantium, the large bureaucratic government established one of the oldest civil intelligence agencies, so civil agents provided information about foreign armies and economic practices of merchants, sellers, sailors, and other businessmen, outside the Mediterranean region; other civilizations used and contributed to the art of espionage, Blogs written since the fifth century mention the use of spies in the Indus Valley, the past 500 years, and in China, Sun Tzu wrote the comprehensive military thesis "The Art of War" that included several chapters devoted to the use of spies inside and outside the battlefield.

No civilization in the ancient world relied heavily on intelligence, nor promoted the development of espionage more than ancient Rome. More than a thousand years ago, the Romans established the largest empire in the ancient world, which necessitated more expansive governance of infrastructure, military, bureaucracy.

Rome's most famous case of espionage and conspiracy culminated in the assassination of Julius Caesar on March 15, 44 B.C., and the exact details of the assassination plot remained a mystery to historians, but blogs established that the Romanian intelligence services knew the plot in advance and provided information to Caesar or his assistants the names of many of the conspirators but were ignored by intelligence services.

The expanding Roman Empire often spied on its neighbors, intelligence agents not only provided comprehensive reports on military power and resources to those outside the empire, but also the Roman Army used intelligence forces to penetrate tribal organizations and persuade leaders to join the alliance with Rome, and if it is judged, the population is hostile by informers, reaching the military, and this type of intelligence campaign was very successful in the Italian peninsula during the fourth century B.C., but much less effective in subsequent campaigns to conquer

northern Africa and northern Europe.

The Roman Empire possessed a fondness for the practice of political espionage, so spies were involved in both external and internal political processes, in measuring the political climate of the empire and the surrounding lands by eavesdropping in forums or in public places such as markets.

There are several ancient accounts, especially in the first century AD, that mention the existence of the secret police force, and the Fromentry (the eyes and ears of the czar);⁽⁵⁾ and by the third century, Roman writers observed excessive censorship and rampant secret police forces, likening it to an authoritarian force or a professional army.

Political espionage was not confined to the most complex parts of the Romans' vicinity, but was also practiced in Rome itself by rival factions in the government, some ministries were using saboteurs, so interest in government competition necessitated the creation of the courier service⁽⁶⁾, which is the first exclusive force to combat espionage (Kleef, 2010).

3. 3 In The Middle Ages:

After the collapse of the Roman Empire in Europe, espionage and intelligence activities were limited to periods of war or local services; warring factions, under the barbarian princes, used strategic espionage to measure the strength of their opponents or know the enemy's defenses, but there were no written records of these activities, and the only significant political force in Europe during the dark ages was the Catholic Church; the operations in the European environment were restricted to monastic outposts that were struggling to survive.

In the Middle Ages, the birth of large nation-states, such as France and England, in the ninth and tenth centuries facilitated the need for intelligence in a diplomatic situation, organized messengers, translators, and royal messengers transmitted diplomatic messages between kings or fiefs, and since illiteracy was widespread, even in royal courts, messages were delivered literally carefully by their couriers.

Espionage remained mostly limited to battles, but the development of the feudal system created a complex network of loyalty that led to the

⁽⁵⁾- *The eyes and ears of Caesar, his intelligence officers are tasked not only with infiltrating enemy society, but also carry out his campaigns of terror. They operate separately from the main Legion forces and are handpicked by Caesar himself. In 2281, their commander is Vulpes Inculta, the fourth-most powerful man in the Legion.*

⁽⁶⁾- *The late Roman imperial courier service and general agents of the central government from the 4th to the 7th centuries. The agentes in rebus*

emergence of laws prohibiting betrayal, dual loyalty, and political espionage against allied emperors.

In the eleventh century, the Catholic Church rose to prominence in European politics, and with the large bureaucratic network, the resources of feudal military forces, and the largest treasury in the world, the church instituted policies that ruled Europe and throughout the Middle Ages, the Crusades and the inquisition, strengthened the authority of the church and created a long-term intelligence society in the Middle Ages.

In 1095, Pope Urban II called for the First Crusade, a military campaign to restore Jerusalem and the Holy Land from Islamic and Byzantine rule, so the church mobilized large armies, and used spies to report defenses surrounding Constantinople and Jerusalem where specialized intelligence agents infiltrated prisons to liberate the Crusader captives, or sabotage palaces, mosques, military defenses; the Crusades lasted for nearly four centuries depleting the military intelligence resources of most of the kings of Europe.

3.4. During Renaissance:

The Renaissance marked the eclipse of the Church's domination of the world and Europe moved to more local and national government paradigms, and with every nation or city employing its own intelligence force, and when states and cities became wealthier and gained more power, espionage returned, as competition for hegemony over trade and exploration in the new world changed the political climate in Europe and forced the regimes to adopt ingenious measures to protect political, military, and economic interests.

Imperialism did not only change the global political balance, but also transformed the economy. Modern industrial espionage was born in the European national revolutions of 1848, a series of regional conflicts that incited workers against the nobility and liberals against conservatives, monarchies against Republicans and Communists, and other political groups, so many governments especially England, France, and Prussia, spies were used to penetrate political and labor organizations and to report any anti-government activities and often these organizations spied on each other, reporting working conditions, factory operations, and coronary, mining, and other concerns.

Radical workers' organizations carried out numerous acts of sabotage, destroying factories and mines, and government property; and after the armed conflict subsided, many governments continued to monitor dissident groups and workers, and within a decade, the same principles of

industrial espionage against foreign economic interests increased (N.O., Espionage and Intelligence, Early Historical Foundations, 2020).

Spy hangover during the Cold War

With Western restrictions on the export of materials likely to increase the military capabilities of the Soviet Union, Soviet industrial espionage was auxiliary to other espionage activities until the 1980s (Philip, 1987), and in April 1984 reports, for example, that although the Soviets sought to develop microelectronics, it was found that this technology is several years late compared to the West, Soviet CPUs required multiple chips and looked like copies or a duplicate document for American products such as Intel 3000 and... (Ruth, 1984)

After the collapse of the Soviet Union and the end of the Cold War, commentators, including the Intelligence Committee of the US Congress, noticed that there was a redirection within the spy system by shifting from military targets to industrial ones with Western and former communist countries by taking advantage of "masked" spies and expanding programs directed to stole these information (Nasheri, 2005).

Spy remnants during this period not only included staff redirection but the use of spy devices such as computer databases, eavesdropping scanners, spy satellites, and wires.

During the Cold War the United States was the main target not only of its opponents but also of its main allies, and its spy policies emerged on the macroeconomy of the former Soviet Union, Russia, Japan and France.

The Cold War included intense espionage activity between the United States and its allies, the Soviet Union, China, and their allies, especially with regard to nuclear weapons secrets. Recently, spy agencies have targeted the illegal drug trade and those considered terrorist and since 2008 the United States has accused at least 57 people of trying to spy for China (Mubarakpuri, January 1, 2011).

The former Soviet Union – Russia

There is a large part of the literature on the former Soviet Union that refers to many instances of total economic espionage. Since the 1920s the former Soviet Union had been trying to obtain high-tech industrial technology from the United States and Western Europe through espionage (Corson W.R. & Crowley R.T., 1985), and the value of foreign technology was recognized first as a target for agencies Soviet Intelligence, the special committee for the struggle against counter-revolution and subversion that worked in the collection and acquisition of US technology.

Macroeconomic espionage contributed to the rise of the relative economic strength of the Soviet Union and, according to a former leader of K.G.B., the use of economic intelligence obtained had had a major impact on his country's industry while boasting of the value of the information obtained from the West by covering the functional expenses of operations, thus in the late 1970s, The Soviets negotiated favorable agreements to buy grain from the United States due to objections to communications between members of economic and financial departments in the United States, and they got that by eavesdropping on phone calls between members of Americans merchant representatives in the US Department of Agriculture; the goal of the Soviet Union was not only to acquire Western technology for military reasons, but also to support the decline of its domestic economy (W.T. ,1994) in the short and long terms. Economic espionage operations allowed participation in the arms race, yet it failed to prevent the growing gap between the Soviet and Western technology, especially outside the field of defense.

Branhild Campaign

Some of these activities were directed through the State Security Service in East Germany, and one of these operations was known as the "Branhilde Operation" and was used between the mid-1950s and early 1966, employing spy workers from many countries of the Communist bloc, and through at least 20 invasions, many Western European industrial secrets were exposed to danger (Palmer, 1974), and among the members of this workshop was a Swiss chemical engineer known as the "Air Bubble" who disclosed information about the industrial espionage conducted by the workshop, including the fact that Russian agents had obtained details about the "Concorde" Advanced Electronics System, and testified against two company employees " The Duck ", who live and work in Britain during the trial in which they were accused of transferring to the (Swiss engineer) information on industrial processes, but were acquitted at the end (Palmer, 1974).

Soviet special records system "spetsinformatsiya"

In a secret report of the Military Industrial Commission of the Soviet Union from 1979 to 1980, detailing how to use this system in twelve different military industrial zones, in a bulletin for scientists at atomic, Philip Hanson wrote in detail about the aforementioned system that developed more than ten industrial sub-ministries requests for information aiding in technological development in their military programs.

The acquisition plans are described as working on two and five year cycles with about 3,000 ongoing missions each year, efforts targeting both civilians and military industrial targets such as the petroleum and chemical industries, and some information has been obtained by comparing the levels of competitors with Soviet technological advances, also much unclassified information collected, which impeded the clarity of the borders with "competitive intelligence".

The Soviet army was acknowledged much better using the gained information, compared to civilian industries whose records were duplicated and lacked the development of industrial technology (Hanson, 1987).

Japan

Japan has a more integrated and sophisticated intelligence apparatus compared to other allies of the United States. In the last four decades, Japanese governments have facilitated the creation of a decentralized national framework for gathering economic intelligence. Japan is the only country that has established its intelligence with a major goal of achieving high levels of prosperity and improving the lives of citizens (Deacon Richard, 1983).

Taking into account the tendency of Japanese traditions to seek and collect useful intelligence information from abroad, improving, and implementing it in their local community, this is not a new policy, but the creation of Japanese intelligence according to this tradition finds the difference in it between Japanese intelligence and the services of other countries in that spying operations in Japan relies less on official secret services and more on an extensive network of institutions and Japanese society.

USA

The United States has a long history of collecting macroeconomic intelligence as its operations dated back to the end of 1776. The first US intelligence agency called the "Confidential Correspondence Committee of the Continental Congress" sent William Carmichael to Europe, disguised as a merchant, in order to collect intelligence on the economic issues that the new US government paid great attention. In November 1776, Carmichael sent a reassuring email from Amsterdam, providing reports that: "You are threatened by Ukraine's intention to supply Europe with tobacco, there is a long time before this can happen. Some of that tobacco is here, and the best is worse than any plant on our land (Zelikow, 1997)."

During World War I, an agency led by John Foster Dallas was established in the United States, and its goal was to gather and analyze

important economic information. President Wilson, in preparation for the Versailles Peace Conference, transformed into a private company called "investigation" that gathered economic intelligence (Zelikow, 1997).

Germany ignored the importance of economic intelligence, as recognized by the leaders of its intelligence services. In the 1930s, Germany did not make the same mistake. According to Walter Lacker, "German economic intelligence worked well during the war, contrary to its scientific intelligence."

During World War II, economic intelligence played a major role for US agents from strategic services offices. Other analysts had the task of "knowing not only the enemy's military preparations but also the knowledge of smuggling tungsten metal and smuggling diamonds, knowing the production of ball bearings, and the supply of Swedish iron ore to Germany, and other such topics."

It was a common ground that such issues addressed strategic issues of great importance to conduct war. Also, during World War II, the mission of the newly created Economic War Council was to study the Japanese economy and analyze the role of commodities (Zelikow, 1997). and taking into account this tradition, from the contradiction to saying the truth that The United States ignored scientific and technological intelligence because it misjudged the fact that the power of the United States was too great and the technological knowledge was superior to its opponents who had nothing to learn from it but rather a classic case to reduce the enemy's capabilities (Walter, 1993).

3.5. In The modern history:

The various intelligence agencies evaluate some techniques in collecting intelligence on others, the former Soviet Union, for example, favored human resources over open source research, while the United States tends to emphasize technological means such as analogy, signature, and intelligence photography, and assessing officers in both Soviet political intelligence (KGB) and military intelligence (GRU) (Nasheri, 2005) according to the recruited agents number.

In the centuries following the Renaissance, European powers began to realize that technology could give them an economic advantage over their competitors. Soon after conquering the Aztecs, the Spaniards were able to establish a profitable process of handling chocolate and taking it to the extreme to keep the product as confidential as possible, however; The Spanish monopoly of this industry did not last long as an Italian explorer was able to find out the secret cocoa farms in Spain while on a trip to the

New World, and upon his return to Italy, he circulated the recipe in his native country, which soon spread throughout Europe.

During the age of exploration, European countries spent a lot of time and money in charting the world and securing trade routes to East Asia. After the most sought-after commodities, the role of Chinese ceramics came on the basis that it was an easily breakable commodity that could not withstand long and difficult rides, so there was a lot of effort made to copy Chinese art into making porcelain, but most attempts proved unsuccessful.

However, in the 18th century, a Jesuit priest named Francis Xavier managed to infiltrate the porcelain center in China, and with great accuracy, recorded what he saw and passed secret messages about the details of the process to his homeland France, and by using these instructions, French craftsmen managed to successfully reproduce the desired object and undermine China's monopoly on this lucrative trade.

However, that was not the only French attempt at industrial espionage; France continued to launch intelligence efforts against its rival England especially in the 18th and 19th centuries and the French government intentionally sought and enlisted British glassmakers, shipbuilders, and metal artists in order to harness their expertise, though, England did not complain of many French plots; after all this, the British East India Company launched a campaign of industrial espionage on its own, stealing tea from China to grow in India, not only the Europeans involved in the theft of trade secrets.

Samuel Slater was born in England in the 18th century, and when he was still young, he was able to secure a job opportunity in one of the most advanced textile factories in the country, and when he immigrated to America in 1789, he took extensive knowledge of the large production quantities of textiles, and opened many of advanced factories in the United States, to become a self-made millionaire and tycoon, to reverse the curse inflicted on his home country, the pay tribute to Slater in the United States for helping this young country gain a technologically competitive advantage over the UK.

Nearly a century later, Great Britain again became a victim of industrial espionage, as Alfred Krupp, a 19th-century German industrialist, created a network of spies to protect his company's trade secrets and to gain intelligence about his competitors, and in the process, he managed to obtain with extensive knowledge of steelmaking techniques in Britain; Krupp used this information to improve his operations and became one of Germany's

leading businessmen. In fact, his success was pivotal in developing Germany's industrial heartland "The Ruhr Valley".

Industrial espionage continued in the 20th century during the Cold War, and it remains a threat to the present day. Fortunately, modern companies have tools to protect themselves unlike companies in the past that are often lacking. Patents, international agreements, and legislation that protect trade secrets help them in Guarding their intellectual property even if they hard-won them, however, industrial espionage remained a threat for several centuries, and it is likely to continue for centuries, and for this reason, despite modern legislation and legal protection, companies must continue to exercise vigilance against this threat more than ever.

France

It is one of the main players in macroeconomic espionage on the table of the global espionage chess, which has at its disposal a well-organized intelligence apparatus, and it is characterized by experts who are considered one of the most aggressive information collectors in the world (Peter, 1996).

In the mid-nineties, there was a shift in French policy regarding economic espionage, and because of the influence of the new school of thought and the conclusion that it was impossible for France to win economic war in the way of economic espionage, so it decided to follow the Japanese method that focuses on open sources, although in general 1996 witnessed a decrease in economic espionage (and macroeconomic espionage in particular) by France, and the US intelligence community was especially careful.

United State

The responsibility for collecting and analyzing economic intelligence information during the fifties and sixties was entrusted to the relations between the Central Intelligence Agency and the Ministry of Foreign Affairs; in two priority lists related to gathering intelligence information published by the CIA between 1975 and 1986, the presence of macroeconomic goals was clear and included the monitoring of OPEC and the strategies related to its price policy, the size of the annual crop of the Soviet Union and the quality of its computers, debt financing in developing countries, international energy shortages, the supply of food worldwide, scientific progress and technology (Zelikow, 1997); it's claimed that in the early 1980s, American intelligence agencies placed "packaged software" in the computers of the World Bank and other international financial

institutions in order to provide early warning to American policy makers as much as concern about the Latin American bank crisis.

3.6 Notable cases:

France and the United States

Between 1987 and 1989, it was thought that IBM and Texas Instruments were targeted by French spies with the aim of assisting the French group called "Paul" and in 1993; it was also thought that American airlines were targeted by French interests (Joyal, 1996).

During the early 1990s, France was described as one of the fiercest pursuers of espionage to win foreign industrial and technological secrets, although it was the United States that accused of trying to sabotage its high-tech industrial base in an attempt by the Government of France to return charges related to continuous industrial espionage against aerodynamics and American space companies (Nolan).

Volkswagen Automobile Company

In 1993, Opel, the manufacturer of cars (a subsidiary of General Motors), accused Volkswagen of industrial espionage after the Director General of Production and seven of the CEOs moved to Volkswagen, and later threatened it with filing a suit for defamation, which led to a four-year legal battle; the case, which was finally settled in 1997, resulted in one of the largest settlements in the history of industrial espionage with Volkswagen agreeing to pay \$ 100 million to General Motors and buying at least \$ 1 billion worth of spare parts from the company for more than 7 years, although it did not explicitly apologize about this behavior (Meredith, 1997).

Hilton and Starwood

On April 2009, the US-based Starwood Company for Tourism and Hotels accused its competitor Hilton in a "massive" case of industrial espionage, after it was bought by private equity group Blackstone; Hilton hired 10 executives from Starwood, and under intense pressure to improve profits, it accused Starwood Hilton By stealing company information related to its luxury brand concepts used in creating hotel stays; its group former head was specifically accused of downloading "a truckload of documents" from a laptop to a personal email account (Andrew, 2009).

GhostNet

It was a kind of system of extensive surveillance "by Canadian researchers based at the University of Toronto in March 2009 and by e-mail messages that posed a threat to thousands of computers of government organizations which enabled hackers to search for information and transfer

them back to" a digital storage facility in China. (Markoff & Barboza, 2010)"

Google and the Aurora process

On January 13th, 2010, Google announced that operators, from within China, had penetrated into Google's operation in China, stealing intellectual property, and in particular, accessing email accounts of human rights activists and it was thought that the attack was a part of a broader attack on Companies in China that became known as the Aurora Process.

Intruders thought that they launched a zero-hour attack, exploiting vulnerability in Microsoft's Internet browser. Malware was used as a modification of the Trojan horse and given concern about the possibility that hackers could benefit from this vulnerability that was previously unknown in Microsoft's browser, the governments of Germany and France subsequently issued warnings not to use this browser (Murad, 2010).

There was speculation that "infiltrators" had participated in the attack, with some Google employees in China denying them access to the company's internal networks after the announcement, and on February 2010, computer experts from the US National Security Agency claimed that attacks on Google may have originated from two Chinese universities they had Computer science experience, including Shanghai University and another university closely related to the Chinese army.

Google claimed that at least 20 other companies were targeted in cyber attacks, which were part of an "ambitious and sophisticated attempt to steal secrets from victims of unintended companies," including defense, finance, and technology companies, and instead of viewing this act as an individual act or organized crime, at its level of development, it was clearly more typical of a country, and some commentators speculated that the attack was a part from a coordinated Chinese industrial espionage process aimed at obtaining "high-tech information for the launch of its economy; this view was criticized by saying it was a slack stance by foreign companies in China to protect its intellectual property, thus they were allowed to work and then copying their engineered technology for the benefit of " Chinese national heroes ", for this, Google closed its operations in China.

Cyber incubator and green dam

On January 2010, the US-based company, CyberSitter, announced that it was suing the Chinese government and other US companies for stealing their anti-pornography programs in China which was used by the state to censor children in accessing the Internet; the company accused the

creators of In the Green Dam by copying about 3000 lines of code describing it as a "dirty job of copying" while still directing people to use some of the instructions lines to its site, and in this regard the company's lawyer said, "I don't think I had seen such a clear theft in my life."

4. Conclusion:

Industrial espionage, economic espionage, and corporate espionage are expressions used to prescribe espionage conducted for commercial and economic purposes, as opposed to national security ones; it's a long history, thus one of the oldest known attempts at economic and industrial espionage in history involved that by the Europeans to acquire the closely secret of China's porcelain manufacturing process in the seventh century, then and according to historian and philosopher Thucydides, the Egesta citizens deceived the members of the delegation by falsifying their true resources and thus mistook the Athenians in their economic situation and the trick was successful.

In the sixth century AD, in order to avoid the taxes on gold imposed by Persia in cases in which Byzantium imported silk from China, and in order to undermine the discount economy, Justinian reached an agreement with the Ethiopians, which stipulated that they were going to buy silk and transport it to Byzantium.

In the centuries following the Renaissance, European powers began to realize that technology could give them an economic advantage over their competitors. Then, during the Cold War the United States was the main target not only of its opponents but also of its main allies, and here spy policies emerged on the macroeconomy of the former Soviet Union, Russia, Japan and France.

Today, in a globalized economy, international intelligence agencies try to fit themselves with the data of the economic conflict raging between the states actors in the global arena. Of course, economic espionage is not limited to gathering information and benefiting from, but it goes beyond it to sabotage and destroy the economies of opponents. Commercial competition has become clearer, so the world has witnessed and will witness more industrial and economic espionage.

Results:

- Economic espionage is not born of the present, but goes back thousands of years
- Economic espionage targets the economy directly or indirectly
- Commercial competition has become more evident, leading to more industrial and economic espionage

- All countries are accused of defiance and struggle to collect scientific and technological information
- Everyone is spying on everyone in all important economic fields
- There is a hidden war led by economy spies in more than one country and this threatens the achievements of companies
- Despite the illegitimacy of espionage, in the contemporary world of espionage, economic espionage has often become almost lawful for what global developments imposed on intelligence agencies

5. References:

Andrew, C. (2009, April 17). "Starwood sues Hilton for 'stealing trade secrets'". The Guardian (London). Retrieved January 1, 2020, from <https://www.theguardian.com/business/2009/apr/17/industrial-espionage-hotel-industry-lawsuit>

B.J.C, N. K. (1992). *Go Spy the Land: Military Intelligence in History*. Praeger Publishers.

Barboza, J. M. (2010, February 18). "2 China Schools Said to Be Tied to Online Attacks". Retrieved January 1, 2020, from <https://www.nytimes.com/2010/02/19/technology/19china.html>

Corson W.R., C. R. (1985). *Engine of Soviet Power*. Brighton: The Harvester Press Ltd.

Cthulhu. (n.d.). *Espionage*. www.erepublik.com. Retrieved January 1, 2020, from <https://www.erepublik.com/en/article/2414528>

Dan, L. (2010, MAY 24). "Federal Judge Trashes Novel Economic Espionage Case". <http://www.law.com>. Retrieved DECEMBER 1, 2019, from http://www.law.com/?id=1202458668065&Federal_Judge_Trashes_Novel_Economic_Espionage_Case

Deacon Richard, K. T. *A History of the Japanese Secret Service*. (B. B. Inc, Ed.) 1983: Beaufort Books Inc.

Hagon, C. (2012, september 29). *Intellectual Property Protection & the History of Industrial Espionage*. Retrieved January 3, 2020, from <http://www.imgsecurity.net/intellectual-property-protection-the-history-of-industrial-espionage/>

Hansol, P. (1987, AVRIL). *Soviet industrial espionage*. Bulletin of the Atomic Scientists, 43(3), p.25.

John, H. (1998). *Industrial Espionage and Technology Transfer: Britain and France in the Eighteenth Century*. Aldershot: Ashgate Publishing Limited.

Joyal, P. M. (1996). *Industrial Espionage Today and Information Wars of Tomorrow*. In I. S. Services (Ed.), 19th National Information Systems Security Conference (pp. 1-14). altimore Convention Center Baltimore, MD: INTEGER Security Inc. Information and Analytic Services.

Kleef, M. L. (2010, April 26). *Greece in the Late Roman Period*. Master Thesis. Leiden university.

- Loch, J. K. (1996). *Secret Agencies: U.S. Intelligence in a Hostile World*. London, UK: Yale University Press.
- Meredith, R. (1997, January 10). VW AGREES TO PAY G.M. \$100 MILLION IN ESPIONAGE SUIT. (T. N. Company, Ed.) The New York Times, Section A, p 1.
- Mubarakpuri, S. R. (January 1, 2011). *The Sealed Nectar* . Darussalam.
- Murad, A. (2010, January 18). "Google cyber-attack from China 'an inside job'". The times. Retrieved February 1, 2020, from <https://www.thetimes.co.uk/article/google-cyber-attack-from-china-an-inside-job-qdbn0xbjf9w>
- N.O. (2020, MARCH 1). faqs. Retrieved MARCH 1, 2020, from faqs: <http://www.faqs.org/espionage/Ep-Fo/Espionage-and-Intelligence-Early-Historical-Foundations.html>
- N.O. (2020, March 2). historynet. Retrieved January 1, 2020, from historynet: <https://www.historynet.com/espionage-in-ancient-rome.htm>
- Nolan, J. A. (n.d.). "A Case Study in French Espionage: Renaissance Software". (hanford) Retrieved from http://www.hanford.gov/oci/maindocs/ci_r_docs/frenchesp.pdf
- Palmer, R. (1974). *Espionage threat to British industry: Spies don't only operate in books and films. They can be for real. And their target might be your industrial secrets*. Industrial Management, 74(7/8), pp.10-13.
- Peter, S. (1996). *The Growth of Economic Espionage: America Is Target Number One*. Foreign Affairs, 75(1), p.11.
- Philip, H. (1987). *Soviet industrial espionage*. Bulletin of the Atomic Scientists, 43(3), pp.25-29.
- Reuters. (1996, may 12). *Volkswagen Sues GM for \$6.6 Million, Accusing U.S. Firm of Defamation* . Ruth, H. (1984, APRIL). Soviet Microprocessors and Microcomputers. BYTE MAGAZINE, p.348.
- Samuel, P. (1998). *Economic and Commercial Interests and Intelligence Services*. (i. P. (ed.), Ed.) Carleton University Press.
- Shapira, I. (2020). *Strategic intelligence as an art and a science: creating and using conceptual frameworks*. Intelligence and National Security, 35 (02).
- Soustelle, J. (2002). *Daily Life of the Aztecs*. (Phoenix, Ed.) L'Île-Bizard, Quebec, Canada: Phoenix Press daily life series.
- Thompson, S. J. (1995). *Tilting with Machiavelli: Fighting Competitive Espionage in the 1990s*. International Journal of Intelligence and Counterintelligence, 07(02), p.170.
- W.T., W. *International Technology Transfer and Economic Espionage*. International Journal of Intelligence and Counterintelligence, 7(2), p.2.
- Walter, L. (1993). *The Uses and Limits of Intelligence*. Transaction Publishers.
- William, R., & Timothy, B. (2009). *China's Last Empire: The Great Qing*. Cambridge, Massachusetts: The Belknap Press of Harvard University Press.